



POLICY REPORT · 2026

Inteligência Artificial

e

Cibersegurança

*Riscos sistêmicos, governança e caminhos
para uma cooperação estratégica Brasil e Reino Unido*

TURING CLUB · CAPÍTULO BRASIL

Embaixada Britânica · Brasília

12 de março de 2026

Ressalvas



Este relatório constitui uma síntese das discussões abertas realizadas durante o seminário do Turing Club · Capítulo Brasil. O documento reflete a diversidade de perspectivas, temas e possíveis áreas de diálogo futuro levantados por participantes de diferentes setores.

As opiniões e visões aqui registradas correspondem às manifestações individuais das pessoas que participaram do diálogo e não refletem a posição institucional dos órgãos, empresas, universidades ou demais organizações eventualmente mencionadas ou representadas pelos participantes.

Não deve ser interpretado como uma declaração de política pública do Governo Britânico, como uma proposta formal do Governo Britânico, nem como compromisso do Governo Britânico ou de qualquer outro participante com posições, recomendações, programas ou formas específicas de cooperação futura.

As referências a instituições, publicações ou experiências do Reino Unido são incluídas apenas para fins de contextualização, comparação e intercâmbio de experiências.

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME (INCC)

Inteligência Artificial e Cibersegurança: riscos sistêmicos, governança e caminhos para uma cooperação estratégica Brasil e Reino Unido., Brasília ; São Paulo : INCC, 2026.

32 p. : il. color.

Relatório elaborado pelo Instituto Nacional de Combate ao Crime (INCC) no âmbito do Turing Club · Capítulo Brasil, iniciativa apoiada pelo Governo Britânico em colaboração com o INCC.

1. Inteligência Artificial. 2. Cibersegurança. 3. Governança digital. 4. Cooperação Brasil e Reino Unido. I. Título.

Sumário

1. Sumário Executivo	3
2. Introdução: Arquitetura do Debate e Relevância Estratégica	5
3. Inteligência Artificial e a Reconfiguração do Ecossistema de Ameaças.....	7
4. A Dualidade da IA: Amplificação do Risco e Potencial de Defesa	10
5. Desinformação, IA e a Fragilidade da Confiança Democrática	13
6. O Impacto da Tecnologia Deepfake e Respostas Institucionais	14
7. Brasil: Coordenação Institucional, Marco Normativo e Desafios	16
8. Governança Internacional de IA e Cibersegurança	19
9. Cooperação Brasil e Reino Unido: Uma Agenda Estratégica	22
10. Áreas Estratégicas para o Brasil e Oportunidades de Cooperação	25
10.1 Explorar caminhos para uma governança integrada	26
10.2 Integração regulatória entre IA e cibersegurança	27
10.3 Fortalecimento de competências em IA e cibersegurança	28
10.4 Aplicações de IA para resiliência de infraestruturas críticas	29
10.5 Compartilhamento de inteligência de ameaças	30
10.6 Centralidade da integridade informacional.....	31
10.7 Consolidar agenda estruturada de cooperação Brasil e Reino Unido	31
10.8 Padrões e certificações de segurança: referências internacionais e boas práticas.....	32
11. Conclusão	33
Referências	35

1. Sumário Executivo

A convergência entre inteligência artificial (IA) e cibersegurança representa uma transformação estrutural no ambiente digital global, alterando de forma profunda a natureza dos riscos, a dinâmica entre agentes ofensores e defensores e os fundamentos da governança tecnológica.

Diferentemente de ciclos anteriores de inovação, a IA não apenas amplia capacidades existentes, mas tende a reduzir as barreiras técnicas para a execução de ataques sofisticados, acelerar a exploração de vulnerabilidades e ampliar a escala de operações maliciosas. Esse movimento ocorre em um contexto de crescente dependência de infraestruturas digitais críticas e de intensificação da competição tecnológica entre Estados.

O *Global Risks Report 2025*, publicado pelo World Economic Forum (2025), classifica a desinformação e os ataques cibernéticos entre os principais riscos globais de curto prazo. Em direção convergente, o relatório do *National Cyber Security Centre* sobre o impacto da IA na ameaça cibernética até 2027 (NCSC, 2025a) projeta aumento tanto no volume quanto no impacto das intrusões, à medida que a tecnologia aprimora táticas, técnicas e procedimentos já existentes.

No Brasil, esse cenário se insere em um ambiente institucional em processo de evolução, marcado por avanços relevantes, como a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet, a Estratégia Brasileira de Inteligência Artificial (EBIA) e a Estratégia Nacional de Segurança Cibernética (E-Ciber), e pelo contínuo fortalecimento da coordenação, da implementação e do desenvolvimento de capacidades.

Paralelamente, o país se encontra em uma fase significativa de consolidação normativa, refletida na tramitação do Projeto de Lei de Regulamentação da Inteligência Artificial no Congresso Nacional e do Marco Legal da Cibersegurança no Senado Federal. Esses debates legislativos apontam para possíveis ajustes estruturais na governança digital brasileira, cuja implementação oferece oportunidades para ampliar a integração entre os diferentes instrumentos e atores envolvidos.

O lançamento do Turing Club · Capítulo Brasil, iniciativa apoiada pelo Governo Britânico, destacou, a partir das discussões realizadas, que os riscos associados à inteligência artificial transcendem a dimensão técnica, afetando diretamente a integridade informacional, a resiliência institucional e a confiança em sistemas democráticos.

Os diálogos iniciais também apontaram percepções compartilhadas de que, no curto prazo, a IA pode ampliar as capacidades de agentes maliciosos, reforçando a importância de abordagens orientadas à antecipação de riscos, à prevenção e ao desenvolvimento de modelos de governança adaptativa, em consonância com debates internacionais em curso.

Mensagens-chave

- A IA reduz barreiras técnicas para operações ofensivas e amplia a escala de campanhas de desinformação, reforçando a necessidade de governança adaptativa.
- O Brasil dispõe de um arcabouço regulatório e estratégico relevante em IA e cibersegurança, com oportunidades para promover maior integração entre iniciativas e instrumentos em desenvolvimento.
- A cooperação Brasil e Reino Unido oferece espaço para co-construção de boas práticas, ancorada na expertise britânica, incluindo o NCSC e o *AI Security Institute* (AISi).
- A integridade informacional emerge como uma forma de infraestrutura crítica e merece tratamento estratégico integrado.

Contexto global · números que orientam a agenda

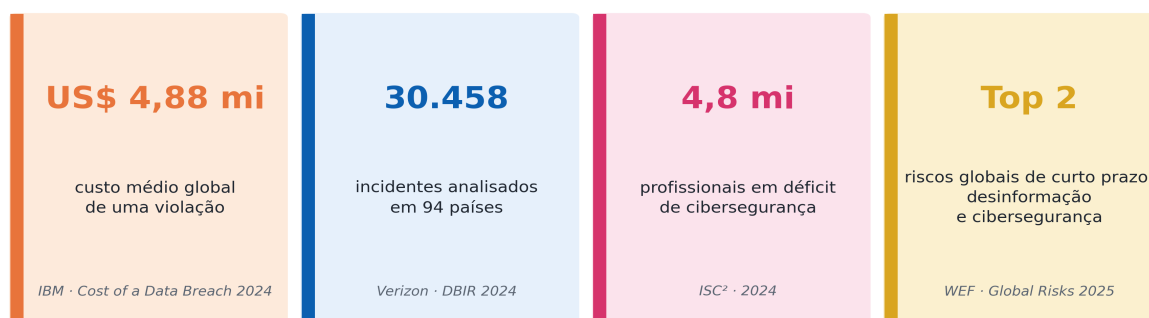


Figura 1: Contexto global da agenda de cibersegurança e IA. Fontes: IBM Cost of a Data Breach 2024, Verizon DBIR 2024, ISC² 2024, WEF Global Risks 2025.

2. Introdução: Arquitetura do Debate e Relevância Estratégica

O Turing Club · Capítulo Brasil foi concebido como um espaço multissetorial de alto nível voltado à discussão de temas estratégicos na interface entre tecnologias emergentes, incluindo inteligência artificial, cibersegurança e propriedade intelectual, com o objetivo de aproximar perspectivas institucionais distintas e fomentar a construção de agendas comuns entre Brasil e Reino Unido.

Realizado na Embaixada Britânica em Brasília, o primeiro encontro reuniu representantes com atuação em formulação de políticas públicas, pesquisa acadêmica e operação de sistemas críticos. A composição plural, com contribuições de instâncias de governo, da diplomacia, do setor privado e da academia, articuladas por moderação especializada, permitiu uma análise multidimensional dos desafios associados à convergência entre IA e cibersegurança.



Foto: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Imagem 1: Abertura do Turing Club · Capítulo Brasil. Embaixada Britânica, Brasília, 12 de março de 2026.

Participaram do debate Guilherme Fitzgibbon, assessor especial do Ministério das Relações Exteriores com atuação em governança internacional de tecnologias emergentes, incluindo IA, e *alumnus* do programa Chevening¹; Danielle Ayres, representante do Gabinete de Segurança Institucional, com foco em segurança da informação e coordenação de políticas públicas; Alexandre Cardoso, da British Telecom, trazendo a perspectiva operacional de um grupo multinacional com atuação em mercados com diferentes níveis de maturidade digital; e a Dra. Beatriz Buarque, da London School of Economics, com contribuição centrada nas dimensões éticas, sociais e políticas da inteligência artificial.

A discussão foi mediada por Eduardo Paranhos, especialista em direito digital, inteligência artificial e governança, que lidera o grupo de trabalho de IA da Associação Brasileira das Empresas de Software (ABES) e coordena o eixo de regulação da Estratégia Brasileira de IA.

A dinâmica do encontro, estruturada a partir de perguntas orientadoras e intervenções breves, favoreceu um debate fluido e interativo, permitindo a exposição de diferentes perspectivas e a identificação de convergências e divergências relevantes.

A abordagem adotada favoreceu uma discussão aprofundada e analítica. As reflexões indicaram que a convergência entre inteligência artificial e cibersegurança não se configura como um desafio isolado ou setorial, mas como uma questão de natureza sistêmica, envolvendo dimensões

¹Chevening: programa internacional de bolsas de estudos do Governo Britânico voltado a lideranças emergentes de mais de 160 países, com forte rede de alumni ativa no Brasil, particularmente em áreas de política pública, diplomacia e tecnologia.

técnicas, institucionais, econômicas e geopolíticas, o que reforça a necessidade de respostas coordenadas e multidisciplinares.

A composição plural do grupo permitiu uma análise abrangente dos desafios associados à convergência entre inteligência artificial e cibersegurança. O diálogo incorporou perspectivas institucionais, acadêmicas e operacionais, abordando desde questões de coordenação e capacitação no setor público até implicações éticas, sociais e democráticas, bem como desafios práticos enfrentados por organizações que operam em ambientes digitais complexos.

CONTEXTO

Sobre o Turing Club · Capítulo Brasil

Inspirado em Alan Turing e na tradição britânica de inteligência computacional, o Turing Club · Capítulo Brasil materializa, em formato bilateral, o caráter exploratório e colaborativo proposto pelo Governo Britânico para o diálogo internacional sobre IA. A iniciativa busca facilitar o intercâmbio de boas práticas e a co-construção de agendas em comum entre Brasil e Reino Unido, em sintonia com os esforços internacionais de governança e segurança digital.

3. Inteligência Artificial e a Reconfiguração Estrutural do Ecossistema de Ameaças

A inteligência artificial está promovendo uma transformação qualitativa no ecossistema de ameaças cibernéticas, alterando não apenas a escala, mas a natureza dos riscos enfrentados por Estados, empresas e indivíduos. Diferentemente de ciclos anteriores de inovação tecnológica, nos quais a sofisticação de ataques estava diretamente associada ao nível de especialização técnica dos agentes, a IA tende a reduzir essa barreira, permitindo que atores com menor conhecimento técnico executem operações complexas. Essa avaliação é sustentada por Parihar (2025), que analisa como sistemas de IA aplicados à cibersegurança alteram tanto os mecanismos de detecção e resposta quanto os padrões de ataque observados.

Ao longo das discussões do Turing Club, contribuições acadêmicas observaram que ferramentas de inteligência artificial permitem, por meio de interações aparentemente simples, acessar conhecimento operacional sensível, incluindo formas de explorar vulnerabilidades ou desenvolver artefatos ilícitos. No debate, esse fenômeno foi descrito como uma democratização do risco tecnológico, na qual o conhecimento especializado deixa de ser um fator limitante para a ação maliciosa.

Ecossistema de ameaças amplificadas por IA



Figura 2: Ecossistema de ameaças amplificadas por IA. Elaboração própria a partir das discussões do Turing Club.

Essa leitura ecoa a avaliação do *National Cyber Security Centre*² (NCSC, 2025a) sobre o impacto da IA na ameaça cibernética até 2027, segundo a qual, no curto prazo, apenas atores estatais altamente capazes conseguirão explorar plenamente o potencial ofensivo da IA, muito embora a proliferação de ferramentas habilitadas por IA tenda a ampliar o acesso a tais capacidades por uma gama mais ampla de agentes. Em complemento a esse diagnóstico de ameaças, o *Code of Practice for the Cyber Security of AI*³, publicado pelo *Department for Science, Innovation and Technology* do Reino Unido (DSIT, 2025a), estabelece princípios de segurança de linha de base (*baseline*) aplicáveis a todo o ciclo de vida de sistemas de IA.

A literatura internacional confirma essa tendência. Como demonstra Bisht (2024) ao analisar o *Data Breach Investigations Report 2024* da Verizon, foram examinados 30.458 incidentes de segurança em 94 países, com 10.626 violações confirmadas, evidenciando a escala e a recorrência das ameaças. Complementarmente, o *Cost of a Data Breach 2024* publicado pela IBM (2024) aponta que o custo médio global de uma violação atingiu US\$ 4,88 milhões, refletindo não apenas a frequência dos ataques, mas seu impacto econômico crescente.

No contexto brasileiro, dados consolidados pelo Instituto Nacional de Combate ao Crime Cibernético (INCC) e por relatórios setoriais indicam um aumento consistente na sofisticação de ataques digitais,

²NCSC (National Cyber Security Centre): órgão britânico responsável pela cibersegurança nacional, criado em 2016 como braço público da GCHQ. Publica orientações, avaliações de ameaças e diretrizes técnicas para os setores público e privado do Reino Unido.

³Code of Practice for the Cyber Security of AI (DSIT, 2025): código de prática voluntário criado pelo Department for Science, Innovation and Technology (Reino Unido) em conjunto com o NCSC. Seu escopo abrange todo o ciclo de vida de sistemas de IA, da concepção ao descomissionamento, e serviu de base para a especificação técnica ETSI TS 104 223, referência internacional emergente.

particularmente em fraudes financeiras e engenharia social. A incorporação de inteligência artificial nesses processos amplia sua eficiência, permitindo a automatização de ataques em larga escala, a personalização de abordagens e a exploração mais rápida de vulnerabilidades.

Olhares trazidos por organizações do setor privado destacaram que essa transformação se manifesta no ambiente corporativo, especialmente nos desafios associados à gestão de incidentes e à proteção de infraestruturas críticas. Episódios envolvendo ameaças internas, como tentativas de comprometimento de sistemas por funcionários, evidenciam que a superfície de ataque não se limita a agentes externos. A IA potencializa esse risco ao facilitar a exploração de credenciais, automatizar processos internos e contornar mecanismos de segurança.

Esse cenário sugere uma inversão parcial da lógica tradicional de cibersegurança. Historicamente, a defesa se beneficiava da assimetria a seu favor, exigindo que o atacante encontrasse uma vulnerabilidade específica, enquanto o defensor poderia se apoiar em camadas de proteção. Com a IA, essa assimetria tende a se reduzir, favorecendo agentes ofensores que podem testar múltiplas vulnerabilidades simultaneamente e adaptar suas estratégias em tempo real.

A implicação direta para políticas públicas e estratégias organizacionais é a necessidade de migração de modelos reativos para modelos preditivos e preventivos. Conceitos como *security by design*, *zero trust architecture* e monitoramento contínuo⁴ deixam de ser boas práticas desejáveis e passam a constituir requisitos fundamentais para a resiliência digital, conforme evidenciado tanto por Parihar (2025), na literatura acadêmica, quanto pelas orientações práticas do NCSC (2023) para o desenvolvimento seguro de sistemas de IA.

Da resposta reativa à defesa preditiva · maturidade institucional em cibersegurança

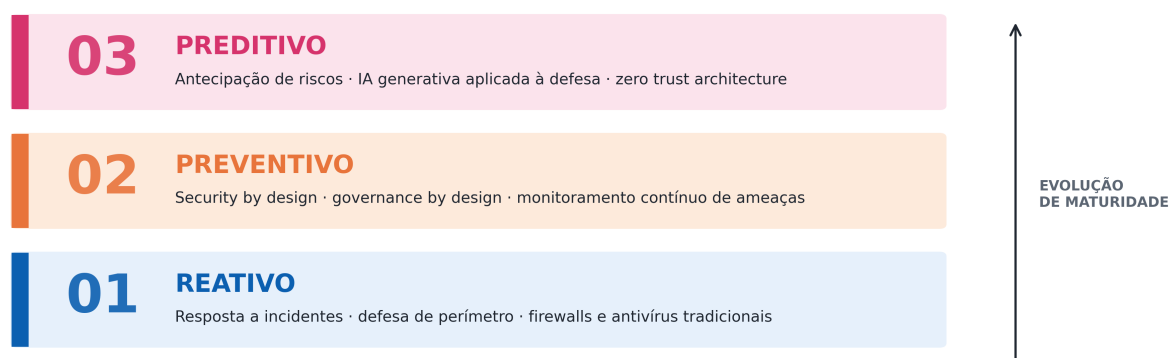


Figura 3: Evolução de maturidade institucional em cibersegurança: de modelos reativos a modelos preditivos.

⁴Security by design: incorporação de requisitos de segurança desde a concepção de sistemas. Zero trust architecture: princípio que assume ausência de confiança implícita entre dispositivos e usuários, exigindo verificação contínua. Monitoramento contínuo: coleta e análise permanente de eventos para detecção e resposta rápida a incidentes (NCSC, 2023).

4. A Dualidade da Inteligência Artificial: Amplificação do Risco e Potencial de Defesa

Um dos eixos centrais do debate foi a dualidade inerente à inteligência artificial no campo da cibersegurança: a mesma tecnologia que potencializa ataques pode, simultaneamente, fortalecer mecanismos de defesa. No Turing Club, contribuições trazidas por perspectivas governamentais e diplomáticas sublinharam que a capacidade de defesa baseada em IA depende diretamente do nível de maturidade institucional e tecnológica dos países. Essa leitura é convergente com a análise de Akhtar et al. (2021), que examina o uso da IA como capacidade dual em cibersegurança, ora ampliando o potencial defensivo, ora sofisticando as ferramentas ofensivas.

A dualidade da IA · simultaneamente vetor de risco e capacidade de defesa

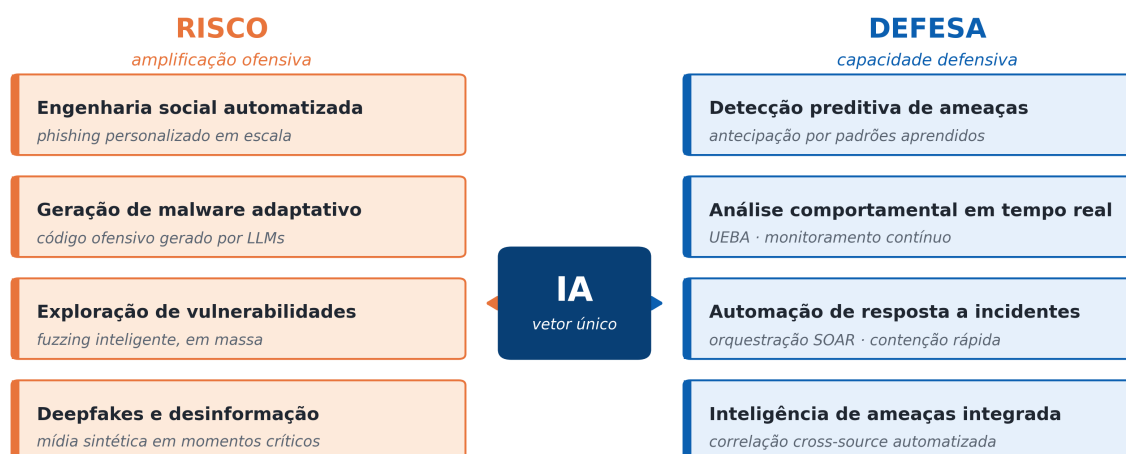


Figura 4: Dualidade da IA: vetores de risco e capacidades de defesa convivem em um mesmo conjunto de tecnologias.

Em contextos em que há investimento em infraestrutura, qualificação de pessoal e desenvolvimento de soluções próprias, a IA pode representar um avanço significativo na capacidade de detecção e resposta a incidentes. Na ausência dessas condições, a tecnologia tende a ampliar vulnerabilidades, tornando Estados e organizações mais expostos a ataques sofisticados.

Essa assimetria é um elemento central do debate contemporâneo sobre segurança digital. Enquanto agentes ofensores podem concentrar seus esforços exclusivamente na exploração de vulnerabilidades, agentes defensores precisam equilibrar múltiplas dimensões, incluindo proteção de sistemas, continuidade operacional, conformidade regulatória e experiência do usuário.

Durante as discussões do Turing Club, foi destacado, na perspectiva governamental, que o desenvolvimento de soluções baseadas em IA para uso legítimo exige que seus criadores considerem, simultaneamente, o potencial de uso indevido. Esse alinhamento entre debate e literatura é reforçado

pelo estudo de Radanliev et al. (2024), que examina frameworks de segurança para o desenvolvimento de soluções de IA aplicadas à cibersegurança. Essa necessidade de antecipação, incorporando riscos desde a concepção, reforça a importância de abordagens como *safety by design* e *governance by design*⁵, que integram considerações de segurança e governança ao ciclo de vida das tecnologias.

Referências internacionais ilustram a operação prática desse princípio. O Cabinet Office (2025) do Reino Unido, por meio do *Mitigating Hidden AI Risks Toolkit*, oferece um modelo passo a passo para identificar, monitorar e mitigar riscos comportamentais e organizacionais associados à adoção de IA. De forma complementar, o DSIT (2025a), no *AI Cyber Security Code of Practice*, estabelece princípios de segurança aplicáveis a todo o ciclo de vida de sistemas de IA, da concepção ao descomissionamento. Já o *AI Security Institute* (AISI, 2025), instituto público britânico com atuação em pesquisa e avaliação de riscos sistêmicos de IA, reforça a intenção do Reino Unido de tratar a segurança da IA como tema primário de política pública.

A visão trazida pelo setor privado durante o encontro evidenciou que mesmo organizações com estruturas avançadas de segurança enfrentam desafios significativos na implementação de sistemas de defesa baseados em IA. A necessidade de equilibrar automação e controle, evitar falsos positivos e garantir continuidade operacional torna esse processo complexo e altamente dependente de governança e maturidade institucional.

Nesse contexto, a análise sugere que a inteligência artificial não é inerentemente um vetor de risco ou de proteção. Seus efeitos dependem, em grande medida, da qualidade dos arranjos de governança, da maturidade institucional e do nível de integração das políticas públicas. Diferentes níveis de desenvolvimento dessas capacidades podem resultar em impactos assimétricos, tanto em termos de benefícios quanto de riscos associados à adoção da tecnologia.

REFERÊNCIA BRITÂNICA

Referências em destaque

- **NCSC, *Guidelines for secure AI system development* (2023):** princípios para projetar, desenvolver, implantar e operar sistemas de IA com segurança desde a concepção.
- **DSIT, *AI Cyber Security Code of Practice* (2025):** primeiro código de prática voluntário voltado à cibersegurança de sistemas de IA, com versão internacionalizada via ETSI TS 104 223.
- **Cabinet Office, *Mitigating Hidden AI Risks Toolkit* (2025):** orientação prática para mitigar riscos comportamentais e organizacionais decorrentes da adoção de IA.
- **AI Security Institute (AISI, 2025):** instituição pública voltada a avançar a base científica de evidências sobre os riscos mais sérios da IA.

⁵Safety by design: incorporação de considerações de segurança do usuário e mitigação de danos desde a concepção do sistema. Governance by design: princípio análogo aplicado à governança, com definição prévia de regras, papéis e mecanismos de supervisão desde a arquitetura da tecnologia.

5. Desinformação, IA e a Fragilidade da Confiança Democrática

A relação entre inteligência artificial e desinformação foi um dos pontos mais sensíveis e estratégicos do debate, evidenciando que os riscos associados à IA extrapolam a dimensão técnica e alcançam o núcleo da estabilidade institucional e democrática.

A capacidade de gerar conteúdo sintético altamente convincente, incluindo áudio, vídeo e texto, levanta preocupações sobre a manipulação da informação e a erosão da confiança pública nas instituições e plataformas de mídia. O Reino Unido tem tratado essa questão como prioridade política: as orientações sobre inteligência artificial (2024) e a nota do NCSC (2025b) sobre preservação da integridade na era da IA generativa ressaltam que a proliferação desses sistemas amplifica a perda de confiança em dados e mídias e intensifica riscos reputacionais e de engenharia social.

A percepção de riscos e a confiança nas tecnologias de IA são fundamentais para sua aceitação social. Como aponta Gerlich (2023), essa dimensão é destacada também pelos princípios de IA confiável da Comissão Europeia, que enfatizam segurança e governança responsável. A revisão de Lockey et al. (2021) sobre confiança em sistemas de IA, por sua vez, indica que a construção dessa confiança depende de mecanismos adequados de governança, transparência e gestão de riscos, bem como da consideração das vulnerabilidades e expectativas de diferentes partes interessadas.

Em linha com essa perspectiva, o *Trusted Third-Party AI Assurance Roadmap*, publicado pelo DSIT (2025b) em setembro de 2025, propõe modelos de garantia de qualidade para sistemas de IA e busca estruturar um ecossistema britânico de *AI assurance* que possa servir de referência internacional. A confiança pode ser comprometida por fatores como a opacidade dos algoritmos e a limitada responsabilização em sua implementação, aspectos que exigem reflexão cuidadosa sobre os impactos da IA na desinformação e na estabilidade social.

Reforçando esse cenário, o *Global Risks Report 2025*, publicado pelo World Economic Forum (2025), posiciona desinformação e ciberataques entre os principais riscos globais de curto prazo, sublinhando seu potencial de impactar processos democráticos e gerar instabilidade social.

6. O Impacto da Tecnologia *Deepfake* e Respostas Institucionais



Foto: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Imagem 2: Plateia atenta às contribuições sobre integridade informacional e deepfakes (mídia sintética) durante o Turing Club.

As tecnologias de *deepfake* e os modelos generativos permitem a criação de narrativas falsas com alto grau de verossimilhança, dificultando a distinção entre informação legítima e manipulada. Esse fenômeno tem implicações profundas sobre a integridade das informações circulantes.

Olhares acadêmicos compartilhados durante o debate, inclusive a partir de perspectivas vinculadas à tradição britânica de pesquisa em risco e democracia, ilustraram cenários em que conteúdos sintéticos podem ser disseminados em momentos críticos, como períodos eleitorais ou crises institucionais.

A literatura acadêmica corrobora essas preocupações trazidas ao debate: o estudo de Pandey (2025), intitulado "AI's Dark Side: The Rise of Deepfakes and the Battle for Truth", analisa como a proliferação de *deepfakes* vem intensificando os desafios de manipulação da opinião pública e a erosão da confiança em ecossistemas informacionais, oferecendo evidência acadêmica independente dos relatos qualitativos apresentados pelos participantes.

A dificuldade de verificar a autenticidade de conteúdos em tempo real pode comprometer a capacidade de resposta de governos e a confiança da população nas instituições. Esse desafio é amplamente reconhecido em análises internacionais. O NCSC (2024), na seção *Artificial Intelligence* de seu portal, organiza orientações e advertências para gestores e tomadores de decisão, destacando

explicitamente a manipulação de mídia para campanhas de *deepfake* como vetor crescente de risco. De forma complementar, o NCSC (2025c), por meio da coleção *Defending Democracy*, consolida orientações voltadas a indivíduos de alto risco e a organizações responsáveis por eleições.

No contexto brasileiro, essa discussão se conecta diretamente com o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios para o uso da internet, e com debates regulatórios em curso sobre a responsabilidade das plataformas digitais. A crescente sofisticação das tecnologias de IA convida à atualização dessas discussões, incorporando novos vetores de risco e mecanismos de mitigação.

PARA REFLEXÃO

Um ponto particularmente relevante do debate

A democracia pode ser tratada como uma forma de infraestrutura crítica. Assim como sistemas de energia, telecomunicações e finanças, o ambiente informacional é essencial para o funcionamento do Estado e da sociedade, sendo, portanto, suscetível a ataques e demandando proteção estruturada.

Esse diagnóstico, formulado durante o debate, aponta para a importância de abordagens integradas que articulem cibersegurança, comunicação institucional, educação digital e regulação de plataformas. Ele encontra ressonância na literatura acadêmica: Modupeola et al. (2025), ao propor um índice de detecção de *deepfakes* e cibersegurança, demonstram como a coordenação entre esses domínios contribui para mitigar riscos informacionais preservando, ao mesmo tempo, direitos fundamentais e a confiança no ambiente digital.

7. Brasil: Coordenação Institucional, Marco Normativo e Desafios de Implementação

O Brasil não parte de um vazio institucional no que diz respeito à governança digital. Ao contrário, ao longo da última década, o país construiu um conjunto relevante de instrumentos normativos e estratégicos voltados à regulação da internet, proteção de dados, transformação digital e segurança da informação. Como evidenciado ao longo do debate, o desafio central tende a estar menos na ausência de políticas e mais nas oportunidades de articulação e implementação entre elas. Essa leitura converge com a análise de Nicolás e Sampaio (2024) sobre o impacto da automação por IA em políticas públicas no Brasil, que também identifica os desafios de coordenação como elemento central da agenda brasileira.

Linha do tempo · arcabouço regulatório brasileiro de IA e cibersegurança



Figura 5: Linha do tempo do arcabouço regulatório brasileiro em IA e cibersegurança (2014-2026).

O Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios fundamentais para o uso da internet no Brasil, incluindo a proteção da liberdade de expressão, a neutralidade de rede e a responsabilidade dos agentes envolvidos no ecossistema digital. Posteriormente, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) introduziu um marco regulatório abrangente para o tratamento de dados, alinhando o país a padrões internacionais de proteção de privacidade. Bioni, Garrote e Guedes (2023), em estudo sobre interoperabilidade regulatória, demonstram como esse marco brasileiro se articula com os movimentos regulatórios locais, regionais e globais em IA.

Mais recentemente, o governo federal brasileiro avançou na formulação de estratégias específicas para inteligência artificial e segurança cibernética. A Estratégia Brasileira de Inteligência Artificial (EBIA), instituída pelo Ministério da Ciência, Tecnologia e Inovações, define diretrizes para o desenvolvimento e uso ético da IA no contexto brasileiro, com foco em inovação, competitividade e inclusão. Paralelamente, a Estratégia Nacional de Segurança Cibernética (E-Ciber), parte da Política Nacional de Segurança da Informação (PNSI), estabelece objetivos para fortalecer a resiliência do país frente a ameaças digitais.

Governança de Inteligência Artificial e Cibersegurança no Brasil

À luz desse arcabouço, as discussões no âmbito do Turing Club sugeriram que as diferentes iniciativas em curso no Brasil se encontram em estágios distintos de desenvolvimento e articulação. Nesse contexto, foi ressaltado durante o diálogo que um dos desafios recorrentes no debate público diz respeito à articulação entre múltiplas agendas, incluindo inteligência artificial, cibersegurança, proteção de dados e transformação digital, que evoluem em paralelo no âmbito estatal.

A necessidade de maior alinhamento entre esses domínios assume particular relevância agora, marcado pela tramitação de propostas legislativas estruturantes. O Projeto de Lei de Regulamentação da Inteligência Artificial, atualmente em discussão no Congresso Nacional, busca estabelecer princípios, direitos e deveres para o desenvolvimento e uso da IA no país, incluindo

dispositivos relacionados à classificação de riscos e à atribuição de responsabilidades, dimensões que o trabalho de Cavalcante (2024), publicado pela Blavatnik School of Government (Oxford), analisa sob a ótica de *accountability* algorítmica. Paralelamente, o Marco Legal da Cibersegurança, em debate no Senado Federal, pretende consolidar diretrizes para proteção de infraestruturas críticas, resposta a incidentes e coordenação entre diferentes atores, tema abordado por Krasodonski et al. (2024) em sua coletânea sobre governança global responsável de IA.

Um aspecto destacado durante o debate foi a importância de promover a articulação entre as diferentes iniciativas em desenvolvimento nas áreas de inteligência artificial e cibersegurança. À medida que esses marcos normativos avançam, oportunidades de alinhamento entre instrumentos regulatórios, políticas públicas e estruturas de governança podem contribuir para maior coerência e efetividade em sua implementação.

PARA REFLEXÃO

Janela legislativa: a importância da articulação

- **PL de IA:** classificação de risco, deveres dos agentes e supervisão.
- **Marco Legal da Cibersegurança:** proteção de infraestruturas críticas, resposta a incidentes, coordenação.
- **LGPD / ANPD:** proteção de dados pessoais e governança de tratamento de dados.
- **Referência britânica:** o DSIT (2025c) apresentou, em novembro de 2025, o *Cyber Security and Resilience Bill*⁶, instrumento que ilustra como uma atualização ampla do regime da Network and Information Systems Directive (NIS)⁷ pode aproximar as agendas de segurança digital, IA e infraestrutura crítica em um único marco legal.

Além da dimensão normativa, o debate destacou desafios estruturais relacionados à capacidade estatal. A escassez de profissionais qualificados em cibersegurança é um dos principais gargalos. Dados do International Information System Security Certification Consortium (ISC2, 2024) indicam um déficit global de aproximadamente 4,8 milhões de profissionais na área, cenário que se reflete de forma particularmente aguda em países em desenvolvimento.

No Brasil, análises produzidas pelo INCC apontam que a dificuldade de retenção de talentos no setor público compromete a capacidade de implementação de políticas e resposta a incidentes. Diferenças de remuneração em relação ao setor privado, combinadas com a rápida evolução

⁶Cyber Security and Resilience Bill: em tradução livre, "Projeto de Lei de Cibersegurança e Resiliência". Apresentado pelo Reino Unido em novembro de 2025, atualiza o regime NIS (Network and Information Systems) e aproxima as agendas de segurança digital, IA e proteção de infraestrutura crítica. Disponível em: gov.uk/collections/cyber-security-and-resilience-bill

⁷Network and Information Systems (NIS): diretiva europeia (Diretiva 2016/1148) que estabeleceu o primeiro regime obrigatório de segurança para operadores de serviços essenciais e prestadores de serviços digitais na União Europeia. O Reino Unido, após o Brexit, mantém sua transposição doméstica (NIS Regulations 2018), atualizada pelo Cyber Security and Resilience Bill.

tecnológica, tendem a criar pressões adicionais sobre a capacidade do setor público de atrair e reter competências especializadas, em um contexto de ameaças em constante transformação.

Outro aspecto destacado refere-se às assimetrias entre diferentes níveis de governo. Enquanto iniciativas em nível federal avançam na formulação de estratégias e marcos de referência, estados e municípios frequentemente operam sob restrições mais significativas de recursos e capacidade técnica para a implementação de políticas de segurança digital. Esse desafio assume particular relevância em setores como saúde, educação e segurança pública, cada vez mais dependentes de infraestruturas digitais.

Nesse contexto, as discussões sugerem que a consolidação das agendas de inteligência artificial e cibersegurança no Brasil poderá se beneficiar de esforços contínuos voltados ao fortalecimento de capacidades, à coordenação institucional e à implementação de iniciativas em diferentes níveis de governo.

8. Governança Internacional de IA e Cibersegurança: Modelos, Convergências e Limitações

A governança da inteligência artificial e da cibersegurança está em rápida evolução no cenário internacional, refletindo tanto a urgência dos riscos quanto as diferentes abordagens adotadas por Estados e blocos regionais. Como observam Qader, Ashfaq e Sarwar (2025), tecnologias emergentes como a inteligência artificial estão transformando rapidamente as dinâmicas de poder e segurança no âmbito global.

O debate no Turing Club evidenciou que, embora existam avanços relevantes em termos de princípios e frameworks, ainda não há um modelo consolidado e plenamente eficaz capaz de lidar com a complexidade da governança global. A pesquisa de Barakat (2025), sobre inteligência de ameaças orientada por IA em frameworks internacionais de cibersegurança, reforça essa percepção compartilhada: a autora demonstra a relevância de integrar soluções de IA nas estruturas de cibersegurança e indica que a colaboração internacional é essencial para enfrentar esses desafios de forma eficaz.

Modelos internacionais de governança de IA e cibersegurança

JURISDIÇÃO	INSTRUMENTO CENTRAL	ABORDAGEM
União Europeia	AI Act	Baseada em risco · prescritiva
Reino Unido	Pró-inovação	Princípios · adaptativa · NCSC
Estados Unidos	NIST AI RMF	Frameworks técnicos · setorial
Brasil	PL de IA + LGPD	Em consolidação · multissetorial

Figura 6: Comparativo de modelos internacionais de governança de IA e cibersegurança.

CONTEXTO

Box comparativo: três abordagens internacionais

União Europeia, abordagem prescritiva e baseada em risco. O *AI Act* estabelece obrigações por nível de risco e prevê proibições para usos inaceitáveis, conforme analisado por Kaur, Gabrijelčič e Klobučar (2023) em sua revisão sobre IA para cibersegurança. Em revisão, o *AI Act* evidencia o desafio de manter regulações estáveis em ambiente tecnológico dinâmico.

Reino Unido, abordagem orientada a princípios e flexível, com forte papel de órgãos técnicos como o NCSC e o AISI. O *AI Cyber Security Code of Practice* (DSIT, 2025a), o *Trusted Third-Party AI Assurance Roadmap* (DSIT, 2025b) e o *Cyber Security and Resilience Bill* (DSIT, 2025c) ilustram um modelo de *layered governance*⁸ que combina *soft law*, *hard law* e capacitação.

Estados Unidos, governança fortemente apoiada em frameworks técnicos do *National Institute of Standards and Technology* (NIST), como o *Cybersecurity Framework* e o *AI Risk Management Framework*. Sem caráter legalmente vinculante, exercem grande influência em boas práticas e padrões globais.

⁸Layered governance: modelo de governança em camadas que combina instrumentos de diferentes naturezas. Soft law: normas não vinculantes (códigos de prática, orientações). Hard law: normas juridicamente vinculantes (leis, regulamentos).

A diversidade de abordagens reflete não apenas diferenças institucionais, mas também fatores geopolíticos e econômicos. Países e blocos regionais buscam equilibrar a proteção de seus ecossistemas digitais com a promoção da inovação e a competitividade internacional.

Em particular, o *Code of Practice for the Cyber Security of AI* do Reino Unido (DSIT, 2025a), articulado entre DSIT e NCSC, foi convertido em base do *Technical Specification ETSI TS 104 223*, uma referência internacional emergente para segurança do ciclo de vida de sistemas de IA. Esse movimento ilustra como abordagens flexíveis e baseadas em princípios podem ser convertidas em padrões internacionalmente reconhecidos.

Contribuições trazidas por interlocutores diplomáticos destacaram, em complemento, o papel de mecanismos multilaterais na construção de referências e padrões mínimos compartilhados. A Recomendação da UNESCO sobre Ética da Inteligência Artificial (2021) representa um exemplo relevante de tentativa de estabelecer princípios compartilhados, abrangendo temas como direitos humanos, transparência e responsabilidade.

As discussões também indicaram que, em um cenário internacional marcado por maior complexidade geopolítica, diferentes formatos de cooperação tendem a coexistir. A dificuldade de alcançar consensos amplos em fóruns multilaterais tem sido acompanhada pela valorização de arranjos plurilaterais e bilaterais entre países com interesses convergentes, frequentemente descritos como *like-minded partners*.

Nesse contexto, o debate indicou que a cooperação entre Brasil e Reino Unido se insere em um alinhamento mais amplo de prioridades estratégicas no campo da governança digital. O compromisso compartilhado com inovação responsável, segurança digital e participação na construção de normas internacionais posiciona a cooperação bilateral como um vetor relevante para o fortalecimento de capacidades e o intercâmbio de boas práticas, em complementaridade aos esforços multilaterais.

9. Cooperação Brasil e Reino Unido: Uma Agenda Estratégica para Governança, Segurança e Inovação

A convergência entre inteligência artificial e cibersegurança, evidenciada ao longo do Turing Club · Capítulo Brasil, dificilmente pode ser enfrentada de forma isolada por Estados individuais. Essa percepção, compartilhada pelos participantes, é corroborada por Fauziyyah et al. (2025), cujo estudo avaliativo sobre riscos de segurança cibernética em sistemas de IA aplicados à infraestrutura digital governamental demonstra a natureza transnacional das vulnerabilidades. A velocidade de evolução tecnológica, por sua vez, sugere a relevância de modelos de cooperação internacional ágeis, adaptáveis e baseados em confiança mútua, conforme argumenta Kurniati (2024) em seu estudo sobre o papel da IA na segurança de infraestruturas críticas de informação.

Nesse contexto, a relação entre Brasil e Reino Unido apresenta características particularmente favoráveis para o desenvolvimento de uma agenda estruturada de cooperação. Ambos os países compartilham valores democráticos, possuem ecossistemas tecnológicos relevantes e demonstram interesse em fortalecer sua atuação em governança digital global.

Complementaridade estratégica · Brasil e Reino Unido

O que cada lado traz e onde a cooperação se encontra

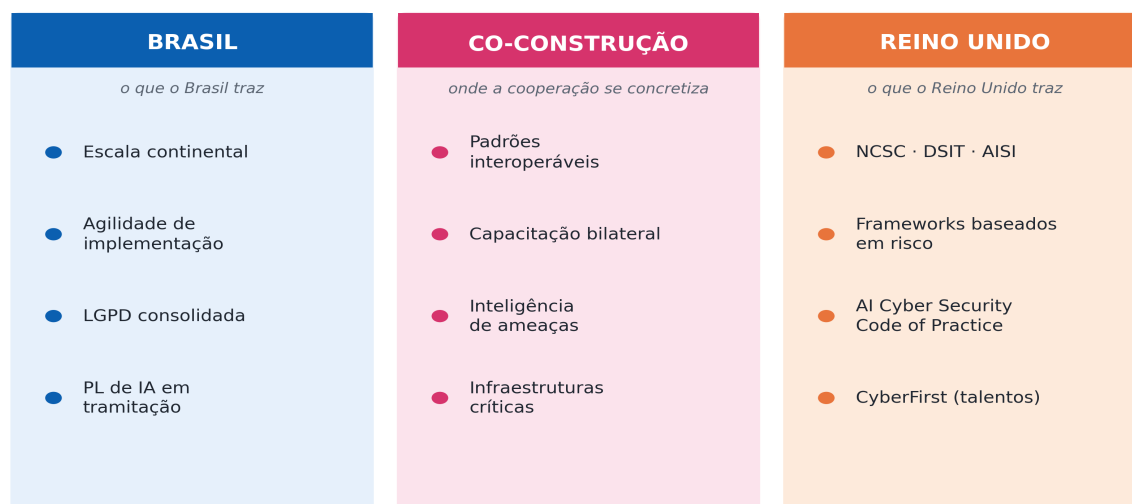


Figura 7: Complementaridade estratégica Brasil e Reino Unido: espaços de co-construção identificados durante o debate.

O Potencial Estratégico da Cooperação Brasil e Reino Unido

O debate destacou que essa cooperação poderia evoluir para um modelo mais estruturado, capaz de gerar impacto concreto em políticas públicas, desenvolvimento tecnológico e segurança institucional. Um dos elementos centrais dessa agenda é a complementaridade entre as abordagens dos dois países.

MENSAGEM-CHAVE

Resumo: complementaridade Brasil e Reino Unido

- **Reino Unido:** rigor analítico, modelos baseados em princípios, frameworks como o *AI Cyber Security Code of Practice* (DSIT, 2025a) e o *AI Assurance Roadmap* (DSIT, 2025b).
- **Brasil:** escala, agilidade na implementação de políticas públicas e marcos regulatórios, experiência em adaptação de instrumentos normativos a contextos complexos e capacidade de rápida resposta a desafios emergentes.
- **Espaço de co-construção:** combinar análise rigorosa, capacidade de execução e intercâmbio de evidências para informar políticas, padrões e capacitação conjunta.



Foto: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Imagem 3: Painel "Cooperação Brasil e Reino Unido": diálogo bilateral entre representantes de governo, diplomacia, setor privado e academia.

Olhares acadêmicos compartilhados durante o debate sublinharam que o Reino Unido tende a adotar uma abordagem mais estruturada e analítica na formulação de políticas, com forte ênfase em diagnóstico, mapeamento de atores e construção de frameworks. Essa caracterização é reforçada pela análise de Hurzhii (2023), que examina as particularidades do uso de IA em questões de cibersegurança sob a ótica britânica. O Brasil, por sua vez, demonstra significativa agilidade na implementação e capacidade de adaptação a contextos complexos, frequentemente descrita como uma habilidade de resposta rápida a desafios emergentes. Essa complementaridade, identificada pelos participantes do Turing Club, representa uma oportunidade estratégica.

A combinação entre rigor analítico e capacidade de execução pode contribuir para modelos inovadores de governança, capazes de lidar com a complexidade da inteligência artificial e da cibersegurança de forma mais eficaz. No campo da governança, há espaço para a construção de padrões interoperáveis e alinhamento regulatório.

Como *takeaway* das discussões, a experiência do Brasil com a Lei Geral de Proteção de Dados (LGPD), inspirada no GDPR europeu, ilustra a viabilidade de processos de convergência normativa, dinâmica examinada por Craglia et al. (2018), no relatório do Joint Research Centre da Comissão Europeia sobre a perspectiva europeia de IA. Um movimento semelhante poderia ser explorado em relação à inteligência artificial e à cibersegurança, especialmente no contexto das discussões em torno do PL de IA e do Marco Legal da Cibersegurança, com inspiração nos princípios consolidados pelo *AI Cyber Security Code of Practice* britânico (DSIT, 2025a).

Além disso, a cooperação poderia se beneficiar da experiência britânica na construção de capacidades institucionais. O NCSC (2025d), em seu Annual Review 2025, documenta o modelo de coordenação entre governo, setor privado e academia sustentado pelo Centro, incluindo suporte técnico, diretrizes práticas e resposta a incidentes; a adaptação de elementos desse arranjo ao contexto brasileiro poderia contribuir para fortalecer a capacidade de resposta e a coordenação interinstitucional no país.

Outro eixo relevante é o compartilhamento de conhecimento e a formação de talentos. A escassez de profissionais qualificados em cibersegurança é um desafio global, mas assume relevância particular no Brasil. Iniciativas conjuntas de capacitação, intercâmbio acadêmico e desenvolvimento de competências, inclusive inspiradas em programas britânicos como o *CyberFirst*, que, segundo o NCSC (2025d), já alcançou mais de 350.000 estudantes, podem contribuir para reduzir essa lacuna e fortalecer o ecossistema de segurança digital.

No campo operacional, há oportunidades para cooperação em áreas como inteligência de ameaças, resposta a incidentes e proteção de infraestruturas críticas. A natureza global das ameaças cibernéticas torna o compartilhamento de informações elemento essencial para a prevenção e mitigação de riscos. Modelos de cooperação que permitam a troca segura e ágil de dados podem ampliar significativamente a capacidade de resposta de ambos os países, em sintonia com as prioridades expressas no *Cyber Security and Resilience Bill* britânico.

Contribuições trazidas por perspectivas diplomáticas reforçaram a importância de explorar diferentes níveis de cooperação, combinando iniciativas multilaterais, plurilaterais e bilaterais. Em um cenário geopolítico marcado por tensões e fragmentação, acordos entre países com interesses convergentes, os chamados *like-minded partners*, podem avançar mais rapidamente e gerar resultados concretos.

Nesse contexto, foram mapeadas áreas estratégicas de interesse comum entre Brasil e Reino Unido, incluindo o uso de inteligência artificial no combate ao crime, a proteção de dados em ambientes orientados por IA e o desenvolvimento de padrões para a segurança de sistemas automatizados. O aprofundamento do diálogo nesses temas pode, de forma incremental, alimentar iniciativas em espaços multilaterais e contribuir para o aprimoramento da governança internacional.

10. Áreas Estratégicas para o Brasil e Oportunidades de Cooperação Brasil e Reino Unido

As discussões realizadas no Turing Club · Capítulo Brasil indicam que os desafios na interface entre inteligência artificial e cibersegurança se beneficiariam de respostas estruturais, coordenadas e orientadas à implementação. Essa leitura converge com a literatura acadêmica: Rios-Campos et al. (2024) fornecem uma revisão abrangente sobre cibersegurança e inteligência artificial e Urbanovics (2022) analisa comparativamente políticas cibernéticas na América Latina; ambos os estudos sugerem a relevância de abordagens holísticas que integrem capacitação, detecção de crimes cibernéticos e governança.

A seção a seguir apresenta elementos estratégicos identificados a partir da sistematização analítica dos debates, combinando as contribuições dos participantes com evidências empíricas e experiências internacionais. Os subtítulos foram formulados como convites ao diálogo, em consonância com o caráter exploratório e colaborativo do Turing Club.

10.1 Explorar caminhos para uma governança integrada de IA e cibersegurança

Ao longo do debate emergiu a percepção de que níveis limitados de articulação institucional podem representar um desafio para a efetividade das políticas públicas no Brasil. A coexistência de diferentes estratégias, como a EBIA, a E-Ciber e iniciativas no âmbito da proteção de dados, em estágios distintos de implementação, reforça a importância de mecanismos de coordenação, especialmente diante de riscos emergentes associados à convergência entre IA e cibersegurança. A necessidade desses mecanismos, discutida no Turing Club, também é sustentada por Cavalcante (2024), que examina medidas de governança propostas para lidar com potenciais riscos associados à IA e à *accountability* algorítmica.

Ao longo do debate, ressaltou-se a importância de promover sinergias entre as diferentes iniciativas relacionadas à inteligência artificial, à cibersegurança e à proteção de dados. A evolução contínua de estratégias como a EBIA, a E-Ciber e outros instrumentos de governança digital oferece oportunidades para fortalecer a coordenação institucional e apoiar abordagens mais integradas diante dos desafios emergentes que considerem ameaças híbridas.

Entre as alternativas discutidas, mencionou-se a existência de estruturas formais de coordenação, com mandatos claros, que poderiam envolver instâncias centrais de governo, como a Casa Civil ou o Gabinete de Segurança Institucional, bem como a participação de órgãos com atuação relevante no tema, incluindo o Ministério das Relações Exteriores, o Ministério da Ciência, Tecnologia e Inovação e a Autoridade Nacional de Proteção de Dados.

Como referência internacional, o NCSC (2025d), sustentado pela colaboração entre o DSIT, o GCHQ⁹ e o ecossistema acadêmico britânico, ilustra uma abordagem baseada na articulação entre capacidades técnicas, formulação de políticas e cooperação com diferentes setores, arranjo também analisado por Krasodonski et al. (2024) em sua coletânea sobre governança global responsável de IA. As discussões do Turing Club sugeriram que o intercâmbio dessas experiências e boas práticas pode informar reflexões sobre caminhos possíveis para fortalecer a coordenação e a efetividade das políticas no contexto brasileiro.

10.2 Integração regulatória entre IA e cibersegurança: oportunidades

O avanço paralelo do Projeto de Lei de Inteligência Artificial e do Marco Legal da Cibersegurança foi identificado no debate como um momento relevante para refletir sobre a articulação entre diferentes iniciativas regulatórias relacionadas à governança digital.

A literatura acadêmica sugere que, em contextos nos quais múltiplos instrumentos normativos evoluem simultaneamente, a promoção de complementaridade entre princípios, definições e obrigações contribui para maior coerência e efetividade regulatória. Nesse sentido, Olanrewaju e Onianwa (2025) analisam desafios, oportunidades e frameworks globais para a regulação da IA em cibersegurança, e Kulothungan (2024) discute os imperativos éticos e regulatórios urgentes para a cibersegurança orientada por IA, ambos os trabalhos oferecendo lentes complementares à discussão trazida no debate.

Nesse contexto, as discussões apontaram para a relevância de mecanismos de harmonização regulatória que favoreçam a coerência entre princípios, definições e obrigações estabelecidos em diferentes instrumentos normativos, incluindo a articulação de conceitos como classificação de risco, responsabilidade por danos e requisitos de segurança desde a concepção.

Adicionalmente, as discussões indicaram a relevância de incorporar, nos marcos regulatórios, princípios associados a *security by design* e *governance by design*, de modo a considerar riscos ao longo de todo o ciclo de vida das tecnologias. Nesse sentido, o *AI Cyber Security Code of Practice* e o *Cyber Security and Resilience Bill*, ambos liderados pelo DSIT (2025a e 2025c, respectivamente), oferecem referências práticas relevantes para essa integração.

10.3 Fortalecimento de competências em IA e cibersegurança

O desenvolvimento de competências especializadas foi identificado, no debate, como elemento relevante para o fortalecimento das capacidades nacionais em cibersegurança e inteligência artificial. Em um contexto marcado pela rápida evolução tecnológica e pela crescente demanda por profissionais qualificados, iniciativas de formação, atualização contínua e retenção de talentos

⁹GCHQ (Government Communications Headquarters): agência britânica de inteligência de sinais e cibersegurança. O NCSC (National Cyber Security Centre) é o braço público da GCHQ responsável pela cibersegurança do Reino Unido.

assumem importância estratégica, dimensão examinada por Velev e Zlateva (2024) em sua análise multissetorial sobre desafios de força de trabalho em cibersegurança e IA.

As discussões do Turing Club sugerem o valor de explorar uma estratégia nacional de formação e retenção de talentos, com foco em programas de capacitação em larga escala, em parceria com universidades e o setor privado; incentivos para a permanência de profissionais no setor público; criação de carreiras específicas para especialistas em cibersegurança e IA; e programas de intercâmbio internacional, especialmente com o Reino Unido. O potencial dessas iniciativas é ilustrado pelo programa *CyberFirst* do NCSC (2025d), que envolveu mais de 350.000 estudantes e gerou £41,4 milhões em valor social em 2024-2025, com retorno de £5,94 por libra investida, números que a análise de Conduț (2024) sobre validação e priorização de competências para inteligência cibernética utiliza para argumentar a favor de programas estruturados de formação nessa área.

No Brasil, programas como o "Hackers do Bem" representam avanços relevantes; sua escala e integração a uma estratégia nacional mais abrangente podem ser fortalecidas, considerando as competências essenciais para enfrentar ameaças cibernéticas. O AISI (2025), em seu *Year in Review*, sinaliza que modelos de cooperação bilateral com o Reino Unido, inclusive aproveitando o aprendizado do *CyberFirst* e do próprio AISI, podem oferecer caminhos relevantes para essa ampliação.

10.4 Aplicações de IA para a resiliência de infraestruturas críticas

O debate destacou que a proteção de infraestruturas críticas, incluindo energia, telecomunicações, finanças e serviços públicos, é uma prioridade central na agenda de cibersegurança. Chinelo, Umeanozie e Alozie (2025), em estudo sobre inteligência de ameaças aplicada à proteção de infraestruturas críticas via IA, argumentam de forma convergente que uma abordagem proativa de defesa cibernética é essencial para lidar com esses ativos estratégicos.

As discussões sugeriram que aplicações de inteligência artificial podem contribuir para o fortalecimento da resiliência desses ativos, por meio da detecção preditiva de ameaças, da integração de sistemas de monitoramento em tempo real, da definição de padrões mínimos de segurança para operadores e de exercícios de simulação de incidentes em larga escala.

Essa perspectiva encontra respaldo em Yu (2024), que trata a IA como infraestrutura crítica em si e discute mecanismos para salvaguardar a segurança nacional na era da inteligência artificial. Ilustram essa aplicação prática as pesquisas do Alan Turing Institute (2025), conduzidas por seu *AI for Cyber Defence Research Centre* (AICD) e pelo *Autonomous Cyber Defence Innovation and Research Lab* (ACD-IRL), que exploram como modelos de IA podem ser aplicados à proteção ativa de infraestruturas críticas.

A combinação entre marco legal renovado, capacitação e a adaptação inteligente de princípios britânicos, como os consolidados pelo DSIT (2025c) no *Cyber Security and Resilience Bill*, poderia representar um vetor promissor para que o Brasil avance na resiliência de seus serviços essenciais. A

referência ao modelo britânico deve, contudo, ser calibrada à realidade brasileira, considerando as especificidades regulatórias, institucionais e operacionais do país, sob o risco de perder efetividade quando aplicada sem essa adaptação.

10.5 Compartilhamento de inteligência de ameaças: práticas e oportunidades

A natureza dinâmica e transnacional das ameaças cibernéticas destaca a relevância da cooperação e do compartilhamento de informações entre governo, setor privado, academia e sociedade civil.

As discussões do Turing Club indicaram que mecanismos voltados à troca segura de informações e ao fortalecimento da colaboração multissetorial podem contribuir para ampliar a compreensão de riscos e apoiar respostas mais eficientes a incidentes. Essa é uma abordagem amplamente reconhecida na literatura, como demonstra a revisão de Ansari, Dash, Sharma e Yathiraju (2022) sobre o impacto e as limitações da IA na cibersegurança, que identifica o compartilhamento de inteligência de ameaças como fator central para o avanço da segurança cibernética em diversas indústrias.

Modelos internacionais demonstram que a colaboração entre diferentes setores tende a ampliar significativamente a capacidade de prevenção e resposta. O levantamento de Tao, Akhtar e Zhang (2021) sobre o futuro da IA em cibersegurança evidencia essa dinâmica ao mapear iniciativas que utilizam IA para monitorar, detectar e mitigar ameaças. No Brasil, arranjos desse tipo poderiam ser desenhados de forma a incluir não apenas grandes organizações, mas também pequenas e médias empresas, que frequentemente representam pontos vulneráveis em cadeias produtivas.

10.6 A centralidade da integridade informacional no ecossistema digital

A discussão sobre desinformação evidenciou a relevância da integridade do ambiente informacional para a confiança pública, a resiliência institucional e o funcionamento de sociedades cada vez mais dependentes de ecossistemas digitais. Trata-se de um tema que ganha reconhecimento internacional crescente como componente essencial da resiliência social e institucional.

O debate sugeriu o valor de tratá-la como uma forma de infraestrutura crítica, com políticas específicas para monitoramento de campanhas de desinformação, resposta rápida a incidentes informacionais, cooperação com plataformas digitais e educação midiática e digital da população. Essa formulação dialoga com a análise de Yu (2024), que discute a IA como infraestrutura crítica e suas implicações para a segurança nacional. A experiência britânica oferece referências relevantes nesse eixo: o NCSC (2024), em sua seção *Artificial Intelligence*, e o NCSC (2025c), na coleção *Defending Democracy*, consolidam orientações voltadas à proteção de processos eleitorais e ao enfrentamento da manipulação sintética de mídia.

Essa abordagem pode beneficiar-se da integração entre políticas de cibersegurança, comunicação institucional e regulação de plataformas, garantindo uma resposta coordenada e

proporcional aos riscos, aspecto examinado por Hunnewell (2024) em seu estudo sobre preocupações de segurança nacional envolvendo IA e infraestrutura crítica civil.

10.7 Consolidar uma agenda estruturada de cooperação Brasil e Reino Unido

A cooperação bilateral entre Brasil e Reino Unido oferece oportunidades para aprofundar o diálogo e o intercâmbio de experiências em inteligência artificial e cibersegurança. As discussões do Turing Club destacaram áreas de interesse compartilhado, incluindo capacitação, governança digital, intercâmbio de especialistas, compartilhamento de boas práticas e proteção de infraestruturas críticas, dimensões que Tao, Akhtar e Zhang (2021), em levantamento sobre o futuro da IA em cibersegurança, apontam como pilares para agendas cooperativas eficazes.

Como sugerem Craglia et al. (2018) em seu relatório sobre a perspectiva europeia de IA, esse tipo de cooperação bilateral poderia servir de base para iniciativas plurilaterais, ampliando o impacto em fóruns internacionais e contribuindo para a difusão de padrões interoperáveis, como a especificação técnica ETSI TS 104 223, derivada do *AI Cyber Security Code of Practice* britânico (DSIT, 2025a).

10.8 Padrões e certificações de segurança: referências internacionais e boas práticas

A adoção de padrões e frameworks reconhecidos internacionalmente desempenha papel relevante na promoção da consistência, da interoperabilidade e da confiança em práticas de segurança digital. Hamon, Junklewitz, Soler Garrido e Sánchez (2024), em análise sobre os desafios para tornar seguros os sistemas de IA no contexto das regulações vigentes, evidenciam a importância desses referenciais internacionais para o desenho de políticas coerentes.

As discussões destacaram a relevância de referências amplamente utilizadas, incluindo as normas ISO/IEC 27001 e 27701, os frameworks desenvolvidos pelo NIST e o *Implementation Guide for the AI Cyber Security Code of Practice* do DSIT (DSIT, 2025a).

Políticas públicas podem incluir incentivos fiscais, requisitos regulatórios e programas de certificação para estimular a adoção dessas práticas, especialmente entre pequenas e médias empresas. O *Trusted Third-Party AI Assurance Roadmap* (DSIT, 2025b) oferece referência adicional, ao consolidar três modelos complementares de garantia da qualidade de sistemas de IA: (i) *first-party assurance*, em que o próprio desenvolvedor atesta conformidade; (ii) *second-party assurance*, em que clientes ou parceiros contratuais realizam avaliações; e (iii) *third-party assurance*, com auditoria independente. Ao articular esses três níveis, o *Roadmap* amplia a confiança do mercado ao mesmo tempo em que reduz assimetrias de informação entre fornecedores, adquirentes e reguladores. Complementarmente, prevê um *AI Assurance Innovation Fund* destinado a fortalecer o mercado britânico de *AI assurance*, financiando ferramentas, metodologias e capacitação, modelo cuja lógica de estímulo estruturado pode inspirar arranjos análogos em outras jurisdições.

11. Conclusão: Da Convergência Tecnológica à Construção de um Novo Paradigma de Governança



Foto: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Imagem 4: Encerramento do Turing Club · Capítulo Brasil: registro do diálogo bilateral.

A convergência entre inteligência artificial e cibersegurança representa uma das transformações mais profundas da era digital contemporânea. Ao longo das discussões do Turing Club · Capítulo Brasil, foi evidente que essa transformação não se limita à ampliação de capacidades tecnológicas, mas redefine as bases sobre as quais se estruturam a segurança, a confiança e a governança em sociedades altamente digitalizadas, dinâmica também observada por Fauziyyah et al. (2025) em estudo empírico sobre riscos de cibersegurança em sistemas baseados em IA aplicados à infraestrutura digital governamental.

Os debates evidenciaram que os riscos associados à inteligência artificial não são apenas incrementais, mas sistêmicos. A capacidade de automatizar ataques, explorar vulnerabilidades em escala e manipular ambientes informacionais introduz um novo patamar de complexidade, no qual a distinção entre segurança técnica e estabilidade institucional se torna cada vez mais difusa. Nesse contexto, a proteção de infraestruturas críticas passa a incluir não apenas sistemas físicos e digitais, mas também o próprio ambiente informacional que sustenta processos democráticos.

Ao mesmo tempo, a inteligência artificial permanece como um dos principais vetores de inovação e desenvolvimento econômico. Como demonstram Widaningsih, Abdurrahman e Busairi (2025) em sua análise comparativa sobre governança de IA e cibersegurança em estratégias nacionais de defesa, essa dualidade, risco e oportunidade, convida a uma mudança de paradigma na formulação de políticas públicas. Não se trata de conter o avanço tecnológico, mas de estruturá-lo de forma responsável, integrando segurança, governança e inovação desde a concepção das tecnologias.

No contexto brasileiro, as discussões indicaram que a governança de inteligência artificial e cibersegurança se apoia em um conjunto relevante de iniciativas, estratégias e instrumentos normativos em evolução. Entre eles destacam-se a regulamentação da inteligência artificial, a Estratégia Brasileira de Inteligência Artificial (EBIA), a Estratégia Nacional de Segurança Cibernética (E-Ciber) e outros marcos voltados à proteção de dados e à transformação digital. A consolidação dessas agendas oferece oportunidades para ampliar a coordenação institucional, o desenvolvimento de capacidades e a implementação em diferentes níveis de governo.

Nesse contexto, o Turing Club destaca o valor do diálogo internacional e da cooperação entre múltiplos setores na promoção do compartilhamento de experiências, do intercâmbio de boas práticas e da construção de entendimentos comuns sobre desafios emergentes da governança digital. A continuidade desses espaços de diálogo pode contribuir para fortalecer conexões entre Brasil e Reino Unido e apoiar respostas integradas a temas de interesse compartilhado.

REFERÊNCIA BRITÂNICA

Em síntese

- A convergência entre IA e cibersegurança é sistêmica e exige abordagens integradas de governança.
- O Brasil conta com um arcabouço relevante em IA, cibersegurança e proteção de dados.
- A cooperação Brasil e Reino Unido cria oportunidades para fortalecimento de capacidades e intercâmbio de experiências.
- A integridade informacional consolida-se como tema central para a resiliência digital.

Referências

As referências seguem o padrão APA (7.ª edição). Fontes britânicas oficiais (NCSC, DSIT, Cabinet Office, AISI, Alan Turing Institute) estão destacadas e disponíveis em fontes open source.

Akhtar, Z. B., et al. (2021). Artificial intelligence in cyber defence and offence: A capability-based assessment.

Alan Turing Institute. (2025). Defence and National Security, AI for Cyber Defence Research Centre (AICD).

Disponível em: <https://www.turing.ac.uk/aicd>

AI Security Institute (AISI). (2025). Our 2025 year in review.

Disponível em: <https://www.aisi.gov.uk/blog/our-2025-year-in-review>

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review.

DOI: <https://doi.org/10.17148/ijarcce.2022.11912>

Barakat, A. (2025). AI-driven threat intelligence: Strengthening cyber defense mechanisms in international cybersecurity frameworks.

Bioni, B., Garrote, M., & Guedes, P. (2023). Key themes in AI regulation: The local, regional, and global in the pursuit of regulatory interoperability. Data Privacy Brasil.

Bisht, R. K. (2024). Cybersecurity and artificial intelligence: How AI is being used in cybersecurity to improve detection and response to cyber threats.

Cabinet Office. (2025). The Mitigating "Hidden" AI Risks Toolkit. GOV.UK.

Disponível em: <https://www.gov.uk/government/publications/a-human-centred-approach-to-scaling-and-de-risking-ai-tools>

Cavalcante, P. (2024). Artificial intelligence and algorithm accountability: Potential risks and proposed governance measures. Blavatnik School of Government, University of Oxford.

Chinelo, E. C. E., Umeanozie, P., & Alozie, C. (2025). Enhancing threat intelligence for critical infrastructure protection through artificial intelligence: A proactive cyber defence approach.

Condrut, C. (2024). Validation and prioritization of knowledge, skills and abilities for cyberintelligence analysis in intelligence and national security.

Craglia, M. (Ed.), Annoni, A., Benczur, P., Bertoldi, P., Delipetrev, P., De Prato, G., & Feijóo, C. (2018). Artificial intelligence: A European perspective. European Commission, Joint Research Centre.

Department for Science, Innovation and Technology (DSIT). (2025a). AI Cyber Security Code of Practice and Implementation Guide. GOV.UK.

Disponível em: <https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice>

Department for Science, Innovation and Technology (DSIT). (2025b). Trusted Third-Party AI Assurance Roadmap. GOV.UK.

Disponível em: <https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap>

Department for Science, Innovation and Technology (DSIT). (2025c). Cyber Security and Resilience Bill, policy statement and explanatory documents. GOV.UK.

Disponível em: <https://www.gov.uk/government/collections/cyber-security-and-resilience-bill>

Fauziyyah, G., Maulana, I., Komarudin, K., & Selamat, R. (2025). Risk security cyber in system AI-based: Study evaluative on Indonesian government digital infrastructure.

- Gerlich, M. (2023). Perceptions and acceptance of artificial intelligence: A multi-dimensional study. *Social Sciences*, 12(9).
- DOI: <https://doi.org/10.3390/socsci12090502>
- Hamon, R., Junklewitz, H., Soler Garrido, J., & Sánchez, I. (2024). Three challenges to secure AI systems in the context of AI regulations.
- DOI: <https://doi.org/10.1109/access.2024.3391021>
- Hunnewell, B. (2024). National security concerns for artificial intelligence and civilian critical infrastructure.
- Hurzhii, S. (2023). The special features of using the artificial intelligence in the matters of cybersecurity.
- IBM. (2024). Cost of a Data Breach Report 2024.
- INCC, Instituto Nacional de Combate ao Cibercrime. (2025). Análises setoriais sobre o cenário brasileiro de fraudes digitais e engenharia social. INCC.
- ISC2. (2024). Cybersecurity Workforce Study. International Information System Security Certification Consortium.
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions.
- DOI: <https://doi.org/10.1016/j.inffus.2023.101804>
- Krasodomski, A., Gwagwa, A., Jackson, B., Jones, E., King, S., Lane, M., & Mantegna, M. (2024). Artificial intelligence and the challenge for global governance: Nine essays on achieving responsible AI.
- Kulothungan, V. (2024). Securing the AI frontier: Urgent ethical and regulatory imperatives for AI-driven cybersecurity.
- Kurniati, A. (2024). Study of the artificial intelligence role in achieving cybersecurity for critical information infrastructure.
- Lockey, S., Gillespie, N., Holm, D., & Someh, I. (2021). A review of trust in artificial intelligence: Challenges, vulnerabilities and future directions.
- DOI: <https://doi.org/10.24251/hicss.2021.664>
- Modupeola, T. O., Oluwasusi, V. A., Nobari Azar, N. A., & Ichull, A. P. (2025). Deepfake detection and cybersecurity index: The role of computer vision as a digital forensic tool.
- National Cyber Security Centre (NCSC). (2023). Guidelines for secure AI system development. GOV.UK / NCSC.
- Disponível em: <https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development>
- National Cyber Security Centre (NCSC). (2024). The near-term impact of AI on the cyber threat. NCSC.
- Disponível em: <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>
- National Cyber Security Centre (NCSC). (2025a). Impact of AI on cyber threat from now to 2027. NCSC.
- Disponível em: <https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027>
- National Cyber Security Centre (NCSC). (2025b). Preserving integrity in the age of generative AI. NCSC Blog.
- Disponível em: <https://www.ncsc.gov.uk/blog-post/preserving-integrity-in-age-generative-ai>
- National Cyber Security Centre (NCSC). (2025c). Defending Democracy collection. NCSC.
- Disponível em: <https://www.ncsc.gov.uk/collection/defending-democracy>
- National Cyber Security Centre (NCSC). (2025d). NCSC Annual Review 2025, CyberFirst and Resilience at Scale.
- Disponível em: <https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf>
- Nicolás, M. A., & Sampaio, R. C. (2024). Balancing efficiency and public interest: The impact of AI automation on social benefit provision in Brazil.

- Olanrewaju, B. A., & Onianwa, B. (2025). Regulating AI in cybersecurity: Balancing challenges, opportunities, and global frameworks.
- Pandey, A. (2025). AI's dark side: The rise of deepfakes and the battle for truth.
- Parihar, R. (2025). Investigating the impact of artificial intelligence on cybersecurity threat detection and response mechanisms.
- Qader, A., Ashfaq, K., & Sarwar, Z. (2025). Technological innovation and global governance: The role of AI, cyber, and space in international relations.
- Radanliev, P., et al. (2024). Frameworks for AI safety and security in the development of cybersecurity solutions.
- Rios-Campos, C., Venegas Paz, S. C., Orozco Vilema, G., Robles Díaz, L. M., Flores Zambrano, D. P., Mendoza Zambrano, G. M., & Luzuriaga Viteri, J. C. (2024). Cybersecurity and artificial intelligence (AI).
- Tao, F., Akhtar, M. S., & Zhang, J. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey.
DOI: <https://doi.org/10.4108/eai.7-7-2021.170285>
- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence.
- Urbanovics, A. (2022). Cybersecurity policy-related developments in Latin America.
- Velev, D., & Zlateva, P. (2024). Workforce challenges in cybersecurity and artificial intelligence: A multi-sector analysis.
- Verizon. (2024). Data Breach Investigations Report 2024.
- Widaningsih, Abdurrahman, S. S., & Busairi, H. (2025). Artificial intelligence and cybersecurity governance: Comparative insights into national defense strategies.
- World Economic Forum. (2025). Global Risks Report 2025: A world of growing divisions.
Disponível em: <https://www.weforum.org/publications/global-risks-report-2025/>
- Yu, C. (2024). AI as critical infrastructure: Safeguarding national security in the age of artificial intelligence.
DOI: <https://doi.org/10.31219/osf.io/u4kdq>



Créditos

INICIATIVA E REALIZAÇÃO

Governo Britânico

COORDENAÇÃO TÉCNICA E SISTEMATIZAÇÃO DOS DEBATES

Luana Tavares

ELABORAÇÃO DO RELATÓRIO

Instituto Nacional de Combate ao Cibercrime (INCC)

EVENTO

Turing Club · Capítulo Brasil

Embaixada Britânica em Brasília

12 de março de 2026

EDIÇÃO

1.^a edição

Brasília / São Paulo · março de 2026

Distribuição gratuita · Uso institucional

SOBRE A INICIATIVA TURING CLUB

Inspirado em Alan Turing e na tradição britânica de inteligência computacional, o Turing Club · Capítulo Brasil é um espaço bilateral de diálogo estratégico sobre tecnologias emergentes, incluindo IA, cibersegurança e governança digital, apoiado pelo Governo Britânico no âmbito da agenda de cooperação Brasil e Reino Unido.

© 2026 · Turing Club · Capítulo Brasil

Uma iniciativa de diálogo estratégico sobre inteligência artificial, cibersegurança e governança digital.