ISSN: 2525-457X
Análise Estratégica
v. 35, n.4, set./nov. 2024

PODER INTELIGENTE: O IMPACTO DA QUINTA REVOLUÇÃO INDUSTRIAL NAS INSTITUIÇÕES SECURITÁRIAS DO REINO UNIDO

SMART POWER: THE IMPACT OF THE FIFTH INDUSTRIAL REVOLUTION ON UK SECURITY INSTITUTIONS

FERNANDO HENRIQUE CASALUNGA

RESUMO

O ensaio objetiva compreender como o desenvolvimento técnico-científico pode contribuir para ampliar a robustez das instituições securitárias do Reino Unido para que possam perseguir os interesses nacionais de modo eficiente. Com base em documentos oficiais identifica as principais estruturas responsáveis pela inteligência britânica, explora aspectos chave que perpassam a formulação da estratégia nacional, e destaca a transformação das Forças Armadas resultante da incorporação de novas tecnologias informacionais como a pedra angular das capacidades de projeção de poder do Reino Unido. Para tanto, emprega metodologia qualitativa de análise documental historiográfica para realizar um esquadrinhamento profundo do conteúdo de fontes primárias recém publicadas.

Palavras-chave: Tecnologia da Informação; Conflitos Interestatais; Ordem Internacional; Mudança Institucional.

ABSTRACT

The goal of the essay is to comprehend how scientific and technological advancements can strengthen the security institutions of the United Kingdom and enable them to effectively serve national interests. Relying on official documents, it delineates the principal structures accountable for British intelligence, examines crucial elements that influence the development of the national strategy, and underscores the evolution of the Armed Forces as a consequence of the integration of novel information technologies as the cornerstone of the United Kingdom's capacity to project power. In order to achieve this, it thoroughly examines the content of freshly released original sources using a qualitative technique of historiographical documentary analysis.

Keywords: Information Technology; Interstate Conflicts; International Order; Institutional Change.

O AUTOR

Doutor em Ciência Política (UFRGS/2024), Mestre em Ciência Política (UFPE/2020), Bacharel em Ciência Política com ênfase em Relações Internacionais (UFPE/2019), Bacharel e Licenciado em História (UNESP/2010). Realizou instância de investigação doutoral no Instituto Universitário de Lisboa (Portugal). Membro da Associação Brasileira de Estudos de Defesa; Associação Brasileira de Ciência Política e dos grupos de pesquisa do CNPq 'O Brasil e as Américas' e 'Segurança e Política Internacional'. Pesquisador do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército (NEP - CEEEx) no ciclo 2024-2025.

1 INTRODUÇÃO

O presente ensaio é o segundo de uma série de cinco produtos que serão desenvolvidos pela linha de pesquisa em Inteligência do Centro de Estudos Estratégicos (CEEEx) no âmbito do Núcleo de Estudos Prospectivos (NEP) entre 2024 e 2025[1].

O primeiro quartil deste século apresenta uma série de desafios provocados por disputas geopolíticas que sinalizam o ímpeto de alguns Estados em promover mudanças significativas na balança de poder que regula a ordem internacional. Por esse motivo, tanto a pandemia de COVID-19 como o avanço das tropas russas sobre territórios do leste ucraniano foram percebidos pelos britânicos como fenômenos perturbadores da segurança nacional e da região Euro-Atlântica (Reino Unido, 2023b; 2023c).

Ante ao contexto, o Reino Unido tem promovido um processo de mudança ancorado no desenvolvimento e introdução de novas tecnologias na dinâmica de atuação institucional política e securitária. Por esse ângulo, cabe questionar: como a inteligência têm se beneficiado da 'quinta revolução industrial' no desempenho de suas atividades?

Tendo a análise do papel da inteligência no planejamento estratégico nacional como foco de investigação, ao abordar o problema, considero o argumento hipotético-dedutivo de que a incorporação de novas tecnologias informacionais, a exemplo da: inteligência artificial, aprendizagem de máquina, e computação quântica às estruturas de defesa e segurança nacional, aponta para a consolidação de uma realidade na qual as mesmas dependerão, substantivamente, de tais ferramentas pra desempenharem suas funções de modo efetivo.

A fim de verificar sua plausibilidade, este ensaio está dividido em três seções: i) apresenta um mapeamento da estrutura de inteligência do Reino Unido; ii) examina a estratégia de segurança nacional britânica; iii) destaca a resposta das instituições securitárias para lidar com ameaças contemporâneas. Por fim, assente nos resultados obtidos, apresento breves considerações sobre os pontos em destaque.

2 ESTRUTURA DE INTELIGÊNCIA DO REINO UNIDO: UM MAPEAMENTO INTRODUTÓRIO

Nesta seção apresento um mapeamento introdutório das principais instituições securitárias responsáveis pela inteligência no Reino Unido, com foco na identificação de competências e diretrizes que orientam a condução de suas atividades.

Sem embargo, a Publicação Conjunta de Doutrina, Inteligência, Contra-Inteligência e Apoio à Segurança para Operações Conjuntas (JDP 2-00) de 2023 apresenta os três níveis de inteligência -estratégico, operacional e tático-, indicando a finalidade de cada um deles para o desempenho das suas competências institucionais.

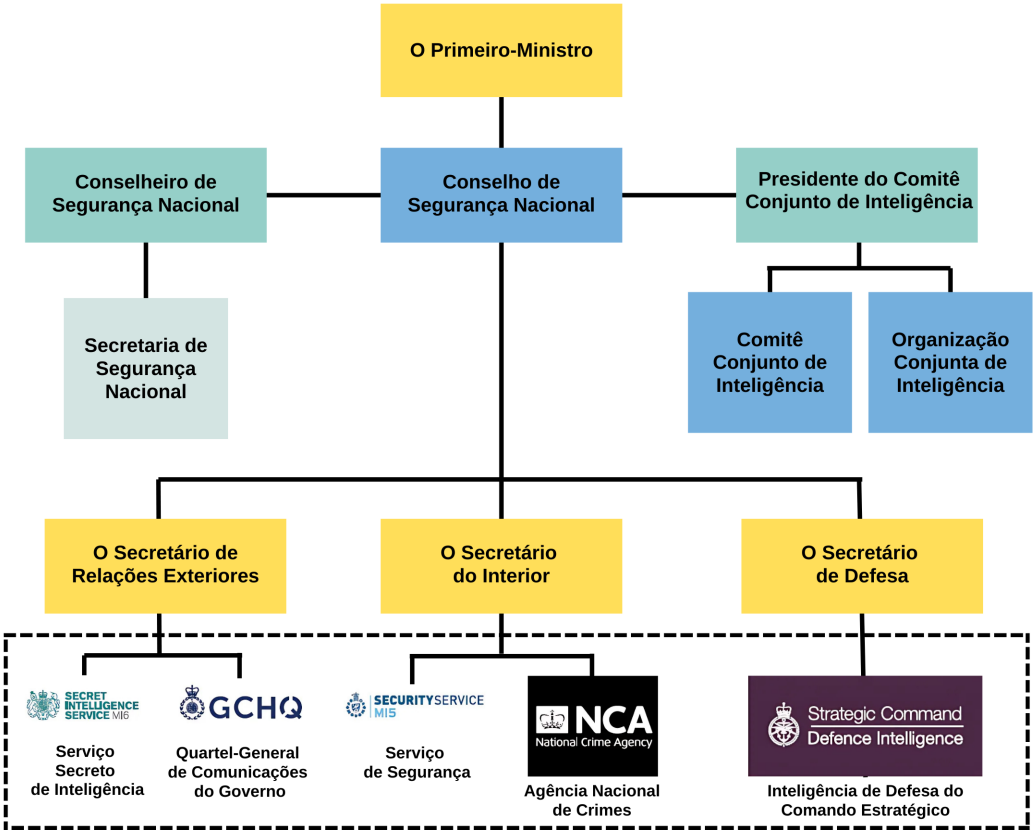
Útil aos propósitos analítico deste ensaio, a inteligência estratégica é definida como a atividade "necessária para a formulação de políticas, planejamento militar e fornecimento de indicações e avisos a nível nacional e/ou internacional" (Reino Unido, 2023a, p. 29) em atenção a demanda das esferas política e militar trabalha para adquirir informações a respeito do movimento de ameaças à segurança nacional.

[1] Com base nos achados dos ensaios desenvolvidos ao longo deste ciclo, um artigo científico será erigido para comparar a robustez institucional de três países, Reino Unido, Brasil e Colômbia. Por fim, os subsídios deste ciclo darão origem a um *Policy Paper* que deverá indicar possíveis implicações e recomendações ao Exército Brasileiro.

Cientes da importância estratégica do papel desempenhado pelas instituições securitárias responsáveis recolha e processamento de informações concernentes ao ambiente e às capacidades e intenções de ameaças à segurança nacional, os britânicos criaram o Ambiente Único de Inteligência (SIntE) para concatenar esforços interagências e interdepartamentais, proporcionando a troca de informações e desenvolvimento de capacidades multidomínios. Cuja principal função é "harmonizar todos os elementos do processo de inteligência" (Reino Unido, 2023a, p. 17), a fim de assegurar que as atividades permitam às lideranças conduzirem processos de "tomadas de decisão eficazes com base na compreensão abrangente [da realidade] derivada de todas as fontes de inteligência" (Reino Unido, 2023a, p. 17).

A Figura 1 apresenta as principais estruturas responsáveis pelo setor no Reino Unido, dentre as quais, de vultuosa relevância estratégica, destaco: o Serviço Secreto de Inteligência (SIS/MI6) que atua no monitoramento de ameaças externas; o Serviço de Segurança (MI5) responsável pelo controle de ameaças internas[2]; e a Sede de Comunicações do Governo (GCHQ) que apoia a formulação de políticas e orquestração de operações do governo e/ou militares, além de proteger dados sensíveis.

Figura 1 - Estrutura da inteligência do Reino Unido



Fonte: Adaptado da JDP 2-00, 2023[3]

[2] Dentre as quais sublinha: "(...) a espionagem, terrorismo e sabotagem, das atividades de agentes de potências estrangeiras e de ações destinadas a derrubar ou minar a democracia parlamentar por meios políticos, industriais ou violentos" (Reino Unido, 2023a, p. 14).

[3] A imagem apresenta somente as principais organizações; várias outras organizações contribuem com avaliações de inteligência sobre questões estratégicas, incluindo, por exemplo, o Centro Conjunto de Análise do Terrorismo (CCAT) e o Centro Nacional de Segurança Cibernética (CNSC) (Reino Unido, 2023a).

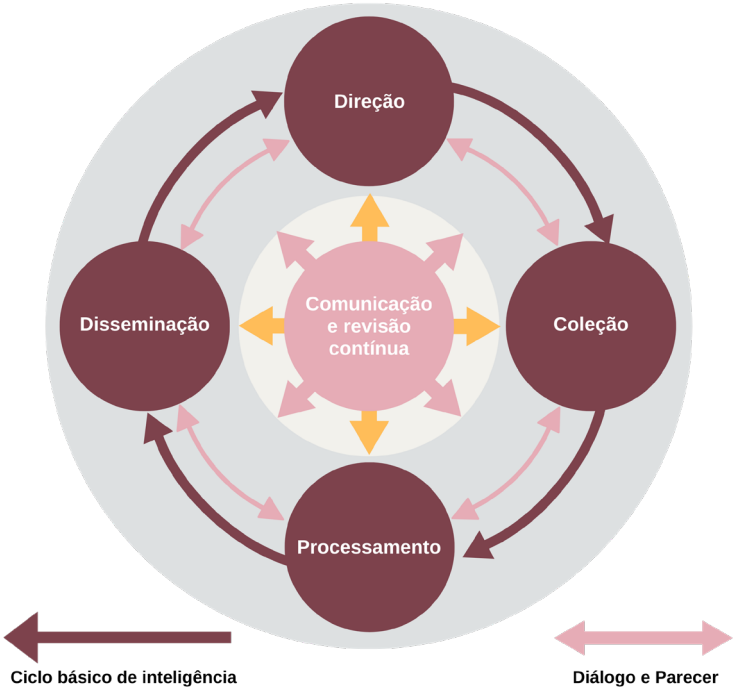
No tocante à esfera política, com base nas informações provenientes do Conselho Nacional de Segurança (NSC) -espaço de comunicação ministerial no qual se discutem aspectos securitários a nível estratégico-, responsável por coordenar decisões políticas interdepartamentais em matérias relativas a defesa, política externa, desenvolvimento e resiliência, o Conselheiro de Segurança Nacional (NSA) oferece suporte ao Primeiro-Ministro e ao Gabinete para formulação da estratégia de segurança nacional (Reino Unido, 2023a).

Assente nesta estrutura, a Secretária de Segurança Nacional (NSS) coordena as atividades do conselho e implementa as decisões formuladas, enquanto que ao Comitê Conjunto de Inteligência (JIC) compete a condução de processos de avaliação de ameaças, e promoção dos interesses nacionais no exterior, em auxílio ao chefe do executivo e ao NSC. Já a Organização Conjunta de Inteligência (JIO) atende a processos de avaliação e desenvolvimento da capacidade analítica da inteligência (Reino Unido, 2023a).

De nosso particular interesse, a inteligência de defesa se encontra a cargo do Comando de Inteligência de Defesa (CDI), órgão de governo subordinado ao Ministério da Defesa (MOD), incumbido de avaliar os produtos de inteligência provenientes de fontes distintas sobre temas de interesse nacional. Dentre as suas atividades, desenvolve ações colaborativas com uma ampla gama de organizações nacionais e internacionais, respondendo pela orientação de processos decisórios que envolvam aspectos "políticos, estratégicos e [a] permanência de compromissos operacionais, [ademais] informa decisões de aquisição de Defesa e apoia operações militares" (Reino Unido, 2023a, p. 13).

A Figura 2 destaca a composição do ciclo de atividades de inteligência que se divide em quatro funções: direção, coleta, processamento e disseminação, conduzidas em estreia atenção aos preceitos metodológicos e avaliativos que atestam a consistência e significância dos produtos dele resultantes.

Figura 2 - Ciclo de Inteligência do Reino Unido



Fonte: Adaptado da JDP 2-00, 2023

Depreende-se da JDP 2-00 que as atividades de inteligência objetivam detectar padrões de mudança e tendências emergentes que possibilitem assegurar o controle da iniciativa em caso de crises que demandem resposta imediata. Mais do que isso, visam indicar pontos de vista alternativos, contribuir para criar uma narrativa estratégica baseada em evidências, explorar múltiplas versões em cenários prospectivos e produzir indicadores e alertas sobre futuros potenciais de alto impacto (Reino Unido, 2023a)[4].

No tocante à defesa, a direção dos esforços institucionais para aquisição, depuração e comunicação das informações é dada pelo comandante e o seu estado-maior apresentando os questionamentos que deverão ser respondidos, em tempo hábil, pela atividade de inteligência. Trata-se da requisição de ativos de relevância sumária para lideranças que ocupam cargos do mais alto nível hierárquico, para os quais a compreensão burilada da realidade objetiva se faz imprescindível (Reino Unido, 2023a).

A coleta e exploração dos dados é realizada por atores institucionais competentes, as informações podem ser provenientes de fontes: i) controladas por agencias ou organizações diretamente conectadas ao nível estatal; ii) descontroladas produzidas ao nível externo; iii) casuais provenientes de desertores ou refugiados, verificadas com precisão em razão de sua baixa confiabilidade (Reino Unido, 2023a).

Uma vez adquiridos, tais ativos são processados e analisados a fim de que possam produzir resultados tangíveis com altos níveis de confiança, somente a partir de então é que serão repassados aos decisores interessados. A avaliação sistemática dos processos conduzidos durante a coleta considera as provas, suposições e julgamentos com atenção a eliminação de possíveis vieses cognitivos que possam invalidar os resultados obtidos, com frequência os agentes recorrem ao uso de Técnicas de Análise Estruturada (TAEs) para construção de modelos preditivos que reduzem a incerteza no conhecimento de um determinado fenômeno sob escrutínio (Reino Unido, 2023a).

Contida no conjunto de diretrizes que as orientam, vale ressaltar a centralidade dos dados[5], percebida como aspecto fundamental para compreensão da realidade objetiva. A chave dessa abordagem está no acesso aos dados como requisito de primeira ordem para explorar e compreender as lacunas de inteligência, em efeito, os britânicos esperam reduzir a carga sobre recursos finitos (ativos analíticos, de inteligência, vigilância e reconhecimento) com o intuito de oferecer suporte à tomada de decisão em tempo hábil (Reino Unido, 2023a).

À vista disso, a formulação de políticas direcionadas à proteção e armazenamento de grandes volumes de informação são apontadas como medidas necessárias para assegurar a efetividade da inteligência, sua consolidação depende do funcionamento de infraestrutura apropriada, e conjuntos de habilidades corretos (Reino Unido, 2023a). Outrossim, a observância de alguns conceitos como: objetividade, perspectiva, agilidade, oportunidade, colaboração, continuidade, segurança e observância aos princípios adicionais da Organização do Tratado do Atlântico Norte (OTAN) é considerada basilar para o aperfeiçoamento das atividades de inteligência.

Naquilo que tangencia aos propósitos analíticos deste ensaio, a definição de agilidade merece atenção, pois, engloba noções como resiliência, adaptação e flexibilidade que acentuam a

[4] Dentre as principais atividades do setor, o documento registra: o suporte à formulação de estratégia que busca identificar as capacidades e intenções de adversários e/ou intervenientes neutros; produção de avaliações preditivas que permitem avaliar riscos e identificar oportunidades de ação mediante a construção de cenários mais ou menos prováveis de se concretizarem; fornecimento de indicadores e alertas sobre movimentos de ameaças; contra inteligência e monitoramento de atores estatais e/ou não estatais com potencial para produzir efeitos perversos sobre a segurança nacional (Reino Unido, 2023a).

[5] O conceito diz respeito a significância da análise de dados para preencher as lacunas na compreensão da realidade objetiva por parte dos decisores interessados nos produtos da inteligência. Nesse sentido, a capacidade de lidar com alto volume de informação de modo eficiente permite a alocação assertiva de recursos escassos com a finalidade de proporcionar o suporte necessário à tomada de decisão em tempo oportuno (Reino Unido, 2023a, p. 27).

necessidade da construção de capacidades acuradas para explorar oportunidades e reduzir incertezas, mediante ampla verificação das possibilidades de sucesso operacional; alocação eficiente de recursos; e compreensão da volatilidade das circunstâncias contextuais (Reino Unido, 2023a).

Deste modo, cabe a inteligência contribuir com "o planejamento e execução de atividades para criar ou manter as atitudes que constituem o comportamento" (Reino Unido, 2023a, p. 4), uma vez que os comandantes precisam adquirir consciência sobre a narrativa estratégica que se pretende adotar em determinada linha de ação. Somente assim é possível organizar esforços institucionais para produção dos efeitos desejáveis sobre um determinado público alvo (Reino Unido, 2023a).

Por consequência, as instituições de inteligência britânicas se concentram em fornecer informações depuradas que contribuam para desenvolver tal compreensão "Isto inclui não só responder às principais questões de inteligência sobre quem, o quê, onde, quando, por que e como, que fornecem o contexto e a narrativa dos acontecimentos, mas também a análise dedutiva e preditiva" (Reino Unido, 2023a, p. 6).

Não obstante, a JDP 2-00 marca a percepção das instituições securitárias de que estamos presenciando um novo século, no qual o objetivo tradicional da inteligência sofreu uma alteração significativa devido aos efeitos causados pela emergência de novos domínios operacionais sobre as dinâmicas que envolvem as disputas interestatais por poder e influência (Reino Unido, 2023a)[6].

Ante a conjuntura, a inteligência de Defesa assume o compromisso com o desenvolvimento de ferramentas que impulsionem a produção de conhecimento sobre a "natureza das circunstâncias, situações e cenários de segurança militares, socioeconômicos, culturais, físicos, políticos e humanos globais" (Reino Unido, 2023a, p. 7). No que se refere à incorporação de novas tecnologias para desempenho de suas competências, os britânicos preveem, ainda, a criação de incentivos que viabilizem a formação de quadros capacitados a fazer bom uso de tais recursos (Reino Unido, 2023a).

Destarte, no futuro próximo, consideram que avanços nas capacidades de tratamento e interpretação de dados, por meios humanos ou automatizados, deverão permitir às lideranças alcançarem níveis satisfatórios de entendimento sobre a objetiva da realidade que se encontre sob escrutínio com maior eficiência e discrição

> A inteligência precisa ser capaz de lidar com '*big data*' (dados de alta velocidade, dados de variedade crescente, volume crescente e de veracidade variável) que são difíceis de serem processados, armazenados e analisados pela Defesa usando métodos analíticos tradicionais e arquitetura de gerenciamento de informações. Novos desenvolvimentos nos campos da automação, inteligência artificial, aprendizagem automática e outras tecnologias relacionadas com dados proporcionarão oportunidades significativas para melhorar a forma como os negócios de inteligência são conduzidos (Reino Unido, 2023a, p. 20).

Em virtude disto, a inteligência vital[7] tornou-se mais acessível, a medida em que novas tecnologias têm permitido o monitoramento sistemático dos movimentos de potenciais ameaças. Entretanto, "embora a recolha de informações tenha sido transformada (...), ainda não é necessariamente preditiva, mesmo a melhor inteligência pode estar sujeita a uma série de interpretações" (Reino Unido, 2023a, p. 2).

[6] Até pouco tempo atrás, o foco tradicional da atividade de inteligência era "identificar e conhecer os adversários para neutralizá-los ou derrotá-los". Atualmente, as operações em multidomínios operacionais exigem "uma compreensão mais ampla de todos os públicos", a inteligência deve oferecer suporte aos comandantes para que obtenham tal compreensão (Reino Unido, 2023a, prefácio, p. iii)

[7] Embora os documentos oficiais analisados careçam de uma definição precisa deste conceito, o contexto indica que se refere ao incremento nas capacidades de execução das atividades por parte das instituições securitárias que, ao fazerem uso de sensores e algoritmos sofisticados em processos de identificação de perigos e oportunidades, permitem a entrega de produtos requisitados por decisores políticos e militares em tempo oportuno (Reino Unido, 2023a).

Fundamentado neste breve mapeamento introdutório, podemos afirmar que as instituições securitárias responsáveis pela inteligência do Reino Unido possuem características peculiares que correspondem a uma estruturação cuidadosa de suas competências e capacidades para execução de atividades. Tendo por finalidade o provimento de informações confiáveis e relevantes para apoio das lideranças na condução de processos decisórios que visam a atender aos interesses nacionais.

Ante o exposto, na próxima seção procuro explorar a estratégia de segurança nacional britânica a fim de identificar como se dá a formulação de tais interesses, bem como examinar a relevância da incorporação de novas tecnologias como ferramentas necessárias para sua consecução.

3 ESTRATÉGIA DE SEGURANÇA NACIONAL BRITÂNICA: UMA ABORDAGEM INTEGRADA

Nesta seção procuro examinar a estratégia de segurança nacional do Reino Unido com foco no processo de incorporação de novas tecnologias da informação como força motriz das capacidades de promoção dos interesses e provimento da segurança nacional.

Sem embargo, a Atualização da Revisão Integrada (IRR) publicada em 2023 pelo então Primeiro-Ministro Rishi Sunak, foi formulada com base na percepção de quatro tendências que deverão provocar forte impacto sobre a ordem internacional nos próximos anos, "mudanças na distribuição do poder global; competição interestatal e "sistêmica" sobre a natureza da ordem internacional; rápida mudança tecnológica; e agravamento dos desafios transnacionais" (Reino Unido, 2023b, 2023, p. 7)[8].

O documento procura atualizar o ritmo em que as mesmas estão a materializar o processo de transição para um sistema multipolar, fragmentado e contestado "período de elevado risco e volatilidade que provavelmente durará para além da década de 2030" (Reino Unido, 2023b, p. 7)[9]. Frente ao cenário, retoma a preocupação com os efeitos provocados pela concorrência interestatal sobre o equilíbrio securitário internacional e doméstico.

A Federação Russa é descrita como uma ameaça crítica à segurança não apenas do Reino Unido, mas, sobretudo, de toda a região Euro-Atlântica, já a República Popular da China é percebida como um ator interessado em aproveitar a conjuntura para lançar mão estratégias que procuram promover mudanças na ordem internacional (Reino Unido, 2023b). À conta disso, os britânicos consideram que essas disputas representam um confronto entre regimes com consequências para o desenvolvimento das sociedades futuras em termos securitários e valorativos (Reino Unido, 2023b).

A narrativa reforça o desejo de atuar em regiões específicas como a Euro-Atlântica e Indo-Pacífico de modo assertivo. Nesse sentido, aponta para a invasão ao território ucraniano, bem como a ocupação de territórios na Geórgia pela Federação Russa como alvo das preocupações securitárias imediatas, a estratégia russa é considerada um ataque direto aos valores e à segurança europeia (Reino Unido, 2023b).

[8] Ao considerar a celeridade de mudanças estruturais na conjuntura internacional como fator que impõe a necessidade de revisão dos objetivos estratégicos do Reino Unido em um mundo volátil e contestado, o documento marca a atualização da Revisão Integrada (IR), publicada durante o governo do então Primeiro-Ministro Boris Johnson em 2021.

[9] Vale ressaltar que o conteúdo deste documento atende às avaliações provenientes de instituições securitárias responsáveis pela inteligência tais como: o Comitê Conjunto de Inteligência; Avaliação de Risco à Segurança Nacional, Inteligência de Defesa, Comissão de Relações Exteriores, Comissão de Defesa, Comissão de Inteligência e Segurança e Comissão de Relações Internacionais e Defesa dos Lordes, dentre outras, que destacam a necessidade de atualização das capacidades da defesa do Reino Unido com base nas experiências coletadas ao longo dos conflitos no Afeganistão e Ucrânia, considerados laboratórios importantes para a construção do planejamento futuro das Forças Armadas (Reino Unido, 2023b, p. 11).

Em resposta, enfatiza o comprometimento em investir 2,5% do Produto Interno Bruto (PIB) em Defesa nos próximos anos, a fim de manter posição de liderança na OTAN, e assegurar a modernização das Forças Armadas com base no aprendizado adquirido na guerra russo-ucraniana (Reino Unido, 2023b).

> [...] com os pontos fortes únicos e a profunda parceria do Reino Unido, combinados com os nossos excelentes serviços armados, rede diplomática, experiência em desenvolvimento, agências de aplicação da lei e de inteligência, protegeremos e promoveremos os nossos interesses e desempenharemos um papel ativo na defesa da abertura, liberdade e a regra da lei (Reino Unido, 2023b, p. 4).

Naquilo que se refere ao Indo-Pacifico, destaca a implementação de medidas para contrabalançar a influência chinesa, movimentos orquestrados em conjunto com aliados e parceiros na região. Como efeitos, sublinha o aprofundamento das relações com a Associação das Nações do Sudeste Asiático (ASEAN), e a magnitude da relação do Reino Unido com os Estados Unidos da América "desde a inteligência até à coordenação militar e diplomática que continua a ser um pilar absolutamente essencial da segurança nacional" (Reino Unido, 2023b, p. 9). Contudo, em matéria de Política Internacional, pondera que o pragmatismo da China possa ser explorado a fim de que se construam elos de confiança para atender a zonas de interesse mútuo (Reino Unido, 2023b).

Não obstante, o monitoramento e a mitigação de ameaças são considerados funções positivas das instituições securitárias com poder de polícia e inteligência. Nesse quesito, problemas relacionados a imigração, ações terroristas, e o radicalismo ideológico como os mais preponderantes, grupos organizados que têm se beneficiado "dos avanços tecnológicos para desenvolver novos modelos operacionais e ocultar as suas identidades e atividades" (Reino Unido, 2023b, p. 8) figuram dentre os maiores desafios.

Diante do quadro, novas 'arenas' de conflito ganham relevância estratégica ao passo em que demonstram potencial para borrar as divisões tradicionais entre guerra e paz, numa "competição constante e dinâmica acima e abaixo do limiar do conflito armado" (Reino Unido, 2023b, p. 9) com implicações diretas sobre o equilíbrio securitário e regulatório das disputas por poder no sistema internacional.

> Em algumas áreas – como a IA – a tecnologia avançou e tornou-se mais amplamente disponível. Além de impulsionar a mudança social e econômica, estes avanços estão a conduzir a uma maior capacidade de ameaçar, prejudicar e danificar países, sociedades e indivíduos remotamente e, em alguns casos, anonimamente. A utilização de *spyware* comercial, *ransomware* e capacidades cibernéticas ofensivas por intervenientes estatais e não estatais proliferou, realçando a importância do envolvimento com empresas tecnológicas e da definição de normas de comportamento responsáveis no que diz respeito ao ciberespaço e áreas tecnológicas novas e emergentes (Reino Unido, 2023b, p. 9).

Como medidas assertivas a serem tomadas, o documento registra o aprimoramento do sistema de resiliência[10], bem como o investimento em segurança cibernética mediante a criação de

[10] De acordo com o Quadro de Resiliência do Governo do Reino Unido (GRF) publicado em 2022a, o sistema de resiliência representa uma iniciativa integrada, intergovernamental, interdepartamental, e societária, que conta com o apoio de administrações descentralizadas, autoridades locais, serviços de emergência e setores privados, voluntários e comunitários. Sua concepção assenta sobre três princípios estratégicos fundamentais "i) compreensão partilhada dos riscos que enfrentamos; foco em prevenção e preparação; resiliência como conceito que perpassa toda a sociedade" (Reino Unido, 2022b, p. 1).

incentivos que busquem reforçar as capacidades de enfrentamento de ameaças estatais e/ou não-estatais tem por base, considerados chave para consecução de objetivos estratégicos no longo prazo[11].

Aplicada para contenção de riscos internos e externos, a resiliência é descrita como a "capacidade de resistir ou recuperar rapidamente de uma situação difícil, mas também de se antecipar esses riscos e enfrentar os desafios antes que se manifestem" (Reino Unido, 2022b, p. 9). Nesse ensejo, foi constituída a agência de Avaliação de Risco à Segurança Nacional (NSRA), principal estrutura ligada ao governo central, incumbida de examinar as vulnerabilidades e identificar desafios que possam afetar os interesses nacionais, a exemplo de crises decorrentes de disputas político-econômicas, concorrência sistêmica, evolução tecnológica, mudanças climáticas, dentre outras (Reino Unido, 2022b).

Outrossim, tendo em vista a posição de potência tecnológica ocupada pelo Reino Unido, projetos focados no desenvolvimento de ferramentas que potencializem o poder cibernético são considerados de importância estratégica salutar. Por essa lógica, áreas como: "inteligência artificial, computação quântica, engenharia biológica, tecnologia nuclear, cibernética e espacial" (Reino Unido, 2023b, p. 7) são tratadas como ativos de primeira ordem para incrementar as capacidades de projeção de poder nacional.

Ante a demanda, o documento sublinha o aporte de vinte bilhões de euros anuais em pesquisa e desenvolvimento de novas tecnologias de uso dual que permitam alcançar novos patamares de prosperidade e segurança nacional (Reino Unido, 2023b)[12]. Ademais, acentua a criação no nível ministerial executivo, do novo Departamento de Ciência, Inovação e Tecnologia (DSIT) com a finalidade de constituir um "ecossistema certo para que a C&T floresça no Reino Unido e acompanhe os concorrentes estratégicos (Reino Unido, 2023b, p. 14).

A estratégia britânica esta erigida sob quatro pilares de importância sumária: i) moldar o ambiente internacional; ii) dissuadir defender e competir em todos os domínios; iii) abordar as vulnerabilidades através da resiliência; iv) gerar vantagem estratégica[13]. No que tangencia os propósitos analíticos deste ensaio, o terceiro e o quarto pilares são de fundamental significância.

O terceiro pilar reforça a narrativa de que as crises produzidas em ambientes externos podem provocar impactos significativos sobre a segurança doméstica britânica, com efeitos socioeconômicos indesejáveis, sendo assim, o desenvolvimento de capacidades que permitam mitigar as ações de adversários estatais e/ou não estatais se faz imprescindível (Reino Unido, 2023b).

Destarte, o robustecimento do sistema de resiliência é percebido como imperativo

[11] Ao destacar a posição do Reino Unido como uma potência cibernética, reforça que o enfrentamento a essas ameaças continuará a cargo da Força Cibernética Nacional (NCF) constituída em 2020 para lidar de forma responsiva e ética com "redes terroristas, combater a evasão de sanções, apoiar e proteger operações militares e remover material de exploração e abuso sexual infantil online" (Reino Unido, 2023b, p. 36).

[12] No tocante às regras e normas que organizam o comportamento no ciberespaço, o documento enfatiza a posição do Reino Unido como "potência cibernética responsável e democrática, inclusive na utilização de capacidades cibernéticas ofensivas" (Reino Unido, 2023b, p. 28). Em observância ao disposto na Estratégia Cibernética Nacional (NCS) publicada em 2022, destaca o compromisso em liderar processos de construção e aplicação de normas e regulamentos internacionais que restrinja atividades maliciosas por parte de atores estatais e/ou não estatais neste domínio. Ademais, ressalta o interesse em dar continuidade em processos de desenvolvimento de ferramentas "para dissuadir, defender e competir no ciberespaço, abordando as nossas vulnerabilidades cibernéticas nacionais e apoiando os parceiros na construção das suas próprias capacidades" (Reino Unido, 2023b, p. 28).

[13] A fim de persegui-los, os britânicos enfatizam que pretendem dar apoio à manutenção de uma ordem internacional aberta e estável que assegure: a proteção de bens públicos globais; a atuação de maneira integrada para promover a dissuasão em matéria de defesa contra ameaças estatais e/ou não-estatais; a compreensão de modo substantivo das vulnerabilidades e os riscos de exploração que comprometem a segurança nacional; e a cooperação com aliados e parceiros estratégicos para tomar o controle da iniciativa no tocante a competição por poder e riqueza em âmbito internacional (Reino Unido, 2023b, p. 16).

categórico da estratégia nacional que pretende lidar com ameaças contemporâneas[14]. Razão pela qual, em acordo com o disposto pelo Quadro de Resiliência (GRF) (2022a), reforça o interesse em "fortalecer os sistemas e capacidades subjacentes à resiliência, com medidas centradas na avaliação de riscos, responsabilidades e prestação de contas, parceria, comunidades, investimento e competências" (Reino Unido, 2023b, p. 45).

Por este prisma, ao abordarem as vulnerabilidades estratégicas nos mais variados setores, os britânicos intentam reduzir as probabilidades de ocorrência de novas crises ou ataques que possam abalar a segurança nacional[15]. Em efeito, a nível governamental um Novo Subcomitê de Segurança (NSC) foi constituído para tratar da implementação de modelos operacionais que ofereçam condições para que as instituições securitárias possam lidar com a nova realidade dos conflitos contemporâneos (Reino Unido, 2023b).

Não obstante, na esteira da Estratégia Cibernética Nacional (2020; 2022c), o funcionamento das infraestruturas críticas é considerado prioridade. Com o intuído de dar cabo do problema, os britânicos mantêm o compromisso em promover incentivos para construção de capacidades que permitam às instituições securitárias "compreender a natureza do risco; proteger sistemas para prevenir e resistir a ataques cibernéticos; minimizando o impacto dos ataques" (Reino Unido, 2023b, p. 50). Para tanto, destacam o papel do Conselho Consultivo Cibernético Nacional (NCAC), estrutura composta por acadêmicos, representantes de setores industriais e do terceiro setor, constituído para identificar e mitigar a ação de ameaças (Reino Unido, 2023b).

O quarto pilar adota o desenvolvimento técnico-científico como chave para a projeção de poder nacional e consecução dos interesses nacionais. Igualmente, a posição de liderança internacional no domínio cibernético desempenhada de modo responsável e democrático é apontada como símbolo deste poder, motivo pelo qual o desenvolvimento e emprego das cinco tecnologias fundamentais é compreendido como basilar para assegurar a iniciativa em cenários de crises (Reino Unido, 2023b).

No tocante às instituições securitárias responsáveis pela inteligência, reafirma o interesse em "continuar a desenvolver as capacidades e os poderes necessários das agências de inteligência, para apoiar atividades secretas e abertas [...] desenvolver as capacidades de 'varredura de horizontes'[16] e investir numa parceria mais aberta com o setor tecnológico" (Reino Unido, 2023b, p. 59). Nesse sentido, prevê a criação de incentivos para o desenvolvimento de "capacidades humanas e técnicas, incluindo IA e ciência de dados, para garantir que a nossa tomada de decisões seja orientada pelos dados mais precisos e abrangentes disponíveis" (Reino Unido, 2023b, p. 59)[17].

[14] A função da atividade de inteligência é tratar daquelas associadas ao terrorismo, espionagem, sabotagem, e crime organizado. Para tanto, a proteção da confidencialidade das informações e a gestão de riscos é considerada fundamental para permitir a alocação eficiente de recursos e mitigar os riscos impostos pela ação dessas ameaças (Reino Unido, 2023a).

[15] Dentre as áreas vulneráveis identificadas, chama atenção para a 'resiliência democrática e social' como prioridade estratégica, uma vez que ameaças físicas e cibernéticas têm demonstrado grande potencial para interferir em processos eleitorais e funcionamento de infraestruturas críticas. Em razão disso, prevê ações institucionais que reforcem a integridade do sistema democrático tendo por foco o controle à corrupção e redução da influência externa (Reino Unido, 2023b).

[16] O termo representa a análise sistemática do ambiente externo em busca da identificação de potenciais ameaças, perigos e oportunidades, "para fins militares, pode significar examinar fatores além da janela de planejamento operacional" (Reino Unido, 2023a, p. 9).

[17] Dentre as medidas a serem implementadas, prevê a criação de um grupo de trabalho composto por especialistas que atuará em conjunto com o governo e a indústria para indicar ao Primeiro-Ministro e ao Secretário de Estado do Departamento de Ciência, Inovação e Tecnologia (DSIT) cursos de ação prioritários que envolvam uso da inteligência artificial em "ações e investimentos concebidos para beneficiar a nossa sociedade e economia" (Reino Unido, 2023b, p. 57). Além disso, cita a expansão das agências de inteligência para a região noroeste da Inglaterra, em um movimento que objetiva

Em específico, registra o Centro Nacional de Situação (SitCen) como principal responsável por analisar e depurar informações internas e externas ao governo, possibilitando o enfrentamento não apenas de crises pontuais como as provocadas pela invasão russa ao território ucraniano, mas também por fatores de longo prazo como o descontrole climático, operações industriais, dentre outras. Em apoio às atividades, chama a atenção o papel do serviço digital de Troca de Informações e Dados (INDEX) criado para permitir o acesso e compartilhamento de análises e avaliações de dados abertos, relatórios governamentais oficiais e documentos sensíveis (Reino Unido, 2023b, p. 59).

O exame da estratégia nacional britânica apresentado elucida a percepção britânica de que a promoção eficaz de seus interesses dependerá, a médio e longo prazos, da incorporação de novas tecnologias que assegurem a segurança doméstica e a manutenção da ordem internacional sob os moldes do regime democrático. Em virtude disso, a próxima seção verifica como as instituições securitárias preveem atender a tais anseios.

4 MUDANÇA INSTITUCIONAL: A RESPOSTA DAS INSTITUIÇÕES SECURITÁRIAS DO REINO UNIDO À VOLATILIDADE DO AMBIENTE INTERNACIONAL

Nesta seção, procuro verificar os efeitos institucionais provocados pelo processo de incorporação de novas tecnologias como pedra angular das capacidades dissuasórias do Reino Unido, considerada condição necessária para perseguir os interesses dispostos pela estratégia nacional.

Publicada em 2022, a Doutrina de Defesa (JDP 0-01) revela a evolução do pensamento militar britânico, procurando atualizar as capacidades e organizar a cultura para assegurar a preparação adequada para lidar com desafios futuros. Por este ângulo, se soma às abordagens tradicionais das Forças Armadas do Reino Unido como Comandos de missão e Abordagens de Manobra, a noção de ação integrada.

O documento reforça a percepção de que a ordem internacional se encontra fragmentada, marcada pelo aumento da competição interestatal por interesses, normas e valores, contexto no qual a defesa do *status quo* se mostra insuficiente (Reino Unido, 2022a, p. 2)[18]. Diante do contexto, o investimento na construção de capacidades dissuasórias torna-se fulcral, pois, embora a natureza da guerra tenha permanecido perene, "violenta, competitiva, caótica" (Reino Unido, 2022a, p. 3) as formas de seu emprego apresentaram alterações significativas devido ao impacto da evolução tecnológica nos campos econômico, sociocultural e securitário[19].

Ante a conjuntura, a doutrina identifica a intenção de adversários em testar a resiliência nacional, contestando as normas que regulam a ordem internacional através de ações ofensivas híbridas

fortalecer as redes de "excelência pública, privada e acadêmica e a fazer pleno uso da capacidade dos talentos de nosso país" (Reino Unido, 2023b, p. 59),bem como tenciona "estabelecer um novo centro de inteligência de código aberto (OSINT) para atualizar e integrar melhor a capacidade do Governo de recolher e analisar informações disponíveis pública e comercialmente" (Reino Unido, 2023b, p. 59).

[18] O JDP 0-01 reforça a imagem da Federação Russa como adversário na região Euro-Atlântica. Ademais, chamada atenção para a tensão entre regimes de governo e a ordem do sistema internacional, ao descrever adversários como Rússia, China e Irã como expoentes de sistemas autoritários que têm buscado ampliar sua capacidade de influência e contestação das normas internacionais em vigor (Reino Unido, 2022a, p. 49).

[19] A velocidade acelerada do ritmo e difusão da informação, evolução tecnológica afeta principalmente os domínios espacial e cibernético, nos quais as tecnologias disruptivas demonstram potencial para perturbar as barreiras que separam "entre público e privado, estrangeiro e doméstico, estatal e não estatal, e virtual e físico" (Reino Unido, 2022a, p. 3).

que envolvem desinformação e ataques a infraestrutura crítica (Reino Unido, 2022a). Através dela, as forças de defesa reforçam a preocupação com a segurança Euro-Atlântica em virtude da invasão russa do território ucraniano, compreendida como violação das normas do sistema internacional que provocou forte instabilidade securitária na região. Em resposta, frisam a necessidade de atuarem em conjunto com aliados e parceiros para "fortalecer a resiliência e reforçar a dissuasão e a defesa para enfrentar este desafio" (Reino Unido, 2022a, p. 4).

De acordo com a doutrina, o cenário político internacional contemporâneo impõe às instituições securitárias o aprimoramento do sistema de resiliência, chave das capacidades de contenção de ameaças à segurança nacional. Por essa lógica, as operações estratégicas contemporâneas demandam a atuação assertiva e integrada entre setores militares, indústria e academia, mediante emprego de ferramentas tecnologicamente avançadas que permitam alcançar êxito nos objetivos traçados (Reino Unido, 2021; 2022a)[20].

Não obstante, a construção de uma narrativa uníssona que vise obter o consenso da população sobre a necessidade de combater desafios internos e externos de modo conjunto e síncrono, empregando "todos os instrumentos do poder nacional a nível doméstico e internacional" (Reino Unido, 2022a, p. 5) é considerada fundamental para assegurar os resultados esperados[21]. Ante ao desafio, estabelece que a comunicação estratégica desenvolvida em apoio aos interesses nacionais deva ser reforçada através da incorporação de novas tecnologias da informação e outros instrumentos que permitam ampliar a eficácia das atividades desempenhadas pelas instituições securitárias (Reino Unido, 2022a, p. 12).

Frente a dinâmica, tais estruturas têm como objetivo impedir a exploração de vulnerabilidades por ameaças com intenção de provocar efeitos nocivos à segurança nacional. Logo, a crescente complexidade de atuação dessas ameaças é vista como fator que amplia, exponencialmente, a importância da inteligência na proteção de infraestruturas críticas e robustecimento do sistema de resiliência (Reino Unido, 2022a).

A significância da inteligência neste processo dá-se em função da "integração da equipe de operações de informação e planejamento, a fim de garantir que toda a gama de atividades de domínio e de informação necessárias para alcançar um resultado bem-sucedido seja aproveitada" (Reino Unido, 2022a, p. 42). Embora a informação não seja considerada um domínio *per se*, as atividades do ciclo de inteligência se conectam ao domínio operacional ao passo em que produzem efeitos cognitivos.

> A integração bem-sucedida de ações, dentro e entre domínios, permite ao comandante ganhar e manter a iniciativa, melhorando a prevenção, a surpresa, a simultaneidade, o ritmo e a exploração. Isso gera maior liberdade de manobra no espaço de engajamento para criar efeitos físicos, virtuais e cognitivos dentro de sua área de operações (Reino Unido, 2022a, p. 42).

Por consequência, a segurança no domínio cibernético e eletromagnético é apontada como requisito para a execução adequada das atividades relacionadas a operações de redes interdependentes

[20] Para lidar com esse cenário, o investimento nos campos da Ciência, Tecnologia, Engenharia e Matemática (STEM) é encarado como prioridade da defesa que intenta aprimorar capacidades operacionais em áreas como a nuclear, espacial e cibernética, atuando em estreita parceria com governo, indústria e acadêmica "o nosso grupo de engenheiros, especialistas cibernéticos, analistas de dados e cientistas serão os guerreiros digitais do futuro e ajudarão a sustentar o crescimento e a prosperidade nacionais" (Reino Unido, 2023c, p. 21).

[21] Dissuasão envolve: negar benefícios e impor custos que inibam as ações ofensivas de adversários do Reino Unido. Para ser efetiva, a dissuasão depende da comunicação assertiva, capaz de organizar uma narrativa comum orientada para reforçar a significância da estratégia "Narrativas vagas ou pouco claras também aumentam a probabilidade de confusão, má interpretação e escalada potencialmente não intencional" (Reino Unido, 2022, p. 51).

de infraestruturas informacional e proteção de dados sensíveis. Isto inclui "a rede mundial de computadores, redes de telecomunicações, sistemas informáticos, processadores embarcados, controladores e ondas eletromagnéticas" (Reino Unido, 2022a, p. 42).

Tendo como referência as diretrizes da JDP 0-01 (2022) e da IRR (2023), as Forças Armadas preparam um novo documento que orienta a construção de meios que facilitem o atendimento aos objetivos traçados. Assim, em julho de 2023, o Ministério da Defesa, publica o Documento de Comando de Defesa (DCP) indicando os militares pretendem responder aos desafios impostos pelo agravamento da contestação e volatilidade internacional[22].

Partindo do pressuposto de que a invasão russa ao território ucraniano representa um ataque aos valores e a segurança europeia, bem como um choque inconteste na ordem internacional, sublinha a relevância da integração entre as capacidades de dissuasão tradicionais (nucleares e terrestres) e as de nova geração (espaciais e cibernéticas) para produção a consecução de objetivos estratégicos (Reino Unido, 2023c)[23].

Em concordância com a noção de que as mudanças substantivas na forma com que os conflitos tem se desenrolado em razão da constatação do envolvimento, cada vez mais marcante, da ação "conjunta e em todos os domínios, sustentada por dados e informações, tanto de código aberto como altamente confidenciais" (Reino Unido, 2023c), assinala o compromisso em dar continuidade ao processo de modernização das capacidades dissuasórias e preventivas[24] como medida assertiva para aumentar as probabilidades de êxito das operações, ação que requer uma compreensão realista dos efeitos causados pela tecnologia da informação na dinâmica das guerras modernas (Reino Unido, 2023c).

Em específico, no tocante aos efeitos da tecnologia da informação em conflitos contemporâneos, revela o uso de ferramentas sofisticadas de "inteligência, vigilância e seleção de alvos" (Reino Unido, 2023c, p. 33) pelas Forças Armadas britânicas durante a guerra russo-ucraniana como símbolo da revolução nas formas de combate em curso. Por essa lógica, sobressai o uso de "infraestrutura de comunicações, a digitalização de dados e o aumento da automação e autonomia se demonstraram vitais para a segurança dos dados, operações de informação, comunicações, direcionamento, interoperabilidade e letalidade" (Reino Unido, 2023c, p. 33).

> O valor da adaptabilidade em ritmo acelerado – agilidade – no campo de batalha tornou-se claro. Aprendemos que permanecer à frente da ameaça e obter vantagem estratégica pode ser alcançado através de meios novos e criativos, explorando a tecnologia e adaptando sistemas de armas (Reino Unido, 2023c, p. 7).

Diante do cenário, o robustecimento do sistema de resiliência é considerado fulcral para mitigar uma ampla gama de possibilidade de choques futuros, provocados por ameaças complexas

[22] O documento considera a estratégia belicosa russa como o maior desafio ao equilíbrio securitário da região euro-atlântica, representando uma agressão que coloca em questão a ordem internacional vigente por gerações. Conflitos como o provocado com a Ucrânia são percebidos como zonas cinzentas que podem ultrapassar os limites aceitáveis de confrontos interestatais, uma vez que alusões a uma possível escalada nuclear têm sido recorrentes nos discursos do presidente russo (Reino Unido, 2023c).

[23] Embora reconheça a preponderância das forças tradicionais para atuação em conflitos interestatais, o documento enfatiza a relevância de novos domínios de guerra como fatores capazes de produzir efeitos significativos sobre os resultados dos conflitos contemporâneos (Reino Unido, 2023c).

[24] Tais capacidades deverão permitir a redução dos custos impostos pela ação de ameaças híbridas provenientes de atores estatais e/ou não estatais, "neste mundo mais contestado, a dissuasão é mais importante do que nunca, sustentada pelas capacidades e alianças que nos permitirão lutar e vencer, se necessário" (Reino Unido, 2023c, p. 5).

e cada vez mais bem preparadas, "Concentramo-nos em como incorporar as lições da Ucrânia na nossa atividade principal e em recuperar a resiliência de combate necessária para gerar uma dissuasão convencional credível" (Reino Unido, 2023c, p. 2).

O conflito em tela é considerado um marco por ter exigido o exercício da resiliência em todas as suas dimensões, cenário em que as capacidades de adaptação e inovação passaram ao centro das dinâmicas belicosas mediante o aumento da "interconectividade num ambiente de dados em expansão" (Reino Unido, 2023c, p. 33). À conta disso, o uso da tecnologia da informação como pilar central da dissuasão estratégica se torna imperioso, ponto que depende da reformulação das "políticas, estruturas e competências para explorar os benefícios da rápida mudança digital" (Reino Unido, 2023c, p. 33).

De nosso particular interesse, a emergência de um processo de mudança institucional que corresponde a nova percepção militar sobre o papel das tecnologias digitais em conflitos torna-se evidente ao passo em que ferramentas outrora compreendidas como 'facilitadoras' passam a serem tratadas como a pedra angular da abordagem de dissuasão (Reino Unido, 2023c, p. 33)[25].

A centralidade reservada à tecnologia permitirá "uma aceleração na tomada de decisões no campo de batalha, maior produtividade da força e, o mais importante, mais letalidade" (Reino Unido, 2023c, p. 32). Em razão disso, técnicas de aprendizagem de máquina e a inteligência artificial são percebidas como vetores estratégicos capazes de ampliar, sobremaneira, a eficiência das operações, com efeitos sobre a "velocidade e precisão (...) mobilidade e sustentabilidade (...) até a produção de código de missão crítica para atualizar *softwares* vitais para o campo de batalha" (Reino Unido, 2023c, p. 33).

Ante a conjuntura, é possível notar que o desenvolvimento futuro das estruturas de força do Reino Unido é encarado como dependente do uso efetivo destas tecnologias nas campanhas. Desse modo, os britânicos apostam no potencial de sensores quânticos para ampliar as capacidades de coleta de informação; uso de materiais avançados na construção de sistemas operacionais; armas de energia capazes de atingir enxames de drones com precisão, dentre outras capacidades que deverão ser empregadas de "forma segura, ética e responsável, alinhadas com os valores da sociedade que servimos" (Reino Unido, 2023c, p. 32).

Não obstante, tendo por base o potencial destas ferramentas para produção de vantagens estratégicas em operações de combate, reforça a importância da parceria entre governo e indústria para desenvolvimento e aprimoramento de capacidades que permitam a atuação assertiva em distintos domínios de guerra (Reino Unido, 2021; 2023c)[26], assim, o investimento em desenvolvimento e emprego de meios informacionais inovadores é desejável para alavancar a projeção de poder em diversos campos de interesse nacional.

[25] Como medida prioritária destaca o interesse em desenvolver cinco tecnologias críticas: inteligência artificial para construir cenários em que as forças possam obter vitórias rápidas, investir de modo assertivo; engenharia biológica para produção d modelos sintéticos que permitam indicar soluções para o emprego efetivo da força; telecomunicações organizadas com base em infraestrutura nacional; semicondutores que contribuam para a aquisição de ferramentas de detecção, imagem, armas, medidas de combate e comunicações; computação quântica capaz de ampliar significativamente a velocidade no processamento de dados (Reino Unido, 2023c).

[26] Dentre as finalidades da defesa que se dispõe a proteger a segurança nacional britânica, reforça o interesse inequívoco em produzir vantagens estratégicas que permitam atingir a "resiliência econômica e industrial e contribuir para a prosperidade nacional" (Reino Unido, 2023c, p. 9). Para tanto, assume o compromisso de investir em desenvolvimento humano e inovação técnico-científica que permita aumentar a produtividade, aprimorando as capacidades de prontidão e a letalidade das operações (Reino Unido, 2023c).

No tocante aos propósitos analíticos deste ensaio, naquilo que compete às instituições securitárias responsáveis pela inteligência, reforça a importância do compartilhamento de informações com aliados e parceiros em operações conjuntas a fim de obter vantagens estratégicas em conflitos. Já em termos operacionais, prevê o uso de drones, redes e sensores que permitirão a captura de informações depuradas com ajuda de *softwares* avançados para apoio em processos de tomada de decisão de forma ágil e eficiente (Reino Unido, 2023c)[27].

Vale ressaltar que durante o conflito russo-ucraniano, a Inteligência de Defesa do Reino Unido desempenhou papel estratégico importante em processos de avaliação da conjuntura e disseminação de informações críticas aos decisores, e divulgação de outras menos específicas em domínio público por intermédio de canais tradicionais e das redes sociais, num esforço para mitigar tentativas do governo russo de disseminar informações falsas sobre o conflito (Reino Unido, 2023c).

Já no que concerne à constituição de novas estruturas de força responsáveis por incorporar a inteligência artificial às capacidades militares, aponta a criação do Centro de IA de Defesa (DAIC) e do Centro de IA do Exército (AAIC) dedicados a exploração de formas robustas de emprego dessa ferramenta em campanhas. Concomitantemente, o Ministério da Defesa (MOD) tem buscado acelerar o processo de modernização digital através da implementação do programa 'Backbone Digital' que prevê a transformação dos sistemas de comunicação e arquitetura informacional para permitir o melhor uso dos dados em processos de tomada de decisão (Reino Unido, 2023c).

Ademais, frisa a significância de novos agrupamentos como o 'Digital Foundry' constituídos para identificar "novas formas de explorar dados, aproveitar a IA e partilhar e dimensionar novas ideias" (Reino Unido, 2023c, p. 35), bem como do programa de Exploração Digital para Defesa (DX4D) que indica diretrizes para o uso da tecnologia da informação "tanto no espaço de batalha quanto no espaço de negócios" (Reino Unido, 2023c, p. 35).

> Investiremos ainda mais na atualização dos nossos sistemas e no desenvolvimento de ferramentas para que possamos maximizar a utilização dos nossos dados em apoio à nossa tomada de decisões. Sabemos que já não é opcional: dados acessíveis e de alta qualidade são uma componente crítica do nosso poder de combate (Reino Unido, 2023c, p. 35).

É, portanto, axiomático que a rápida evolução das tecnologias de informação impactou decisivamente a estrutura de força britânica neste século, compreendidas como basilares para a consecução de objetivos estratégicos. Nesse ensejo, o documento enfatiza que "o poder das tecnologias e dos dados digitais reforçará a dissuasão, a resiliência e a prosperidade nacional" (Reino Unido, 2023c, p. 33-34).

Destarte, a mudança institucional doravante em relevo pretende promover a construção de uma estrutura quantitativamente reduzida, porém qualitativamente mais produtiva. Para tanto, a DCP apresenta uma série de transformações no modelo operacional que têm sido implementadas com o objetivo primário de fortalecer as capacidades dissuasórias não apenas reduzir riscos e aproveitar

[27] A implementação da estratégia das instituições securitárias para incorporação da inteligência artificial como ferramenta-chave para ampliar a qualidade dos processos decisórios e a eficiência operacional é destacada como prioridade em uma seção específica neste documento que trata do desenvolvimento substantivos de Grandes Modelos Linguísticos (GML) que representam uma revolução nas capacidades destes organismos (RD, 2023). Não obstante, destaca forte preocupação com o uso responsivo e ético destas opções que permitam seu desenvolvimento e emprego de modo seguro a nível mundial (Reino Unido, 2023c).

oportunidades, mas ampliar os níveis de letalidade e prontidão das instituições securitárias (Reino Unido, 2023c)[28].

Tendo em vista a centralidade da exploração de dados para o novo modelo operacional das Forças Armadas britânica, a transformação incide sobre a infraestrutura de rede responsável pelo funcionamento de setores críticos para a defesa nacional. Por este prisma, a segurança cibernética assume papel decisivo para assegurar a resiliência necessária para lidar com as ameaças que procurem causar efeitos cinéticos através de campanhas de reconhecimento e exploração de redes de computador, em resposta as instituições securitárias britânicas pretendem criar incentivos para "mitigar o risco de falhas ou ataques de ativos. Investiremos também para garantir que dispomos de recursos críticos suficientes para permitir a dispersão e a regeneração [destes sistemas]" (Reino Unido, 2023c, p. 46).

Não obstante, o documento enfatiza o interesse da defesa em permanecer na vanguarda do domínio cibernético "pronta para competir constantemente e lutar quando o limiar do conflito armado for ultrapassado, permanecendo ao mesmo tempo resiliente às ameaças" (Reino Unido, 2023c, p. 59). Em efeito, destaca a criação da Força Cibernética Nacional (NCF) como organismo responsável pelo estreitamento dos laços entre a defesa e a inteligência, tendo por base esforços conjuntos orquestrados pelo MOD, GCHQ, MI6 e DSTL, a fim de "apoiar operações militares e prevenir crimes graves" (Reino Unido, 2023c, p. 59).

O documento revela que a NCF possui capacidades cibernéticas ofensivas que deverão ser aprimoradas no futuro próximo, a fim de que possam ser utilizadas em conflitos de modo integrado com os demais domínios de guerra. Mais do que isso, conta com recursos para promover a segurança de sistemas informacionais "proteger, detectar, responder e recuperar de eventos cibernéticos e fornecer operações cibernéticas defensivas, inclusive fora das nossas redes, quando necessário" (Reino Unido, 2023c, p. 60).

Frente ao exposto nesta seção, resta claro que a resposta das instituições securitárias do Reino Unido acha-se diretamente conectada ao atendimento dos interesses britânicos dispostos em sua estratégia nacional. Nesse sentido, o processo de transformação das capacidades destas estruturas para desempenho de suas competências provocou uma mudança no pensamento militar, haja vista que, para além sua consideração como ferramentas de suporte, tais artefatos passaram a ocupar o centro da agenda devido aos impactos que podem causar nas disputas interestatais contemporâneas por poder e influência no sistema internacional.

5 CONSIDERAÇÕES FINAIS

As considerações finais procuram retomar o questionamento central deste ensaio sobre como a inteligência britânica têm se beneficiado da 'quinta revolução industrial' no desempenho de suas atividades, resumindo os principais pontos discutidos acerca do problema.

A primeira seção apresentou a estrutura de inteligência do Reino Unido, altamente institucionalizada e integrada, em cada nível são estabelecidos mecanismos que conectam os sistemas

[28] Depreende-se do documento que a exploração de novas tecnologias se torna imprescindível do alto potencial para impactar de modo significativo as condições em que ocorrem os conflitos contemporâneos "devemos extrair o máximo de eficiência da tecnologia em nossa administração. A transformação está remodelando radicalmente nosso ambiente de treinamento para enfrentar o futuro" (Reino Unido, 2023c, p. 45).

de inteligência com as decisões políticas e militares, movido por sistemáticas de produção e difusão da informação. Como demonstrado, no cumprimento de suas atividades essas instituições precisam incorporar novas tecnologias para encarar o desafio de assessorar processos decisórios em tempo hábil.

A segunda seção discorreu sobre a estratégia do Reino Unido para perseguir os interesses nacionais mediante a percepção da volatilidade do mundo contemporâneo. Frente ao cenário, os britânicos sublinham a importância do processo de construção de incentivos ao desenvolvimento de capacidades de projeção de poder nacional com base em quatro pilares fundamentais que permitam auferir retornos estratégicos crescentes em disputas por poder e influência.

Na terceira seção, o foco sobre a mudança institucional que resulta de transformações significativas no pensamento militar para construção de capacidades e estruturas de força demonstrou como a incorporação de novas tecnologias passou a ocupar o centro nevrálgico das capacidades dissuasórias do Reino Unido, em parte, devido ao teste do sistema de resiliência provocado pela desestabilização do equilíbrio securitário da região Euro-Atlântica. Em resposta, os britânicos promoveram a construção de novas estruturas securitárias competentes para lidar com a incorporação de novas tecnologias informacionais que aprimoram, sobremaneira, a eficiência da inteligência.

Por fim, seja por proporcionarem vantagens estratégicas em conflitos mediante uso ofensivo e/ou contribuírem de modo substantivo para construção da defesa ativa capaz de lidar com as ameaças contemporâneas, as novas tecnologias da informação simbolizam a manifestação dos efeitos provocados pela 'quinta revolução industrial' no Reino Unido. Ante a conjuntura, este ensaio demonstra que o seu emprego em atividades de inteligência tem permitido a construção e entrega, em tempo hábil, de produtos significativos para amparar processos de tomada de decisão, capitaneados por lideranças políticas e militares preocupadas em alavancar os interesses estratégicos nacionais.

REFERÊNCIAS

REINO UNIDO. **National Cyber Security Strategy 2016-2021**. Cabinet Office. 2020. Disponível em:<https://assets.publishing.service.gov.uk/media/5fbceaf08fa8f559e32b4cc1/6.6788_CO_National-Cyber-Security-Strategy-2016-2021_WEB3.pdf>. Acesso em: 06.07.2024.

REINO UNIDO. **National Cyber Strategy 2022**. Cabinet Office. 2022c. Disponível em: < https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>.Acesso em: 04.07.2024.

REINO UNIDO. **Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security sectors**. Presented to Parliament by the Secretary of State for Defence. 2021. Disponível em: <https://assets.publishing.service.gov.uk/media/60590e988fa8f545d879f0aa/Defence_and_Security_Industrial_Strategy_-_FINAL.pdf >. Acesso em: 09.07.2024.

REINO UNIDO. **Joint Doctrine Publication 0-01 UK Defence Doctrine**. Ministry of Defence. 2022a. Disponível em: <https://assets.publishing.service.gov.uk/media/63776f4de90e0728553b568b/UK_Defence_Doctrine_Ed6.pdf >. Acesso em: 13.07.2024.

REINO UNIDO. **The UK Government Resilience Framework**. Cabinet Office. 2022b. Disponível em: <https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html>. Acesso em: 15.07.2024.

REINO UNIDO. **Integrated Review Refresh 2023 Responding to a more contested and volatile world**. Presented to Parliament by the Prime Minister. 2023a. Disponível em: <https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world >. Acesso em: 11.07.2024.

REINO UNIDO. **Defence's reponse to a more contested and volalite world**. Presented to Parliament by the Secretary of State for Defence. 2023c. Disponível em: <https://assets.publishing.service.gov.uk/media/64b55dd30ea2cb000d15e3fe/Defence_Command_Paper_2023_Defence_s_response_to_a_more_contested_and_volatile_world.pdf >. Acesso em: 12.07.2024.

REINO UNIDO. **Joint Doctrine Publication 2-00 Intelligence, Counter-intelligence and Security Support to Joint Operations**. Ministry of Defence. 2023b. Disponível em: <https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf >. Acesso em: 18.07.2024.