JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

Vol. 1, Nº. 1 (Sep./Dec. 2025)

Editorial Board

Contact Information

Editorial Office — Journal of Cybersecurity and Public Policies

contato@cybersecuritypolicies.com.br

Índice

JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

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):

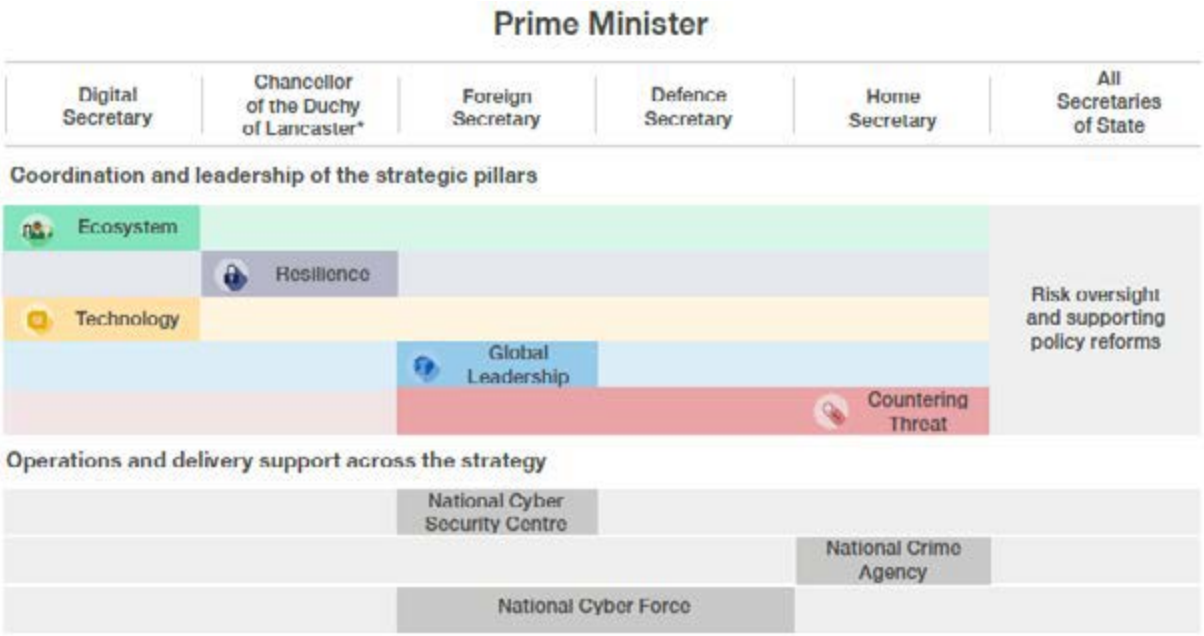


Figura 1. Estratégia Nacional Cibernética – Responsabilidades
Fonte: HM Government, 2021.

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).

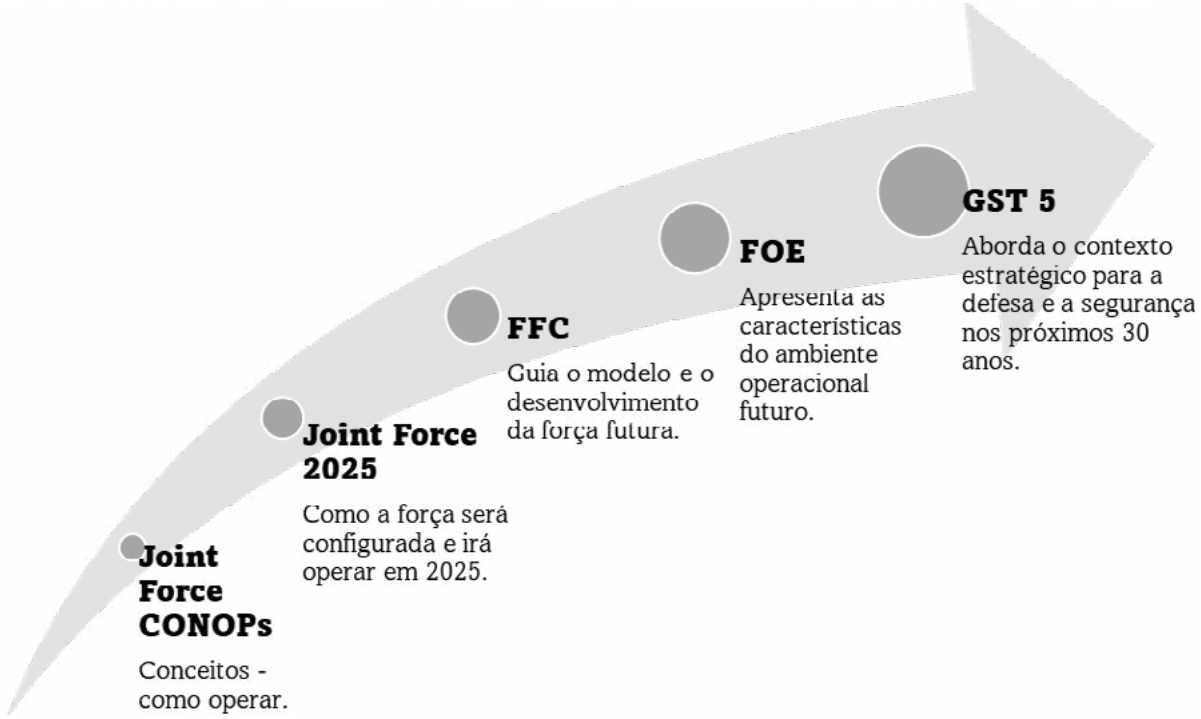
Em virtude de sua natureza descentralizada e dispersa, o ciberespaço permanecerá poroso e vulnerável. Mesmo que contestado por diversos atores, o domínio total será impossível. Diante disso, projetam-se grandes desafios para a segurança da informação e das infraestruturas, com ataques cibernéticos crescendo 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.

JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

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

Cryptocurrencies and Cybercrime: Political and International Challenges in the Digital Age

Rickiã Gabriel de Magalhães Rodrigues[1]

Abstract

How do different regulatory jurisdictions address the international security challenges posed by the intersection of cryptocurrencies and cybercrime? This article analyzes the policy responses of the United States, European Union, United Kingdom, and Singapore through a comparative document analysis of public policy. The findings reveal diverse regulatory approaches—ranging from restrictive models to cooperative frameworks—exposing institutional fragmentation in the face of shared threats. This research contributes to the debate on global governance and cybersecurity, offering empirical input to the field of International Relations by providing guidance for enhancing international cooperation against transnational financial cybercrime.

Keywords: cryptocurrencies; cybercrime; global governance; international security; financial regulation.

1 Master's student in Political Science at the Federal University of Pernambuco (UFPE), where also earned a Bachelor's degree in Political Science (2023). Main research focuses on international political economy, monetary and fiscal policy, interest groups, and cryptocurrencies.

Introduction

The advent of digital technologies has profoundly reshaped the contours of global politics and finance, introducing innovative opportunities alongside unprecedented challenges. Among these innovations, cryptocurrencies have emerged as a revolutionary force, promising decentralized finance, near-instant transactions, and greater financial inclusion (Nakamoto, 2008; Antonopoulos, 2017). However, this transformative potential is increasingly tied to a growing dark side: the deepening nexus between cybercrime and cryptocurrencies (Foley et al., 2019; August et al., 2025). This phenomenon is part of a broader trend where digital infrastructure, initially designed for communication and commerce, is being exploited for illicit activities and state control (Deibert, 2019).

At the same time, ransomware attacks continue to strike critical infrastructure worldwide, with criminals demanding payment exclusively in digital assets (Chainalysis, 2025). These episodes illustrate a central paradox of the digital age: the same technologies that promise to democratize financial access have also become instruments of international security threats.

In response to this landscape of growing criminal sophistication, global powers have intensified efforts to develop comprehensive regulatory frameworks. The United States, European Union, United Kingdom, and Singapore have implemented distinct policies that reflect different philosophies of digital governance and national security priorities (Galasso, 2024). This diversity of approaches highlights the lack of international consensus on optimal governance methods for decentralized digital assets (Ba; Şen, 2024).

How do different regulatory jurisdictions address the international security challenges posed by the intersection of cryptocurrencies and cybercrime? This question emerges as a central governance challenge in contemporary global politics—transcending national borders and defying traditional regulatory frameworks (Farber, 2025). The phenomenon represents a fundamental test of states' capacity to coordinate effective responses to transnational threats in a decentralized digital environment (Choucri; Anaya, 2024).

This study seeks to systematize the main jurisdictional strategies for addressing these emerging threats, providing a comparative diagnosis to guide policymakers. It serves as an empirical basis for developing best practices in digital asset governance, helping to reduce the regulatory fragmentation that benefits malicious actors (Ba; Şen, 2024).

The main objective of this research is to comparatively analyze the regulatory strategies adopted by different jurisdictions to combat the use of cryptocurrencies in cybercriminal activities. Specific objectives include: (i) identifying the main challenges perceived by each jurisdiction at the crypto-cybercrime intersection; and (ii) quantifying the international cooperation mechanisms proposed to address these transnational threats.

Methodologically, this study uses a comparative document analysis of four official public policy documents, applying a structured twelve-question questionnaire to extract data on goals, definitions, identified challenges, and proposed cooperation mechanisms (Prior, 2003; Cardno, 2018). Descriptive statistical analysis of the results will allow for the identification of patterns and divergences in jurisdictional approaches

For policymakers, this article provides a crucial comparative diagnosis for developing more effective international cooperation mechanisms. It also contributes to scholarship by offering the first systematic mapping of jurisdictional variations in responses to the crypto-cybercrime nexus, filling an important gap in the literature on international digital security.

1. Theoretical-Empirical Framework: Cryptocurrencies and Cybercrime in the Digital Age

This section is dedicated to conceptualizing and establishing the fundamental parameters for understanding the intersection of cryptocurrencies and cybercrime in the context of contemporary international relations.

The conceptual framework is structured across four analytical dimensions: (i) operational definitions of cybercrime in the digital age; (ii) technological characteristics of cryptocurrencies as a decentralized financial infrastructure; (iii) international relations theories applicable to transnational digital threats; and (iv) criminological frameworks that explain how specific features of digital assets facilitate illicit activities.

1.1 The Convergence of Digital Crime and Decentralized Finance

The intersection of cryptocurrencies and cybercrime represents a fundamental transformation in both criminal activity and international security dynamics. Cybercrime encompasses a set of illicit activities that use information technologies as a means, target, or environment for execution (Wall, 2007). Modern taxonomies distinguish between "cyber-dependent crimes"—offenses that can only be committed through computer systems—and "cyber-enabled crimes," which amplify traditional criminal activities using digital technologies (McGuire; Dowling, 2013). This distinction proves crucial for understanding how cryptocurrencies permeate both categories, serving simultaneously as targets for attacks and facilitators of criminal activity.

Cryptocurrencies are digital monetary systems based on blockchain technology that operate independently of traditional central authorities (Narayanan et al., 2016). Their defining characteristics—decentralization, pseudo-anonymity, transaction irreversibility, and global reach—create a technological environment offering both legitimate benefits and illicit opportunities.

Decentralization removes single points of failure but eliminates traditional intermediaries that perform compliance and monitoring functions (Ba; Şen, 2024). The pseudo-anonymity of cryptocurrencies creates a layer of obscurity exploitable by malicious actors, though increasingly sophisticated blockchain forensic analyses demonstrate it does not constitute absolute anonymity (World Bank, 2018).

The empirical manifestation of this convergence is most visible in ransomware attacks, which have fundamentally transformed the digital threat landscape. The near-universal preference for cryptocurrency payments stems from their ability to enable fast, cross-border transfers with lower traceability compared to traditional financial systems (Conti et al., 2018). The "Ransomware-as-a-Service" (RaaS) model has democratized access to advanced cybercriminal capabilities, enabling actors with limited technical expertise to conduct sophisticated attacks through cryptocurrency-based service platforms (Chainalysis, 2025).

Table 1. Typology of Cybercrimes Facilitated by Cryptocurrencies

Type of Cybercrime	Role of Cryptocurrency	Examples
Cyber-Dependent Crimes		
Ransomware	Preferred payment method due to pseudo-anonymity and global reach; optimizes monetization.	NotPetya, CryptoLocker, WannaCry
Hacking	Funding for tools/services; payment for stolen data.	Exchange hacking (fund theft), CryptoLocker, funding cyber operations
Malware Distribution	Payment for "malware-as-a-service" ;illicit financial gains.	Distribution of trojans, botnets
Cyber-Enabled Crimes		
Money Laundering (Crypto-washing)	Pseudo-anonymity, speed, cross-border transfer, obfuscation (mixers, layering	Hiding illicit proceeds from drug trafficking, fraud, terrorism financing
Drug Trafficking	Exclusive currency on darknet markets enabling anonymous transactions.	Drug sales on Silk Road, AlphaBay
Terrorist Financing	Financing clandestine operations; anonymous donations; sanction evasion.	Fundraising by Al-Qaeda, Hamas, ISIS; WMD funding by North Korea
Fraud/Scams	Facilitates investment scams, phishing, "romance baiting"; irreversible transactions.	nvestment scams, tech support scams, impersonation of government agents
Sanctions Evasion	Circumventing traditional financial channels; financing illicit trade and WMD programs.	Lazarus Group (North Korea) using crypto for missile development

Source: Author's elaboration (2025)

1.2 Theoretical Perspectives on Transnational Digital Threats

Analyzing the crypto-cybercrime nexus requires theoretical frameworks capturing both power dynamics among states and challenges posed by transnational non-state actors. The theory of complex interdependence by Keohane and Nye (2011) offers insight into how multiple

channels of connection—governmental, international organizational, and transnational—shape responses to threats crossing national borders. The rise of state-sponsored cybercrime further exacerbates the "cybersecurity dilemma," where one nation's defensive measures can be perceived as offensive threats by another, leading to breakdown of trust and arms races in cyberspace (Buchanan, 2017).

From a neorealist perspective, the anarchic structure of the international system creates incentives for states to exploit cryptocurrencies for strategic advantage, whether through sanctions evasion or funding covert operations (Waltz, 1979). This systemic pressure manifests empirically in cases like North Korea's systematic use of cryptocurrencies to evade international sanctions.

The Lazarus Group, linked to the North Korean regime, has generated over $1 billion through attacks on cryptocurrency exchanges since 2015, using sophisticated laundering techniques including mixing services and "chain-hopping" across different digital assets (Oladipupo, 2025). The challenge of attributing cyber attacks to specific actors complicates traditional state responses to these threats (Rid; Buchanan, 2015).

Constructivist perspectives illuminate how emerging norms around cybersecurity and digital governance are socially constructed through interactions among states, international organizations, and private actors (Wendt, 2000). The lack of consensus on appropriate governance norms for cryptocurrencies reflects broader disputes over digital sovereignty and the appropriate role of the state in regulating decentralized technologies. This normative vacuum creates opportunities for malicious actors operating between Westphalian concepts of territorial sovereignty and the borderless nature of digital spaces (Rosenau, 1997).

1.3 Criminal Ecosystems and Money Laundering Evolution

The dark web has established a sophisticated commercial ecosystem where cryptocurrencies serve as the exclusive medium for illicit transactions, creating a parallel economy operating independently of regulated financial systems. Marketplaces such as the historic Silk Road demonstrated how cryptocurrencies enable anonymous global trade in illicit goods—from drug trafficking to sale of stolen personal data (Christin, 2013). The resilience of these markets, evidenced by rapid emergence of successors after law enforcement takedowns, illustrates how crypto-decentralization allows for more efficient "crime displacement" than traditional criminal networks (Barratt; Aldridge, 2016).

The "Crypto-laundering" represents a major evolution in money laundering techniques, leveraging unique characteristics of digital assets to obscure origins of illicit funds (Albrecht et al., 2019; Houben; Snyers, 2018). The traditionally three-phase laundering process—placement, layering, and integration—has been adapted to the digital environment through crypto-to-fiat

conversions, transfers across multiple blockchains, and use of decentralized exchanges with weaker compliance measures (Fanusie; Robinson, 2018). The ability to conduct high-value operations potentially amounting to billions of dollars with low likelihood of detection makes cryptocurrency-based money laundering highly attractive (Irwin; Milad, 2016).

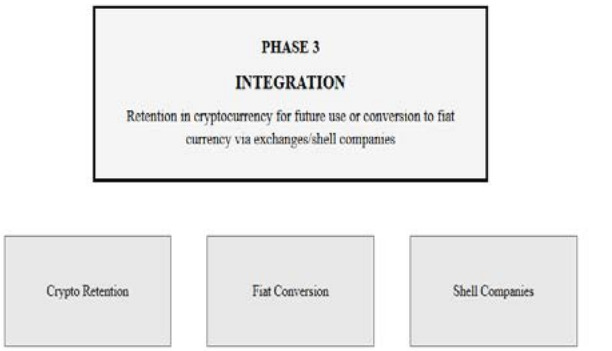


Figure 1. Flowchart of the cryptocurrency money laundering process

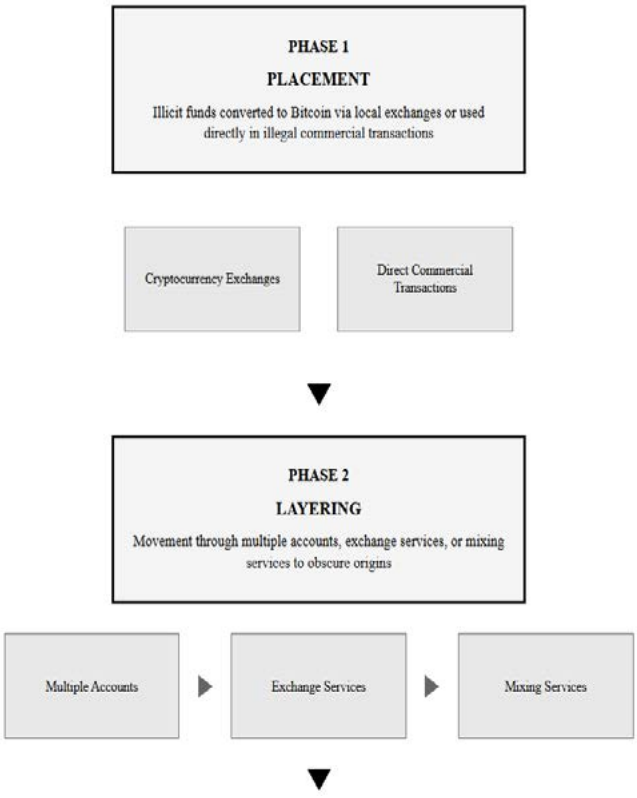


Figure 1. Flowchart of the cryptocurrency money laundering process

Source: Author's elaboration based on the three-phase money laundering model adapted for cryptocurrencies. The flowchart illustrates the operational sequence used by criminals to legitimize illicit funds through digital assets, following the classic steps of placement, stratification, and integration into the traditional financial system. (2025).

Criminological models, particularly environmental criminology, offer analytical lenses for understanding how specific features of cryptocurrencies facilitate criminal activity. Rational

Choice Theory posits that criminals are rational actors evaluating costs and benefits of their actions (Clarke; Felson, 1993).

From this perspective, cryptocurrencies significantly reduce perceived costs due to lower risks of detection and prosecution while maximizing potential benefits through access to global markets and greater operational efficiency. Routine Activity Theory suggests crimes occur when motivated offenders, suitable targets, and absence of capable guardians converge (Cohen; Felson, 1979).

2. Regulatory Responses and International Cooperation

2.1 Ransomware and the Transformation of Digital Crime

National responses to the crypto-cybercrime nexus reflect distinct regulatory traditions, foreign policy priorities, and institutional capacities. The United States maintains a fragmented approach characterized by overlapping oversight from multiple federal agencies—FinCEN, CFTC, and SEC—creating a complex regulatory landscape potentially exploitable by malicious actors (Hughe; Middlebrook, 2015).

The establishment of the FBI's Virtual Asset Unit represents centralization attempts, though coordination gaps persist. The European Union seeks harmonization through the Markets in Crypto-Assets (MiCA) regulatory framework, complemented by the NIS2 Directive on cybersecurity and the Cyber Resilience Act (Zetzsche et al., 2020).

Singapore has developed comprehensive preventive frameworks emphasizing compliance and rigorous KYC/AML requirements, while the United Kingdom balances operational enforcement with technological innovation. Brazil's evolving approach through Law No. 14,478/2022 establishes a legal framework for virtual assets while extending existing AML laws to cryptocurrency operations (Brasil, 2022). China maintains highly restrictive policies, treating cryptocurrencies as "specific virtual commodities" rather than legitimate monetary instruments, enacting sweeping bans on trading and mining activities (Hu, 2024).

Table 2. Comparative Analysis of National Cryptocurrency Regulations

Country/ Bloc	Regulatory Stance	Key Legislation/ Guidelines	Primary Regulatory Bodies	Main AML/ KYC Requirements	Policy Challenges/ Gaps
EUA	fragmented, Evolving	Bank Secrecy Act, FinCEN Guidance, CFTC/SEC Decisions	FinCEN, CFTC, SEC, FBI (VAU)	Evolving, applied to money transmitters	Regulatory fragmentation, potential for capture, DeFi vulnerabilities, data gaps

UE	Harmonized, Progressive	Markets in Crypto-Assets (MiCA), NIS2 Directive, Cyber Resilience Act	European Commission, ESMA, EBA, Europol	Strict, applied to Virtual Asset Service Providers (VASPs)	Unlicensed exchanges, privacy coins, obfuscation techniques, enforcement difficulties
Brasil	Evolving, Cautious	Law No. 14,478/2022 (BVAL), Decree No. 11,563/2023	Central Bank of Brazil (BCB), CVM	Existing AML laws extend to crypto	Lack of specific AML regime, governmental concerns, legislative proposals still under development[2]
China	Highly Restrictive, Prohibitive	"Notice on Preventing Bitcoin Risks" (2013), "Announcement on Preventing Token Issuance Financing Risks" (2017), "Notice on Further Prevention and Resolution of Virtual Currency Trading and Speculation Risks" (2021)	People's Bank of China (PBOC), Cyberspace Administration of China (CAC)	Strict, mandatory data collection	Regulatory vacuum (offshore platforms), legal ambiguity, consumer protection, global asset flow vs. single-state regulation

Source: Author's elaboration (2025)

The fragmentation in regulatory approaches creates arbitrage opportunities for criminal actors who exploit jurisdictional gaps. The problem is compounded by increasing use of cryptocurrencies by state-sponsored actors functioning as "cyber mercenaries" to achieve political and financial objectives (Maurer, 2018). This challenge is particularly acute with privacy coins and decentralized finance protocols operating beyond traditional regulatory reach.

2.2 International Cooperation Mechanisms and Institutional Challenges

International organizations play increasingly central roles in coordinating responses to crypto-cybercrime, though facing significant structural limitations. The Financial Action Task Force (FATF) has established standards for Virtual Asset Service Providers through its 40 Recommendations, but implementation varies substantially across member jurisdictions (FATF, 2019). The pseudo-anonymous nature of cryptocurrencies and lack of centralized ownership records hinder effective enforcement of these standards.

Interpol coordinates transnational operations through its Cybercrime Directorate, employing tools such as blockchain analytics to trace illicit flows. However, it faces challenges posed by rapid evolution of criminal tactics and limited technical capabilities of national security forces.[3] The UNODC has developed training programs on cryptographic and darknet

2 https://www.ibanet.org/Brazil-legal-framework-for-cryptoassets-and-upcoming-regulation
3 https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

investigations, acknowledging that technical knowledge gaps restrict effectiveness of national responses.[4] The emergence of Central Bank Digital Currencies (CBDCs) adds another layer of complexity to the regulatory landscape, potentially offering greater control but also new vulnerabilities (Auer; Böhme, 2020).

3. Methodology

3.1 Research Design

This research employs comparative documentary analysis to examine how different jurisdictions address the international security challenges posed by the crypto-cybercrime nexus. The methodological choice is justified by the need to capture systematic variations in official public policies, enabling structured comparison between distinct jurisdictional approaches while maintaining fidelity to the conceptual frameworks and priorities expressed by each government.

Table 3. General Methodological Information

Sections	Description
Research Question	How do different regulatory jurisdictions address the international security challenges posed by the intersection of cryptocurrencies and cybercrime?
Unit of Analysis	Official public policy documents from four jurisdictions representing different regulatory traditions
Temporal Delimitation	Contemporary documents from 2024-2025 to ensure current relevance
Sources	Government agencies and official regulatory bodies
Techniques	Comparative documentary analysis with structured questionnaire (12 questions), categorical content analysis
Software	Google Docs, Sheets and R for visual elements
Data Repository	OSF with the raw answered questions and comparative table matrixes[5]

Source: Author's elaboration (2025)

3.2 Corpus Documental and Selection Criteria

The corpus consists of four official public policy documents selected to represent different regulatory traditions and strategic approaches to the crypto-cybercrime nexus. The selection is justified by the need to capture systematic variations in institutional responses from jurisdictions with different regulatory capacities, legal traditions, and foreign policy priorities:

1. **Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service** - (Monetary Authority of Singapore)

4 https://www.unodc.org/roseap/en/2022/02/cryptocurrencies-darknet-investigations/story.html
5 https://osf.io/m654j/

2. **2024 National Strategy for Combating Terrorist and Other Illicit Financing** - (US Department of Treasury)
3. **National Strategic Assessment 2025 of Serious and Organised Crime** - United Kingdom
4. **Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances** (Europol)

These documents were selected based on three criteria: (i) jurisdictions with high economic relevance in the global crypto ecosystem; (ii) advanced institutional capacities for enforcement; and (iii) significant international normative influence. The preference for official primary sources ensures analysis captures policies effectively implemented by states, while temporal selection (2024-2025) guarantees contemporary relevance.

3.3 Data Collection Instrument

A structured questionnaire with 12 questions was developed to extract comparable information from the selected documents, following principles established by Bowen (2009) for reducing interpretive bias and enabling comparability. The questionnaire covers four analytical dimensions:

Framework 1: Questionnaire for Documentary Analysis

Nº	Question	Description / Application
1	What is the responsible government body for the document?	Identify whether it is a central bank, security agency, justice ministry, or another official body.
2	What are the main objectives of the document regarding cryptocurrencies and cybercrime?	E.g., money laundering prevention, ransomware crackdown, cryptoasset traceability.
3	How does the document define cybercrimes involving cryptoassets?	Check for distinctions between ransomware, fraud, tax evasion, etc.
4	Does the document define or approach the concept of "cryptoassets" or "virtual assets"?	Analyze the scope and technical depth of the definition.
5	What are the key challenges identified at the intersection of cybercrime and cryptocurrencies?	E.g., anonymity, regulatory gaps, cross-border jurisdiction issues.
6	Are specific malicious actors mentioned as threats?	Investigate whether hackers, transnational groups, terrorists, or hostile nations are cited.
7	Does the document mention international cooperation to combat cybercrime involving cryptoassets	E.g., references to Interpol, FATF/GAFI, bilateral agreements, information exchange.
8	Does the document propose partnerships with specific international organizations?	E.g., UN, FATF, OECD, Europol, World Bank.
9	What specific enforcement or law enforcement mechanisms are proposed?	Identify regulatory tools, penalties, and investigation procedures.

10	Is there mention of private sector engagement (e.g., exchanges, fintechs, banks)?	Indicate whether institutional dialogue or participatory regulation is included.
11	Does the document discuss national and international jurisdiction issues in crypto-related crimes?	Identify legal barriers and the search for cross-border legal solutions.
12	Are emerging technologies for tracking and combating crypto-related crime discussed?	E.g., blockchain analytics, artificial intelligence, tech partnerships.

Source: Author's elaboration (2025)

Step 1: Reading and Extraction

Each document was read in its entirety to locate answers to the 12 questionnaire questions. This "close reading" process is fundamental in documentary analysis, enabling familiarization with content before formal coding (O'Leary, 2014). Relevant information was extracted and recorded in a comparative spreadsheet, maintaining references to original pages for traceability.

Step 2: Response Coding

Extracted responses were coded into categories to enable comparison between jurisdictions, following content analysis procedures described by Schreier (2012). For example:

a) For the question about challenges (question 5), responses were categorized as: "anonymity," "jurisdiction," "transaction speed," "lack of regulation," etc.

b) For international cooperation (question 7), mentions of specific organizations were identified: "FATF," "Interpol," "bilateral agreements," etc.

Step 3: Descriptive Statistical Analysis

Coded data were analyzed quantitatively to identify frequencies, convergence patterns, divergence patterns, and gaps. This approach of transforming qualitative data into quantitative through categorical coding is widely used in comparative policy analysis (Rihoux; Ragin, 2009). Results are presented through frequency tables and comparative graphs, enabling clear visualization of similarities and differences between jurisdictional approaches.

3.4 Methodological Limitations

The main limitation is the differential availability of official documents between jurisdictions - a common challenge in comparative public policy studies (Yanow, 2007). While the United States, European Union, and United Kingdom produce detailed reports on crypto-cybercrime, many Global South jurisdictions lack equivalent documents, resulting in under-representation of these perspectives.

Additionally, documentary analysis captures only formally expressed policies, not their practical implementation or real effectiveness (Colebatch, 2009). The analysis is also limited to English-language documents, potentially missing nuanced approaches from non-English speaking jurisdictions.

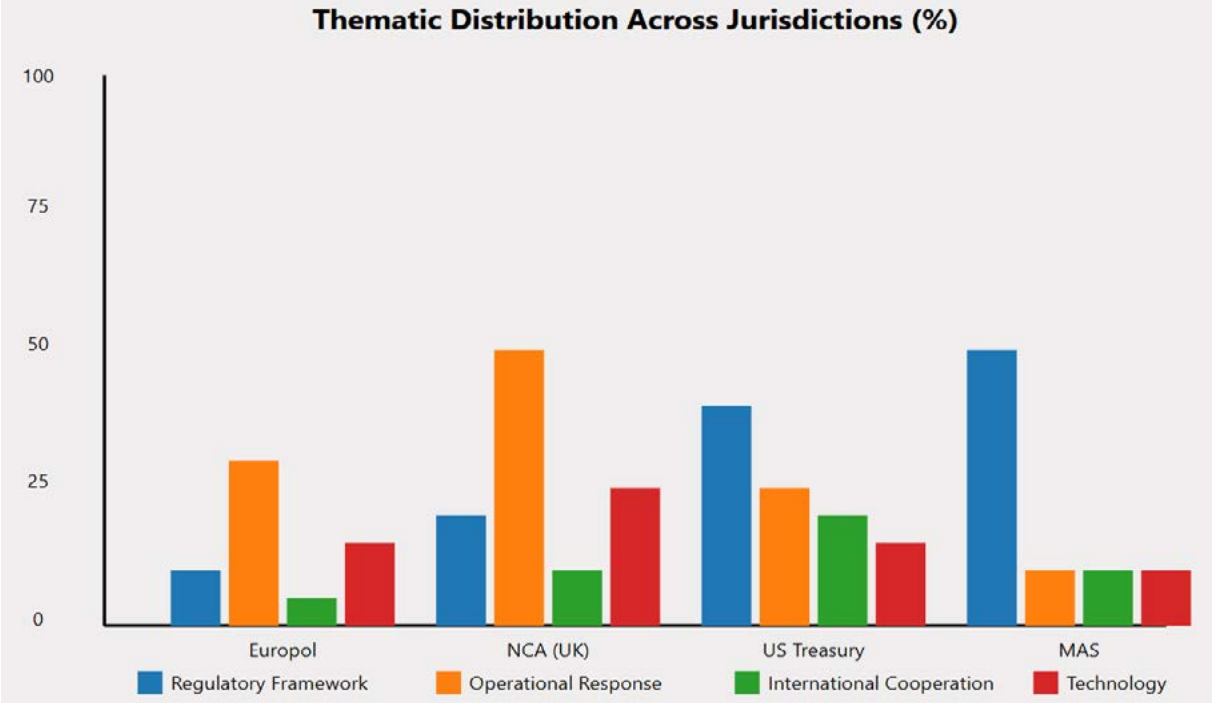
4. Results

The comparative analysis of the four official documents reveals distinct patterns in jurisdictional approaches to the crypto-cybercrime nexus, evidencing both convergences and significant divergences in regulatory and operational strategies.

4.1 Comparative Analysis of Jurisdictional Strategies

Documentary analysis identified substantial variations in regulatory approaches among the examined jurisdictions. Graph 1 presents the thematic distribution of main focuses in each analyzed document.

Graph 1. Thematic distribution across jurisdictions (%)



Source: Author's elaboration (2025)

As demonstrated in Graph 1, distinct jurisdictional profiles emerge: Singapore (MAS, 2024) concentrates 45% of its content on detailed regulatory frameworks, reflecting a preventive

compliance-based approach. In contrast, the United Kingdom (NCA, 2025) dedicates 35% to operational response, showing focus on enforcement and practical cases. The United States (US Treasury, 2024) presents a more balanced distribution, with emphasis on regulatory modernization (30%) and international cooperation (20%), while Europol (2024) prioritizes criminal trend analysis and operational cases.

4.2 Convergence and Divergence Patterns

The analysis identified common and divergent elements in jurisdictional approaches to combating crypto-cybercrime. Table 4 synthesizes the main challenges identified by each jurisdiction.

Table 4. Key Challenges Identified by Jurisdiction

Challenge Category	Europol (2024)	NCA (2025)	US Tresury (2024)	MAS (2024)
Anonymity/Privacy	High	Medium	High	High
Transaction Speed	Medium	Low	High	High
Cross-border Nature	High	High	High	High
Regulatory Gaps	Medium	High	High	Medium
Technology Evolution	Medium	High	High	Low
Volume Estimation	High	High	Medium	Not Mentioned

Legend: High = Major focus/concern | Medium = Moderate attention | Low = Limited Discussion | Not mentioned = absent from document.

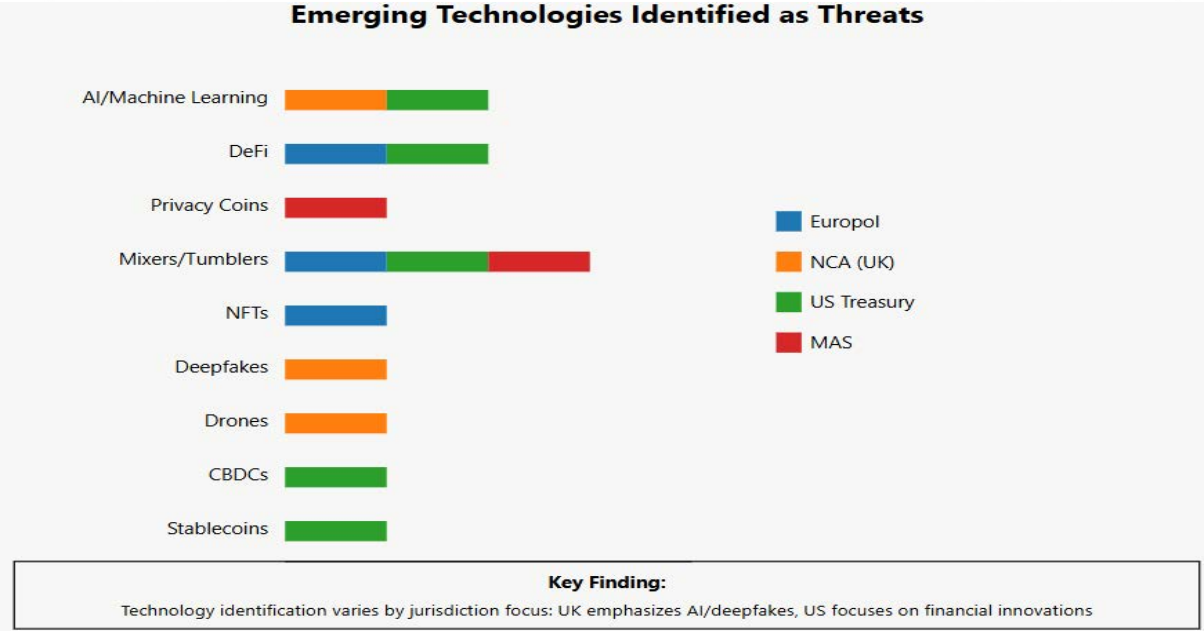
Source: Author's elaboration (2025)

The cross-border nature of transactions emerges as universal consensus, identified as the principal challenge by all jurisdictions. However, significant divergences appear in the prioritization of other challenges: while the USA (US Treasury, 2024) and Singapore (MAS, 2024) emphasize transaction speed as a critical obstacle to enforcement, the United Kingdom (NCA, 2025) dedicates greater attention to technological evolution and regulatory gaps.

4.3 Common Challenges and Differentiated Responses

The analysis reveals that although jurisdictions face similar challenges, their responses vary significantly. Figure 3 illustrates the intensity of focus on different enforcement mechanisms.

Figure 3. Emerging Technologies Identified as Threats



Source: Author's elaboration (2025)

The United States (US Treasury, 2024) demonstrates the most comprehensive approach, with strong emphasis on regulatory updates, sanctions, and asset recovery. Singapore (MAS, 2024) concentrates efforts on regulatory frameworks and rigorous KYC/AML requirements, while the United Kingdom (NCA, 2025) balances operational enforcement with technological innovation. Europol (2024), limited by its regional mandate, focuses primarily on operational coordination and intelligence analysis.

4.4 International Cooperation Mechanisms

International cooperation emerges as an area of significant divergence between jurisdictions. Table 5 maps the international organizations and cooperation mechanisms mentioned in each document.

Table 5. International Cooperation Mechanism by Jurisdiction

Organization/Mechanism	Europol (2024)	NCA (2025)	US Tresury (2024)	MAS (2024)
FATF	Not Mentioned	Not Mentioned	Extensive	Extensive
Interpol	Not Mentioned	Limited	Via FATF	Not Mentioned
Bilateral Agreements	Operational	Multiple	Extensive	RFAs Mentioned
G7 / G20	Not Mentioned	Not Mentioned	Active	Not Mentioned
UN Security Council	Not Mentioned	Not Mentioned	Referenced	Sanctions
Regional Bodies	EU framework	Post-Brexit	FSRBs	FSRBs
Task Forces	Operational	CRONOS	REPO	Not Mentioned

Legend: Extensive = Major focus with detailed discussion | Limited =Briefly Mentioned | Not mentioned = absent from document.

Source: Author's elaboration (2025)

The analysis reveals significant fragmentation in international cooperation mechanisms. The United States (US Treasury, 2024) and Singapore (MAS, 2024) demonstrate strong alignment with FATF frameworks, while operational documents (Europol, 2024; NCA, 2025) focus primarily on bilateral cooperation and specific task forces. This divergence suggests disconnection between strategic and operational levels of international cooperation.

4.5 Summary of Main Findings

The comparative analysis reveals three fundamental patterns in jurisdictional responses to the crypto-cybercrime nexus:

Despite universal recognition of cross-border nature as the principal challenge, jurisdictions diverge substantially in operational priorities and response mechanisms. This fragmentation is particularly evident in the identification of emerging technologies and implementation of international cooperation frameworks.

Each jurisdiction has developed distinctive competencies aligned with their institutional priorities - Singapore with preventive regulatory frameworks, United Kingdom with operational response and intelligence, United States with regulatory modernization and sanctions, and Europol with regional coordination and trend analysis.

The absence of FATF mentions in operational documents (Europol, NCA) versus their centrality in strategic documents (US Treasury, MAS) suggests disconnection between governance levels. Similarly, variation in identifying malicious actors - from specific criminal groups by nationality (NCA) to emphasis on state actors (US Treasury) - indicates lack of common taxonomy for threats.

These results evidence that although the crypto-cybercrime problem is globally recognized, responses remain fragmented and potentially inadequate to face threats that operate without jurisdictional restrictions. The next section will discuss the implications of these findings for international cooperation and public policy development.

Conclusion

The study identified three fundamental patterns: First, jurisdictions have developed distinct specializations aligned with institutional priorities - Singapore emphasizes preventive regulatory frameworks, the UK focuses on operational intelligence, the US prioritizes regulatory modernization with sanctions, and Europol concentrates on regional coordination. Second, significant fragmentation exists in international cooperation, with strategic documents (US, Singapore) aligning with FATF frameworks while operational documents (Europol, UK) focus on bilateral cooperation, suggesting disconnection between governance levels. Third, jurisdictions show varying capacity to identify emerging technological threats, indicating absence of common threat assessment frameworks.

This research faced important limitations including differential document availability across jurisdictions, under-representation of Global South perspectives, and focus on English-language sources. Documentary analysis captures only formally expressed policies rather than practical implementation or effectiveness. Future research should complement this analysis with empirical studies examining policy implementation and real-world outcomes.

Despite limitations, this research provides valuable insights for practitioners. Small and medium-sized jurisdictions can adapt proven approaches identified here, such as Singapore's compliance frameworks or the UK's intelligence-driven enforcement. Law enforcement agencies can benefit from understanding jurisdictional differences in crime categorization to improve information sharing.

The normative implications of these divergences extend beyond technical regulatory challenges. The fragmentation in responses reflects deeper disputes about digital sovereignty, state authority in decentralized systems, and balance between innovation and security. The increasing sophistication of state-sponsored cybercrime and emergence of "cyber mercenaries" challenges traditional distinctions between criminal and national security threats, requiring new frameworks for international cooperation transcending conventional law enforcement paradigms. The rapid evolution of technologies like privacy coins, decentralized finance protocols, and potential CBDCs demands adaptive regulatory approaches capable of responding to innovation while maintaining security imperatives.

Future research should focus on empirical implementation studies examining how policies translate into operational outcomes, longitudinal analysis of regulatory evolution tracking adaptation to emerging threats, and expanded geographical coverage incorporating Global South perspectives currently underrepresented in scholarly literature. Quantitative effectiveness assessments measuring actual impact of different regulatory approaches on crime reduction would provide crucial evidence for policy optimization. The crypto-cybercrime nexus represents a defining challenge for global governance in the digital age, requiring innovative coordination mechanisms transcending traditional territorial sovereignty while respecting legitimate concerns about digital autonomy and innovation.

References

ALBRECHT, Chad; DUFFIN, Kristopher; ALBRECHT, Conan; ROCHA, Victor Morales. The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, v. 22, n. 2, p. 210-216, 2019. DOI: 10.1108/JMLC-12-2017-0074.

ANTONOPOULOS, A. M. *Mastering Bitcoin: Programming the Open Blockchain*. 2. ed. Sebastopol: O'Reilly Media, 2017.

AUGUST, T.; ZHANG, M.; CHEN, Z. The impact of cryptocurrency on cybersecurity. *Management Science*, v. 71, n. 3, p. 1282-1299, 2025. DOI: 10.1287/mnsc.2023.00969.

AUER, Raphael; BÖHME, Rainer. The technology of retail central bank digital currency. *BIS Quarterly Review*, 1 mar. 2020. Disponível em: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

BA, H.; ŞEN, Ö. F. Explaining variation in national cryptocurrency regulation: implications for the global political economy. *Review of International Political Economy*, v. 31, n. 5, p. 1-25, 2024. DOI: 10.1080/09692290.2024.2325403

BARRATT, M. J.; ALDRIDGE, J. Everything you always wanted to know about drug cryptomarkets (*but were afraid to ask). *International Journal of Drug Policy*, v. 35, p. 1-6, 2016. DOI: 10.1016/j.drugpo.2016.07.005

BOWEN, G. A. Document analysis as a qualitative research method. *Qualitative Research Journal*, v. 9, n. 2, p. 27-40, 2009. DOI: 10.3316/QRJ0902027

BRASIL. Lei nº 14.478, de 21 dez. 2022. Dispõe sobre o marco legal dos ativos virtuais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14478.htm.

BUCHANAN, B. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University Press, 2017.

CARDNO, Carol. Policy document analysis: a practical educational leadership tool and a qualitative research method. *Educational Administration: Theory and Practice*, v. 24, n. 4, p. 623-640, 2018. Disponível em: https://files.eric.ed.gov/fulltext/EJ1305631.pdf.

CHAINALYSIS. *2025 Crypto Crime Report*. New York: Chainalysis Inc., 2025.

CHOUCRI, N.; ANAYA, J. CyberIR@MIT: Exploration and Innovation in International Relations 2.0. *MIT Political Science Department Research Paper* 2024-4, 2024. DOI: 10.2139/ssrn.3936863

CHRISTIN, N. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In: *Proceedings of the 22nd International Conference on World Wide Web*. Rio de Janeiro: ACM, 2013. p. 213-224.

CLARKE, R. V.; FELSON, M. (Ed.). *Routine Activity and Rational Choice*. New Brunswick: Transaction Publishers, 1993.

COHEN, L. E.; FELSON, M. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, v. 44, n. 4, p. 588-608, 1979. DOI:10.2307/2094589

COLEBATCH, H. K. *Policy*. 3. ed. Maidenhead: Open University Press, 2009 [1. ed. 1997].

CONTI, M.; GANGWAL, A.; RUJ, S. On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security*, v. 79, p. 162-189, 2018. DOI: 10.1016/j.cose.2018.08.008.

DEIBERT, R. Three painful truths about social media. *Journal of Democracy*, v. 30, n. 4, p. 77-90, 2019 Disponível em: https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/

FANUSIE, Y.; ROBINSON, T. *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Washington: Center on Sanctions and Illicit Finance, 2018.

FARBER, S. The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *SSRN Electronic Journal*, 2025. Disponível em: http://dx.doi.org/10.2139/ssrn.5228798

FATF – Financial Action Task Force. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF/OECD, 2019.

FOLEY, S.; KARLSEN, J. R.; PUTNIŅŠ, T. J. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, v. 32, n. 5, p. 1798-1853, 2019. Disponível em: http://dx.doi.org/10.2139/ssrn.3102645

GALASSO, J. The crypto revolution: A comparative analysis of crypto regulation in the United States and the European Union. *Touro Law Review*, v. 39, n. 4, p. 1-45, 2024. Disponível em: https://digitalcommons.tourolaw.edu/lawreview/vol39/iss4/12

HOUBEN, R.; SNYERS, A. *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. Bruxelas: European Parliament, 2018. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)619024.

HU, J. The regulation of cryptocurrency in China. *International Journal of Digital Law and Governance*, v. 1, 2024.

HUGHES, S. J.; MIDDLEBROOK, S. T. Advancing a framework for regulating cryptocurrency payments intermediaries. *Yale Journal on Regulation*, v. 32, n. 2, p. 495-559, 2015. Disponível em: https://www.cs.yale.edu/homes/jf/Hughes.pdf

IRWIN, A. S. M.; MILAD, G. The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, v. 19, n. 4, p. 407-425, 2016. DOI: 10.1108/JMLC-01-2016-0003

KEOHANE, R. O.; NYE, J. S. *Power and Interdependence*. 4. ed. Boston: Longman, 2011.

MAURER, T. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

MCGUIRE, M.; DOWLING, S. *Cyber crime: A review of the evidence*. Londres: Home Office, 2013. (Research Report 75).

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.

O'LEARY, Z. *The essential guide to doing your research project*. 2. ed. Londres: SAGE Publications, 2014.

OLADIPUPO, O. Sanctions evasion 2.0: unpacking the role of cryptocurrency in North Korea and Iran's external trade relations. *Lead City Journal of the Social Sciences*, v. 10, n. 1, 2025. Disponível em: https://www.researchgate.net/publication/392312032_Sanctions_Evasion_20_Unpacking_the_Role_of_Cryptocurrency_in_North_Korea_and_Iran's_External_Trade_Relations.

PRIOR, Lindsay. *Using documents in social research*. Londres: SAGE Publications, 2003.

RID, T.; BUCHANAN, B. Attributing cyber attacks. *Journal of Strategic Studies*, v. 38, n. 1-2, p. 4-37, 2015.DOI: 10.1080/01402390.2014.977382.

RIHOUX, B.; RAGIN, C. C. (Ed.). *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques*. Thousand Oaks: SAGE Publications, 2009. DOI: 10.4135/9781452226569.

ROSENAU, James N. *Along the domestic-foreign frontier: exploring governance in a turbulent world*. Cambridge: Cambridge University Press, 1997. DOI: 10.2307/2585471.

SCHREIER, M. *Qualitative content analysis in practice*. Londres: SAGE Publications, 2012.

WALL, D. S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007.

WALTZ, Kenneth N. *Theory of international politics*. Reading, MA: Addison-Wesley, 1979.

WENDT, A. (2000). *A Social Theory of International Politics*. Social Theory of International Politics. 26. DOI 10.1017/CBO9780511612183

WORLD BANK. *Cryptocurrencies and Blockchain: Policy Objectives and Regulatory Approaches*. Washington: World Bank Group, 2018.

YANOW, Dvora. Qualitative-interpretive methods in policy research. In: FISCHER, Frank; MILLER, Gerald J.; SIDNEY, Mara S. (Ed.). *Handbook of public policy analysis: theory, politics, and methods*. Boca Raton: CRC Press, 2007. p. 405-415.

ZETZSCHE, D. A.; ARNER, D. W.; BUCKLEY, R. P.; WEBER, R. H. The Markets in Crypto-Assets regulation (MICA) and the EU digital finance strategy. *Capital Markets Law Journal*, v. 15, n. 2, p. 203-225, 2020. Disponível em: http://dx.doi.org/10.2139/ssrn.3725395

JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

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

CSPP ENTREVISTA

O BRASIL PODE SER POTÊNCIA EM CIBERSEGURANÇA MAS O TEMPO ESTÁ ACABANDO

ENTREVISTADO

Dr. Marcelo Antonio Osller Malagutti

Assessor Especial do Gabinete de Segurança Institucional (GSI) da Presidência da República e Secretário-Executivo do Comitê Nacional de Cibersegurança (CNCiber).

"Fale sobre o papel do Brasil no cenário global de cibersegurança"

CSPP O senhor possui uma formação acadêmica diversificada, com passagens, entre outros, pelo King's College London e Escola de Comando e Estado Maior do Exército (ECEME). Como essa combinação de experiências acadêmicas moldou sua visão sobre cibersegurança e defesa nacional? E, como sua experiência no setor privado influenciou sua abordagem atual em políticas públicas de cibersegurança?

M *Costumo considerar que boa parcela daquilo que somos é resultado de nossas experiências. Em outras palavras, nossas vivências prévias moldam em grande medida a forma como enxergamos o mundo. Afinal, como diz a "lei do instrumento" de Abraham Maslow, "se a única ferramenta que você tem é um martelo, todos os problemas começam a se parecer com pregos". Assim, ter uma* ***experiência variada*** *permite o entendimento de percepções diferentes, o que facilita a construção de consensos. Então não são apenas minhas experiências acadêmicas que moldam minha atuação, mas a soma delas com minha experiência nos setores privado e público. Aliás, me orgulho de ter atuado nos três elementos que constituem a chamada Tríplice Hélice do conhecimento e da inovação – universidade, indústria e governo.*

M *Somo a isso a* ***oportunidade de conhecer diferentes realidades*** *de outros países, ao longo da minha trajetória. O conjunto de vivências me conferiu uma percepção ampliada das demandas de cibersegurança, desde as necessidades práticas do mercado, conceituais da academia até a política da gestão pública, o que, hoje, contribui para um mapeamento mais eficiente das dificuldades e para o fornecimento de respostas mais factíveis e aprimoradas aos problemas.*

Linha DO TEMPO

Anos 1990-2000
Atuação no setor bancário por cerca de 30 anos, desenvolvendo soluções de segurança digital e automação.

2009
Conclui MBA em Estratégia Empresarial e apresenta propostas para fortalecer a indústria brasileira de software.

2010
Curso de Altos Estudos na ESG; caso Stuxnet desperta atenção para riscos cibernéticos no Brasil.

CSPP O que o motivou a dedicar sua carreira à cibersegurança e à defesa nacional?

M *Dediquei aproximadamente trinta anos ao desenvolvimento de tecnologia de automação bancária, onde a confidencialidade, integridade, autenticidade e disponibilidade de informações são fatores essenciais, desde muito antes da existência da série ISO 27000 ou da Lei Geral de Proteção de Dados Pessoais (LGPD), por exemplo. Nesse ambiente, sempre enfrentamos oponentes tecnicamente capazes e motivados, o que nos obrigava a atuar com foco na prevenção e na construção de soluções seguras. Paralelamente, lidei com iniciativas para o fortalecimento da indústria nacional e da qualidade do software.*

M *Tem ainda a famosa frase de John F. Kennedy (1961): "Não pergunte o que o seu país pode fazer por você, mas o que você pode fazer pelo seu país", que reflete um tanto de minha personalidade e da minha cultura familiar. Em 2009, pouco após a conclusão do MBA em Estratégia Empresarial com um trabalho final em que apresentei propostas para uma estratégia de desenvolvimento para a indústria brasileira de software, fui convidado a participar do Curso de Altos Estudos de Política e Estratégia, na Escola Superior de Guerra (ESG), em 2010. Aquele foi o ano do* ***Stuxnet,*** *e foi muito fácil perceber que se um malware semelhante tivesse como alvo o Brasil teria sido desastroso.* ***Não estávamos minimamente preparados para esse novo contexto****. Aprofundei, então, meus estudos sobre a cibersegurança e a sua relação com a defesa e a segurança nacionais, propondo ações que poderiam ser adotadas pelo Brasil. Em 2011, soube que algumas das propostas haviam sido efetivadas.*

M *Em 2013, o ano do Caso Snowden, fui condecorado pelo Ministério da Defesa com a Medalha do Pacificador e retornei para o meio acadêmico, sendo aceito no prestigioso Departamento de Estudos de Guerra do King´s College London para realização do mestrado, iniciado em 2015. Desse ponto foi um passo natural voltar ao Brasil e ingressar no recém-criado doutorado em Ciências Militares do Instituo Meira Mattos (IMM) da ECEME, tal e qual foi me aproximar do Comando de Defesa Cibernética, em particular, no Exercício Guardião Cibernético, o qual realiza, em 2025, sua 7ª edição.*

2011
Algumas de suas propostas são adotadas pelo governo.

2013
Recebe a Medalha do Pacificador do Ministério da Defesa.

2015
Inicia mestrado no King's College London, onde cria o conceito de "Software Power".

2016-2018
Faz doutorado na ECEME; aprofunda estudos em cibersegurança e atua no Comando de Defesa Cibernética.

2019
Integra o GSI e passa a liderar a Política Nacional de Cibersegurança (PNCiber) e o CNCiber.

2021/2022
Ganha o Prêmio Tiradentes por sua tese de doutorado.

2023
Assinatura da PNCiber; consolidação da agenda nacional de cibersegurança.

2025
Atua na criação da Agência Nacional de Cibersegurança (ANCiber) e coordena o 7º Exercício Guardião Cibernético.

"ME ORGULHO DE TER ATUADO NOS TRÊS ELEMENTOS DA TRÍPLICE HÉLICE UNIVERSIDADE, INDÚSTRIA E GOVERNO."

M *Desde então trabalhar para o GSI, na criação da Política Nacional de Cibersegurança (PNCiber), na criação e na secretaria-executiva do Comitê Nacional de Cibersegurança (CNCiber) e na articulação pela criação de uma Agência ou Autoridade Nacional de Cibersegurança (ANCiber), ainda em processo de discussão interna ao governo, e sobre a qual falaremos mais adiante, foram evoluções naturais.*

"Fale mais sobre qual será o papel da ANCiber"

CSPP O senhor aborda o conceito de "Software Power" como ferramenta de ciberdissuasão. Como essa ideia pode ser aplicada na prática pelas políticas públicas brasileiras?

"O CONJUNTO DE VIVÊNCIAS ME CONFERIU UMA PERCEPÇÃO AMPLIADA DAS DEMANDAS DE CIBERSEGURANÇA."

M *O conceito de Software Power surge no mestrado, quando em minha dissertação faço uma "brincadeira", isto é, um paralelo, com os conceitos de hard power e soft power do Joseph Nye, criando o conceito de* ***Software Power*** *como um potencial relevante para o Brasil. O conceito advinha da percepção de que* ***o Brasil perdera o timing de sua inserção no mercado de desenvolvimento de hardware****, mas que ainda seria possível "pegar o trem" do desenvolvimento de software de cibersegurança e ciberdefesa, aproveitando-se de um conjunto de características do institucionalismo brasileiro.*

M *No doutorado investi energia no aprofundamento da ideia e, essencialmente, defendo que o jogo de forças e interesses geopolíticos faz com que todo mundo desconfie dos interesses dos outros países. Logo, uns não vendem certas coisas para outros, com medo de serem atacados ou de que usem o know-how para desenvolvimento de novas armas. De outra parte, uns não compram certas coisas de outros, com medo de que existam backdoors ou outras vulnerabilidades que possam ser exploradas contra eles.* ***Considerando que o Brasil historicamente não é belicoso, beligerante, poderia vender ciberarmas defensivas, e os lucrativos serviços a elas associados, com mais facilidades, pois ninguém se sentiria ameaçado pelo Brasil****.*

*O Brasil, menos beligerante que outras potências do mesmo porte, poderia se valer de três das seis formas de dissuasão que identifico****[1]****, e se aproveitar da sua pujante indústria de software para desenvolver uma* ***indústria capaz*** *não apenas de proteger nossa soberania e interesses no campo cibernético, como também reduzir os prejuízos causados a nossa economia e sociedade pelos ciberataques, além de abrir*

GLOSSÁRIO

ANCiber (Agência Nacional de Cibersegurança)
Órgão proposto para regular e coordenar a cibersegurança no Brasil.

APTs (Ameaças Persistentes Avançadas)
Ataques digitais sofisticados e patrocinados por Estados, que invadem redes críticas de forma silenciosa.

Backdoor
Brecha proposital ou acidental que permite acesso secreto a sistemas.

Ciberdissuasão
Estratégia para desencorajar ataques aumentando custos e riscos para invasores.

CNCiber (Comitê Nacional de Cibersegurança)
Grupo que reúne governo, setor privado e sociedade civil para definir políticas nacionais de cibersegurança.

CTIR Gov (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo)
Unidade do GSI que monitora e reage a ataques cibernéticos no setor público.

*um gigantesco mercado nacional e internacional de produtos e serviços em cibersegurança. **Um ótimo negócio, do ponto de vista estratégico, econômico e social.** Foi motivo de orgulho ser premiado no concurso de teses de doutorado em defesa nacional, o Prêmio Tiradentes, no biênio 2021/2022.*

Hoje, com informações e conhecimentos mais recentes, estou muito mais convicto das ideias que desenvolvi na tese, e de sua aplicabilidade ao Brasil, não apenas para minimizar riscos, mas fundamentalmente para gerar emprego e renda e inserir o País numa importante frente tecnológica global.

CSPP Quais são os principais desafios para implementar uma estratégia eficaz de ciberdissuasão no contexto brasileiro?

M *Minha pesquisa, e minha experiência, ao longo dos anos, mostraram que **algumas das nossas dificuldades advém justamente do nosso institucionalismo histórico**. A nossa certeza de que "Deus é brasileiro" nos faz achar que nada de mal nos acontecerá. Nossa confiança no "jeitinho brasileiro" nos faz acreditar que, numa eventual crise, vamos ter uma forma criativa de nos safarmos. Somos um país que encara com naturalidade a ideia de "leis que pegam e leis que não pegam". E a maioria dos brasileiros tem certeza de que, como não somos beligerantes, ninguém jamais nos atacará. Ainda, temos uma tradição de evitar o empoderamento do Estado, por medo de sua atuação contra o indivíduo, de sorte que evitamos ações como o fortalecimento de capacidades militares e de inteligência, consideradas normais às potências médias e grandes pelo mundo. Então, eliminamos, culturalmente, várias das formas de dissuasão. Kissinger, um dos expoentes do realismo nas Relações Internacionais, teria dito que "diplomacia sem recursos de poder é um mero exercício de retórica". Isto posto, nações com uma cultura pautada pelo Realismo não considerariam seriamente uma ameaça nossa.*

E-Ciber (Estratégia Nacional de Cibersegurança)
Documento com diretrizes e metas para fortalecer a proteção digital do Brasil.

Edge Computing (Computação de Borda)
Processamento de dados próximo à origem, permitindo respostas mais rápidas e seguras.

ISACs (Information Sharing and Analysis Centers)
"Cooperativas" de empresas para compartilhar informações sobre ataques e defesas.

LLMs (Large Language Models)
Modelos de IA, como ChatGPT, que geram textos e são explorados por hackers para ataques mais sofisticados.

M *Dessa forma, sobram poucas alternativas para exercermos capacidades dissuasórias. Uma delas é a "**dissuasão pela negação**", elevando nossas capacidades defensivas para "negar ao oponente" um acesso fácil aos seus objetivos. Essencialmente, teríamos que "subir a barra" das defesas, subindo os custos e o risco de exposição do ataque e do atacante para superá-las, tornando a relação do custo/benefício do objetivo menos atrativa. Outra, bastante associada à primeira, consiste em capacidades de investigação e atribuição melhores,*

ReGIC / ReNGIC (Rede de Gestão de Incidentes Cibernéticos)
Sistema colaborativo de análise e resposta a ciberataques no Brasil.

de forma a permitir a dissuasão por individualização". Ao invés de acusarmos um país, o que não é do nosso perfil e tradição diplomática, acusaríamos um cidadão específico, denunciando-o em tribunais e, numa eventual condenação, acionaríamos ***sanções internacionais*** *- um instrumento a que EUA, Reino Unido, França, Alemanha, entre outros, têm recorrido cada vez mais. Essas capacidades defensivas e investigativas, também, permitem até um tipo de retaliação (elemento de deterrência ou dissuasão por ameaças), do tipo que cria constrangimentos, públicos ou mesmo privados.* ***Não são muitas as opções, mas temos algumas.***

CSPP Na sua visão, quais são as principais ameaças cibernéticas que o Brasil enfrenta atualmente?

M *Temos várias! No campo das ciberameaças* ***o ransomware é uma praga que nos assola****. Cresce muito o número de casos, o número de setores vitimados, e o número de gangues que nos atacam ano a ano. Vazamentos de dados, frequentemente associados ao ransomware, também crescem muito. São dezenas de milhares de casos aqui, centenas de milhares ali, e nunca para. Outro problema é a* ***proliferação de APTs*** *(as ameaças persistentes avançadas) que andam bisbilhotando nossas redes, em particular aquelas de provedores de serviços essenciais e de operadores de infraestruturas críticas. APTs atuam patrocinadas por Estados. Então não é uma questão exclusivamente de criminalidade, mas ter agentes a serviço de outro Estado Nacional dentro de nossas redes não é bom. Aliás, lá por meados dos anos 2010, um então comandante do USCyberCom disse algo mais ou menos como* ***"nada de bom pode vir de alguém bisbilhotando nossas redes".*** *Esse conceito ainda é 100% atual.*

Ransomware
Malware que sequestra dados e exige pagamento para liberá-los.
Software Power
Conceito criado por Malagutti: usar a força da indústria de software brasileira para proteger o país e gerar negócios.

Stuxnet
Malware famoso de 2010 que sabotou o programa nuclear do Irã; citado como marco global da cibersegurança.

M *Acredito que nossa principal ameaça não é o malware, e não vem de fora. É a nossa* ***falta de cultura de cibersegurança e segurança da informação****. Demora-se a convencer um decisor, público ou privado, de que cibersegurança é investimento, e não despesa; ou de que ela pode ser uma questão existencial para uma instituição. Isso dificulta muito as coisas. Num recente artigo intitulado "Cibersegurança: O Custo de Não Fazer"* ***[2]*** *eu e meu colega do CNCiber Rony Vainzof apontamos argumentos para mostrar que investir na governança nacional da cibersegurança é um ótimo investimento para sociedade e governo. Todo mundo sempre soube que o número de ataques ao setor Financeiro era grande, bem como aos setores Governo e Justiça. Mas setores*

"FOI MUITO FÁCIL PERCEBER QUE, SE UM MALWARE COMO O STUXNET TIVESSE COMO ALVO O BRASIL, SERIA DESASTROSO."

que sempre se sentiram poucos atrativos agora disputam, e até superam, aqueles, como Saúde, Varejo, e Manufatura, dentre outros tantos. Ninguém está imune! ***Não se trata mais de "SE alguém vai ser atacado, mas de QUANDO".*** *E a questão que trabalhamos agora é:* ***COMO responderemos****. A resiliência - capacidade de seguir operando, ainda que de forma limitada, evitando uma total disruptura das operações - é fundamental no contexto de Serviços Essenciais.*

"EM 2011, SOUBE QUE ALGUMAS DAS PROPOSTAS HAVIAM SIDO EFETIVADAS."

M *Uma outra questão é que o Brasil tem diversas ilhas de excelência em cibersegurança. Mas elas são pequenas. Muito pequenas! Razão pela qual costumo dizer que temos uma "****micronésia de ilhas de excelência****" no tema, como alguns setores do GSI, CERT.Br, RNP, ANATEL e Banco Central, MGI e SERPRO, Polícia Federal e algumas polícias estaduais, para citar algumas. E que produzem dezenas de boas iniciativas isoladas. Mas nos falta capacidade de coordenação e de multiplicação dos resultados.* ***Precisamos com urgência de uma ANCiber, uma entidade especializada, tecnicamente qualificada, de natureza permanente*** *(de Estado),* ***de abrangência nacional*** *(três poderes, União, estados e municípios, iniciativa privada),* ***e civil*** *(mas com boa interação com a ciberdefesa, que toca aos militares e na qual, a despeito de recursos limitadíssimos, fazem um trabalho de excelência), para regular, fiscalizar, coordenar e controlar a cibersegurança nacional. Quando começamos o processo, há pouco mais de dois anos, diziam que seria impossível. Hoje não acho mais apenas possível, mas provável, termos isso, e sinto que não vai demorar muito mais. Em termos de "tempo de Estado", digo.*

ANCiber

"O BRASIL PERDEU O 'TIMING' DO HARDWARE, MAS AINDA PODE PEGAR O TREM DO SOFTWARE."

"Cite algumas das ilhas de excelência para o conhecimento dos leitores."

CSPP Como o país pode equilibrar a necessidade de segurança cibernética com a proteção das liberdades individuais e da privacidade dos cidadãos?

M ***Essa é sempre a questão fundamental a ser debatida****. Diz um ditado popular que "a virtude está no meio". Há que sempre haver um equilíbrio. Uma das funções precípuas do Estado é garantir a liberdade do cidadão. Outra é garantir a segurança desse mesmo cidadão. Thomas Hobbes nos ensinou que o preço da segurança é ceder uma parte de nossa liberdade. Se todo mundo faz o que quer, com total liberdade, não há segurança. E John Philpot Curran estabeleceu que o preço da liberdade é a eterna vigilância. Quem estabelece os limites*

dessas coisas é a lei. E para garantir a lei o Estado precisa ter força. Sem a presença do Estado não há a aplicação da lei. E um dos princípios da soberania de um Estado é a sua capacidade de aplicar a lei. Tudo somado, temos que ter um Estado forte, soberano e vigilante, para fazer valer a lei estipulada livremente por seu povo, assegurando a esse povo liberdade e segurança, inclusive contra excessos desse mesmo Estado. Isso só se consegue com um debate franco, aberto, e com base em princípios e conceitos claros. Fácil, não é?

"O BRASIL PODE VENDER CIBERARMAS DEFENSIVAS SEM AMEAÇAR NINGUÉM."

M *Fácil não é! Mas Einstein dizia que "Tudo deve ser feito o mais simples possível, mas não mais simples do que isso". Então, devemos simplificar as coisas tanto quanto possível, mas sem que essa simplificação as tornem irrelevantes nem incompreensíveis. Vamos exemplificar com um dos problemas da cibersegurança, que é a mistura de conceitos. Por exemplo, algumas pessoas associam a cibersegurança com o controle de conteúdo de plataformas digitais. Mas, são coisas muito diferentes.*

"A INDÚSTRIA DE SOFTWARE É UMA OPORTUNIDADE ESTRATÉGICA, ECONÔMICA E SOCIAL."

A cibersegurança, essencialmente, consiste na garantia da Confidencialidade, da Integridade, da Autenticidade e Disponibilidade (resumidas no acrônimo CIAD) da informação processada, transmitida ou armazenada em ciberativos (hardware, software ou dados). *Mas a cibersegurança não se ocupa do conteúdo dessa informação (ou desinformação). Então, temos que pensar em como uma determinada informação será acessada apenas por quem de direito (confidencialidade), que ela vem de quem deveria vir (autenticidade), que ela não foi adulterada no processamento ou transporte (integridade), e que ela esteja disponível quando e onde necessária (disponibilidade). Logo, em nenhum momento o conteúdo dela é relevante do ponto de vista da cibersegurança. O conteúdo pode vir a ser um caso de calúnia ou difamação, ou de apologia ao crime, ou de outros ilícitos penais. E como tal deve ser tratado, por quem de direito. Mas isso, reitero, não é uma questão de cibersegurança. Similarmente, se algum algoritmo impulsiona artificialmente determinado tipo de mensagem, com base em seu conteúdo, e isso beneficia ou prejudica alguém de forma indevida, isso também não é uma questão de cibersegurança.*

"A NOSSA CERTEZA DE QUE 'DEUS É BRASILEIRO' NOS FAZ ACHAR QUE NADA DE MAL NOS ACONTECERÁ."

Se uma pessoa cai num golpe a partir de uma mensagem recebida numa rede social, e entra voluntariamente na sua conta bancária e envia dinheiro para o fraudador, há que se separar o problema em suas componentes. Um golpe é uma fraude, que é crime. Mas, seria também se o usuário caísse

na conversa de alguém na porta de uma agência bancária, entrasse, sacasse dinheiro, e desse para o criminoso em troca de um "bilhete premiado de loteria". Não se trata de uma questão de cibersegurança. Mas se alguém envia uma mensagem com um malware que se instala em seu celular, e depois rouba os dados de acesso ao seu banco, isso é um problema de cibersegurança.

"SOMOS UM PAÍS QUE ENCARA COM NATURALIDADE A IDEIA DE 'LEIS QUE PEGAM E LEIS QUE NÃO PEGAM'."

M *Outra questão um tanto mal-entendida é a cibersegurança e o vazamento de dados. Há quem ache que a ANPD (Autoridade Nacional de Proteção de Dados) seria o bastante para garantir a cibersegurança nacional. Ledo engano! Costumo dizer que a cibersegurança é ex-ante, enquanto o vazamento de dados é ex-post. Ainda, o vazamento de dados pode ocorrer por meios físicos, não digitais. Então, é possível ocorrer um vazamento de dados sem um ciberincidente. Por exemplo, se alguém entra numa sala e rouba dados de uma pasta de documentos de um gaveteiro. Assim como, existem diversos ciberincidentes graves que não vazaram dados. Mais ainda, a ANPD trata de dados pessoais sensíveis. E há vazamento de dados que não envolvem dados pessoais, e muito menos ainda dados pessoais sensíveis. Exemplos são os vazamentos de dados de projetos industriais (a chamada espionagem industrial). Então,* ***não podemos achar que a cibersegurança se limita à proteção de dados pessoais.***

"KISSINGER DISSE: 'DIPLOMACIA SEM PODER É MERA RETÓRICA'."

Entendidos esses conceitos, fica mais fácil evoluirmos o debate sobre a necessidade de cibersegurança, e de como é possível fazermos isso sem avançarmos sobre os direitos individuais. Mas é preciso termos serenidade e honestidade intelectual nesse debate. E senso de urgência!

"NÃO SE TRATA MAIS DE 'SE' VAMOS SER ATACADOS, MAS DE 'QUANDO'."

Até agora, os exemplos que dei foram relativos ao cidadão comum, coisas que todos sofremos ou conhecemos alguém próximo que já sofreu. Mas a cibersegurança no Brasil vai muito além disso. Um ciberataque recentemente paralisou o INCA (Instituto Nacional do Câncer), impedindo a realização de cirurgias e tratamentos para pacientes em situações delicadas. Outro ciberincidente afetou as operações do IPEN (Instituto de Pesquisas Energéticas e Nucleares), paralisando a produção de radiofármacos por mais de duas semanas. E esses fármacos, por sua natureza de decaimento radiativo, têm ciclo de vida muitíssimo curto, sendo difícil sua importação. Logo, essa paralisação da produção prejudicou a realização, por exemplo, de exames de imagem com contraste, o tratamento de radioterapia, e provocou tantos outros problemas. Imagine-se o impacto da paralisação do sistema

elétrico, por exemplo. Ou do PIX. Ou da rede de telefonia. ***A prevenção desses incidentes envolvendo serviços essenciais e infraestruturas críticas, notadamente por causa cibernéticas, é uma questão de cibersegurança de enorme relevância. E deve ser uma questão de Estado, sem ideologia.*** *Não é de esquerda ou de direita. O governo trabalhista do Reino Unido está incrementando a já avançada (em relação à nossa) cibersegurança britânica. O governo conservador italiano também. Assim como o governo socialista de Portugal. Os EUA, a Rússia, a China, o Japão, a Coreia, a Alemanha, a França, a Austrália, o Canadá, o Uruguai, o Chile... Todos eles estão trabalhando forte para aumentarem o escopo de suas ações. E todos eles já têm suas "agências de cibersegurança", como são chamados esses órgãos no jargão da área, há alguns anos.* ***O Brasil está bastante atrasado nisso.*** *E, em parte, por causa da dificuldade de se discutir o tema com serenidade, por conta da mistura de assuntos que são muito mais polêmicos que a cibersegurança em si. Se a gente separar o debate, tenho convicção de que o tema da cibersegurança avança fácil.*

"TEMOS UMA MICRONÉSIA DE ILHAS DE EXCELÊNCIA EM CIBERSEGURANÇA."

CSPP A PNCiber foi assinada em fins de 2023, estabelecendo diretrizes estratégicas para a proteção dos ativos digitais do país. Na sua avaliação, quais são os principais desafios que o Brasil enfrenta atualmente para sua efetiva implementação?

M *A situação fiscal do país é complexa, e como eu disse muita gente pensa na criação de um órgão de governança como um custo, e não como um investimento. Avalio que a criação da PNCiber, e em seu bojo a do CNCiber, colocou na pauta nacional o tema da cibersegurança. O assunto foi amadurecendo, e foi ganhando mais e mais apoios. Estamos, hoje, em um contexto, no qual a sociedade civil, que tem uma representação importante no CNCiber, pede ativamente uma ação mais incisiva do Governo. O Legislativo, que criou uma Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética, também. As engrenagens se movimentam. Numa recente reunião do CNCiber houve um momento em que um representante do Governo comentou que, em 20 anos de vida pública, era a primeira vez que ele via a iniciativa privada pedir regulação. E um representante da Sociedade respondeu, com humor: "e gasto público"! Isso porque* ***a percepção já começa a mudar para a visão de que não é gasto, mas investimento.*** *E que os riscos de não ter regulação desse tema num país como o nosso já estão inaceitáveis. Acho, ou melhor, sinto, que estamos perto de grandes avanços.*

"PRECISAMOS DE UMA ENTIDADE ESPECIALIZADA, TÉCNICA, CIVIL, NACIONAL E PERMANENTE."

CSPP Considerando os avanços obtidos até agora, quais seriam, na sua visão, os próximos passos estratégicos para consolidar um ecossistema nacional de cibersegurança robusto, inclusivo e adaptado aos riscos emergentes?

M *Temos alguns passos essenciais iniciados. Primeiro, uma* ***atualização da nossa Estratégia Nacional de Cibersegurança****, a E-Ciber, que agora o decreto da E-Ciber foi assinado em 04/08/25 e publicado em 05/08/25. Segundo, a discussão de um Marco Legal da Cibersegurança e do Órgão de Governança da Cibersegurança. Quanto a esse, em minha visão pessoal, o melhor arranjo, considerando o institucionalismo histórico nacional, seria o de uma Agência Reguladora. Mas não creio que minha opinião deva ser um entrave no processo, motivo pelo qual acredito que um arranjo institucional como o do IBAMA ou INMETRO, autarquias reguladoras que não são agências reguladoras, pode funcionar também. Como diz a sabedoria popular, "o ótimo é inimigo do bom". E o bom seria muitíssimo melhor do que nada! Podemos avançar, aprender, desenvolver processos, conhecimento, normas, e depois evoluir institucionalmente, quando condições mais propícias se apresentarem. "Uma longa jornada começa com um primeiro passo", diz o provérbio chinês.*

"CIBERSEGURANÇA NÃO SE OCUPA DO CONTEÚDO DA INFORMAÇÃO."

M *No tocante aos riscos emergentes, temos uma questão muito importante a considerar, que são as chamadas Tecnologias Computacionais Emergentes, um conjunto de tecnologias computacionais que têm capacidades disruptivas e que certamente afetarão a cibersegurança da sociedade num tempo não muito distante.*

Todo mundo pensa logo em Inteligência Artificial (IA). Isso porque os Grandes Modelos de Linguagem (LLMs), estão em evidência para o grande público, e assim chamam a atenção da mídia e dos legisladores, por exemplo. ***Já temos muitos ciberincidentes envolvendo exploração de vulnerabilidades e phishing gerados por sistemas de IA baseados em LLMs recentemente, aumentando a velocidade e a precisão dos ataques****, e elevando a capacidade técnica de atacantes não muito qualificados. Mas a IA é muito mais que apenas os LLMs. Temos ainda em desenvolvimento a IA Geral, com a capacidade de compreender, aprender e realizar qualquer tarefa intelectual que um ser humano seja capaz de fazer, além apenas da linguagem. E a IA Física, a IA integrada a sensores, dispositivos, máquinas ou robôs que têm uma presença tangível no mundo real.*

"TEMOS QUE SEPARAR CIBERSEGURANÇA DE REGULAÇÃO DE CONTEÚDO."

"A CIBERSEGURANÇA É EX-ANTE. O VAZAMENTO DE DADOS É EX-POST."

Para além da IA, temos a materialização da promessa da Computação Quântica, que promete mudar a escala da capacidade computacional, trazendo o potencial de revolucionar diversas indústrias e resolver problemas considerados intratáveis pela computação clássica. *Um impacto direto desse aumento da capacidade computacional seria a capacidade de quebra dos algoritmos de criptografia hoje em uso, que levariam séculos de processamento com os atuais computadores para serem quebrados, em alguns minutos ou mesmo segundos. Por isso, há relatos de nações que estariam copiando gigantescas bases de dados criptografadas de outras nações, para decriptografá-las daqui a alguns anos e ter acesso aos dados que hoje estão protegidos. É claro que algumas informações, naquele momento, terão perdido seu valor. Mas, é fácil pensarmos em muitos dados que continuarão relevantes daqui a 20 anos. O combate a isso pode ser feito com o uso de algoritmos de criptografia quantum-resistant, comumente (e erroneamente) chamados de pós-quânticos.*

M *Outra tecnologia que preocupa no âmbito da cibersegurança são as redes de alta velocidade e baixa latência (5G e 6G, por exemplo), que permitiriam que volumes cada vez maiores de dados fossem exfiltrados (roubados) mais rapidamente, ou que microcâmeras e microfones, cada vez menores e com melhor definição, sejam implantados de forma a permitirem a captura de dados sensíveis.*

"O BRASIL ESTÁ ATRASADO. MAS HOJE NÃO ACHO MAIS APENAS POSSÍVEL – ACHO PROVÁVEL."

Exemplifiquei apenas algumas que já colocam problemas de segurança reais para os países, empresas e pessoas. Mas a lista não acaba aí. Temos um rol enorme, que inclui Computação de Alto Desempenho (HPC), Computação de Borda (Edge Computing), Computação em Nuvem, Computação Espacial, Computação Neuromórfica, Computação Verde, Computação Distribuída por Software, Biocomputação, Interfaces Neurais (BCI), Automação Robótica, Robótica Avançada, Robótica Colaborativa, Sistemas Autônomos, Veículos Autônomos, IoT Avançada, IoT Industrial, Manufatura Aditiva Avançada... Tem para todos os gostos! E desgostos, quando pensamos em termos de cibersegurança e segurança da informação.

E uma coisa interessante dessas tecnologias é que elas se realimentam. Umas potencializam, e amplificam o alcance e o risco, de outras. Tecnologias que pareciam dominadas, e com riscos controlados, passam a oferecer novos riscos. Posso citar como exemplos Big Data, Cidades Inteligentes (Smart Cities), Criptoativos, Energias Renováveis Inteligentes, Identidade Digital, Realidade Estendida (XR), Redes Inteligentes (Smart

Grids), e Tecnologias de Descentralização. Várias delas são potencializadas pelos sensores, elemento fundamental do IoT, e pela capacidade de processamento ampliada, oferecendo pontos de preocupação relevantes que precisam ser pensados, debatidos, e quase certamente, em alguma medida, regulados, fiscalizados e controlados. E isso tudo está aí, à nossa porta!

CSPP Como o Comitê Nacional de Cibersegurança está estruturado e qual é o papel das diferentes entidades governamentais e da sociedade civil nesse comitê?

M *Integram o CNCiber 13 entidades da administração federal direta (ministérios), 3 entidades da administração indireta (ANATEL, BACEN e CGI) e 9 representantes da sociedade, divididos em 3 grupos: 3 entidades de direito digital; 3 entidades de ciência, tecnologia e inovação; e 3 entidades representando o setor empresarial. Participam ainda, como convidados, e assim apenas com direito a voz, sem voto, a ABIN e o TCU.*

"ESSE DEBATE PRECISA DE SERENIDADE, HONESTIDADE INTELECTUAL E SENSO DE URGÊNCIA!"

O papel desse Comitê é o de formular propostas para a evolução da PNCiber, e por extensão do contexto da cibersegurança nacional. *A forma usual de trabalho é a criação de grupos de trabalho temáticos, os GTTs, que se debruçam sobre determinado tema por alguns meses, e elaboram propostas que depois são apreciadas pelo Pleno do CNCiber e, se aprovadas, encaminhadas para o Governo Federal. Essa estrutura assegura às discussões uma visão bastante plural dos temas discutidos. Todos os partícipes apresentam seus argumentos, e ouvem os argumentos dos demais. Na grande maioria dos casos os documentos produzidos são elaborados num processo colaborativo, em que cada termo é escolhido de forma consensuada. No próprio Pleno do CNCiber a enorme maioria das deliberações se resolve por unanimidade, depois de apresentados os argumentos de todos os interessados. Posso dizer que é um processo muito produtivo e muito rico.*

"A CIBERSEGURANÇA DEVE SER UMA QUESTÃO DE ESTADO, SEM IDEOLOGIA."

CSPP Qual é o papel do setor privado na construção de uma estratégia nacional de cibersegurança?

M *É um papel enorme, "gigante", como se diz popularmente! Diversas instituições apresentaram propostas de temas a serem tratados. Outras cobraram atenção a esse ou àquele tema. Tivemos dezenas de encontros, seminários, reuniões, visitas. E posso assegurar que vamos sair de uma E-Ciber de primeira geração para uma E-Ciber quase de terceira*

geração. Quase pelo fato de que não teremos como dar um "salto quântico" e pular todos os pontos das estratégias de segunda geração pelo atraso institucional que ainda temos em relação às nações mais avançadas no tema, várias das quais já foram citadas.

"INTELIGÊNCIA ARTIFICIAL, COMPUTAÇÃO QUÂNTICA E 6G TRAZEM RISCOS REAIS E IMINENTES."

E esse papel persiste nos demais temas. Nas audiências no Senado temos reiteradamente ouvido manifestações do Setor Privado em apoio às nossas iniciativas, e costumeiramente pedindo mais ações e celeridade. Essa cobrança permanente é um importante combustível para a ação da administração pública.

CSPP Como o governo federal tem trabalhado para fomentar parcerias com empresas e instituições acadêmicas nessa área?

M *Além dos representantes formalmente participando do CNCiber, temos instituições outras que interagem bastante conosco. No campo acadêmico posso exemplificar com a SBC (Sociedade Brasileira de Computação), que nos prestigia convidando a participar de seus eventos e discussões. No campo das empresas temos um bom exemplo com a FECOMÉRCIO-SP, que mantém contato permanente conosco. E há várias outras empresas, associações e congêneres participando ativamente, embora de forma indireta, dos debates. E apresentando ideias. Temos também nossos amigos do BID (Banco Interamericano de Desenvolvimento) que nos dão um suporte incrível, geram relatórios de altíssimo nível, com informações importantes, promovem eventos, entre outros instrumentos.*

"O ÓTIMO É INIMIGO DO BOM. PRECISAMOS AVANÇAR COM O QUE FOR POSSÍVEL."

M *Como o processo administrativo-burocrático-legal dos poderes Executivo e Legislativo é mais lento do que a capacidade de organização e inovação do setor privado e da academia, estamos tentando fomentar, por exemplo, a auto-organização do setor produtivo em arranjos de* ***Centros de Análise e Compartilhamento de Dados, internacionalmente conhecidos como ISACs, para a melhoria da proteção e resiliência contra ciberataques.*** *Basicamente, ao invés de cada instituição tentar se proteger sozinha, contratando profissionais que são raros e caros, elas se associam numa espécie de "cooperativa", em que os associados pagam uma taxa, e a "cooperativa" tem pessoal e recursos para receber, analisar e compartilhar dados com os cooperados. E essa cooperativa se associa a uma "federação de cooperativas", no caso a ReGIC (Rede Federal de Gestão de Incidentes Cibernéticos), mantida pelo Centro de Prevenção e Tratamento de Resposta a Incidentes*

Cibernéticos de Governo (CTIR Gov), localizado no GSI. Aliás, esperamos que em breve a ReGIC passe a ser uma ReNGIC (Rede Nacional, e não Federal) e que o CTIR Gov possa passar a ser o CTIR Br, ampliando sua abrangência para o âmbito nacional. E é bom esclarecer que o CTIR Gov também trabalha em cooperação com seus congêneres nacionais, o CERT.Br, ligado ao Comitê Gestor da Internet no Brasil, e o CAIS-RNP, que foca nas redes acadêmicas brasileiras. E também com seus similares internacionais. Portanto, expande-se a abrangência por meio de ***uma estrutura de "rede de redes" de análise e compartilhamento de informações de ameaças, permitindo que a identificação de um potencial problema seja transformada num alerta e em recomendações de como evitar ou interromper um ciberataque****.*

"A CIBERSEGURANÇA NÃO É COISA DE NERD DE TI. NÃO MESMO!"

CSPP Para os jovens profissionais interessados em seguir carreira na área de cibersegurança, que conselhos o senhor daria?

M ***Esse é um campo fantástico. Altamente promissor.*** *E que oferece, e demanda, muitas perspectivas de conhecimento distintas. Minhas duas filhas estão enveredando por esta área. Uma cursou Relações Internacionais, fez mestrado em Conflitos Internacionais (dissertação em cibersegurança) e MBA em cibersegurança. A outra graduou-se em Ciência da Computação e agora cursa um MBA em cibersegurança. As duas já me ajudaram na elaboração de material e na condução dos Exercícios Guardião Cibernético, e em vídeos sobre cibersegurança.*

"É UMA ÁREA ENORME, APAIXONANTE E EM EXPANSÃO. TEM LUGAR PARA TODOS."

M *Então, recomendo aos jovens, de todas as idades, que se interessem, que procurem identificar que tipo de conhecimento podem associar ao seu cabedal, ou background, para ingressarem na área.* ***Há fóruns, cursos e certificações gratuitos****, aos montes, na Internet, para os mais variados níveis de conhecimento. Leiam, pesquisem, atualizem-se. Vocês verão que é uma área enorme, e apaixonante. E é fácil perceber que não é só "coisa dos nerds de TI". Não mesmo*!

CSPP Nosso muito obrigado Dr. Marcelo A. O. Malagutti.

JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

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

Inteligência Artificial e Drones Militares: o futuro da guerra

Professor Ricardo Borges Gama Neto[1]

Resumo

O artigo **Inteligência Artificial e Drones Militares: o futuro da guerra** é um ensaio exploratório sobre a integração entre drones e inteligência artificial (IA), analisando suas origens, usos e implicações para a guerra contemporânea. A texto destaca que tanto os drones quanto a IA têm aplicações civis e militares, mas ganham relevância crescente no campo bélico pela capacidade de alterar táticas e estratégias de combate. A primeira parte revisita a história dos drones, desde experimentos na Primeira Guerra Mundial até o uso intensivo por Israel e, posteriormente, pelos Estados Unidos. Com a Guerra do Vietnã e a Revolução nos Assuntos Militares (RAM), tecnologias de precisão e vigilância passaram a redefinir a guerra. O ápice ocorreu na Guerra do Golfo (1991), quando sistemas inteligentes e armamentos guiados mostraram superioridade estratégica. Hoje, drones variam de microdispositivos bioinspirados até modelos de grande porte, sendo decisivos em conflitos como a guerra russo-ucraniana, onde ampliam o alcance da "zona mortal" e reforçam vigilância e ataques coordenados. A IA, por sua vez, é apresentada desde a teoria de Alan Turing até os sistemas atuais de aprendizado de máquina e deep learning. No campo militar, já foi testada em caças como o F-16 X-62A e o Gripen E, demonstrando potencial para superar pilotos humanos em combates simulados. Projetos nos EUA, Europa, China e outros países apontam para caças de sexta geração integrados a drones autônomos, colaborativos e conectados em "nuvens de combate multidomínio", onde IA terá papel central no comando e controle. A conclusão ressalta o crescente abismo tecnológico entre países desenvolvidos e periféricos, já que a tecnologia de drones e IA é dual e influencia também mercados civis. O autor prevê a expansão para áreas como guerra eletrônica e armas de energia dirigida, mas sublinha que, apesar do avanço tecnológico, a vitória em guerras ainda depende de soldados no terreno.

Palavras-chave: Inteligência Artificial; Drones Militares; Guerra Contemporâneas; Tecnologia de Defesa

1 Professor Ricardo Borges Gama Neto (DCP/UFPE).

Introdução

Este artigo tem como objetivo discutir duas das mais modernas tecnologias do mundo atual: Ambas têm emprego dual, civil e militar, e por causa da velocidade que tem sido desenvolvida e interações operacionais produzem tantas dúvidas e incertezas quanto conclusões negativas e/ou positivas[2]. Estamos falando da interconexão entre drones (aeronaves remotamente ou autonomamente tripuladas)[3] e Inteligência Artificial (IA)[4]. Este texto é mais uma introdução à discussão do que um estudo sistemático final sobre o tema. Por isso sua escrita deve ser lida mais como um ensaio exploratório do que um artigo acadêmico. Em termos metodológicos podemos definir este texto como exploratório-descritivo, na classificação de Gerring (2012), sintético.

Ambas as tecnologias que serão discutidas não são novas, a ideia de veículos aéreos não tripulados pode ser remontada a I Guerra Mundial (1914 -1918)[5], mas tiveram um importante desenvolvimento na segunda guerra mundial (1939 - 1945) quando aviões controlados por ondas de rádio começaram a ser utilizados, como o Queen-Bee britânico e o Fritz X alemão[6]. Ambos foram criados como alvos aéreos. Mas o primeiro drone, no sentido moderno da expressão, surgiu em 1951 quando a Ryan Aeronautical Company (RAC) construiu o Q2 - A Ryan Firebee, um VANT a jato, para ser usado em treinamento de artilharia terra-ar e ar-ar. A questão que pode ser posta na origem dos drones é que muitos projetos de bombas planadores e torpedos aéreos podem também ser considerados projetos de veículos remotamente tripulados, se tomarmos como referência os drones atualmente conhecidos como kamikazes (também chamados de munições vagantes), exemplos deste tipo de armamento são o IAI Harop israelense, o Shared – 136 iraniano e o Switchblade – 600 norte americano.

A Inteligência Artificial (IA) tem uma história mais antiga no cinema do que na vida real. No filme Metropolis de 1927, um cientista cria um robô feminino chamado Maschinenmensch. Esta aparição é tão significativa que se torna inspiração para filmes como *Blade Runner* e *Star Wars*. Para os propósitos desse artigo a ideia de inteligência artificial pode ser remontada ao cientista inglês Alan Turing, que num artigo acadêmico de 1936, resolvendo um problema de decisão matemática binária (sim e não), e com o conceito da Máquina de Turing, desenvolveu a ideia de um equipamento teórico, que pode ser concebido como um modelo abstrato de computador. Em 1950 Turing escreve um artigo onde descreve uma possível máquina que "pensasse", capaz de imitar o comportamento de um ser humano inteligente. Seu texto começa com a seguinte pergunta: "Podem as máquinas pensarem?". Onde ele formula o famoso Teste de Turing. Dos primeiros computadores eletromecânicos a sistemas de IA generativa como o Gemini ou ChatGPT se passaram pouco mais de 70 anos.

2 Um exemplo é o livro Nexus de Yuval Hariri.
3 Drone é a palavra inglesa para Zangão. Também são conhecidos como Veículos Aéreos Não-Tripulados (VANT's).
4 Podemos definir Inteligência Artificial, de forma resumida, como a capacidade que computadores possuem de simular a inteligência e o raciocínio humano para realizar tarefas complexas.
5 http://sistemasdearmas.com.br/pgm/asvintro.html, acessado em 27/06/2025.
6 https://blog.lojadji.com.br/historia-dos-drones/#:~:text=Em%20contrapartida%2C%20os%20brit%C3%A2nicos%20criaram,e%20mais%20f%C3%A1ceis%20de%20usar. Acessado em 27/06/2025.

Duas advertências ao leitor, como é um artigo exploratório-descritivo não será executada digressões teóricas sobre o tema e as questões éticas claramente inseridas nesta relação entre Inteligência Artificial e Drones também não serão discutidas[7].

1. Revolução nos Assuntos Militares (RAM)

O impacto da tecnologia nas guerras sempre foi um assunto controverso (Saint-Pierre e Gonçalves, 2018; Teixeira Júnior e Gama Neto, 2022). A Revolução nos Assuntos Militares (RAM) é um conceito que tenta descrever o impacto das novas tecnologias na estratégia e tática militares. A RAM não dever ser confundida apenas com o emprego de novas tecnologia, como semicondutores, lasers, softwares, sistemas de informação, etc., mas na forma como as força armadas são treinadas e organizadas, e atuam no campo de batalha. Na perspectiva da forma que a guerra é conduzida a "redução de mortos" e distanciamento do *front* de batalha são noções prementes na RAM.

Em meado dos anos de 1970 o Departamento de Defesa norte-americano, em face do desastre da Guerra do Vietnã e da distância numérica que existia entre as forças armadas da Organização do Tratado do Atlântico Norte (OTAN) e do Pacto de Varsóvia em armamento convencional e nuclear, estabeleceu o que ficou conhecido como "estratégia de compensação". Durante o governo Jimmy Carter, o secretário de defesa Harold Brown e o subsecretario William Perry, este um engenheiro com fortes ligações com o Vale do Silício, decidiram introduzir pesadamente a tecnologia de semicondutores, computadores e outras novas tecnologias nas forças armadas do país. Novos aviões, mísseis, sistemas de comando, controle e comunicações, e armas guiadas de alta precisão passaram a substituir armamentos "burros" e antiquados, como os primeiros mísseis AIM-9 *Sidewinder* e AIM-7*Sparrow III* que usavam válvulas ainda (Miller, 2023).

O chefe do estado-maior soviético Nikolai Ogarkov (1977-1984) ao analisar o desenvolvimento da tecnologia ocidental percebeu que: "sistemas de combate de longo alcance, altamente precisos e guiados por terminais, máquinas voadoras não tripuladas e sistemas de controle eletrônico qualitativamente novos, (...) transformariam os explosivos convencionais em armas de destruição em massa" (Miller, 2023, p. 187).

> "A União Soviética havia acompanhado passo a passo os EUA na corrida para desenvolver tecnologias cruciais no início da Guerra Fria construindo foguetes poderosos e um formidável estoque nuclear. Agora, os músculos estavam sendo substituídos por cérebros computadorizados. Quando se tratava dos chips de silício que sustentavam esse novo impulsionador de poderio militar, a União Soviética havia ficado para trás. (...). Por métricas tradicionais como quantidade de tanques ou tropas, a União Soviética tinha uma clara vantagem no início da década de 1980. Ogarkov enxergava as coisas de forma diferente: a qualidade superava a quantidade. Ele tinha ideia fixa na ameaça representada pelas armas de precisão dos EUA. Combinada

7 Para uma discussão sobre ética e uso de drones armados ver Chamayou (2015).

> com melhores ferramentas de vigilância estava produzindo uma "revolução técnico-militar, argumentava Ogarkov para quem quisesse ouvir" (Miller, 2023, p. 187-8).

O enorme sucesso da Operação *Desert Storm* fez com que pesquisadores norte-americanos concordassem com a conclusão do general Ogarkov e definissem que estava ocorrendo uma RAM liderada pelos Estados Unidos. A rápida capitulação do que era considerado um dos maiores exércitos do mundo, o iraquiano, em poucas semanas de intenso bombardeio e uma campanha terrestre que, em menos de cinco dias, expulsou todas as forças iraquianas do Kuwait. A velocidade com que as forças iraquianas foram derrotadas coroou a estratégia norte-americana, desenhada contra os soviéticos em 1970. Caças *Stealth* F-117 *Nighthawk,* bombas inteligentes *Paveway*, mísseis de cruzeiro *Tomahawk*, mísseis terra-ar *Patriot*, ataques cibernéticos e de guerra eletrônica foram usados. Apesar das vitórias retumbantes nas primeiras e segundas guerras do Golfo, a derrota para o Taliban no Afeganistão demonstra que mesmo a melhor tecnologia do mundo precisa que a guerra seja vencida no solo por soldados[8].

2. Drones

A evolução da aviação nos séculos XX e XXI é impressionante. Dos primeiros balões de observação militares da segunda metade do século 19[9] aos primeiros aviões de caça da primeira guerra mundial o desenvolvimento de máquinas capazes de singrar o ar foram enormes. Mas todo o desenvolvimento da aviação civil e militar sempre teve no piloto um dos seus principais fundamentos. Vai ser principalmente a partir da evolução da tecnologia embarcada e da miniaturização dos computadores[10] que a ideia de substituir os pilotos de aeronaves surgiu.

Os drones surgiram por uma necessidade prática, treinar artilharia antiaérea e fornecer alvos para pilotos em treinamento. Posteriormente, a necessidade de aeronaves de reconhecimento capazes de atuar em baixa altitude levou ao desenvolvimento de veículos capazes de realizar tal missão. Provavelmente, o uso de drones como arma direta tenha ocorrido na guerra do Yom Kippur em 1973. Israel usou drones Q2- A Ryan Firebee para enganar as defesas antiaéreas egípcias, que dispararam todos seus misseis contra estes alvos. Fato que

8 Como destacam Saint-Pierre e Gonçalves (2018, p.30: "a tecnologia, por si, não é suficiente para mobilizar qualquer transformação, como querem os defensores das RAM porque as condições de combate, ou o emprego de tropas insuficiente ou inadequadamente treinadas, muitas vezes impedem a sua mais eficiente aplicação. Ademais, toda vantagem tecnológica pode ser negada por meio da inteligente aplicação de recursos os mais simples como contramedidas baratas (em custos, não necessariamente em vidas humanas) e eficientes, como durante a Guerra do Vietnã (1964-1975), quando, buscando superar a vantagem do poder aéreo esmagador dos Estados Unidos, o general norte-vietnamita Vo Nguyen Giap ordenou que suas tropas lutassem o mais próximo possível das forcas terrestres americanas, de forma que estas ficassem impossibilitadas de chamar apoio aéreo pesado para esmagar os vietnamitas.

9 Agwu (2018) argumenta que a primeira utilização de armas aéreas foi no cerco a Veneza realizado pela Áustria em 1849, quando estas lançaram balões explosivos contra a cidade.

10 Os primeiros computadores eram máquinas gigantes e de funcionamento complexo. Miller (2024) observa que: "Um computador de última geração batizado de Eniac, montado para o Exército dos EUA na Universidade da Pensilvânia em 1945 para calcular trajetórias de artilharia tinha 18 mil tubos de vácuo. Em média um tudo apresentava defeito a cada dois dias, parando a máquina por inteiro e fazendo com que os técnicos corressem para trocar a peça quebrada. O Eniac era capaz de multiplicar centenas de números por segundo, mais rapidamente que qualquer matemático. No entanto, ocupava um cômodo inteiro porque cada um de seus 18 mil tubos de vácuo era do tamanho de um punho. Claramente, a tecnologia dos tubos era complicada demais, lenta de mais e nada confiável. Enquanto os computadores fossem monstruosidades infestadas de traças, só seriam úteis para utilizações de nicho, como quebra cabeça de códigos a menos que os cientistas encontrassem um formato menor, mais rápido e mais acessível financeiramente" (p.32).

deixou os egípcios sem condições de repor seus misseis deixando a força aérea israelense sem oposição do solo. A mesma tática foi usada em junho de 1982 quando os israelenses destruíram baterias de mísseis terra-ar SAM-6 de fabricação soviética. Neste caso, os israelenses usaram o Tadiran Mastiff, projeto feito no próprio país com a *experiencia* de 1973. O sucesso desta tática fez os Estados Unidos, através da *Defense Advanced Research Projects Agengy* (DARPA), desenvolver protótipos de veículos aéreos não tripulados em combate[11]. Mas outros dois fatores foram importantes para o governo dos Estados Unidos investir no desenvolvimento de projetos de drones de reconhecimento e vigilância eletrônica, custos cada vez crescentes dos aviões e a exposição dos pilotos à morte ***em combate.***

> ***Recognizing the need for force multipliers, our armed forces over the years developed a variety of aircraft. Examples include the Navy's EA-6B Prowler and the Air Force's F-4G Wild Weasel, which can suppress enemy air defenses so more of our bombers and fighters can get through to their targets. Another force-multiplying effort involves development of aircraft that find and track mobile targets on an increasingly fluid battlefield so we can destroy them more efficiently. Examples include our airborne warning and control system (AWACS) and the joint surveillance target attack radar system (]-STARS). All these aircraft are manned, however, which makes them expensive and their loss less acceptable. The expense applies not only to buying, operating, upgrading, and maintaining these technically advanced aircraft but to aircrew training as well. The lives of the aircrews who fly the planes have no price tag, of course, and their survival is increasingly put at risk by ever more capable threats. Because these force-multiplying aircraft are so expensive in terms of people and machines, only a relative few are bought, and we cannot afford to lose many. As a result, we plan to use most manned airborne force multipliers in a standoff role behind friendly lines. This limits their coverage, thus denying our forces the full extent of their capabilities. To ease the dual problems of small numbers and limited usage of current airborne force multipliers, fresh consideration needs to be given to unmanned systems. The idea is not to replace aircrews but to supplement them by letting unmanned aerial vehicles (UAV) conduct those missions for which they are best suited[12].***

Vamos por um momento sermos mais técnicos. Drones[13] ou VANT's podem ser classificados num primeiro momento em dois tipos básicos: quanto a forma que é comandado, o que são remotamente pilotados e os autônomos: o primeiro o piloto está numa estação de controle que pode estar a milhares de quilômetros de distância e o segundo obedece a uma programação *ex-ante*, ou seja, não precisa de uma intervenção humana para a realização do voo. Em termos de propulsão temos os modelos a jato como o RQ-4 Global Hawk ou turboélice como o Hermes 900. Quanto aos tamanhos temos os micros como o norte-americano RoboBee (desenvolvido com base na morfologia e aerodinâmica de abelhas)[14] ou pequenos como o norueguês Black Hornet para situações de vigilância e monitoramento. O drone desenvolvido na Noruega com

11 https://web.archive.org/web/20130804040234/http://www.army-technology.com/features/featureuav-evolution-natural-selection-drone-revolution/ Acessado em 27 de junho de 2025.

12 https://archive.is/7Jk1F. Acessado em 27 de junho de 2025

13 Estamos centrando este artigo no uso de drones aéreos, mas existem drones navais em ação desde 2014 quando a marinha dos EUA testou seus primeiros modelos de barcos-drone em agosto de 2014 (Del Monte, 2018). O drone naval mais famoso é, certamente, o ucraniano Magura V5 que foi responsável por abater um caça Su-30SM russo usando mísseis R-73 adaptados. < https://www.naval.com.br/blog/2025/05/03/drone-naval-ucraniano-abate-caca-su-30sm-russo-no-mar-negro/ >

14 https://revistapesquisa.fapesp.br/microdrones-bioinspirados/ Acessado em 27 de julho de 2025.

seus 16 cm de comprimento, 33 gramas e em formato de helicóptero sendo utilizado amplamente pelo exército ucraniano em sua luta contra o invasor russo e tem sido um grande sucesso de mercado e vendido para forças armadas dos Estados Unidos, França, Marrocos, Argélia, Índia, dentre outras[15]. Estes são drones que podem ser utilizados para missões civis e militares, sua principal função é o reconhecimento em tempo real. Em junho de 2025, a Universidade Nacional de Tecnologia de Defesa da China apresentou sua versão de microdrone do tamanho de um inseto, de três centímetros, muito semelhante ao RoboBee. Todos já utilizam inteligência artificial para o monitoramento sigiloso, medicina de alta precisão, agricultura automatizada, etc. Apesar de não possuírem armamentos, de uma perspectiva puramente militar, são drones ideais para missões onde é necessária coleta de informações em áreas de difícil acesso, ou acesso fortemente contestado, que vão desde instalações militares a campos de batalha[16]. Um exemplo interessante e fictício ocorre no filme *Eye in The Sky* (Decisão de Risco)[17], onde a ação de microdrones e drones armados ocorre em volta de toda uma discussão ética sobre os limites dos drones como arma de guerra, no caso uma guerra híbrida, campo onde os drones e microdrones são utilizados intensamente.

O uso mais destacado do uso de diversos tipos de drones em combate se dá atualmente na guerra russo-ucraniana. As mudanças na tecnologia tiveram importância direta nas frentes e zonas de combate[18]. Durante boa parte da história os conflitos eram frontais, direto entre soldados. Claro que o uso de flexas e balestras alteravam o alcance dos conflitos. Mas boa parte do conflito ocorria com os choques diretos das infantarias. Com o advento do canhão e das armas de fogo, o alcance das primeiras escaramuças aumentou, mas é com o uso intensivo das metralhadoras na Guerra Civil americana que aquilo que foi conhecido como "Terra de Ninguém" na Primeira Guerra Mundial teve seu apogeu. Durante a fase de guerra de trincheiras cercas e arames farpados conjuntamente com o uso de metralhadoras, granadas, minas-terrestres e lança-chamas tornava uma faixa de aproximadamente 150 metros uma zona mortal para os combatentes. Na Segunda Guerra Mundial, com o advento dos tanques e artilharia mais precisa, esta zona de mortandade aumento para uma área de 500 a 750 metros. Na nova guerra, que ocorre na Europa, esta zona mortal aumentou para dezenas de quilômetros. Os drones estão não apenas redesenhando a coleta de informações ou ataques em profundidade, mas também a maneira como o conflito ocorre na frente de batalha, uma novo espaço de vigilância e ataque com vários, as vezes chegando a dezenas de quilômetros, foi estabelecida. Os inimigos se monitoram 24 horas por dia, 7 dias por semana auxiliando apoio aéreo contínuo e coleta de informações para as unidades de infantaria e artilharia, que podem responder de imediato as

15 https://www.flir.com/products/black-hornet-4/?vertical=uas&segment=uis. Acessado em 27 de julho de 2025.

16 https://fenati.org.br/drones-inseto-com-ia-ganham-espaco-campo-e-guerra/#:~:text=Um%20dos%20exemplos%20mais%20conhecidos,durante%20a%20apresentação%20do%20projeto. Acessado em 27 de julho de 2025.

17 https://www.imdb.com/pt/title/tt2057392/ Acessado em 27 de julho de 2025.

18 Wittes e Blum (2015) destacam o processo de robotização das operações militares: "Robotics are playing an ever growing role in military operations more generally, doing everything from scouting terrain to checking for and disarming improvised explosive devices. Numerous new unmanned systems for operations on the ground, in the air, and at sea are in development or have already been deployed. These robots include ground vehicles, infantry substitutes, surveillance devices, supply and guidance systems, evacuation technologies, and, of course, dedicated weapons systems" (p.27).

ações do adversário. A presença de drones de coleta de informações, munições vagantes e o suporte da transmissão via satélite em tempo real aumentou em muito a eficiência das tropas no solo. Não somente as forças terrestres, aviões de combate recebem informações de solo e são capazes de atacar também com mais eficiência alvos terrestres.

Mesmo que tenhamos destacado a ação de drones na frente de batalha do conflito russo-ucraniano, deve ser observado o uso intenso de drones como armas de destruição de cidades e alvos civis considerados prioritários pelos militares como aeroportos, pontes, fábricas e estações de fornecimento de energia. Nesse caso a utilização de ataques de drones em "enxames", buscando saturar as defesas antiaéreas do adversário aparentemente têm feito pouco uso da inteligência artificial, especialmente o uso pelos russos dos modelos iranianos que têm baixíssima tecnologia de aquisição de alvos.

Apesar do destaque que demos, anteriormente, é importante destacarmos que o uso dos diversos tipos de drones na guerra ocorre por uma necessidade prática. O primeiro uso intenso de drones, no campo de batalha, foi feita pelos Estados Unidos em sua guerra ao terror, especialmente no governo Barack Obama[19].

O presidente Barack Obama herdou a guerra ao terror de seu antecessor como consequência dos ataques contra os Estados Unidos, promovidos pela organização terrorista Al-Qaeda (em árabe "a rede" ou "a base") em 11 de setembro de 2001 conta as duas torres do *World Trade Center*, ao Pentágono e ao voo 93 da United Airlines.

O primeiro ataque com drones, provavelmente, aconteceu no Iêmen em 2002. Mas foi a partir da administração Obama que houve um aumento substancial do uso destas armas não tripuladas contra combatentes. O governo George W. Busch ordenou aproximadamente, 50 ataques contra alvos fora das áreas de combate, na administração Obama, e número aumentou pelo menos sete vezes. "A presidência de Obama não apenas acreditava na eficácia da tecnologia de drones como uma arma contra o terror, mas também acreditava em seu pragmatismo ao lidar com os terroristas altamente evasivos; e manteve essa convicção durante toda a presidência, apesar das controvérsias em torno da arma" (Agwu, 2018, p. 151)[20].

O drone MQ-1 *Predator* foi desenvolvido nos anos 1990 para missões de reconhecimento, pela empresa *General Atomics*. O drone, originalmente, carregava apenas câmeras e sensores de vários tipos para missões de reconhecimento para substituir os caríssimos os Lockheed SR-71 BlackBird que haviam sidos retirados de serviço. Outros dois modelos de drones importantes eram o MQ-9 *Reaper* (às vezes chamado *Predator* B) por ser fabricado também pela *General Atomics* e o RQ-4 *Global Hawk*.

19 "A single drone system consists of four aircraft, a ground station, a satellite link, and a maintenance crew at the launch site on a local base, but the system is nonetheless considerably less expensive than a single inhabited fighter jet" (Enemark, 2014, p 52).

20 "Much as playing by the rules of engagement is desirable, drones in asymmetric armed conflicts typically illustrate the saying that it is difficult to make omelets without breaking an egg. It is very difficult to engage terrorists or insurgents in armed conflict the same way that the nation-state would be engaged because insurgents do not engage in conventional warfare, being not capable of any pitched battle or frontal engagement" (Agwu, 2018, p. 187).

Ainda no início da campanha contra o Talibã, o MQ-1 foi armado com mísseis AGM-114 *Hellfire*. O *Hellfire*, um míssil do tipo dispare-e-esqueça, já era utilizado em helicópteros de ataque AH-64 Apache e AH-1 Cobra e considerado bastante confiável.

Os drones foram a forma como o governo Barack Obama (2009 a 2017) encontrou para enfrentar o desgaste ocasionado pela morte de soldados norte-americanos no Afeganistão. Os VANT's podem atacar seus alvos sem expor seus soldados em razão dos ataques serem feitos longe do território da ação, ou seja, em o risco de perda de vidas humanas por quem usa, é uma guerra feita por controle remoto. Segundo Enemark (2014, p 53), desde 2009:

> The Air Force has been training more drone operators than fighter pilots.56 The drone inventory of the Defense Department as a whole has grown rapidly, from 167 in 2002 to nearly 7,500 in 2010,57 and inhabited aircraft made up 69 per cent of all US military aircraft at the end of 2011 (compared to 95 per cent in 2005). The number of drones is expected to increase by a further 35 per cent in the decade to 2020, and the bulk of planned spending is for the more expensive large- and medium-sized drones designed to conduct.

Em 2013, o governo Obama emitiu a *Presidencial Policy Guidance*[21] na tentativa de estabelecer diretrizes e justificar o uso intensivo de drones na guerra do Afeganistão e outros países como: Iêmen, Somália e Líbia. O documento é claro em estabelecer que o uso de drones em:

> CT actions, including lethal action against designated terrorist targets. shall be as discriminating and precise as reasonably possible. Absent extraordinary circumstances, direct action against an identified high-value terrorist (HVT) will be taken only when there is near certainty that the individual being targeted is in fact the lawful target and located at the place where the action will occur.

O documento foi revisado e publicado em agosto de 2016, procurando definir de forma mais clara o uso de drones armados, como instrumentos contra indivíduos que ameaçassem direta e contínua os interesses e pessoas dos EUA. O texto ainda discrimina que devem ser estabelecidos com precisão a periculosidade do terrorista ou outro alvo com alto valor, definindo que a força letal só deve ser usada quando não há uma alternativa, como a captura. A doutrina Obama de 2016 também observava a necessidade de se observar princípios legais internacionais, deixando claro que as agências governamentais como a *Central Intelligence Agency* (CIA) e o Departamento de Defesa devem concordar com o alvo. O governo Trump, pouco meses depois, revogou parte da doutrina liberando o uso dos drones para ações com mais liberdade de ação.

Atualmente, o futuro dos drones aéreos na área militar parece ser substituir não apenas caças tripulados em ações mais arriscadas, mas sim ser um aliado dos pilotos como foi o caso do Northrop Gruman X-47B[22]. Esta aeronave não tripulada de ataque furtivo foi desenvolvida para ser utilizada na USNavy a partir de porta-aviões para missões como reabastecimento

21 https://www.aclu.org/sites/default/files/field_document/presidential_policy_guidance.pdf < acessado em 08 de agosto de 2025 >
22 https://www.northropgrumman.com/what-we-do/aircraft/x-47b-ucas < acessado em 08 de agosto de 2025 >

aéreo e ataque com bombas e mísseis. O X-47 surgiu como desenvolvimento do projeto J-UCAS da DARPA. Outro modelo de drone baseado em porta-aviões é o Boeing MQ-25 *Stingray*, que além das funções de reabastecimento e ataque também deverá realizar missões de inteligência, vigilância e reconhecimento (ISR) e missões antiterrorismo de baixa-intensidade ("low-intensity counter-terrorism missions")[23]. A USAF, atualmente, desenvolve o programa *Collaborative Combat Aircraft (CCAs)* que busca desenvolver um avião de combate que atuará, conjuntamente, com o avião F-35 *Lighting* II. Atualmente, dois projetos concorrem para ser o drone de combate colaborativo da força aérea dos EUA: o YFQ-42A da *General Atomics* e o YFQ-44A da *Anduril Industries.* Como caças leais, estes dois projetos, além de executar as missões de ataque ao solo, reconhecimento e guerra eletrônica[24] servirão como alas dos aviões de combate com pilotos convencionais. A ideia de drones de combate, que atuem como aviões em apoio a aeronaves tripuladas, faz parte do projeto *Skyborg*[25]. Este é um programa que busca desenvolver *software, hardware*, interface homem-máquina e outros aspectos que sejam necessários a avião colaborativa de combate e em vários aspectos também faz parte do *Next Generation Air Dominanc*e (NGAD), que é o projeto de desenvolvimento de um caça de sexta geração, que deverá substituir o F-22 *Raptor* a partir da próxima década (batizado de F-47).

Destacamos os esforços norte-americanos na área de drones colaborativos de combate. Mas do outro lado do Atlântico esforços importantes também estão sendo feitos. Os europeus estão atrás dos Estados Unidos no quesito tecnologia furtiva (stealth). A furtividade é um item essencial nas tecnologias militares atuais, e reduzir a detectabilidade de aeronaves, navios e misseis através da diminuição da seção transversal do radar (RCS) tem sido buscada tanto via novos desenhos de aeronaves como materiais absorventes aos sinais de radar e térmicas.

França e Inglaterra lideram dois diferentes projetos de caça de sexta geração e de drones de combates colaborativos. O primeiro é o *Future Combat Air System* (FCAS), um empreendimento conjunto da *Dassault Aviation*, *Airbus* e Indra, que envolvem os governos da França, Alemanha e Espanha. O futuro avião de combate europeu que surgirá deste consórcio deverá substituir a partir de 2040 o *Eurofighter Typhoo*n, o *Rafale* e o F-18. Como seu congênere norte-americano não se resume a um projeto de caça, mas também um drone está sendo desenvolvido, o que é denominado de *Next Generation Weapon System* (NGWS)[26]. O drone *nEUROn* é um veículo aéreo não tripulado que tem mais participantes que o FCAS, como Grécia, Itália, Suécia e Suíça. O VANT será furtivo e deverá atuar como aeronave de ataque e ala aérea, da mesma forma como os projetos desenvolvidos nos EUA.

23 https://news.usni.org/2018/08/30/navy-picks-boeing-build-mq-25a-stingray-carrier-based-drone < acessado em 08 de agosto de 2025 >

24 "Guerra eletrônica é um termo genérico que engloba todas as ações militares, destinadas a assegurar o uso mais eficaz possível de emissões eletromagnéticas e eletro-ópticas e impedir que o inimigo consiga fazer uso dos seus. Os sistemas que permitem o uso militar e desprendimento desta energia, tanto de forma ofensiva ou defensiva, variam amplamente. Podemos classificar as "ações" da guerra eletrônica em quatro tipos: i. detecção (radares, sonares, receptores de alerta antecipado); ii. coleta de informações (Sigint - Signals Intelligence, Elint - Eletronic Inteligence, Comint - Comunications Inteligence); iii. contramedidas (chaffs, flares, anti-jamming); e iv. interferência intencional (jamming, desvio de sinais/dissimulação e armas do tipo Electo-magnetic Pulse)" (Gama Neto. 2017, p. 209).

25 https://www.airforce.com/experience-the-air-force/airmen-stories/inside-air-force-innovation/project-skyborg < acessado em 08 de agosto de 2025 >

26 https://www.airbus.com/en/products-services/defence/future-combat-air-system-fcas < acessado em 08 de agosto de 2025 >

A Inglaterra lidera o outro projeto, o Global Combat Air Programme (GCAP)[27] em cooperação com Itália e Japão. As empresas líderes são a BAE System, Leonardo e a Mitsubishi Heavy Industries. Também conhecido como *Tempest*, a aeronave será de sexta geração e deverá a partir de 2040 substituir o *Eurofighter Typhoo*n e o Mitsubishi F-2. Os projetos atuais de caça atuam mais como um conjunto sistêmico de programas, e como o GCAP não poderia ser diferente. Ele também incorpora um drone de combate no projeto, o *Taranis*. Contudo, este drone já voa a pelo menos 12 anos e está atualmente como um projeto exclusivo da BAE, sem a participação das outras empresas. Neste caso a participação individual em outros projetos de drones pela Leonardo pode ser um impedimento a um envolvimento mais ativo no projeto.

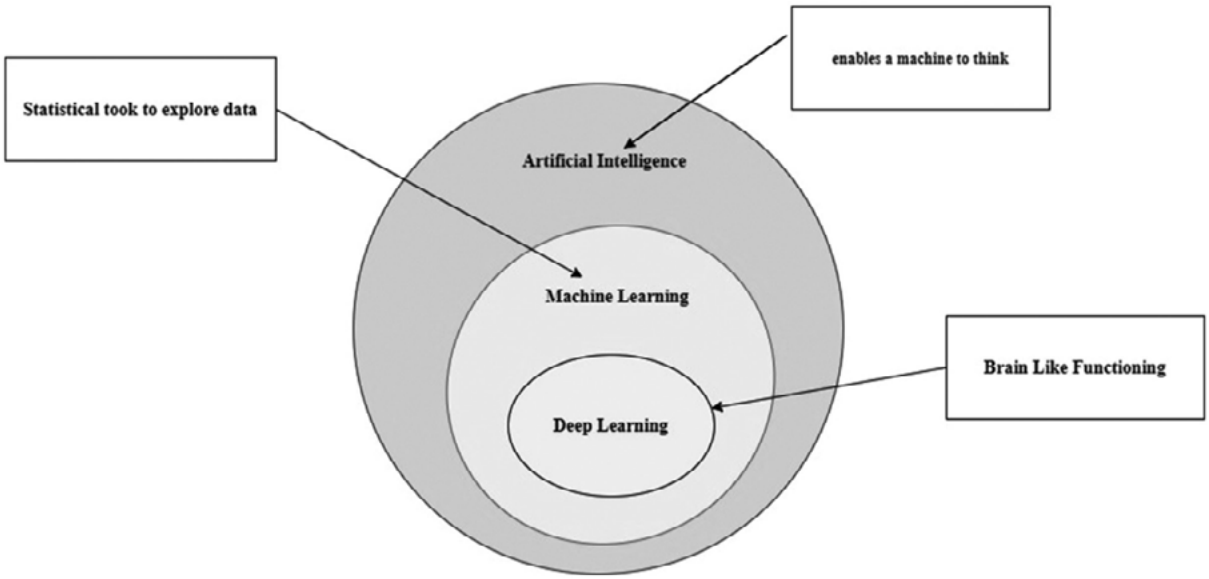
Todos os projetos europeus e norte-americanos elevam o conceito de Guerra Centrada em Redes em um novo nível, o dos Sistemas de Nuvens de Combate, Nuvens de Combate Multidomínio[28] ou Nuvens Militares. Ou seja, o uso da tecnologia em nuvem (*cloud computing*) por instituições militares. Hoje as forças armadas já usam sistemas em nuvens dedicadas em suas atividades rotineiras, que são redes descentralizadas e resilientes a ataques cibernéticos e que conectam as diferentes forças armadas nos domínios: aéreo, espacial, terrestre e marítimo. A tecnologia baseada em nuvem, hoje, já é utilizada em situações de comando e controle da defesa, como é o caso do *Defense Integrated Data Center* (DIDC) da Coréia do Sul, mas no futuro será utilizada para gerenciar e aprimorar a tomada de decisões dos comandantes militares em tempo real. A principal ferramenta de software desta rede será a inteligência artificial (IA).

3. Inteligência Artificial (IA)

Como destacamos a poucas páginas a evolução da Inteligência Artificial (IA) foi rápida e intensa. Praticamente, não existe área do conhecimento e da ação humana que esteja sendo afetada por esta tecnologia. A IA pode ser entendida como uma área da ciência da computação que se dedica a criar sistemas, capazes de realizar tarefas que exigiriam o uso de inteligência humana. Isto quer dizer: raciocínio, aprendizagem, resolução de problemas e tomadas de decisão. Em essência, procura simular a inteligência humana através de computadores. Simular aqui é uma palavra importante. A IA não replica a inteligência humana, mas atua como um simulacro deste. A IA utiliza algoritmos e modelos matemáticos sofisticados para analisar dados, aprender com estes e tomar decisões. Existem basicamente dois tipos de técnicas: a primeira é conhecida como aprendizado de máquinas (*machine learning*), onde os computadores recebem grandes volumes de dados, identificam padrões através de sofisticadas técnicas estatísticas e depois fornecem possíveis soluções; a segunda é a *deep learning* que se baseia em redes neurais artificiais que são modeladas simulando a estrutura e a função do cérebro humano. Uma rede neural funciona em camadas conectadas para que aprendam e tomem decisões a partir de grandes bases de dados não estruturados.

27 https://commonslibrary.parliament.uk/research-briefings/cbp-10143/ < acessado em 08 de agosto de 2025 >
28 https://www.airbus.com/en/products-services/defence/multi-domain-combat-cloud < acessado em 08 de agosto de 2025 >

Figura 01 – Hierarquia da Inteligência Artificial



Fonte: Lal, Tarar e Smieee, 2023, p. 202.

Os drones atuais, civis ou militares usam a inteligência artificial para vigilância e controle em tempo real. Inspecionam terrenos e permitem o controle e redução de ações de risco. Agricultores usam drones com IA da *Skycatch* para monitor terrenos e autoridades de segurança publica utilizam as soluções de inteligência da *DroneSense* para coleta de dados que vão de trânsito a pessoas que deveriam estar presas. No âmbito militar, o uso de drones vem mudando a forma da concepção e ação do combate. Apesar das enormes questões éticas embutidas[29].

Entre dezembro de 2022 a setembro de 2023, a USAF conjuntamente om a DARPA, dentro do projeto *Air Combat Evolution* (ACE), fizeram testes com um caça F-16D Viper (biplace, com um piloto humano na cabine traseira, em caso de emergência com capacidade de desligar a IA, caso necessário) modificado (denominado X-62A Vista) com inteligência artificial. Foram necessários vários testes e treinamentos preliminares com milhares de alterações, até o momento que o modelo de teste foi colocado à prova, contra um experiente piloto de F-16. A aeronave com inteligência artificial abateu seu adversário humano em um combate dentro do alcance visual (dogfight)[30].

Em junho de 2025, a sueca Saab em conjunto com a empresa de software alemã Helsing anunciaram a integração do caça Gripen E, a inteligência artificial "*Centaur*". Neste caso, a integração faz parte do projeto *Beyond*. "Durante os voos, o Gripen E cedeu o controle ao

29 https://www.economist.com/technology-quarterly/2017/06/08/the-future-of-drones-depends-on-regulation-not-just- < acessado em 08 de agosto de 2025 >technology?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=19495686130&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclsrc=aw.ds&gad_source=1&gad_campaignid=19495464887&gbraid=0AAAADBuq3IgFJIAP-IgwV5AnbU4QKrA2&gclid=EAIaIQobChMIptnOmK-AjwMVhWdIAB3VPA40EAAYAiAAEgIlM_D_BwE < acessado em 08 de agosto de 2025 >

30 https://www.defenseone.com/technology/2024/04/man-vs-machine-ai-agents-take-human-pilot-dogfight/395930/ < acessado em 08 de

Centaur, que executou de forma autônoma manobras complexas em um cenário de combate seguindo o conceito BVR (*Beyond Visual Range*, ou além do alcance visual), sinalizando ao piloto o momento ideal para o disparo"[31]. Apesar dos poucos detalhes técnicos, aparentemente a solução da Saab não envolveu o desenvolvimento de um hardware específico para a integração IA e caça. O *Centaur* dentro da arquitetura do Gripen E/F funciona atualmente como um co-piloto virtual, mas no futuro talvez possa ser o piloto principal em missões de combate.

A China tem desenvolvido rapidamente soluções de inteligência artificial e robótica[32], em várias áreas. Apesar da China não ter apresentado uma tecnologia de IA integrada ao seu principal avião de combate, o J-10C, sabe-se que estes pilotos têm treinado contra simuladores com IA, e sendo derrotados. No início, os pilotos derrotam as IA's com facilidade que aprendem a cada combate, até que no final ficam melhores que os pilotos humanos[33]. O caça furtivo de quinta geração Chengdu J-20S, que estão sendo fabricados, já incorporam tecnologia de IA. Ao contrário da Saab, que apostou numa estratégia de IA completamente baseada em software, o caça chinês, aparentemente, aposta numa arquitetura dedicada computador-software, utilizando o espaço do segundo lugar da aeronave para a instalação de um novo computador, que entre outras funções poderão ser capaz de controlar drones alas. O avião de sexta geração Chengdu J-36[34], certamente, já virá com um sistema de inteligência artificial capaz, não somente de controlar drones alas, enxames e armas autônomas, mas transmitir todas as informações capacitadas por seus sensores a sistemas de Nuvens de Combate Multidomínio.

Rússia, Coréia do Sul e Turquia também possuem projetos de caças com inteligência artificial integrada. No caso, são respectivamente os aviões Sukhoi – 57, o KF-21 Boramae e o KAAN. Os dois primeiros caças de quarta geração melhorados (4.5+) e o último de quinta. O modelo russo já voa, mas há muita pouca informação sobre sua atuação na guerra Rússia-Ucrânia. O modelo coreano também já em forma de protótipos e com uma nova versão mais furtiva (EX) projetada. O modelo turco ainda está na fase de protótipo, mas tem chamado à atenção por oferecer não apenas um caça furtivo, mas uma solução integrada com drones como os da família Bayraktar (como o ala leal Kizilelma) e o jato de treinamento TAI Hürjet. Em todas as soluções nativas de desenvolvimento de IA's são integradas a seus caças e drones.

agosto de 2025 >

31 https://www.saab.com/pt-br/markets/brasil/noticias/2025/saab-atinge-marco-inedito-em-inteligencia-artificial-com-o-gripen-e < acessado em 08 de agosto de 2025 >

32 Inclusive com uma fábrica de mísseis completamente robotizada. < https://www.sociedademilitar.com.br/2025/05/china-revela-fabrica-de-misseis-que-opera-sem-humanos-linha-de-producao-100-robotica-vira-alerta-mundial-apos-misseis-automatizados-derrubarem-cacas-rafale-e-sukhoi-em-segundos-na-guerra-entre-afch.html < acessado em 08 de agosto de 2025 >

33 https://forcaaerea.com.br/pilotos-chineses-estao-treinando-contra-aeronaves-com-ia/ < acessado em 08 de agosto de 2025 >

34 https://www.aereo.jor.br/2025/01/04/chengdu-j-36-uma-interpretacao-chinesa-da-guerra-aerea-do-futuro/ < acessado em 08 de agosto de 2025 >

Conclusão

Como observamos na introdução este é um texto exploratório sem maiores pretensões teóricas e analíticas. É essencialmente uma exploração a um novo e conjunto de tecnologias. O que mais destaco, neste final, é o aumento cada vez maior do fosso tecnológico que está se formando entre os países que detém grandes parques tecnológicos e fazem vultosos investimentos em defesa. Como parte dessa tecnologia é dual, um exemplo claro é o uso do *DeepSeek* por oficiais e projetistas de armas chinesas. Ficar fora do desenvolvimento tanto da tecnologia dos drones quanto da inteligência artificial para fins militares alija parte dos países da capacidade de desenvolverem tecnologias para o mercado internacionais de equipamentos eletrônicos e semicondutores.

Voltando mais especificamente ao texto, estamos vendo uma nova integração de tecnologia que ainda vai se desenvolver muito no futuro. Drones e IA's fazem parte de nossa vida, analisando o tráfego de veículos nas cidades, procurando por insetos como o *aedes aegypt*, operando, etc... Dentro de pouco tempo, veremos veículos aéreos civis de mobilidade aérea, como o EVA da Embraer ou o drone civil da Rosel Holding (Rostec) que vão tomar o mercado dos helicópteros menores.

Faltou neste texto uma discussão, que será aprofundada no futuro, do uso de drones e inteligência artificial com guerra eletrônica e armas de energia dirigida.

Bibliografia

AGWU, Fred. *Armed Drones and Globalization in The Asymmetric War on Terror: challenges for the law of armed conflict and global political economy*. New York/London: Routledge, 2018.

CHAMAYOU, Grégorie. *Teoria do Drone*. São Paulo. Cosac Naify, 2015.

ENEMARK, Christian. *Armed Drones and The Ethics of War: military virtue in a post-heroic age*. New York/London: Routledge, 2014.

GAMA NETO, Ricardo Borges. Guerra Cibernética / Guerra Eletrônica – conceitos e espaços de interação. *Política Hoje*, Recife, vol. nº26, n. 01, pp. 201 – 217.

GERRING, John. Mere Description. *British Journal of Political Science*, London, vol. 42, nº 04, pp. 721-746, 2012.

HARIRI, Yuval. *Nexus: uma breve história das redes de informação, da idade da Pedra à inteligência artificial*. São Paulo: Companhia das Letras, 2024.

LAL, Roshan, TARAR, Sandhaya e SMIEEE, Naveen. Challenges and Opportunities of Machine Learning and Deep Learning Technique of The Internet of Drones. IN: SOLANKI, Arun; TARAR, Sandahya; SINGH, Simar e TAYAL, Akash. (eds). *The Internet of Drones; AI applications for smart solutions*. Palm Bay: Apple Academic Press, 2023.

MILLER, Chris. *A Guerra dos Chips: a batalha pela tecnologia que move o mundo.* Rio de Janeiro: Globo Livros, 2023.

SAINT-PIERRE, Héctor e GONÇALVES, Leandro. Nem Revolução (RM) em Assuntos Militares (RAM), apenas mudanças de longa duração condensadas na guerra pelo gênio militar. *Revista Brasileira de Estudos de Defesa*, São Paulo, vol. nº 5, nº 02, pp. 1***3-36, 2018.***

TEIXEIRA JUNIOR, Augusto Wagner e GAMA NETO, Ricardo Borges. The Brazilian Army's Concept of Transformation: Technology and military change. Revista Brasileira de Estudos de Defesa. Brasilia, vol. nº 09, n.º 01, pp. 43 – 68, 2022

WITTES, Benjamim e BLUM, Gabriella. The Future of Violence: robot and germs, hackers and drones. New York: Basic Books. 2015.

JCPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

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

INTELIGÊNCIA ARTIFICIAL E PODER AEROESPACIAL: UM INTROITO

Gills Lopes[1]
Érika Rigotti Furtado[2]
Alexandre Manhães[3]
André Luiz Anjos de Figueiredo[4]

Resumo

O artigo analisa a crescente intersecção entre inteligência artificial (IA) e Poder Aeroespacial, destacando sua influência na tomada de decisão, vigilância, comunicações e operações militares. A IA tem transformado sistemas espaciais em plataformas autônomas, ampliando a capacidade de dissuasão, controle e projeção de poder. O presente estudo aborda aplicações em conflitos contemporâneos, como na guerra russo-ucraniana, e discute como IA e aprendizado de máquina (ML) incrementam missões de Inteligência, Vigilância e Reconhecimento (IVR), comunicações satelitais e consciência situacional espacial. Também são analisados os dilemas éticos e jurídicos no uso militar da IA, especialmente no Direito Internacional dos Conflitos Armados. No caso brasileiro, recomenda-se a formulação de uma Estratégia Nacional específica para o setor espacial, contemplando pesquisa e desenvolvimento, uso dual e parcerias. Conclui-se que o domínio dessa tecnologia disruptiva é essencial para a soberania aeroespacial brasileira.

Palavras-chave: Defesa; Inteligência artificial; Poder Aeroespacial.

Abstract: The article analyses the growing intersection between artificial intelligence (AI) and aerospace power, highlighting its influence on decision-making, surveillance, communications, and military operations. AI has transformed space systems into autonomous platforms, expanding the capacity for deterrence, control, and power projection. This study addresses applications in contemporary conflicts, such as the Russian-Ukrainian war, and discusses how AI and machine learning (ML) enhance Intelligence, Surveillance and Reconnaissance (ISR) missions, satellite communications and spatial situational awareness. It also analyses the ethical and legal dilemmas in the military use of AI, especially in International Law of Armed Conflict. In the case of Brazil, it is recommended that a specific National Strategy be formulated for the space sector, covering research and development, dual use, and partnerships. It is concluded that mastery of this disruptive technology is essential for Brazilian aerospace sovereignty.

Keywords: Defence; Artificial intelligence; Aerospace power.

1 Professor Permanente do Programa de Pós-Graduação em Segurança Desenvolvimento e Defesa (PPGSDD) da Escola Superior de Defesa (ESD) e do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA). Doutor em Ciência Política pela Universidade Federal de Pernambuco (UFPE).

2 Professora Adjunta na Escola Superior de Defesa (ESD). Doutora em Ciências Aeroespaciais pelo PPGCA/UNIFA.

3 Doutorando em Ciências Aeroespaciais pelo PPGCA/UNIFA. MBA em Gestão Empresarial e em Gerenciamento de Projetos, ambos pela Fundação Getúlio Vargas (FGV). *Project Management Professional* (PMP) pelo *Project Management Institute* (PMI). Capitão na Força Aérea Brasileira (FAB).

4 Doutorando em Ciências Aeroespaciais pelo PPGCA/UNIFA. Professor Assistente na Universidade Federal Rural do Rio de Janeiro (UFRRJ).

Introdução

Devido à sua inerente inquietude, as sociedades buscaram, ao longo da história, compreender, modelar, controlar, gerenciar e prever a realidade que as cercava, explicando acontecimentos, suas próprias criações e fenômenos (Kissinger; Schmidt; Huttenlocher, 2021). Contudo, com o advento da inteligência artificial (IA), esse protagonismo passou a ser desafiado, sobretudo no âmbito da tomada de decisão.

Novas formas de comunicação entre dispositivos conectados no ciberespaço tornaram-se instantâneas, e tarefas como leitura, buscas, compras, linguagem, registro, vigilância, planejamento e gestão militar passaram a ser executadas de maneira automatizada, impulsionadas por essa tecnologia disruptiva.

O avanço da IA vem transformando profundamente as capacidades dos sistemas espaciais contemporâneos, permitindo tomadas de decisão automatizadas, com maior autonomia, velocidade e eficiência na coleta, processamento e uso dos dados. Em outras palavras, está fazendo dos satélites de meros transmissores de dados a sistemas inteligentes e autônomos, integrados a ecossistemas algorítmicos multissensoriais de defesa e vigilância na/da Terra.

Mais do que uma ferramenta tecnológica, a IA representa um vetor de superioridade estratégica no domínio aeroespacial, ampliando as possibilidades de dissuasão, controle e projeção de poder nesta e em outras dimensões. Desta forma, toda essa transformação requer novas abordagens políticas e regulatórias para extrair o máximo potencial destas tecnologias.

Nesse sentido, o presente trabalho tem o objetivo geral de apresentar discussões introdutórias sobre o uso dessa tecnologia disruptiva nos terceiro e quarto domínios estratégicos.

Para tanto, o texto se subdivide em quatro seções principais. A primeira trata da relação entre IA e o poder aéreo. Na segunda, é a vez do poder especial encontrar a IA. A seguinte versa sobre questões normativas atinentes ao emprego militar dessa tecnologia. Por fim, elencam-se algumas sugestões ao caso brasileiro.

1. IA e Poder Aéreo

Conforme Russell e Norvig (2022) e Kissinger, Schmidt e Huttenlocher (2021), o campo da IA vai além de compreender a inteligência; busca, em verdade, construir entidades inteligentes — máquinas capazes de computar formas de agir eficazmente e segura em uma ampla variedade de novas situações. Atualmente, a IA abrange uma grande diversidade de subcampos, que vão desde os mais gerais, como aprendizagem, raciocínio e percepção, até áreas mais específicas, como jogar xadrez, demonstrar teoremas matemáticos, criar poesia, dirigir automóveis e diagnosticar doenças. Trata-se, portanto, de um campo universal, relevante para praticamente qualquer tarefa intelectual.

Assim como a IA redefine a forma de processar informações e de tomar decisões no ciberespaço, o Poder Aeroespacial representou, desde o início do século XX, um marco semelhante na transformação da soberania e da estratégia militar. William "Billy" Mitchell foi um dos primeiros a defender o potencial transformador do poder aéreo, definindo-o como a capacidade de "fazer algo no ou através do ar", destacando uma dimensão global em que nenhuma parte do planeta estaria imune à sua influência. Embora sua definição inicial não distinguisse usos civis e militares, capturava a essência da versatilidade dessa nova ferramenta (Chun, 2001; Douhet, 2019; Gray, 2012).

Giulio Douhet foi fundamental ao introduzir as ideias de comando e domínio do Ar como objetivo prioritário em qualquer campanha. Para ele, o poder aéreo deveria atuar como força ofensiva independente, recorrendo a bombardeios estratégicos contra centros vitais do inimigo com o uso de aeroplanos de combate. A introdução do avião inaugurou, de acordo com o pensador italiano, uma decisiva "terceira arte da guerra": a guerra aérea (Douhet, 2019).

Com o avanço tecnológico, o conceito expandiu-se para Poder Aeroespacial, incluindo tanto o ambiente aéreo quanto o espacial na busca por objetivos nacionais. Essa evolução refletiu-se em capacidades e ativos aeroespaciais como velocidades supersônicas, furtividade e mobilidade ampliada, enquanto os sistemas espaciais se tornaram essenciais para comunicações, meteorologia, navegação, alerta precoce, vigilância e inteligência, atuando como verdadeiros habilitadores de operações militares (Chun, 2001). Gray (2012) reforça que, apesar das mudanças tecnológicas, o poder aéreo conserva atributos físicos duradouros, como velocidade, alcance, altura, onipresença, agilidade e concentração, mas também limitações persistentes, como carga restrita, fragilidade, custo elevado, dependência de bases e vulnerabilidade a condições climáticas. Algumas dessas limitações podem ser contrabalanceadas por tecnologias e soluções disruptivas, providas, inclusive, por IA.

Um exemplo paradigmático do uso dessa tecnologia como ativo aéreo é a guerra russo-ucraniana iniciada em 2022. Por exemplo, as forças armadas de Kiev utilizaram IA acopladas em drones para selecionar alvos estratégicos, tais como refinarias de petróleo (DRONES[...], 2024) e aeronaves russas (Adams, 2025).

Gray (2012) argumenta que, embora aplicado no nível tático, o poder aéreo gera efeitos de natureza estratégica, cujo valor se define pelo impacto histórico que produz e não apenas pela sofisticação tecnológica. Dessa forma, a convergência entre as dimensões cibernética e aeroespacial evidencia um cenário em que tecnologia, soberania e dissuasão se tornam indissociáveis, constituindo pilares centrais para a manutenção da supremacia estratégica e para a definição dos rumos da segurança internacional contemporânea.

Mas o uso de IA no ambiente aeroespacial não se restringe ao domínio do Ar; pelo contrário, o domínio do Espaço, como uma das dimensões da guerra (Lonsdale, 1999, *passim*), também apresenta múltiplas opções para o desenvolvimento – e avanço – dessa tecnologia, conforme a seção seguinte.

2. IA e Poder Espacial

As tecnologias espaciais ligadas à IA e associadas ao aprendizado de máquina (ML, de *machine learning*) são uma das principais tendências tecnológicas no setor espacial para o ano de 2025 (Lockheed Martin, 2024). A integração dessas tecnologias aos sistemas espaciais aumenta a velocidade da tomada de decisão, por meio da análise e processamento de dados, incrementando a consciência situacional e a adaptabilidade aos desafios impostos por condições de defesa e segurança.

A título de exemplo, a gigante do setor aeroespacial Lockheed Martin possui 80 programas e projetos ativos que usam IA/ML em sistemas espaciais, algumas em colaboração com a NVIDIA – primeira empresa a ultrapassar os US$ 4 trilhões em valor de mercado (Vitorio, 2025) –, exemplificando como as empresas estão investindo pesadamente em tais tecnologias, seja por conta própria, seja em parcerias (Lockheed Martin, 2024).

Neste sentido, vê-se que a IA também está impactando o poder espacial, ao incrementar as capacidades dos serviços proporcionados pelas diversas missões espaciais, em particular as de Inteligência, vigilância e reconhecimento (IVR), comunicações satelitais (ComSat) e consciência situacional espacial.

Além disso, a IA também contribui para otimizar o posicionamento de satélites nas suas respectivas constelações, favorecendo seu emprego como um enxame integrado, ao invés de um agrupamento desconexo de satélites (Husain, 2025). Em termos mais técnicos, esses sistemas empregam inteligência diferenciável (*differentiable intelligence*) e ML embarcada, gerando sistema de redes neurais capaz de aprender por inferência a todo momento (Izzo *et al.*, 2022). Desta forma, o emprego destas capacidades não se restringe somente a fins civis e comerciais, mas também a militares, isto é, são duais.

Assim, a IA/ML está transformando a forma de como as missões de observação da Terra acontecem, em particular as relacionadas à IVR. Com os *softwares* de IA/ML embarcados nos satélites, a análise e processamento de imagens já acontece em órbita, reduzindo a necessidade de fazer a transmissão destes dados para as estações terrestres (*downlink*), quando então seriam processadas. Com isso, otimiza-se o uso de telemetrias e acelera-se a identificação das imagens com alvos de maior valor, ao descartar dados desnecessários. Isso ocorre por meio da comparação de imagens do mesmo local e de períodos diferentes, destacando movimentações de interesse, entregando resultados com maior potencial de emprego estratégico. Além do mais, o *software* "aprende" quais são as áreas com maior potencial de ter dados de importância, desconsiderando as informações desnecessárias (Izzo *et al.*, 2022). Por exemplo, o Japão emprega esta capacidade para monitorar a região do Indo-Pacífico, a qual é importante para a sua segurança nacional (Brewster, 2022; Reinecke, Dutcher, 2025).

Um outro exemplo interessante deste uso é o monitoramento de *dark ships*, navios que saem do porto com o seu sistema de identificação (*Automatic Identification System*, AIS) ligado, mas o desligam durante a viagem para que não sejam identificados. Desta forma, eles aproveitam para fazer operações ilegais, como transferência de bens entre navios e pirataria, visando contornar sanções econômicas ou restrições legais. A detecção destes navios e procedimentos se tornou mais viável por meio do emprego de *softwares* de IA/ML como o *Artificial Intelligence Retraining In Space* (AIRIS), da Mitsubishi Heavy Industries (2024). North (2024) explica que esse sistema realiza a análise embarcada das imagens feitas pelo satélite, ao invés de enviá-las para estações terrestres para processamento. A IA identifica as imagens com alvos de interesse, como os *dark ships*, as seleciona e, só então, as transmite, otimizando o tempo de processamento e a quantidade de trânsito de dados. Além disso, a Mitsubishi Heavy Industries (2024) afirma que é possível treinar e retreinar o AIRIS, com base não só em atualizações de *software*, mas também no aprendizado do processo de detecção dos navios, que emprega as imagens satelitais e as cruza também com os dados disponíveis.

Assim como no emprego do poder aéreo, este tipo de emprego de IA para fins de IVR ocorre em conflitos, como na Guerra Russo-ucraniana, para avaliação de danos. Bondar (2024, p. 3, tradução nossa) afirma que as tecnologias de IA são cruciais para os ucranianos nessa tarefa, para a qual também são empregadas imagens de satélite para "análise de danos, perdas e devastação, e para estimar o esforço para a recuperação". Assim sendo, fica evidente que o emprego de IA otimiza e incrementa as capacidades de IVR dos sistemas espaciais de forma singular e decisiva.

Da mesma forma, a IA também impacta positivamente o emprego das comunicações satelitais, ainda mais quando associada ao ML. Esta combinação melhora a performance dos sistemas espaciais, bem como a sua eficiência e adaptabilidade, para prover serviços que atendam às demandas por conectividade e processamento de dados (Fontanesi *et al*, 2025). Um exemplo é o projeto da Agência Espacial Europeia, chamado *Open Source Satellite* (OPS-SAT), capaz de analisar sua própria telemetria e aplicar correções de transmissão, minimizando a intervenção humana e aumentando a confiança na eficiência da missão espacial (Intersputnik, 2025). Algo semelhante acontece nas missões que provêm capacidades Posicionamento, Navegação e Tempo (PNT), contra as quais se tenta negar ou impedir seu uso por meio de técnicas de *jamming* e *spoofing*, resultando na redução da acurácia do sinal de PNT ou a sua perda total – é o que se nomeia de *Navigation Warfare* (NavWar). Nestes casos, a IA, junto à ML, é empregada para monitorar o sinal de radiofrequência do dispositivo de PNT para identificar variações no sinal que sejam compatíveis com *jamming*/*spoofing*. Uma vez que seja identificada a possível interferência, o equipamento age para se proteger, meio da troca da frequência de operação, além de avisar o operador e o escalão superior, para que outras medidas possam ser tomadas, como tentar identificar a fonte emissora da interferência, visando neutralizá-la (McKinney, 2025).

As capacidades de Consciência Situacional Espacial também estão se beneficiando das potencialidades da IA. Tran *et al.* (2024) destacam que a IA contribui para integrar dados de sensores terrestres e em órbita a fim de formar um cenário situacional mais completo dos objetos que estão orbitando a Terra. A análise de imagens feita pela IA não só realiza o *data fusion* destes sensores, como também é capaz de identificar detalhes que escapam aos olhos humanos. Além disso, a aplicação do ML permite que se identifique qual sensor é o mais eficiente para determinada tarefa, otimizando, assim, o *sensor tasking* e reduzindo a produção desnecessária de dados e menos relevantes, obtendo-se o resultado pretendido de forma mais objetiva.

Para além das capacidades de sistemas espaciais, a IA também contribui para treinar operadores do poder espacial, como está acontecendo na *United States Space Force* (USSF). A ferramenta *Thinking Agent for Logical Operations and Strategy* (TALOS) emprega IA para simular um ambiente do domínio espacial que seja similar às operações e comportamentos dos sistemas espaciais reais. Além disso, o sistema também é capaz de simular ameaças aos sistemas espaciais (Easley, 2025).

Neste sentido, a IA tem se tornado tão importante para o emprego militar, que forças aeroespaciais, que a USSF, por exemplo, divulgou um Plano de Ação Estratégico para Dados e Inteligência Artificial para o ano de 2025, cujo objetivo principal é garantir a continuidade dos serviços de dados pelos sistemas espaciais (Estados Unidos da América, 2025).

3. Questões normativas atinentes ao emprego militar da IA

A crescente utilização da IA suscita diversos desafios no âmbito do emprego do Poder Aeroespacial, entre os quais se inserem as questões relacionadas à adequação normativa.

Por vezes, as transformações sociais ultrapassam a capacidade de o Direito fornecer respostas ágeis para a estabilização das novas demandas, tanto mais diante de questões envolvendo avanços tecnológicos.

No âmbito do Poder Aeroespacial, a IA promete a possibilidade de maior precisão nas operações militares, o aumento da autonomia de sistemas de combate e a otimização logística e de comunicações. O Plano Estratégico Militar da Aeronáutica 2024-2033/ PCA 11-47/2024 (Comando da Aeronáutica, 2024), diante das novas dinâmicas tecnológicas, prevê ações no sentido de incentivar empreendimentos e iniciativas voltadas ao desenvolvimento de tecnologias críticas, relacionadas ao emprego do Poder Aeroespacial.

Esse mesmo potencial, entretanto, traz em seu bojo desafios de ordem ética e jurídica, em especial no âmbito do Direito Internacional dos Conflitos Armados (DICA). Isso porque as normas em vigor foram construídas em um mundo no qual a guerra não contemplava a possibilidade de utilização de ferramentas destinadas a substituir a presença humana como única fonte de tomada de decisão.

Entre outros aspectos implicados na utilização da IA em operações aeroespaciais, o problema da responsabilidade figura entre um dos mais complexos, pois as normas internacionais, ao limitarem o uso da força, exigem a responsabilização por atos ilícitos, proibindo a utilização de armas que causem sofrimentos desnecessários e, essencialmente, que não sejam capazes de distinguir entre combatentes e não combatentes, a exemplo da Convenção sobre a Proibição do Uso, Armazenamento, Produção e Transferência de Minas Antipessoal e sobre sua Destruição (ONU, 1997).

As minas antipessoal são um demonstrativo de como armamentos podem ser programados para cumprir seu ciclo de funcionamento, independentemente da intervenção humana, mesmo que utilizem um mecanismo simples, como um termostato ou um sensor de movimento. Importante notar, assim, que a IA é um processo em constante aperfeiçoamento, condicionado à utilização de estímulos que auxiliam na tomada de decisão. Buchanan e Miller (2017, p. 5, tradução nossa), esclarecem que:

> ao contrário da programação tradicional de *software,* o ML envolve a programação de computadores para aprenderem sozinhos a partir de dados, em vez de instruí-los a realizar determinadas tarefas de determinadas maneiras.

Por conseguinte, a autonomia de uma máquina consiste na respectiva capacidade de realizar uma tarefa ou função por conta própria, no que, em um sistema de arma completamente autônomo, além do sentir, decidir e agir atribuído à máquina, a realização da tarefa ocorre sem a intervenção humana (Scharre, 2018).

Dessa maneira, em uma ação que utilize *drones*, por exemplo, a autonomia atribuída ao sistema irá reivindicar a averiguação da responsabilidade, seja pela coordenação da investida, seja com relação à possibilidade sempre presente de danos colaterais. O problema da autonomia reside, portanto, na possibilidade de a máquina reagir a um falso positivo, quando civis podem tornar-se alvos, uma vez confundidos com um objetivo militar legítimo (Scharre, 2018).

A lacuna normativa observada no direito internacional sobre o uso da IA em contextos como esses consiste, portanto, é uma questão a ser amplamente debatida nas esferas nacional e internacional, a fim de se buscar um padrão minimamente aceitável, no qual o ser humano possa ser preservado. Nesse sentido, o Comitê Internacional da Cruz Vermelha (CICV) aponta para as preocupações decorrentes do uso indiscriminado da IA, destacando a necessidade de se firmarem iniciativas voltadas a promover diálogos a respeito, especialmente vocacionados à criação de um possível acordo internacional acerca do tema (Stewart; Hinds, 2023)

Entre os instrumentos internacionais que tangenciam o problema da responsabilidade encontra-se o Manual de Tallinn 2.0 (OTAN, 2017, tradução nossa), focado essencialmente nas questões das operações cibernéticas, estabelecendo na Regra 6 que “um Estado tem responsabilidade jurídica internacional por uma operação cibernética que lhe seja atribuível e que constitua uma violação de uma obrigação internacional”. A despeito da relevância do Manual

de Tallinn como uma referência para uma possível regulação do uso da IA no contexto dos conflitos armados, sua abrangência é limitada, pois não detém o *status* de tratado internacional.

Diante dos dilemas decorrentes das lacunas normativas relacionadas ao emprego da IA, cumpre a observância das regras atualmente em vigor, adequadas, na medida das possibilidades, à necessidade, por exemplo, da delimitação da responsabilidade por ataques malsucedidos.

4. Recomendações para o Brasil

O Brasil possui iniciativas relevantes no que se refere à IA, havendo, inclusive, estratégias ministeriais para direcionar as iniciativas e o desenvolvimento desta tecnologia no País, como a Estratégia Brasileira de Inteligência Artificial (EBIA), lançada em 2021 (Brasil, 2021). Entretanto, considera-se importante o País estabelecer uma Estratégia desse tipo voltada especificamente para o setor espacial, com foco nas aplicações duais – civis e militares. Assim como os Estados Unidos da América, um documento deste tipo evidenciaria a centralidade da IA para o desenvolvimento de capacidades disruptivas no domínio espacial, que busquem garantir a continuidade e a resiliência dos serviços prestados por sistemas espaciais. Uma política brasileira nessa direção poderia contemplar diretrizes para a pesquisa e desenvolvimento (P&D), além do uso seguro e soberano de IA/ML em satélites de observação, comunicações, navegação e consciência situacional, incentivando, ainda, parcerias com atores privados e instituições científicas nacionais e internacionais.

Espera-se também priorizar investimentos em constelações satelitais equipadas com IA/ML embarcadas, a fim de reduzir a dependência das estações de solo para processamento de dados e aumentar a autonomia operacional dos sistemas espaciais, como faz o AIRIS, já mencionado neste artigo. Atualmente, o Brasil depende de *downlink* para realizar estas análises, o que representa uma desvantagem tática e estratégica, em termos militares, por exemplo. A incorporação de IA embarcada em satélites nacionais, existentes e futuros, pode reduzir um gargalo técnico e operacional da Defesa Espacial brasileira, e deve ser considerado por empresas estratégicas do setor aeroespacial brasileiro como a Visiona e a Alada.

Para além das questões de operação de sistemas espaciais, a Estratégia também deveria incentivar o uso de IA para o treinamento dos operadores espaciais. Desta forma, buscar-se-ia implementar ambientes de simulação com IA, para aumentar a qualificação técnica e a capacidade de resposta frente a cenários complexos e ameaças emergentes, como a ferramenta TALOS. É importante destacar que estes simuladores também são importantes para o planejamento de missões e o desenvolvimento e validação de doutrina. É uma empreitada que o País poderia pesquisar e desenvolver por meio de parcerias entre o Ministério da Defesa, a Agência Espacial Brasileira (AEB), Universidades Federais e Força Aérea Brasileira (FAB), garantindo a preparação de operadores para um ambiente espacial crescentemente automatizado e contestado.

Considerações finais

Apesar de apresentar capacidades superiores à mente humana em determinados aspectos — como tomar decisões, formular conclusões e realizar previsões —, a IA não possui consciência, sentimentos, ética ou valores, tampouco superou plenamente os seres humanos, cujo potencial permanece desconhecido pela ciência. Ademais, os sistemas de IA são imprecisos, inconsistentes, dinâmicos, emergentes e sujeitos a erros, ainda que sejam capazes de aprender continuamente. Em algumas situações, confundem objetos que qualquer ser humano distinguiria de forma rápida e simples, exigindo que seus resultados sejam reexaminados. Assim, tanto a IA quanto o Poder Aeroespacial representam mudanças paradigmáticas na forma de exercício do poder e da segurança.

De um lado, a IA amplia a capacidade de análise, previsão e tomada de decisão, ao mesmo tempo em que introduz vulnerabilidades decorrentes de sua imprevisibilidade e dependência de dados. Kissinger, Schmidt e Huttenlocher (2021) salientam que a ascensão da IA desloca o ser humano de seu papel exclusivo de intérprete e controlador da realidade, impondo novos desafios para a autonomia e a soberania. De outro lado, o Poder Aeroespacial assegura superioridade estratégica ao proporcionar maior alcance, mobilidade e letalidade, ainda que permaneça sujeito a limitações como custo elevado, dependência de infraestrutura e vulnerabilidade a condições ambientais.

A crescente integração da IA e ML aos sistemas espaciais está transformando profundamente o modo como o poder espacial é exercido, ampliando sua eficácia, autonomia e capacidade de resposta frente a desafios contemporâneos. Como demonstram os casos de Japão, Europa, Estados Unidos e Ucrânia, essas tecnologias já são empregadas de forma operacional em áreas críticas como IVR, comunicações satelitais, PNT, Consciência Situacional Espacial e treinamento de operadores.

Diante desse cenário, torna-se evidente que o Brasil precisa acelerar sua inserção nesse movimento, adotando políticas públicas específicas, fomentando a inovação nacional e promovendo sinergias entre defesa, academia e setor produtivo – tríplice hélice da inovação. O domínio dessas tecnologias não é apenas uma questão de modernização tecnológica, mas, sim, um fator decisivo para a soberania e a relevância do País no cenário espacial internacional.

Diante da rápida evolução das capacidades associadas à IA no domínio espacial, é fundamental que o Brasil avance de forma coordenada e estratégica no desenvolvimento e aplicação dessas tecnologias. Embora o País já possua uma diretriz nacional voltada à IA, a ausência de uma estratégia específica para o setor espacial representa uma lacuna que pode comprometer a competitividade e a autonomia nacional. A formulação de uma política dedicada permitiria alinhar esforços civis e militares em torno de objetivos comuns, promovendo inovação, soberania tecnológica e maior eficiência operacional. A experiência internacional

demonstra que a IA embarcada, o uso de algoritmos para IVR, a proteção dos sinais de PNT e o emprego de ambientes de simulação para formação de operadores são medidas viáveis e altamente impactantes. Portanto, a adoção de uma Estratégia Brasileira de IA para o Setor Espacial não é apenas oportuna, mas necessária para posicionar o Brasil como um ator relevante e resiliente no cenário espacial global.

Importante lembrar, finalmente, que a normatividade almejada não pode passar ao largo da ética intrinsecamente emaranhada na conformação da aplicação das regras do DICA, pois, conforme aduz Asaro (2012), o principal problema decorrente do uso de sistemas de armas letais autônomos reside na violação de direitos e da dignidade humana. Nesse sentido, defende o autor, a indispensável necessidade de manutenção da intervenção humana no processo de automação das máquinas, de maneira a não se delegar à IA a plena capacidade de decidir, mesmo porque, o ML não é capaz de nela incutir os primados da ética e da justiça.

Referências

ADAMS, Paul. Ataque de drones da Ucrânia: como a operação surpresa contra a Rússia muda a guerra. **BBC**, 5 jun. 2025. Disponível em: https://www.bbc.com/portuguese/articles/cqj7py14dplo. Acesso em: 6 ago. 2025.

ASARO, Peter. On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. **International Review of the Red Cross**, v. 94, n. 886, p. 687-709, 2012.

BONDAR, Kateryna. Understanding the Military AI Ecosystem of Ukraine. **Center for Strategic and International Studies**, 2024. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-11/241112_Bondar_Ukraine_Military.pdf. Acesso em: 30 jul. 2025.

BREWSTER, David. New satellite-based technologies a game changer for Indo-Pacific maritime security. Australian Strategic Policy Institute. **The Strategist**, 2022. Disponível em: https://www.aspistrategist.org.au/new-satellite-based-technologies-a-game-changer-for-indo-pacific-maritime-security. Acesso em: 6 jul. 2025.

BUCHANAN, Ben; MILLER, Taylor. **Machine Learning for Policymakers**: What It Is and Why It Matters. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017. Disponível em: https://www.belfercenter.org/publication/machine-learning-policymakers. Acesso em: 10 abr. 2025.

CHUN, Clayton K. S. **Aerospace power in the twenty-first century**: a basic primer. Colorado Springs: United States Air Force Academy; Maxwell Air Force Base: Air University Press, 2001.

BRASIL. Comando da Aeronáutica. **Plano Estratégico Militar da Aeronáutica 2024-2033** (PCA 11-47/2024). Brasília, DF: Comando da Aeronáutica, 2024. Disponível em: https://www.fab.mil.br/Download/arquivos/PEMAER_2024_2033.pdf. Acesso em: 11 ago. 2025.

Brasil. Estratégia Brasileira de Inteligência Artificial (EBIA). Brasília, DF: Ministério da Ciência, Tecnologia e Inovação (MCTI), 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 30 jul. 2025.

DOUHET, Giulio. **The command of the air**. Tradução: Dino Ferrari. Maxwell AFB: Air University Press, Curtis E. LeMay Center for Doctrine Development and Education, 2019.

DRONES de longo alcance: Ucrânia usa IA para atingir refinarias de petróleo. **Uol**, São Paulo, 3 abr. 2024. Disponível em: https://noticias.uol.com.br/internacional/ultimas-noticias/2024/04/03/ucrania-usa-drones-com-ia-para-atingir-industria-energetica-da-russia.htm. Acesso em: 6 ago. 2025.

EASLEY, Mikayla. Slingshot's new AI-enabled tool helps Space Force train for satellite ops. Space. DefenseScoop. 2025. Disponível em: https://defensescoop.com/2025/07/29/space-force-ai-training-satellite-operations-slingshot-aerospace-talos/. Acesso em: 30 jul, 2025.

ESTADOS UNIDOS DA AMÉRICA. **Data and Artificial Intelligence FY 2025 Strategic Action Plan**. United States Space Force, 2025. Disponível em: https://www.spaceforce.mil/Portals/2/Documents/SAF_2025/USSF_Data_and_AI_FY2025_Strategic_Action_Plan.pdf. Acesso em: 30 jul. 2025.

FONTANESI, Gianluca *et al*. Artificial Intelligence for Satellite Communication: a Survey. **IEEE Communications Surveys & Tutorials**, 2025. Disponível em: https://ieeexplore.ieee.org/document/10886927. Acesso em: 30 jul. 2025.

GRAY, Colin S. **Airpower for strategic effect**. Maxwell Air Force Base: Air University Press, Air Force Research Institute, 2012.

HUSAIN, Amir. The military applications of artificial intelligence in space. **Forbes**, 19 ago. 2024. Disponível em: https://www.forbes.com/sites/amirhusain/2024/08/19/the-military-applications-of-artificial-intelligence-in-space/. Acesso em: 30 jul. 2025.

INTERSPUTNIK. Artificial Intelligence and Modern Satellite Communications. 2025. Disponível em: https://www.intersputnik.int/member-directory/?post=artificial-intelligence-and-modern-satellite-communications. Acesso em: 30 jul. 2025.

IZZO, Dario; MEONI, Gabriele; GÓMEZ, Pablo; DOLD, Dominik; ZOECHBAUER, Alexander. Selected Trends in Artificial Intelligence for Space Applications. *In*: MADI, MATTEO; SOKOLOVA, Olga (Ed.). **Artificial Intelligence for Space**: AI4SPACE. Boca Raton: CRC Press, 2023. Disponível em: https://doi.org/10.1201/9781003366386. Acesso em: 30 jul. 2025.

KISSINGER, Henry A.; SCHMIDT, Eric; HUTTENLOCHER, Daniel. **The age of AI**: and our human future. New York: Little, Brown and Company, 2021.

LOCKHEED MARTIN. Top 10 'Out of this World' Space Technology Trends for 2025. News Hub. Lockheed Martin. 2024. Disponível em: https://www.lockheedmartin.com/en-us/news/features/2024/space-technology-trends-2025.html. Acesso em: 30 jul. 2025.

LONSDALE, David. Information power: Strategy, geopolitics, and the fifth dimension. **Journal of Strategic Studies**, v. 22, n. 2-3, p. 137-157, 1999.

MCKINNEY, Brooks. Artificial Intelligence helps protect troops in denied GPS Environments. Northrop Grumman, 2025. Disponível em: https://www.northropgrumman.com/what-we-do/mission-solutions/artificial-intelligence-and-machine-learning/protects-troops-in-denied-gps-environments. Acesso em: 30 jul. 2025.

MITSUBISHI HEAVY INDUSTRIES. MHI Develops an Onboard AI-Based Object Detector Utilizing a Next-Generation Space-Grade MPU. 2024. Disponível em: https://www.mhi.com/news/240306.html. Acesso em: 30 jul. 2025.

NORTH, Madeleine. How AI can help satellites track 'dark ships' from space. **Home. Spectra**, 2024. Disponível em: https://spectra.mhi.com/how-ai-can-help-satellites-track-dark-ships-from-space. Acesso em: 30 jul. 2025.

ONU. **Anti-Personnel Landmines Convention**. Ottawa: UNODA, 1997. Disponível em: https://disarmament.unoda.org/anti-personnel-landmines-convention/. Acesso em: 11 ago. 2025.

OTAN. NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **Tallinn manual 2.0 on the international law applicable to cyber operations.** Cambridge: Cambridge University Press, 2017. Disponível em: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9. Acesso em: 7 ago. 2025.

REINECKE, Adriana; DUTCHER, Mizumi Fujita. The Possibilities for Quad Cooperation in Space. **The Diplomat**. Asia Defense. Security. 2025. Disponível em: https://thediplomat.com/2023/05/the-possibilities-for-quad-cooperation-in-space/. Acesso em: 6 jul. 2025.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência Artificial**: uma abordagem moderna. Tradução: Daniel Vieira e Flávio Soares Corrêa da Silva. 4 ed. Rio de Janeiro: LTC/GEN, 2022.

SCHARRE, Paul. **Army of none***:* autonomous weapons and the future of war. New York: W. W. Norton & Company, 2018.

STEWART, Ruben; HINDS, Georgia. Algoritmos da guerra: uso de inteligência artificial para tomar decisões em conflitos armados. **Humanitarian Law & Policy Blog**, 1 dez. 2023. Disponível em: https://blogs.icrc.org/law-and-policy/pt-br/2023/12/01/algoritmos-da-guerra-uso-de-inteligencia-artificial-para-tomar-decisoes-em-conflitos-armados/. Acesso em: 11 ago. 2025.

TRAN, Jonathan; PURI, Prateek; LOGUE, Jordan; JACQUES, Anthony; ZHANG, Li Ang; LANGELAND, Krista; NACOUZI, George; BRIGGS, Gary J. Artificial Intelligence and Machine Learning for Space Domain Awareness: the development of two Artificial Intelligence case studies. Rand Corporation. 2024. Disponível em: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2318-2/RAND_RRA2318-2.pdf. Acesso em: 30 jul. 2025.

VITORIO, Tamires. Como a Nvidia alcançou os US$ 4 trilhões e se tornou a empresa mais valiosa do mundo. Exame. Invest. 2025. Disponível em: https://exame.com/invest/mercados/como-a-nvidia-alcancou-os-us-4-trilhoes-e-se-tornou-a-empresa-mais-valiosa-do-mundo. Acesso em: 7 ago. 2025.