



CIBERTERRORISMO E USO DA FORÇA NA ORDEM MUNDIAL

9 setembro 2026

O ciberespaço tornou-se uma infraestrutura essencial das sociedades e, simultaneamente, um domínio de competição estratégica, coerção e produção de riscos transnacionais. O ciberterrorismo coloca, neste contexto, uma questão particularmente sensível para a ordem mundial: em que circunstâncias uma operação cibernética pode produzir efeitos e consequências que aproximem o incidente do limiar jurídico do uso da força ou de um ataque armado?

O artigo articula a teoria da sociedade do risco com o Direito Internacional aplicável ao ciberespaço e com a evolução recente das políticas de cibersegurança. Defende-se que a principal dificuldade não reside na ausência de normas, mas na sua aplicação a operações cuja autoria, escala, intensidade, efeitos e contexto podem ser difíceis de determinar. A análise é atualizada com dados recentes da União Europeia, desenvolvimentos nas Nações Unidas e na NATO, e novos instrumentos europeus de resiliência. A investigação sustenta que a resposta mais consistente com a estabilidade internacional passa por prevenção, resiliência, atribuição, cooperação e proteção de infraestruturas críticas, reservando o recurso à força para situações excepcionais, juridicamente qualificadas e politicamente sustentáveis.

O ciberespaço já não pode ser tratado como uma dimensão meramente técnica da sociedade internacional. Energia, transportes, saúde, finanças, administração pública, comunicações e defesa dependem de sistemas digitais interligados, frequentemente suportados por cadeias de fornecimento e prestadores que atravessam múltiplas jurisdições. A vulnerabilidade digital passou, por isso, a integrar a própria estrutura do poder internacional. A atualidade da questão é evidenciada pelos dados da European Union Agency for Cybersecurity (ENISA): o *Threat Landscape* 2025 analisou 4.875 incidentes ocorridos entre julho de 2024 e junho de 2025, identificando os ataques de negação de serviço distribuído (DDoS) como o tipo de incidente mais frequente e o *ransomware* como a ameaça de maior impacto. (ENISA, 2025).

Ciberespaço e sociedade do risco

Ulrich Beck concebeu a sociedade do risco como uma sociedade em que a modernização produz simultaneamente

benefícios, dependências e riscos de alcance potencialmente transnacional (Beck, 1992, 2008). Anthony Giddens associou a modernidade tardia à gestão reflexiva de riscos e à crescente dependência de sistemas especializados (Giddens, 2005). O ambiente digital torna visível esta dinâmica: a mesma conectividade que aumenta eficiência, mobilidade e comunicação também amplia a superfície de ataque e permite que uma perturbação localizada tenha efeitos em cadeia.

A segurança digital converte-se, consequentemente, numa questão de governação internacional e de resiliência sistémica.

O risco cibernético é, assim, simultaneamente técnico, económico, político e jurídico. Não se limita à perda de confidencialidade, integridade ou disponibilidade de dados; pode afetar a continuidade de serviços essenciais, a confiança nas instituições e a capacidade de decisão do Estado. O problema é agravado pela interdependência das redes: servidores,

fornecedores, operadores, utilizadores e atacantes podem estar distribuídos por vários países. A segurança digital converte-se, consequentemente, numa questão de governação internacional e de resiliência sistémica.

Os dados mais recentes confirmam esta tendência. A ENISA registou, no período analisado no seu relatório de 2025, uma forte incidência de DDoS, enquanto o *ransomware* permaneceu particularmente relevante pelo impacto operacional. A mesma avaliação mostra que a administração pública foi o setor mais visado na União Europeia, representando 38,2% dos incidentes identificados, seguida pelos transportes, infraestruturas e serviços digitais e finanças (ENISA, 2025). Estes números não permitem concluir que tais incidentes sejam ciberterroristas; demonstram, contudo, por que razão a proteção das infraestruturas críticas é central para a segurança internacional.

O uso da força na ordem internacional

A Carta das Nações Unidas estabelece, no artigo 2.º, n.º 4, a proibição da ameaça ou do uso da força nas relações internacionais. O artigo 51.º preserva o direito inerente de legítima defesa em caso de ataque armado, sem prejuízo da compe-

FIGURA 1. INDICADORES RECENTES DA AMEAÇA CIBERNÉTICA NA UNIÃO EUROPEIA

Fonte: Elaborado pelo autor com base em ENISA (2025) e CERT-EU (2026). Os indicadores utilizam metodologias e universos de observação distintos e não devem ser somados entre si.

Indicador	Dados	Relevância
Incidentes analisados pela ENISA	4.875 (jul. 2024–jun. 2025)	Dimensão e diversidade da superfície de ameaça
DDoS	77% dos incidentes reportados	Predomínio de operações de disrupção de serviços
Ransomware	Ameaça de maior impacto	Risco para continuidade e recuperação operacional
Administração pública	38,2% dos setores visados	Centralidade do Estado e dos serviços públicos
Atividade contra entidades da UE em 2025	174 atores distintos	Maior diversidade e complexidade do ecossistema de ameaça



tência do Conselho de Segurança. Este enquadramento continua a ser o ponto de partida para analisar operações cibernéticas com possíveis efeitos internacionais. A evolução das discussões nas Nações Unidas não aponta para um vazio jurídico. O relatório final do *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, transmitido em 2025, consolidou o processo multilateral sobre segurança das tecnologias de informação e comunicação e a aplicação do Direito Internacional ao ciberespaço (United Nations, 2025). A questão essencial é, portanto, interpretativa e operacional: como aplicar princípios jurídicos existentes a operações cuja materialidade pode ser predominantemente digital, distribuída e difícil de atribuir?

O Tallinn Manual 2.0 continua a ser uma referência doutrinária importante para esta análise. Não é um tratado internacional nem exprime a posição oficial da Organização do Tratado do Atlântico Norte (NATO, na sigla inglesa); trata-se de um estudo de especialistas sobre a aplicação do Direito Internacional às operações cibernéticas. A sua utilidade reside precisamente na construção de uma escala que permite distinguir operações ilícitas de menor intensidade, intervenção, violação da soberania, uso da força e ataque armado (Schmitt, 2017).

Do ciberincidente ao limiar da força

A qualificação jurídica de uma operação não deve resultar apenas da sua sofisticação técnica nem da existência de perdas económicas. A análise deve considerar, de forma integrada, a escala, a intensidade, a duração, os efeitos, a natureza dos alvos, o contexto e as consequências. Os danos físicos, as mortes, a destruição de bens e as perturbações graves de serviços essenciais constituem indicadores particularmente relevantes, mas a avalia-

ção não pode prescindir da atribuição e da natureza do contexto em que a operação ocorre. A doutrina sobre o uso da força em operações cibernéticas tem, precisamente, procurado avaliar em que medida efeitos e consequências podem aproximar uma operação do limiar do artigo 2.º, n.º 4, da Carta das Nações Unidas (Roscini, 2015; Waxman, 2011).

A existência de uma operação cibernética ilícita, mesmo com efeitos significativos, não desencadeia automaticamente o direito de legítima defesa. O limiar deve ser apreciado à luz do conjunto das circunstâncias e da intensidade dos efeitos.

A atribuição é uma das maiores dificuldades. Um atacante pode recorrer a infraestruturas de terceiros, sistemas comprometidos, técnicas de *spoofing*, intermediários ou cadeias de fornecedores situadas em diferentes países. A decisão política pode, assim, ter de ser tomada antes de existir certeza forense completa. Daqui resulta uma assimetria perigosa: a urgência da resposta pode ser superior à velocidade de produção de evidência. Uma atribuição errada pode atingir um terceiro Estado e transformar um incidente limitado numa crise internacional.

De igual modo, é essencial distinguir uso da força de ataque armado. A existência de uma operação cibernética ilícita, mesmo com efeitos significativos, não desencadeia automaticamente o direito de

legítima defesa. O limiar deve ser apreciado à luz do conjunto das circunstâncias e da intensidade dos efeitos. Esta prudência é particularmente importante no caso de atores não estatais, porque a identificação do autor material não resolve, por si só, a questão da imputação jurídica a um Estado.

Ciberterrorismo: conceito e fronteiras

O conceito de ciberterrorismo permanece controvertido. A dificuldade começa pela própria definição de terrorismo, que não dispõe de uma definição universal única aceite em todos os instrumentos internacionais. Em termos analíticos, podem identificar-se elementos recorrentes: intenção de provocar violência ou ameaça de violência, finalidade de intimidar ou coagir uma população ou governo e prossecução de objetivos políticos, ideológicos ou religiosos.

Neste particular, é fundamental distinguir três situações. A primeira é a utilização de tecnologias digitais por organizações terroristas para propaganda, radicalização, recrutamento, financiamento, comunicação ou planeamento. A segunda é a realização de operações cibernéticas concebidas para produzir efeitos terroristas, nomeadamente contra infraestruturas críticas. A terceira corresponde a operações cibernéticas inseridas num conflito armado, sujeitas às regras aplicáveis do Direito Internacional Humanitário. A utilização da Internet por grupos terroristas não é, por si só, sinónimo de ciberterrorismo. Esta distinção é particularmente importante quando se analisam redes terroristas enquanto estruturas de conectividade, coordenação e aprendizagem (Guedes, 2007).

A Organização das Nações Unidas tem reforçado esta distinção. O Gabinete de Combate ao Terrorismo das Nações Unidas (UNOCT, na sigla inglesa) identifica como preocupação crescente a utilização de tecnologias de informação e comunicação por atores terroristas para cometer, incitar, recrutar, financiar ou planear atos terroristas e desenvolve programas orientados para a prevenção de ciberataques contra infraestruturas críticas. A abordagem assenta na cooperação entre Estados, organizações internacionais, setor privado e sociedade civil, incluindo a proteção dos direitos humanos (UNOCT, 2026).

FIGURA 2. ESCALA DE RESPOSTA: DA INTRUSÃO À FORÇA

Fonte: Elaborado pelo autor com base na Carta das Nações Unidas, Schmitt (2017) e United Nations (2025). A tabela é uma síntese analítica e não uma codificação normativa dos limiares.

Patamar	Questão dominante	Resposta prioritária
Intrusão/atividade ilícita de baixa intensidade	Violação de regras aplicáveis, sem efeitos graves	Investigação, cooperação policial, medidas diplomáticas
Operação com efeitos relevantes	Soberania, intervenção ou danos significativos	Atribuição, resposta diplomática, económica ou cibernética
Uso da força	Escala e efeitos aproximam-se do conceito de força	Avaliação jurídica e política reforçada; necessidade e proporcionalidade
Ataque armado	Efeitos e contexto atingem o limiar relevante	Análise do artigo 51.º e das condições da legítima defesa



Esta distinção tem consequências diretas para a ordem mundial. Um crime cibernético exige instrumentos de investigação e justiça criminal; uma operação de espionagem suscita questões de soberania e contrainteligência; uma operação militar ativa categorias próprias do Direito dos conflitos armados; e uma operação ciberterrorista exige articular prevenção do terrorismo, cibersegurança, proteção de infraestruturas críticas e cooperação internacional. A classificação do incidente é, portanto, uma decisão estratégica com consequências jurídicas (Guerreiro, 2018).

Segurança, liberdade e resposta estatal

A proteção contra o ciberterrorismo não pode ser separada do Estado de direito. A Constituição da República Portuguesa consagra o direito à liberdade e à segurança no artigo 27.º e estabelece, no artigo 18.º, exigências para as restrições aos direitos, liberdades e garantias (Canotilho & Moreira, 2014). A segurança, entendida também como dimensão de proteção do cidadão, deve ser articulada com soberania, cidadania e limites jurídicos ao poder público (Gouveia, 2018). O aumento da ameaça digital não pode converter-se numa autorização genérica para vigilância ou compressão permanente de direitos.

A teoria da sociedade do risco ajuda a compreender este equilíbrio. O risco digital é frequentemente invisível, difuso e tecnicamente difícil de explicar ao público. Essa característica pode aumentar a percepção de vulnerabilidade e criar pressão para respostas imediatas. A política de segurança deve resistir tanto à insuficiência de proteção como à sobre reação. A necessidade, adequação e proporcionalidade devem orientar a adoção de medidas de prevenção, investigação e resposta.

A atual evolução regulatória europeia mostra que a resposta está a deslocar-se para a resiliência. O Regulamento (UE) 2025/38, conhecido como *Cyber Solidarity Act*, entrou em vigor em 4 de fevereiro de 2025 e criou mecanismos europeus para reforçar a deteção, preparação e resposta a ameaças e incidentes significativos, incluindo uma arquitetura de centros nacionais e transfronteiriços de cibersegurança. O objetivo é aumentar a capacidade coletiva de deteção e resposta sem depender de uma reação coerciva posterior ao dano (União Europeia, 2025).

Da cibersegurança à estratégia

A evolução das políticas de defesa confirma que o ciberespaço é hoje um domínio estratégico. A NATO reconheceu-o como domínio de operações e, na Cimeira de Washington de 2024, os Aliados decidiram estabelecer o *NATO Integrated Cyber Defence Centre* para reforçar a proteção das redes, a consciência situacional e a integração operacional do ciberespaço. A NATO mantém, contudo, uma abordagem caso a caso: um ciberataque significativo pode ser considerado para efeitos do artigo 5.º do Tratado de Washington, mas a aplicação do mecanismo depende da avaliação dos Aliados sobre a natureza e as circunstâncias do evento (NATO, 2024).

A soberania não desaparece, mas passa a depender também da capacidade de proteger redes, regular operadores, assegurar resiliência e cooperar além-fronteiras. Esta transformação acompanha a crescente relevância do ciberespaço enquanto espaço de poder, conectividade e disputa estratégica.

A evolução institucional não significa militarização automática de todos os incidentes. Pelo contrário, reforça a importância da capacidade de absorção, continuidade e recuperação. O relatório do CERT-EU sobre 2025 identificou 174 atores distintos envolvidos em atividades maliciosas contra entidades da União e respetivo ecossistema, contra 110 em

2024. Ciberespionagem e *prepositioning* representaram 38% da atividade registada, enquanto o cibercrime representou 30%. O relatório assinala, ainda, o crescimento da engenharia social apoiada por inteligência artificial, incluindo clonagem de voz, conteúdos de *phishing* personalizados e *deepfakes* (CERT-EU, 2026). Estes dados são relevantes para a ordem mundial porque mostram uma zona crescente de competição abaixo do limiar do conflito armado. Espionagem, intrusão, sabotagem, influência, hacktivismo, criminalidade instrumentalizada e operações contra infraestruturas podem produzir efeitos estratégicos sem que exista uma situação juridicamente equivalente a uma guerra. A estabilidade internacional depende, por isso, da capacidade de gerir esta zona intermédia sem banalizar o recurso à força.

Implicações para a ordem mundial

A questão do ciberterrorismo e do uso da força é, em última análise, uma questão de ordem mundial porque desafia categorias construídas em torno de território, fronteiras e materialidade física. Um ator pode operar à distância, utilizar infraestruturas privadas e produzir efeitos transnacionais sem uma presença física equivalente. A soberania não desaparece, mas passa a depender também da capacidade de proteger redes, regular operadores, assegurar resiliência e cooperar além-fronteiras. Esta transformação acompanha a crescente relevância do ciberespaço enquanto espaço de poder, conectividade e disputa estratégica (Guedes & Santos, 2015).

A primeira transformação é a do poder. O poder internacional inclui agora capacidades de intrusão, proteção, disrupção, influência e controlo de infraestruturas digitais. A segunda é a dificuldade crescente de separar paz, competição e conflito. A terceira é institucional: as Nações Unidas continuam a fornecer princípios

FIGURA 3. EVOLUÇÃO RECENTE DA GOVERNAÇÃO CIBERNÉTICA

Fonte: Elaborado pelo autor com base em NATO (2024), União Europeia (2025), United Nations (2025) e CERT-EU (2026).

Ano	Desenvolvimento	Implicação
2024	NATO: decisão de criar o <i>NATO Integrated Cyber Defence Centre</i>	Reforço da defesa coletiva e da consciência situacional
2025	Regulamento (UE) 2025/38 – <i>Cyber Solidarity Act</i>	Deteção e resposta coordenadas a incidentes significativos
2025	ONU: relatório final do OEWG 2021–2025	Consolidação do quadro multilateral sobre comportamento responsável
2026	CERT-EU: <i>Threat Landscape Report 2025</i>	Evidência de maior diversidade de atores e uso crescente de IA

fundamentais – proibição do uso da força, resolução pacífica de controvérsias, legítima defesa e segurança coletiva –, mas a aplicação desses princípios exige práticas de atribuição e avaliação cada vez mais sofisticadas.

A quarta transformação é a centralidade crescente das empresas tecnológicas e dos operadores privados. Saliente-se que grande parte das infraestruturas, serviços de nuvem, sistemas de autenticação, plataformas e cadeias de fornecimento essenciais à segurança nacional encontra-se fora do controlo direto do Estado. A segurança internacional passa, assim, a depender de relações público-privadas que não substituem a soberania, mas condicionam a sua eficácia.

Por último, existe uma dimensão cognitiva do risco. Um ciberincidente pode produzir efeitos estratégicos mesmo quando o dano físico é limitado, se gerar percepções de vulnerabilidade, perda de controlo ou incapacidade estatal. A segurança passa, deste modo, a incluir confiança, continuidade de serviços e credibilidade institucional. O ciberterrorismo pode explorar precisamente essa dimensão: a capacidade de gerar medo pode ampliar os efeitos políticos para além do dano técnico inicial.

Conclusão

O ciberterrorismo constitui uma expressão particularmente complexa da sociedade do risco porque combina dependência tecnológica, vulnerabilidade sistémica, potencial de intimidação e dificuldade de atribuição. A sua relevância para a ordem mundial não decorre apenas da possibilidade de causar danos materiais, mas da capacidade de explorar interdependências e desafiar a capacidade dos Estados para assegurar segurança e continuidade.

A análise permite concluir que o Direito Internacional não deixou de ser aplicável ao ciberespaço. Pelo contrário, a evolu-

ção multilateral mais recente confirma a centralidade de um quadro normativo existente, cuja aplicação exige clarificação progressiva. A proibição do uso da força e o direito de legítima defesa continuam a constituir referências fundamentais, mas não autorizam respostas armadas automáticas perante qualquer ciberataque.

Para a ordem mundial, a questão decisiva não é saber se o ciberespaço está fora do Direito, mas como assegurar que o Direito continua a limitar o poder coercivo num ambiente em que tecnologia, poder económico e capacidade de disrupção se encontram distribuídos por Estados e atores não estatais.

A resposta juridicamente mais robusta deve seguir uma sequência: caracterização do incidente; preservação e avaliação da evidência; atribuição com grau de confiança explicitado; análise da escala, intensidade, contexto e efeitos; determinação do limiar jurídico relevante; identificação das opções disponíveis; e avaliação da necessidade, adequação e proporcionalidade da resposta. O recurso à força deve permanecer no extremo dessa escala, e não constituir o ponto de partida.

A principal prioridade estratégica situa-se, portanto, antes da força: prevenção, resiliência, inteligência, proteção de infraestruturas críticas, segurança das

cadeias de fornecimento, cooperação internacional e capacidade de recuperação.

A experiência recente da União Europeia, da NATO, das Nações Unidas e das estruturas de cibersegurança demonstra que a segurança digital é, cada vez menos, uma questão exclusivamente nacional.

Para a ordem mundial, a questão decisiva não é saber se o ciberespaço está fora do Direito, mas como assegurar que o Direito continua a limitar o poder coercivo num ambiente em que tecnologia, poder económico e capacidade de disrupção se encontram distribuídos por Estados e atores não estatais. A estabilidade internacional dependerá da capacidade de tornar juridicamente inteligíveis e politicamente previsíveis as fronteiras entre competição, coerção e conflito. ●

<https://doi.org/10.26619/2183-4822.2026.OM.8>

Referências

Beck, U. (1992). *Risk society: Towards a new modernity*. SAGE.

Beck, U. (2009). *World at risk*. Polity.

Canotilho, J. J. G.; Moreira, V. (2014). *Constituição da República Portuguesa anotada* (4.ª ed., Vol. I). Coimbra Editora.

CERT-EU (2026). *Threat landscape report 2025: A year in review*. Computer Emergency Response Team, União Europeia. <https://cert.europa.eu/publications/threat-intelligence/tlr2025/>

European Union Agency for Cybersecurity (2025). *ENISA threat landscape 2025*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

Giddens, A. (2005). *As consequências da modernidade* (4.ª ed.). Celta.

Gouveia, J. B. (2018). *Direito da segurança: Cidadania, soberania e cosmopolitismo*. Almedina.

Guedes, A. M. (2007). *Ligações perigosas: Conectividade, coordenação e aprendizagem em redes terroristas*. Almedina.

Guedes, A. M., & Santos, L. (2015). Breves reflexões sobre poder e ciberespaço. *Revista de Direito e Segurança*, (6), 189–210.

Guerreiro, A. N. (2018). DIP, ciberterrorismo e medidas de luta antiterrorismo. In M. L. Duarte & R. T. Lanceliro (Coords.), *O Direito Internacional e o uso da força no século XXI*. AAFDL Editora, 321-342.

NATO (2024). *Cyber defence*. North Atlantic Treaty Organization <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>

República Portuguesa (1976). *Constituição da República Portuguesa*.

Roscini, M. (2015). Cyber operations as a use of force. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace*. Edward Elgar Publishing, 233–254.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781316822524>

União Europeia (2025). Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho, de 19 de dezembro de 2024, que estabelece medidas destinadas a reforçar a solidariedade e as capacidades na União para detetar, preparar e dar resposta a ciberameaças e incidentes e que altera o Regulamento (UE) 2021/694 (Regulamento de Ciberresiliência). *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32025R0038>

United Nations (1945). *Charter of the United Nations*.

United Nations (2025). *Developments in the field of information and telecommunications in the context of international security: Final report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (A/80/257)*. <https://digitallibrary.un.org/record/4087789>

UNOCT (2026). *Cybersecurity and new technologies*. United Nations Office of Counter-Terrorism. <https://www.un.org/counterterrorism/en/cybersecurity>

Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of Article 2(4). *Yale Journal of International Law*, 36, 421–459.

FIGURA 4. QUATRO PRIORIDADES PARA UMA ORDEM MUNDIAL DIGITALMENTE RESILIENTE

Fonte: Elaborado pelo autor.

Prioridade	Objetivo
Prevenção e resiliência	Reduzir vulnerabilidades e assegurar continuidade de serviços essenciais.
Atribuição e inteligência	Melhorar a qualidade da evidência antes de respostas coercivas.
Cooperação internacional e público-privada	Partilhar informação, capacidades e mecanismos de resposta transfronteiriços.
Clarificação jurídica	Desenvolver entendimento comum sobre soberania, uso da força, ataque armado e legítima defesa no ciberespaço.