REVISTA DCS
FUNDADA EN 2000

A OBSOLESCÊNCIA DOS MODELOS DE GOVERNANÇA DE INFRAESTRUTURAS CRÍTICAS FRENTE À ACELERAÇÃO DAS AMEAÇAS CIBERNÉTICAS

THE OBSOLESCENCE OF CRITICAL INFRASTRUCTURE GOVERNANCE MODELS IN THE FACE OF ACCELERATING CYBER THREATS

LA OBSOLESCENCIA DE LOS MODELOS DE GOBERNANZA DE INFRAESTRUCTURAS CRÍTICAS ANTE LA ACELERACIÓN DE LAS CIBERAMENAZAS

Sandro Christovam Bearare[1], Eduardo Donzeli Paino[2]

DOI: 10.54899/dcs.v23i89.5135
Recibido: 02/03/2026 | Aceptado: 25/03/2026 | Publicación en línea: 02/04/2026.

RESUMO

Os modelos de governança destinados à proteção de infraestruturas críticas foram construídos sobre três premissas que, no cenário contemporâneo, já não correspondem à realidade operacional: que o adversário é identificável, que o Estado detém controle efetivo sobre os sistemas que deve proteger, e que as ameaças evoluem em velocidade compatível com a capacidade de resposta institucional. Este artigo argumenta que a simultânea falência dessas três premissas configura o que se denomina aqui de déficit de governança estrutural, entendido como a lacuna entre o que os modelos institucionais prometem entregar em termos de proteção e o que são efetivamente capazes de produzir diante das ameaças que se configuram na presente década. A metodologia aplicada é a revisão bibliográfica sistemática de natureza qualitativa, com análise de publicações científicas, relatórios de organismos governamentais e casos empiricamente documentados. O estudo examina como a confluência entre a inteligência artificial aplicada ao desenvolvimento de ataques, a aproximação da computação quântica como vetor de ruptura criptográfica, e a dependência crescente de infraestruturas privadas para funções de segurança nacional aprofunda esse déficit de forma que nenhum modelo de governança em vigor responde adequadamente. A questão central proposta para debate científico e político é a seguinte: se a arquitetura de governança é estruturalmente obsoleta, a quem cabe a responsabilidade pela lacuna entre o que as instituições prometem e o que conseguem entregar em termos de segurança nacional? Conclui-se que essa pergunta, ainda sem resposta formalizada em qualquer ordenamento jurídico internacional, é precisamente a que determinará a capacidade de resposta das democracias diante das crises cibernéticas que se aproximam.

Palavras-chave: Governança de Infraestruturas Críticas. Déficit de Governança Estrutural. Segurança Nacional. Ameaças Cibernéticas Emergentes. Responsabilidade Institucional.

[1] Especialista em Cybersegurança, Faculdade Líbano, Adamantina, São Paulo, Brasil. E-mail: s.chris@tutamail.com Orcid: https://orcid.org/0009-0003-2292-7907
[2] Graduado em Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia do Estado de São Paulo (FATEC - SP), Araçatuba, São Paulo, Brasil. E-mail: eduardo.donzeli@gmail.com

ABSTRACT

Governance models for critical infrastructure protection were built upon three premises that no longer correspond to operational reality: that adversaries are identifiable, that the State holds effective control over the systems it must protect, and that threats evolve at a pace compatible with institutional response capacity. This article argues that the simultaneous collapse of these three premises constitutes what is termed here a structural governance deficit, understood as the gap between what institutional models promise to deliver in terms of protection and what they are actually capable of producing against threats taking shape in the present decade. The methodology applied is a systematic qualitative bibliographic review, with analysis of scientific publications, government agency reports, and empirically documented cases. The study examines how the convergence of artificial intelligence applied to attack development, the approaching relevance of quantum computing as a cryptographic disruption vector, and the growing dependence on private infrastructure for national security functions deepens this deficit in ways that no governance model currently in force adequately addresses. The central question proposed for scientific and political debate is: if the governance architecture is structurally obsolete, who bears responsibility for the gap between what institutions promise and what they can actually deliver in terms of national security? It is concluded that this question, still without a formal answer in any international legal order, is precisely the one that will determine the response capacity of democracies in the face of approaching cyber crises.

Keywords: Critical Infrastructure Governance. Structural Governance Deficit. National Security. Emerging Cyber Threats. Institutional Accountability.

RESUMEN

Los modelos de gobernanza diseñados para proteger la infraestructura crítica se basaron en tres premisas que, en el contexto actual, ya no se corresponden con la realidad operativa: que el adversario es identificable, que el Estado ejerce un control efectivo sobre los sistemas que debe proteger y que las amenazas evolucionan a una velocidad compatible con la capacidad de respuesta institucional. Este artículo sostiene que el fallo simultáneo de estas tres premisas constituye lo que aquí se denomina un déficit estructural de gobernanza, entendido como la brecha entre lo que los modelos institucionales prometen ofrecer en términos de protección y lo que son capaces de producir realmente ante las amenazas emergentes de la presente década. La metodología aplicada consiste en una revisión sistemática de la literatura de carácter cualitativo, con análisis de publicaciones científicas, informes de organismos gubernamentales y casos documentados empíricamente. El estudio examina cómo la confluencia entre la inteligencia artificial aplicada al desarrollo de ataques, el enfoque de la computación cuántica como vector de disrupción criptográfica y la creciente dependencia de infraestructuras privadas para funciones de seguridad nacional profundiza este déficit, de tal manera que ningún modelo de gobernanza vigente ofrece una respuesta adecuada. La pregunta central que se plantea para el debate científico y político es la siguiente: si la arquitectura de gobernanza es estructuralmente obsoleta, ¿quién es responsable de la brecha entre lo que las instituciones prometen y lo que logran cumplir en materia de seguridad nacional? Se concluye que esta pregunta, aún sin una respuesta formal en ningún marco jurídico internacional, es precisamente la que determinará la capacidad de las democracias para responder a las inminentes crisis cibernéticas.

Palabras clave: Gobernanza de Infraestructuras Críticas. Déficit de Gobernanza Estructural.

Seguridad Nacional. Amenazas Cibernéticas Emergentes. Responsabilidad Institucional.

INTRODUÇÃO

Toda arquitetura institucional carrega em si uma data de validade que raramente aparece nos documentos que a fundam. As normas são escritas para responder a um problema diagnosticado em um determinado momento histórico. Quando o problema muda de natureza mais rápido do que a instituição consegue se adaptar, o resultado não é necessariamente o colapso visível das estruturas, mas algo mais insidioso: a manutenção da forma sem a substância, a preservação dos rituais de governança sem a capacidade efetiva de governar.

Os modelos de proteção de infraestruturas críticas ilustram esse fenômeno com precisão incomum. As arquiteturas regulatórias e institucionais desenvolvidas pelas principais democracias ocidentais para proteger sistemas essenciais como redes de energia, abastecimento de água, transporte e comunicações foram concebidas a partir de diagnósticos formulados em um ambiente de ameaças significativamente diferente do atual. Naquele ambiente, os adversários relevantes eram primariamente atores estatais com capacidades conhecidas e localizáveis, a infraestrutura crítica era em grande parte de propriedade e operação pública, e o ritmo de evolução tecnológica permitia que os ciclos regulatórios acompanhassem as mudanças no panorama de ameaças com um atraso que, embora existente, era tolerável.

Nenhuma dessas três condições prevalece hoje. O adversário cibernético contemporâneo pode ser um Estado soberano, uma organização criminosa transnacional, um grupo terrorista, um agente contratado por múltiplos patrocinadores simultâneos, ou a combinação dinâmica de todos esses elementos em diferentes fases de um mesmo ataque. A infraestrutura que os Estados devem proteger é majoritariamente de propriedade e operação privada, o que cria uma dependência estrutural do setor privado para a execução de funções de segurança nacional. E o ritmo de evolução das ameaças, acelerado pela disponibilidade crescente de ferramentas baseadas em inteligência artificial, tornou-se estruturalmente incompatível com os ciclos de deliberação, aprovação e implementação que caracterizam os processos regulatórios tradicionais.

Este artigo propõe uma categoria analítica para nomear esse fenômeno: o déficit de

governança estrutural. O conceito designa a lacuna entre o que os modelos institucionais de proteção de infraestruturas críticas formalmente prometem entregar e o que são efetivamente capazes de produzir diante das ameaças que se configuram no presente. A relevância da categoria não está apenas no diagnóstico, mas na pergunta que dela decorre e que permanece sem resposta formalizada em qualquer ordenamento jurídico nacional ou internacional: se a arquitetura de governança é estruturalmente obsoleta, a quem cabe a responsabilidade pela lacuna?

Essa é uma questão filosófica, política e jurídica antes de ser técnica. É precisamente por isso que ela merece atenção científica sistemática: no debate público ela permanece capturada pelo vocabulário especializado de profissionais de segurança da informação, invisível para os campos da ciência política, do direito internacional e da filosofia institucional, que possuem as ferramentas conceituais necessárias para respondê-la. O presente artigo é uma contribuição para tornar essa pergunta visível nesses campos.

METODOLOGIA

Este trabalho foi desenvolvido segundo a metodologia de revisão bibliográfica sistemática de natureza qualitativa. O recorte temático combina três campos que raramente dialogam na literatura especializada: a teoria das instituições e da governança, os estudos de segurança internacional, e a análise crítica de políticas públicas em segurança cibernética. Essa combinação é intencional e constitui parte da contribuição original do artigo: o déficit de governança estrutural só se torna analiticamente visível quando esses três campos são lidos em conjunto.

As fontes consultadas compreendem publicações científicas em periódicos revisados por pares, relatórios de agências governamentais especializadas, documentos de organismos internacionais com atuação na área de segurança cibernética, e produção acadêmica de centros de pesquisa reconhecidos nas áreas de segurança internacional e política cibernética. A seleção priorizou obras que abordam os fundamentos institucionais e jurídicos da governança cibernética, em detrimento de publicações centradas em soluções técnicas, dado que o problema examinado é de natureza política e filosófica, não tecnológica.

A análise segue uma estrutura argumentativa progressiva: parte da identificação das premissas fundadoras dos modelos de governança existentes, demonstra empiricamente a ruptura dessas premissas com base em casos verificáveis, introduz a categoria analítica do déficit de governança estrutural, examina os vetores que o aprofundam na próxima década, e conclui com

a formulação da questão central sobre responsabilidade institucional. O objetivo não é oferecer soluções técnicas, mas delimitar com rigor conceitual um problema que, sem essa delimitação, permanece invisível para os atores políticos e jurídicos que teriam capacidade de endereçá-lo.

DISCUSSÃO

As Três Premissas Fundadoras e sua Ruptura Contemporânea

Todo modelo de governança repousa sobre premissas implícitas acerca da natureza do problema que foi criado para resolver. Tornar essas premissas explícitas é o primeiro passo para avaliar se o modelo ainda serve ao propósito que o fundou. No caso da governança de infraestruturas críticas, três premissas estruturam os frameworks em vigor nas principais democracias ocidentais, e as três apresentam rupturas documentáveis.

A primeira premissa é a da identificabilidade do adversário. Os modelos de segurança nacional tradicionais foram concebidos para um mundo em que a ameaça tinha endereço: um Estado soberano com território, forças armadas identificáveis e interesses estratégicos mapeáveis. Mesmo nos períodos de maior tensão geopolítica do século XX, quando a natureza da ameaça era existencial, ela era ao menos localizável. Os modelos de proteção de infraestruturas críticas herdaram essa lógica: pressupõem que é possível identificar quem ataca, atribuir responsabilidade com suficiente clareza e, a partir daí, acionar mecanismos de resposta, sejam eles diplomáticos, econômicos ou militares.

Essa premissa não corresponde ao ambiente operacional contemporâneo. O ataque ao oleoduto Colonial Pipeline, nos Estados Unidos, em maio de 2021, foi executado pelo grupo DarkSide, uma organização criminosa operando no modelo de ransomware como serviço, provavelmente sediada na Rússia, mas sem vínculo juridicamente comprovado com qualquer governo (CISA, 2023). A investigação subsequente revelou que o ponto de entrada foi uma conta de acesso remoto inativa, sem verificação dupla de identidade, que havia sido comprometida anteriormente. O adversário existia, causou dano de escala nacional, mas não era nem plenamente identificável nem juridicamente responsabilizável dentro dos marcos institucionais disponíveis. O mesmo padrão caracterizou os ataques às distribuidoras de energia elétrica da Ucrânia em dezembro de 2015, atribuídos ao grupo Sandworm por agências de inteligência ocidentais, mas jamais sujeitos a qualquer mecanismo formal de responsabilização internacional (Lee; Assante;

Conway, 2016).

A segunda premissa é a do controle estatal sobre os objetos de proteção. Os modelos de segurança nacional presumem que o Estado tem autoridade operacional sobre o que deve defender. Essa presunção era razoável quando a infraestrutura crítica era predominantemente pública. As ondas de privatização e concessão que caracterizaram a política econômica das últimas décadas em boa parte do mundo ocidental transferiram o controle operacional dessas infraestruturas ao setor privado, ao mesmo tempo em que o Estado permaneceu como titular formal da responsabilidade pela sua segurança. O resultado é uma dissociação estrutural entre responsabilidade e capacidade: os governos respondem politicamente por falhas de segurança em sistemas que não operam, não financiam diretamente e sobre os quais exercem apenas supervisão regulatória indireta. Nos sistemas onde essa dissociação é mais pronunciada, como no setor energético norte-americano e em segmentos do setor de telecomunicações em diversos países, o Estado possui autoridade nominal sem a capacidade operacional que tornaria essa autoridade exequível.

A terceira premissa é a da compatibilidade de ritmos entre a evolução das ameaças e a capacidade de resposta institucional. Conceber, aprovar, implementar e absorver um framework regulatório são processos que operam em ciclos de anos. A premissa implícita é que as ameaças evoluem em velocidade suficientemente compatível com esses ciclos para que o instrumento ainda seja relevante quando finalmente entra em operação plena. Essa compatibilidade de ritmos deixou de existir. O relatório do Government Accountability Office dos Estados Unidos sobre riscos de inteligência artificial para infraestruturas críticas, publicado em 2025, constatou que nenhuma das avaliações de risco setoriais submetidas pelas agências federais cumpriu integralmente os requisitos mínimos para uma avaliação metodologicamente válida, incluindo a estimativa de probabilidade de ocorrência dos eventos identificados (GAO, 2025). Se as agências do país com maior investimento histórico em segurança cibernética não conseguem produzir avaliações de risco metodologicamente completas, a lacuna entre o ritmo de evolução da ameaça e a capacidade de resposta institucional é estrutural, não circunstancial.

O Déficit de Governança Estrutural como Categoria Analítica

A ruptura simultânea das três premissas fundadoras não produz o colapso imediato e visível das instituições de governança. Produz algo mais difícil de diagnosticar e politicamente

mais inconveniente: instituições que continuam operando com plena aparência de legitimidade e funcionalidade, mas que perderam progressivamente a capacidade de cumprir o propósito para o qual foram criadas. É para nomear esse fenômeno que este artigo propõe a categoria do déficit de governança estrutural.

O conceito articula três dimensões analíticas interdependentes. A primeira é a dimensão normativa: quando os padrões e requisitos que compõem um framework regulatório foram estabelecidos para um modelo de ameaça que já não é o prevalente, a conformidade com esses padrões deixa de ser equivalente à segurança efetiva. Uma organização pode estar em plena conformidade com todos os requisitos vigentes e ainda assim ser inteiramente vulnerável a vetores de ataque que os requisitos não contemplam porque emergiram após sua formulação. Conformidade e segurança tornam-se conceitos dissociados, e o framework perde sua razão de ser sem, necessariamente, perder sua vigência formal.

A segunda dimensão é a operacional: a lacuna entre as capacidades que os modelos pressupõem que os atores possuem e as que de fato possuem. O caso brasileiro do Superior Tribunal de Justiça, atacado em novembro de 2020 pelo ransomware RansomExx, ilustra essa dimensão com clareza. O ataque paralisou completamente as operações judiciais por mais de uma semana, comprometeu sistemas de backup, exigiu intervenção do Centro de Defesa Cibernética do Exército Brasileiro, e revelou que uma das mais importantes instituições do Poder Judiciário do país operava sem redundâncias adequadas em sistemas classificáveis como críticos para a continuidade do Estado (Carnegie Endowment, 2023). A existência de estratégias e diretrizes nacionais de segurança cibernética não impediu o ataque, não limitou seus efeitos e não produziu nenhum mecanismo de responsabilização posterior pela falha sistêmica que ele expôs.

A terceira dimensão é a política: a ausência de mecanismos formais de responsabilização pela lacuna como um todo. Quando uma infraestrutura crítica é atacada com sucesso e a investigação demonstra que os modelos de governança em vigor não foram suficientes para prevenir o ataque, a resposta institucional padrão é a formulação de novos requisitos, a criação de novos grupos de trabalho e a publicação de novos guias orientativos. O que não ocorre é a responsabilização formal de qualquer ator institucional pela falha do sistema de proteção como conjunto. Essa ausência de responsabilização não é periférica ao déficit: ela é constitutiva dele, porque elimina o incentivo sistêmico para que os modelos de governança se reformem na velocidade que o ambiente de ameaças exige.

A Inteligência Artificial e a Aceleração Assimétrica das Ameaças

A inteligência artificial introduz no campo das ameaças cibernéticas uma assimetria qualitativa que os modelos de governança existentes não foram projetados para absorver. A questão não é apenas quantitativa, embora o aumento no volume de ataques seja mensurável e significativo. A questão mais relevante é uma mudança na natureza do processo de desenvolvimento e execução de ataques que altera a relação estrutural entre atacantes e defensores.

Historicamente, ataques sofisticados a infraestruturas críticas exigiam recursos humanos altamente especializados, tempo extenso de preparação e reconhecimento, e acesso a ferramentas desenvolvidas por atores com capacidade institucional relevante. O ataque às distribuidoras de energia elétrica da Ucrânia em 2015 levou pelo menos oito meses de preparação antes de sua execução, envolveu reconhecimento meticuloso das redes das três distribuidoras afetadas e exigiu competências técnicas específicas sobre sistemas de controle industrial que apenas um conjunto restrito de atores possuía (Lee; Assante; Conway, 2016). Essa barreira de entrada funcionava como um filtro: limitava o número de atores capazes de executar ataques de alta consequência contra infraestruturas críticas.

A disponibilidade crescente de ferramentas baseadas em inteligência artificial erode essa barreira de forma sistemática. O Departamento de Segurança Interna dos Estados Unidos categorizou os riscos de inteligência artificial para infraestruturas críticas em três tipos distintos: ataques que utilizam inteligência artificial para planejar, escalar ou executar ações maliciosas; ataques que têm os próprios sistemas de inteligência artificial como alvo; e falhas decorrentes de design ou implementação inadequados de inteligência artificial em ambientes de controle crítico (DHS, 2024). Essa taxonomia revela que a inteligência artificial não é apenas uma ferramenta de ataque: ela é simultaneamente um vetor de ataque, um alvo e uma fonte potencial de falha sistêmica não intencional.

Para os modelos de governança, a consequência mais relevante dessa transformação não é técnica: é temporal. Se o tempo necessário para desenvolver e executar um ataque sofisticado se comprime de meses para dias graças à automação, o ciclo de resposta institucional, que opera em escala de meses e anos, torna-se estruturalmente incompatível com a velocidade do problema que deve resolver. Nenhum processo regulatório concebido para funcionar em escala humana de deliberação e implementação consegue ser contemporâneo de ameaças que se desenvolvem em

escala de máquina. Essa incompatibilidade não é uma falha que mais recursos ou melhor gestão podem corrigir dentro dos parâmetros dos modelos existentes: é uma ruptura estrutural que exige repensar as premissas sobre as quais esses modelos foram construídos.

A Computação Quântica e o Horizonte de Ruptura Criptográfica

A computação quântica representa uma ameaça de natureza diferente das discutidas até aqui: não é imediata, mas tem prazo. Especialistas estimam que computadores quânticos com capacidade criptograficamente relevante, ou seja, capazes de quebrar os algoritmos de criptografia assimétrica sobre os quais toda a segurança digital contemporânea repousa, possam emergir dentro da presente década. A ruptura que isso produziria não seria apenas técnica: tornaria obsoletos, de forma simultânea, os fundamentos de segurança de comunicações governamentais, sistemas bancários, redes de controle industrial e qualquer infraestrutura que utilize os padrões criptográficos hoje dominantes.

O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos concluiu, em 2024, após oito anos de desenvolvimento e avaliação, os primeiros padrões definitivos de criptografia pós-quântica, projetados para resistir à capacidade computacional de máquinas quânticas (NIST, 2024). O esforço de transição é de escala comparável a reformas de infraestrutura física: envolve a substituição de componentes em cada sistema que utiliza criptografia assimétrica, incluindo equipamentos industriais com vida útil de décadas que foram projetados sem qualquer previsão de atualização criptográfica.

A questão de governança mais urgente que a computação quântica coloca não é técnica: é temporal e estratégica. Adversários já executam o que especialistas denominam ataques do tipo "coleta agora, descriptografa depois": acumulam hoje volumes de dados criptografados interceptados para descriptografá-los quando a tecnologia quântica tornar isso possível (NIST IR 8547, 2024). Isso significa que informações sensíveis sobre infraestruturas críticas, coletadas de redes que hoje operam com os padrões criptográficos convencionais, podem se tornar acessíveis a adversários em um horizonte de cinco a dez anos. Os modelos de governança existentes foram universalmente projetados para responder a ameaças presentes. Nenhum deles incorpora mecanismos formais para responder a ameaças que se materializarão no futuro com base em ações executadas no presente.

A Privatização da Segurança Nacional e o Desalinhamento de Incentivos

A dependência estrutural do Estado em relação ao setor privado para a proteção de funções essenciais de segurança nacional cria um paradoxo de responsabilidade que os modelos de governança existentes não resolvem: os governos são politicamente responsáveis pela segurança de infraestruturas que não controlam operacionalmente, enquanto as organizações que as controlam operam sob incentivos que não são naturalmente alinhados com prioridades de segurança nacional.

Uma organização privada que opera uma infraestrutura crítica toma suas decisões de investimento em segurança a partir de cálculos que incorporam probabilidades estimadas de incidentes, impactos financeiros diretos, obrigações regulatórias e exposição a responsabilidade civil. Esses cálculos não capturam adequadamente as externalidades de segurança nacional: o custo social de uma interrupção ampla do fornecimento de energia ou de um comprometimento de sistemas de abastecimento de água é incomparavelmente maior do que o custo que a organização operadora internalizaria em qualquer cenário de responsabilização convencional. Parte significativa desse custo é socializada, absorvida pelo Estado e pela população, independentemente das decisões de investimento que o geraram.

O ataque ao Colonial Pipeline ilustra essa estrutura com precisão. A organização operadora pagou um resgate equivalente a 4,4 milhões de dólares para recuperar acesso aos seus sistemas. O custo social do evento, que incluiu escassez de combustível em dezessete estados norte-americanos, declaração de emergência federal, perturbação do transporte aéreo e pânico de abastecimento em milhares de postos de combustível, foi de magnitude incomparavelmente maior e foi absorvido pelo Estado e pela população, não pela organização operadora (CISA, 2023). A vulnerabilidade explorada no ataque era conhecida e corrigível a custo relativamente baixo. O cálculo de risco privado, que não captura o custo social das externalidades que as decisões de investimento geram, não produziu o incentivo suficiente para a correção preventiva.

Os modelos de governança existentes tentam endereçar esse desalinhamento por meio de requisitos regulatórios mínimos e mecanismos de compartilhamento de informações entre governo e setor privado. Esses instrumentos produzem algum efeito, mas são insuficientes para resolver o problema estrutural: nenhum deles cria para os operadores privados uma responsabilidade proporcional ao custo social das externalidades de segurança que suas decisões de investimento geram. Enquanto essa proporcionalidade não for institucionalmente estabelecida,

o desalinhamento de incentivos persistirá independentemente da qualidade dos documentos normativos produzidos.

O Vácuo de Responsabilidade e a Questão que os Ordenamentos Ainda Não Responderam

A confluência das rupturas examinadas anteriormente configura o déficit de governança estrutural como um problema sistêmico de natureza política e jurídica: quem é responsável pela lacuna entre o que os modelos de governança prometem e o que conseguem entregar? Não em sentido moral abstrato, mas em sentido jurídico e institucional concreto. Quando uma infraestrutura crítica é atacada com sucesso e a investigação posterior demonstra que os modelos de governança em vigor não foram suficientes para prevenir o ataque, qual mecanismo formal de responsabilização é acionado? A resposta atual, em qualquer ordenamento jurídico examinado, é: nenhum de caráter sistêmico.

O esforço mais avançado da comunidade internacional para estabelecer um quadro normativo aplicável ao ciberespaço produziu, ao longo de décadas, instrumentos de considerável refinamento intelectual, mas de caráter não vinculante. O Tallinn Manual 2.0, elaborado por um grupo de especialistas internacionais em direito internacional a convite do Centro de Excelência de Defesa Cibernética Cooperativa da OTAN e publicado pela Cambridge University Press em 2017, identifica 154 regras aplicáveis a operações cibernéticas e representa o esforço acadêmico mais abrangente de sistematização do direito internacional aplicável ao ciberespaço. No entanto, o próprio documento reconhece explicitamente seu caráter não vinculante: ele representa a visão de especialistas em sua capacidade individual, não a posição de nenhum Estado ou organização internacional, e não produz qualquer obrigação jurídica formal (Schmitt, 2017). Ao mesmo tempo em que serve como referência para governos e assessores jurídicos ao redor do mundo, o Tallinn Manual ilustra precisamente o paradoxo que caracteriza o campo: o instrumento mais sofisticado disponível para orientar o comportamento estatal no ciberespaço é, por definição, desprovido de força vinculante.

No plano multilateral, acordos sobre comportamento responsável dos Estados no ciberespaço têm sido produzidos em fóruns como o Grupo de Especialistas Governamentais das Nações Unidas em Segurança Cibernética. Esses acordos estabelecem normas de comportamento, reconhecem a aplicabilidade do direito internacional ao ciberespaço e afirmam a responsabilidade dos Estados por atividades cibernéticas maliciosas conduzidas a partir de seu território.

Permanecem, contudo, no campo das normas voluntárias, sem mecanismos de verificação, sem instâncias de adjudicação e sem sanções vinculantes para o descumprimento. A distância entre o acordo político sobre princípios e a capacidade de responsabilizar qualquer ator pelo descumprimento desses princípios é, ela mesma, uma expressão do déficit de governança estrutural em sua dimensão internacional.

No plano doméstico, a situação apresenta variações mas uma característica comum: os instrumentos de governança orientam comportamentos e estabelecem padrões, mas não criam responsabilidade sistêmica pela falha coletiva do sistema de proteção. Essa ausência de responsabilização não é uma omissão acidental. É o reflexo de uma dificuldade genuína: quando a falha de proteção é o resultado da interação entre múltiplos atores institucionais e privados, cada um operando dentro de suas próprias obrigações regulatórias, a responsabilidade pelo resultado sistêmico não se localiza em nenhum deles individualmente. É o que a teoria das instituições denomina de problema de ação coletiva de segundo nível: não apenas a falha de coordenação entre atores para produzir um bem público, mas a falha de qualquer mecanismo de responsabilização que tornasse a coordenação um imperativo para cada ator individualmente (Olson, 1965).

A pergunta que este artigo propõe ao debate científico não é retórica: aponta para uma lacuna conceitual e normativa real que nenhum framework existente preenche. Preencher essa lacuna exige, antes de qualquer solução técnica ou regulatória, que ela seja nomeada, delimitada e reconhecida como um problema de natureza jurídica e política, e não meramente tecnológica, pelos campos disciplinares com as ferramentas conceituais necessárias para respondê-la.

CONSIDERAÇÕES FINAIS

Este artigo partiu de um diagnóstico estrutural: os modelos de governança para proteção de infraestruturas críticas foram construídos sobre premissas que já não descrevem o mundo em que operam. A implicação desse diagnóstico é mais profunda do que a formulação inicial sugere. Não se trata de instrumentos que precisam de atualização técnica, embora isso também seja verdade. Trata-se de uma arquitetura institucional que pressupõe capacidades de identificação, controle e resposta que as democracias contemporâneas não possuem e que, nas condições que se aproximam, terão dificuldade crescente de desenvolver dentro dos parâmetros dos modelos existentes.

A inteligência artificial comprime o tempo entre a concepção e a execução de ataques sofisticados de meses para dias, criando uma incompatibilidade estrutural com ciclos regulatórios que operam em escala de anos. A computação quântica ameaça tornar obsoletos, em um horizonte de aproximadamente uma década, os fundamentos criptográficos de toda a segurança digital contemporânea, incluindo os sistemas de controle de infraestruturas projetados para operar por décadas. O desalinhamento entre os incentivos de mercado das organizações privadas que operam infraestruturas críticas e as exigências de segurança nacional persiste enquanto nenhum mecanismo de responsabilização for capaz de capturar o custo social das externalidades geradas por decisões de investimento privadas.

A questão central que este artigo propõe ao debate científico e político não tem resposta formalizada em nenhum ordenamento jurídico hoje em vigor. Quem é responsável pela lacuna entre o que os modelos de governança de infraestruturas críticas prometem e o que conseguem entregar? Essa pergunta é relevante não porque produz uma resposta fácil, mas porque sua ausência de resposta é ela mesma um dado político de grande importância: revela que as democracias contemporâneas aceitaram implicitamente um nível de risco sistêmico sobre seus sistemas essenciais sem que nenhum agente institucional seja formalmente responsável por esse risco.

O campo científico tem aqui uma contribuição insubstituível a oferecer, não a solução técnica para os problemas identificados, mas a delimitação rigorosa do problema de governança, o desenvolvimento de categorias analíticas que tornem visível o que o vocabulário técnico especializado obscurece, e a formulação das perguntas que os atores políticos e jurídicos precisam responder antes que as consequências do déficit de governança estrutural se materializem de forma que nenhuma resposta posterior consiga adequadamente reparar.

O momento em que o mundo descobrirá que as infraestruturas críticas são vulneráveis já passou. Esse descobrimento ocorreu repetidamente e com evidências abundantes. O que ainda está em aberto é se as democracias construirão a capacidade institucional de responder a essa vulnerabilidade antes que ela produza consequências sistêmicas de maior escala. A resposta a essa questão não está nos instrumentos técnicos disponíveis: está nas escolhas políticas e jurídicas que as sociedades façam sobre como distribuir responsabilidade, autoridade e accountability sobre os sistemas de que dependem para funcionar.

REFERÊNCIAS

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE. **Brazil's cyber strategy under Lula: not a priority, but progress is possible.** Washington: Carnegie Endowment, ago. 2023. Disponível em: <https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible>. Acesso em: mar. 2026.

CISA - CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **The attack on Colonial Pipeline: what we've learned and what we've done over the past two years.** Washington: CISA, 2023. Disponível em: <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>. Acesso em: mar. 2026.

DHS - DEPARTMENT OF HOMELAND SECURITY. **Safety and security guidelines for critical infrastructure owners and operators.** Washington: DHS, abr. 2024. Disponível em: <https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf>. Acesso em: mar. 2026.

GAO - GOVERNMENT ACCOUNTABILITY OFFICE. **Artificial intelligence: DHS needs to improve risk assessment guidance for critical infrastructure sectors.** GAO-25-107435. Washington: GAO, 2025. Disponível em: <https://www.gao.gov/products/gao-25-107435>. Acesso em: mar. 2026.

LEE, R. M.; ASSANTE, M. J.; CONWAY, T. **Analysis of the cyber attack on the Ukrainian power grid.** Washington: SANS ICS; E-ISAC, 2016. 56 p.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Post-quantum cryptography standardization: FIPS 203, FIPS 204, FIPS 205.** Gaithersburg: NIST, ago. 2024. Disponível em: <https://csrc.nist.gov/projects/post-quantum-cryptography>. Acesso em: mar. 2026.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST IR 8547: transition to post-quantum cryptography standards.** Gaithersburg: NIST, nov. 2024. Disponível em: <https://csrc.nist.gov/pubs/ir/8547/ipd>. Acesso em: mar. 2026.

OLSON, M. **The logic of collective action: public goods and the theory of groups.** Cambridge: Harvard University Press, 1965. 176 p.

SCHMITT, M. N. (Ed.). **Tallinn Manual 2.0 on the international law applicable to cyber operations.** Cambridge: Cambridge University Press, 2017. 598 p.