NONAGÉSIMO SÉTIMO PERÍODO ORDINÁRIO DE SESSÕES
3–7 de agosto de 2020
Sessão virtual

OEA/Ser. Q
CJI/RES. 260 (XCVII-O/20)
7 agosto 2020
Original: espanhol

CJI/RES. 260 (XCVII-O/20)

DIREITO INTERNACIONAL E OPERAÇÕES CIBERNÉTICAS DO ESTADO

A COMISSÃO JURÍDICA INTERAMERICANA,

LEVANDO EM CONTA que a Assembleia Geral da OEA, mediante a resolução AG/RES. 2930 (XLIX-O/19), "Direito internacional", no item i sobre "Observações e recomendações sobre o Relatório Anual da Comissão Jurídica Interamericana", solicitou à CJI que informasse permanentemente sobre os progressos alcançados em relação aos temas incluídos em sua agenda, tais como os assuntos relativos aos acordos vinculantes e não vinculantes;

CONSCIENTE da necessidade de fornecer aos Estados membros da OEA parâmetros claros sobre a aplicação do Direito internacional ao ciberespaço, limitando assim os riscos de escalada ou conflito não intencional;

TENDO EM CONTA o documento "*Derecho Internacional y Operaciones Cibernéticas del Estado: Mejora de la Transparencia – Quinto Informe"*, documento CJI/doc.615/20, apresentado pelo Doutor Duncan B. Hollis, relator do tema,

RESOLVE:

1. Agradecer ao Doutor Duncan B. Hollis seu trabalho como relator do tema e a apresentação do referido relatório.

2. Com base nas propostas do relatório acima mencionado, recomendar à Assembleia Geral que apoie a aplicabilidade do Direito internacional às operações estatais no ciberespaço mediante a adoção da seguinte declaração:

> "*A Assembleia Geral da OEA afirma que o Direito internacional, incluindo a Carta das Nações Unidas em sua totalidade, a Carta da Organização dos Estados Americanos, o Direito humanitário internacional, o Direito internacional dos direitos humanos, o dever de não intervenção, a igualdade soberana dos Estados e o Direito de responsabilidade do Estado, é aplicável ao uso das tecnologias da informação e das comunicações (TICs) por parte dos Estados e daqueles que são internacionalmente responsáveis*."

3. Solicitar ao Departamento de Direito Internacional, na sua qualidade de Secretaria Técnica da Comissão Jurídica Interamericana, que apresente à CJI uma proposta para apoiar ou realizar atividades de capacitação sobre a aplicação do Direito internacional ao ciberespaço dirigidas a diversos atores.

4. Manter o tema em sua agenda, expandindo o seu âmbito para além dos temas do Direito internacional relativos à paz e à segurança internacionais, de modo a abranger outros regimes internacionais.

Esta resolução foi aprovada por unanimidade, na sessão ordinária de 7 de agosto de 2020, pelos seguintes membros: Doutores Luis García-Corrochano Moyano, Eric P. Rudge, Mariana Salazar Albornoz, José Antonio Moreno Rodríguez, Milenko Bertrand-Galindo Arriagada, Duncan B. Hollis, Alix Richard, George Rodrigo Bandeira Galindo, Miguel A. Espeche-Gil, Íñigo Salvador Crespo e Ruth Correa Palacio.

NONAGÉSIMO SÉTIMO PERÍODO ORDINÁRIO DE SESSÕES
3 a 7 de agosto de 2020
Sessão virtual

OEA/Ser. Q
CJI/doc.615/20 rev.1
7 agosto 2020
Original: inglês

DIREITO INTERNACIONAL E OPERAÇÕES CIBERNÉTICAS DO ESTADO: MELHORIA DA TRANSPARÊNCIA — QUINTO RELATÓRIO

(Apresentado pelo professor Duncan B. Hollis)

1. Este é o meu quinto e último relatório sobre o tema da melhoria da transparência no que diz respeito à forma como os Estados membros entendem a aplicação do direito internacional às operações cibernéticas estatais. Este projeto visa contribuir para uma tendência mais ampla nas relações internacionais que buscam maior transparência na forma como os Estados nacionais entendem a aplicação do direito internacional ao ciberespaço. Ao fazê-lo, o que se busca é alcançar quatro objetivos:

a) identificar áreas de convergência na forma como os Estados entendem quais são as regras legais internacionais que se aplicam e como o fazem. Quando se combina com declarações existentes de Estados situados fora da região, uma uniformidade de pontos de vista pode fornecer comprovação adicional para delinear as regras de direito internacional consuetudinário pertinentes;

b) identificar pontos de vista divergentes sobre que normas internacionais se aplicam ou como o fazem. Isso pode ajudar a estabelecer uma linha de base para um diálogo adicional, seja para conciliar posições conflituosas, para esclarecer o teor da lei ou talvez até mesmo para buscar modificações na lei;

c) limitar os riscos de escalada ou conflito não intencional, já que os Estados têm interpretações diferentes da aplicação do direito internacional e desconhecem ou não compreendem como os outros veem o problema; e

d) dar à OEA e aos Estados membros uma voz apropriada nos diálogos mundiais sobre a aplicação do direito internacional.

Ao mesmo tempo, é importante reiterar o que este projeto não pretende fazer. Ele não tem por objetivo codificar nem desenvolver progressivamente o direito internacional (nem mesmo identificar as melhores práticas ou a orientação geral). Tampouco pretende oferecer uma perspectiva integral ou geral sobre questões legais internacionais no contexto cibernético.

2. Em vez disso, este projeto destina-se a ser um modesto primeiro passo, e como tal deve ser lido. A Comissão Jurídica (e a OEA em termos mais gerais) pode usar os materiais aqui apresentados para avaliar quais atividades adicionais, se houver, poderiam ser realizadas a fim de conferir mais transparência à forma como se aplica o direito internacional aos Estados da região, a suas operações cibernéticas e a suas reações às ameaças cibernéticas vindas de outros. A Comissão também poderia considerar a possibilidade de aumentar os esforços de capacitação existentes, a fim de aprimorar os conhecimentos e a experiência dos funcionários pertinentes em relação à aplicação do direito internacional ao ciberespaço. Isso pode implicar a compilação (e publicação) de pontos de vista nacionais adicionais e/ou o estabelecimento de plataformas ou outros processos para o compartilhamento de informações e o diálogo sobre a relação do direito internacional com o ciberespaço e as tecnologias da informação e das comunicações (TICs) das quais se deriva.

3. Meu primeiro relatório destacou a visibilidade limitada do direito internacional na regulação das operações cibernéticas estatais, apesar do número crescente desse tipo de operações e de suas implicações econômicas, humanitárias e de segurança nacional[1]. É verdade que muitos Estados confirmaram a aplicabilidade do direito internacional ao seu comportamento no ciberespaço[2]. E, embora a OEA não o tenha feito, outras organizações internacionais (ASEAN, União Europeia e Nações Unidas) também o fizeram[3]. Até à data, porém, os esforços para descrever como os Estados entendem a aplicação do direito internacional ao ciberespaço têm tido um sucesso limitado.

4. Parte do problema na aplicação do direito internacional ao ciberespaço decorre da falta de normas ou padrões sob medida. Quando se trata da paz e da segurança internacionais, por exemplo, não existem tratados específicos de cibersegurança. E aquelas convenções que tratam da criminalidade cibernética — a Convenção de Budapeste e (se algum dia entrar em vigor) a Convenção da União Africana — apenas abordam, por definição, o comportamento dos atores não estatais com o apoio de uma minoria de Estados nacionais[4]. Portanto, a aplicação do direito internacional ao ciberespaço depende da analogia com tratados multilaterais mais gerais (por exemplo, a Carta das Nações Unidas) ou com o direito internacional consuetudinário.

5. Contudo, como sublinhei no meu segundo relatório, em nível mundial não existe um consenso universal entre os Estados sobre quais normas internacionais gerais vigentes se aplicam às operações cibernéticas, muito menos sobre como o fazem[5]. Para vários regimes jurídicos internacionais (por exemplo, defesa própria, direito internacional humanitário, contramedidas, soberania — como regra independente — e devida diligência), um ou mais Estados contestam sua aplicação integral ao ciberespaço, enquanto outros diferem (às vezes drasticamente) na forma como interpretam a aplicação dessas regras às operações cibernéticas estatais e patrocinadas pelo Estado.

---

[1] Ver Duncan B. Hollis, *Direito Internacional e Operações Cibernéticas Estatais: Melhoria da Transparência*, OEA/Ser.Q, CJI/doc.570/18 (9 de agosto de 2018) ("Hollis, Primeiro Relatório"), em http://www.oas.org/en/sla/iajc/docs/CJI_doc_570-18.pdf.

[2] Ver Secretário-Geral da ONU, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶19, U.N. Doc. A/68/98 (24 de junho de 2013) ("o direito internacional, e em particular a Carta das Nações Unidas, aplica-se" ao ciberespaço); ver também Secretário-Geral da ONU, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶24, U.N. Doc. A/70/174 (22 de julho de 2015)

[3] Ver UNGA Res. 266, U.N. Doc. A/RES/73/266 (2 de janeiro de 2019); Declaração dos Líderes da ASEAN e dos Estados Unidos sobre Cooperação em Segurança Cibernética (18 de novembro de 2018), em https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf ; Declaração da União Europeia: Primeiro Comitê das Nações Unidas, debate temático sobre outras medidas de desarmamento e segurança internacional (26 de outubro de 2018) ("*EU Statement*"), em https://eeas.europa.eu/delegations/un-new-york/52894/eu-statement-–-united-nations-1st-committee-thematic-discussion-other-disarmament-measures-and_en. Tanto o G7 como o G20 fizeram afirmações semelhantes. Ver, por exemplo, a Declaração do G7 sobre a Responsabilidade dos Estados por sua Conduta no Ciberespaço (11 de abril de 2017) em https://www.mofa.go.jp/files/000246367.pdf; Comunicado dos Líderes da Cúpula do G20 em Antália (15–16 de novembro de 2015) ¶26, em http://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf.

[4] Conselho da Europa, Convenção sobre o Cibercrime, (Budapeste, 23 de novembro de 2001) CETS Nº 185; Convenção da UA sobre Segurança Cibernética e Proteção de Dados Pessoais, 27 de junho de 2014, AU Doc. EX.CL/846(XXV). A Convenção de Budapeste tem hoje 65 partes, embora vários outros Estados a vejam com alguma hostilidade. Ver Convenção sobre Cibercriminalidade, em http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

[5] B. Hollis, *Direito Internacional e Operações Cibernéticas Estatais: Melhoria da Transparência*, OEA/Ser.Q, CJI/doc 578/19 (21 de janeiro de 2019) ("Hollis, Segundo Relatório"), em http://www.oas.org/en/sla/iajc/docs/CJI_doc_578-19.pdf

6. Os Estados parecem igualmente relutantes em invocar a linguagem do direito internacional quando fazem acusações sobre as operações cibernéticas de outros Estados[6]. Em uma notável exceção, em 2018 cinco Estados (Austrália, Canadá, Países Baixos, Nova Zelândia e Reino Unido) acusaram o GRU, braço de inteligência militar da Rússia, de ser responsável por uma série de operações cibernéticas, como as dirigidas à Organização para a Proibição de Armas Químicas (OPAQ) e à Agência Mundial Antidopagem (AMA). O Secretário das Relações Exteriores do Reino Unido sugeriu que a Rússia tinha um "desejo de operar sem levar em conta o direito internacional ou as normas estabelecidas", enquanto os Países Baixos sugeriram, em termos mais gerais, que essas atividades russas "minam o Estado de direito internacional".[7] Infelizmente, essas acusações não descreveram se todas as supostas operações do GRU violaram o direito internacional ou se apenas algumas o fizeram; nem especificaram quais normas internacionais os acusadores acreditavam que haviam sido violadas. No entanto, a maioria dos casos são semelhantes às recentes acusações de Canadá, Estados Unidos e Reino Unido de que o GRU estaria concentrado na pesquisa da vacina contra a covid-19; não há qualquer menção ao direito internacional[8].

7. Nos últimos anos, vários Estados começaram a oferecer algumas explicações sobre como entendem que o direito internacional se aplica ao ciberespaço. A partir de 2012, os Estados Unidos começaram a oferecer seus pontos de vista em uma série de discursos e declarações oficiais[9]. Em 2018,

---

[6] Ver Dan Efrony e Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-Operations and Subsequent State Practice*, 112 AJIL 583, 586 (2018); Duncan B. Hollis & Martha Finnemore, *Beyond Naming and Shaming*: *Accusations and International Law in Global Cybersecurity,* 33 EURO. J. INT'L L (em breve em 2020).

[7] Comunicado de imprensa, Foreign Commonwealth Office, *UK exposes Russian cyber-attacks* (4 de outubro de 2018), em https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks; National Cyber Security Centre (NCSC), *Reckless campaign of cyber attacks by Russian military intelligence service exposed* (4 de outubro de 2018), em https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed; Ministério da Defesa dos Países Baixos*, Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW* (4 de outubro de 2018), em https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw. A acusação do Canadá incorporou ambas as formulações. Comunicado de imprensa, Global Affairs Canada, *Canada identifies malicious cyber-activity by Russia* (4 de outubro de 2018) em https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html (A atividade russa demonstra "falta de interesse no direito internacional e mina a ordem internacional baseada em regras"). Em contraste, Austrália e Nova Zelândia acusaram a Rússia de "ciberatividade maliciosa", sem fazer qualquer referência ao direito internacional. Ver, por exemplo, Comunicado de imprensa. Governo da Nova Zelândia, Comunicações do Gabinete de Segurança, *Malicious cyber activity attributed to Russia* (4 de outubro de 2018) , em https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/; Comunicado de imprensa, Primeiro-Ministro da Austrália, *Attribution of a Pattern of Malicious Cyber Activity to Russia* (4 de outubro de2018) , em https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia

[8] Ver, por exemplo, NCSC (Reino Unido), Comunicado de imprensa, *UK and allies expose Russian attacks on coronavirus vaccine development* (16 de julho de 2020), em https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development; Communications Security Establishment (Canadá, *Statement on Threat Activity Targeting COVID-19 Vaccine Development* (16 de julho de 2020), em https://cse-cst.gc.ca/en/media/2020-07-16; Serviço de Segurança Central da Agência Nacional de Segurança dos EUA, *NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID-19 Researchers* (16 de julho de 2020), em https://www.nsa.gov/news-features/press-room/Article/2275378/nsa-teams-with-ncsc-cse-dhs-cisa-to-expose-russian-intelligence-services-target/

[9] Ver, por exemplo, Brian Egan, *Remarks on International Law and Stability in Cyberspace* (10 de novembro de 2016), em DIGEST OF U.S. PRACTICE IN INT'L LAW 815 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (outubro de 2016), em DIGEST OF U.S. PRACTICE IN INT'L LAW 823 (2016) ("*2016 US GGE Submission*"); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (outubro de 2014), em DIGEST OF U.S.

o Procurador-Geral do Reino Unido fez uma importante declaração sobre a opinião do Reino Unido[10]. Nos anos seguintes, outros Estados (na sua maioria europeus) começaram a oferecer as suas próprias perspectivas detalhadas, entre eles Austrália[11], Estônia[12], França[13], Alemanha[14] e Países Baixos[15]. Embora seja um fato positivo, o número e a especificidade dessas declarações (ainda) não foram suficientes para que possam servir de comprovação da prática geral do Estado ou da *opinio juris*[16].

8. Vários atores não estatais tentaram preencher esse déficit de informação oferecendo os seus próprios pontos de vista sobre como o direito internacional consuetudinário regula as operações cibernéticas estatais. As duas vozes mais proeminentes são, sem dúvida, a do Comitê Internacional da Cruz Vermelha (CICV) e a do Grupo de Peritos Independentes que escreveu os *Manuais de Tallinn*.[17]

PRACTICE IN INT'L Law 732 (2014) ("*2014 US GGE Submission*"); Harold Koh, *International Law in Cyberspace* (18 de setembro de 2012), em DIGEST OF U.S. PRACTICE IN INT'L LAW 593 (2012). Em 2020, o assessor jurídico do Departamento de Defesa dos EUA ofereceu pontos de vista sobre várias questões-chave da aplicação do direito internacional ao ciberespaço. No entanto, ainda não está claro se seus pontos de vista refletem os dos Estados Unidos como um todo ou apenas os do Departamento de Defesa dos Estados Unidos. Ver Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* (2 de março de 2020), em https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/;

[10] Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century* (23 de maio de 2018), em https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("*U.K. Views*"/Pontos de Vista do Reino Unido").

[11] Missão australiana às Nações Unidas, *Australian Paper—Opened Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (setembro de 2019), em https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf ("*Australian Views*"/Pontos de Vista da Austrália); Commonwealth da Austrália, Departamento de Relações Exteriores e Comércio, *Annex A*: *Australia's position on how international law applies to State conduct in cyberspace*, em AUSTRALIA'S INT'L CYBER ENGAGEMENT STRATEGY (2017) *em*https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf.

[12] Kersti Kaljulaid, Presidente da Estônia, *President of the Republic at the opening of CyCon 2019* (29 de maio de 2019), em https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("*Estonian Views*"/ Pontos de Vista da Estônia")

[13] Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace* (9 de setembro de 2019), https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("French Ministry of Defense Views"/ Pontos de Vista do Ministério da Defesa da França"). I have not labeled these as "French views" as at least one scholar has pointed out that the document is authored by the French Ministry of Defense and its contents may not be attributable to the French State as a whole. *See* Gary Corn, *Punching on the Edges of the Gray Zone: Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (11 de fevereiro de 2020) ("Cabe ressaltar que, apesar das numerosas afirmações em contrário, o documento francês não pretende ser a posição oficial do governo francês. Foi escrito e publicado pelo Ministère des Armées (MdA) francês, no mesmo sentido que o *DoD Law of War Manual*, que não necessariamente reflete os pontos de vista do Governo dos Estados Unidos como um todo").

[14] Discurso do Embaixador Norbert Riedel, Comissário de Política Cibernética Internacional, Ministério Federal das Relações Exteriores da Alemanha (18 de maio de 2015), em https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

[15] *Letter to the parliament on the international legal order in cyberspace*, 5 de julho de 2019, Anexo 1, em https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ("*The Netherlands Views"*/Pontos de Vista dos Países Baixos).

[16] Ver, por exemplo, Egan, nota **Error! Bookmark not defined.** *supra*, em 817.

[17] Ver, por exemplo, CICV, *Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts* (novembro de 2019); MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) ("*Tallinn 2.0*"); ver também CICV, *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflict* (novembro de 2019);

Entretanto, está claro que nem todos os Estados consideram que seu conteúdo reflete o direito internacional.[18]

9. No ano passado, a Assembleia Geral da ONU encarregou um novo Grupo de Peritos Governamentais da ONU ("GPG") a que estudasse as opiniões nacionais sobre o direito internacional.[19] Além disso, no novo GPG, existe também um Grupo de Trabalho de Composição Aberta ("OEWG"/GTCA) sobre Avanços no Campo da Informação e das Telecomunicações no Contexto da Segurança Internacional patrocinado pela ONU, que tem proporcionado aos participantes a oportunidade de fazer declarações, algumas das quais se referem ao direito internacional.[20] Contudo, apenas quatro Estados membros da OEA (Brasil, México, Estados Unidos e Uruguai) participam do GPG. Em contrapartida, o OEWG/GTCA está aberto a todos os Estados membros da OEA. Porém, a maior parte das contribuições relacionadas com o direito internacional têm-se mantido muito generalizadas. E, assim como o GPG, o OEWG/GTCA concentra-se exclusivamente em questões de segurança internacional e, portanto, limita as opiniões do Estado sobre a aplicação do direito internacional.

10. Há, portanto, necessidade de fóruns adicionais nos quais os Estados membros possam ser encorajados — e oportunidades sejam oferecidas — para expressar os seus próprios pontos de vista sobre a aplicação do direito internacional. Este projeto marca uma primeira tentativa (e um tanto cautelosa) de satisfazer essa necessidade na região. Não foi concebido para substituir os processos em curso da ONU nem para competir com eles. O seu objetivo é sim complementar esses esforços, permitindo que todas as vozes da região participem e explorem toda a panóplia da aplicação do direito internacional à conduta do Estado no ciberespaço. Nesse sentido, o trabalho da Comissão está alinhado com o apelo da União Europeia a que os Estados membros da ONU "apresentem contribuições nacionais sobre a questão de como o direito internacional se aplica à utilização [das tecnologias da informação e das comunicações] por parte dos Estados".[21]

11. O projeto atual procurou responder à necessidade de maior transparência regional usando dois métodos diferentes: (i) um questionário preparado em conjunto com o Departamento de Direito Internacional da OEA (com contribuições do CICV) e distribuído pela primeira vez aos Estados membros em fevereiro de 2019; e (ii) uma discussão informal com representantes legais dos Estados membros sob as regras de *Chatham House* (ou seja, as declarações feitas na reunião podem ser repetidas, mas as identidades dos oradores e de outros participantes permanecem confidenciais). Uma

---

CICV, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, (outubro de 2015) 39-44.

[18] Egan, nota **Error! Bookmark not defined.** *supra*, em 817 ("As interpretações ou aplicações do direito internacional propostas por grupos não governamentais podem não refletir a prática ou os pontos de vista legais de muitos ou da maioria dos Estados. O silêncio relativo dos Estados poderia levar à imprevisibilidade no âmbito do ciberespaço, onde os Estados podem fazer suposições sobre as opiniões uns dos demais sobre o quadro legal aplicável. No contexto de um incidente cibernético específico, essa incerteza poderia levar a percepções errôneas e erros de cálculo dos Estados, o que poderia conduzir a uma escalada e, no pior dos casos, a conflitos").

[19] Ver UNGA Res. 266, nota **Error! Bookmark not defined.** *supra*, ¶3 (sobre o mandato do GPG).

[20] Ver U.N. Doc. A/RES/73/27, ¶5 (5 de dezembro de 2018). Vários Estados (ainda em sua maioria europeus) utilizaram os seus comentários sobre os projetos de relatórios do OEWG/GTCA para elaborar pontos de vista sobre como se aplica o direito internacional ao ciberespaço. Ver, por exemplo, Áustria, *Comments on Pre-Draft Report of the OEWG - ICT* (31 de março de 2020); Ministério das Relações Exteriores da República Tcheca, Comentários apresentados pela República Checa em resposta ao relatório "preliminar" inicial do Grupo de Trabalho de Composição Aberta sobre a evolução no campo da informação e das telecomunicações no contexto da segurança internacional (*Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security*). Estas e outras apresentações para o GTCA estão disponíveis em https://www.un.org/disarmament/open-ended-working-group/.

[21] Declaração da UE, nota **Error! Bookmark not defined.** *supra*.

cópia do questionário está incluída como anexo A deste relatório.

12. O meu terceiro relatório forneceu uma atualização sobre o conteúdo do questionário e solicitou uma prorrogação do prazo de resposta, que obteve a concordância da Comissão.[22] O meu quarto relatório diz respeito ao cotejo que fiz das respostas recebidas de nove Estados: Bolívia, Brasil, Chile, Costa Rica, Equador, Estados Unidos, Guatemala, Guiana e Peru.[23] Destas, sete foram substantivas, ao passo que os Estados Unidos remeteram à Comissão suas declarações públicas anteriores.[24] O Brasil destacou seu trabalho pendente no GPG (cujo embaixador ocupa a presidência) como o fórum que deveria tratar de questões sobre a aplicação do direito internacional.[25] Todas as sete respostas substantivas estão anexadas ao presente relatório como anexo B.

13. Além do cotejo das respostas ao questionário, meu quarto relatório catalogou conversas informais adicionais sobre o assunto em concertação com consultas realizadas pela Secretaria da OEA do Comitê Interamericano contra o Terrorismo (CICTE) junto ao Escritório das Nações Unidas para Assuntos de Desarmamento em 15 e 16 de agosto de 2019, e a reunião informal entre sessões do GTCA. Destaquei também três conclusões mais amplas sobre o estado da transparência na região no que diz respeito ao direito internacional no ciberespaço:

- Em primeiro lugar, que todos os Estados membros respondentes têm um interesse permanente no Estado de Direito, incluindo o papel que o direito internacional pode desempenhar na regulação da conduta do Estado no ciberespaço.
- Em segundo lugar, as respostas revelam a desigualdade das capacidades legais do Estado nessa área. Alguns Estados demonstraram profundo conhecimento das operações cibernéticas e dos novos problemas legais internacionais que elas levantam, enquanto outros demonstraram muito menos familiaridade com as normas legais internacionais subjacentes e as questões particulares que suas aplicações levantam no contexto cibernético. Isso sugere a necessidade de uma maior criação de capacidade jurídica internacional para além do excelente trabalho realizado até à data pelo CICTE e por vários

---

[22] Duncan B. Hollis, *Direito Internacional e Operações Cibernéticas Estatais: Melhoria da Transparência: Terceiro Relatório*, OEA/Ser.Q, CJI/doc 594/19 (24 de julho de 2019) ("Hollis, Terceiro Relatório"), em http://www.oas.org/en/sla/iajc/docs/CJI_doc_594-19.pdf.

[23] Ver *Nota do Estado Plurinacional da Bolívia, Ministério das Relações Exteriores, Missão Permanente da OEA junto à Comissão Jurídica Interamericana*, MPB-OEA-NV104-19 (17 de julho de 2019) (contendo respostas ao questionário da CJI formuladas pelo gabinete do comandante em chefe do Estado e inspetor-geral das Forças Armadas) ("Resposta da Bolívia"); *Resposta apresentada pelo Chile ao questionário da Comissão Jurídica Interamericana* (14 de janeiro de 2020) ("Resposta do Chile"); *Comunicação de Carole Arce Echeverria, Costa Rica, Organismos Internacionais, Departamento de Política Externa, Ministério das Relações Exteriores e Culto à OEA* (3 de abril de 2019) (incluindo a carta No. 163-OCRI2019 de Yonathan Alfaro Aguero, Escritório de Cooperação Internacional e Relações, a Carole Arce Echeverria, que inclui uma resposta da "autoridade competente" — o Tribunal de Apelações Criminais da Costa Rica ("Resposta da Costa Rica"); *Nota Verbal 4-2 186/2019 da Missão Permanente do Equador junto à OEA* (28 de junho de 2019) ("Resposta do Equador"); Nota Of. 4VM.200-2019/GJL/lr/bm, do Senhor Gabriel Juárez Lucas, quarto vice-ministro do Ministério do Interior, da República da Guatemala, a Luis Toro Utillano, Secretário Técnico da Comissão Jurídica Interamericana (14 de junho de 2019) ("Resposta da Guatemala"); *Nota No: 105/2019 da Missão Permanente da Guiana à OEA* (30 de julho de 2019) ("Resposta da Guiana"); *Resposta apresentada pelo Peru ao questionário sobre a aplicação do direito internacional nos Estados membros da OEA no contexto cibernético* (junho de 2019) ("Resposta do Peru").

[24] *Ver* nota **Error! Bookmark not defined.**.

[25] Resposta do Brasil à CJI da OEA Nota 2.2/14/19 da OEA CJI (1º de julho de 2019).

Estados membros.[26]

- Em terceiro lugar, a baixa porcentagem de respostas ao questionário da Comissão sugeriu que os Estados continuam relutantes em ser transparentes nos seus pontos de vista sobre a aplicação do direito internacional, mesmo quando lhes são dadas novas oportunidades para fazê-lo. Isso sugere a necessidade de encorajar mais respostas dos Estados ou buscar suas contribuições de maneiras menos formais.

14. Com a aprovação da Comissão, o prazo para responder ao questionário foi prorrogado até 1º de junho de 2020. Infelizmente, não foram recebidas mais respostas. Dito isso, vários Estados membros fizeram declarações pertinentes nos seus comentários escritos sobre os projetos de relatórios OEWG/GTCA sobre segurança internacional.[27]

15. Com a assistência do Departamento de Direito Internacional da OEA, iniciamos um segundo veículo para levar à esfera pública uma gama mais ampla de pontos de vista estatais sobre o direito internacional e o ciberespaço: uma conversa ao estilo de *Chatham House* sobre o tema. Em 23 de junho de 2020, o Departamento de Direito Internacional organizou, e este servidor moderou, uma discussão de quase três horas com representantes legais de 16 Estados membros e do CICV. A discussão aprofundada confirmou várias das conclusões do meu quarto relatório, especialmente a necessidade de mais capacidade legal. Destacou também várias explicações para a relutância dos Estados membros em fazer registrar sua opinião sobre a aplicação do direito internacional ao ciberespaço.

16. Neste relatório, eu me debrucei sobre três aspectos. Em primeiro lugar, estou atualizando e revisando o cotejo das respostas dos Estados ao questionário da Comissão à luz da reunião de 23 de junho, bem como as declarações relevantes dos Estados membros no processo OEWG. A pesquisa revisada consta do anexo B do presente relatório.

17. Em segundo lugar, com base nas consultas de 23 de junho, gostaria de destacar três conjuntos de desafios — técnicos, políticos e legais — para alcançar uma maior transparência por parte dos Estados membros na aplicação do direito internacional ao ciberespaço. Tecnicamente, o chamado "problema da atribuição" complica a capacidade dos Estados membros de falar publicamente sobre a aplicação do direito internacional. Os Estados podem saber que foram vítimas de um ataque cibernético, mas não conseguem discernir se o perpetrador foi um Estado (ou um representante pelo qual um Estado poderia ser responsabilizado legalmente). Sem a capacidade técnica (ou outra) de atribuir uma operação cibernética a um Estado estrangeiro, os Estados não podem invocar o direito internacional, pois essa norma só se aplica se o perpetrador for um Estado ou um ator pelo qual um Estado possa ser legalmente responsável. Da mesma forma, quando os atores operam anonimamente, é difícil identificar a prática estatal necessária (quanto mais a *opinio juris*), uma vez que o comportamento não é atribuível a um Estado.

18. Politicamente, alguns dos problemas de transparência são internos aos Estados membros: vários representantes legais relataram a necessidade contínua de organizar melhor a prestação de contas para tratar de questões relacionadas à cibernética (seus marcos legais e de políticas nacionais ainda não

---

[26] Para mais informações sobre as atividades do CICTE, consulte http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp. Além do CICTE, vários Estados membros também apoiaram o desenvolvimento da capacidade legal. O Canadá e o México, por exemplo, organizaram em conjunto com a OEA um *workshop* em 30 de maio de 2019 para que os países da OEA discutissem a aplicação do direito internacional no ciberespaço.

[27] (Ver, por exemplo, o segundo anteprojeto do relatório do GTCA sobre os progressos no campo da informação e das telecomunicações no contexto da segurança internacional (27 de maio de 2020) (*Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*), em https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf. Os textos de várias declarações nacionais estão disponíveis em https://www.un.org/disarmament/open-ended-working-group/.

atingiram a realidade atual). Embora vários Estados já venham lidando com problemas de cibersegurança há algum tempo, para outros Estados membros essas questões continuam sendo relativamente novas e inéditas. Como tal, vários Estados membros relataram uma falta de experiência governamental (de ou recursos) em questões relacionadas com a cibernética.

19. Em outros casos, trata-se de problemas institucionais; a experiência existe, mas é distribuída de uma forma que dificulta a sua fusão em uma visão formal do Estado que possa ser expressa publicamente. Vários representantes do Ministério das Relações Exteriores enfatizaram em particular a necessidade de um maior diálogo interno para assegurar que as Chancelarias assumam o papel principal nas discussões sobre a diplomacia cibernética, inclusive aquelas pertinentes à aplicação do direito internacional. Ao mesmo tempo, o desejo de certos Estados de manter a liberdade de participar de operações cibernéticas gerou uma relutância em tomar posição sobre quais operações poderiam ser proibidas ou restringidas pelo direito internacional de maneira a não limitar sua liberdade de manobra ou reação futura.

20. Outros participantes das consultas de 23 de junho identificaram desafios políticos externos para uma maior transparência. É evidente que certos Estados (por exemplo, Estados Unidos, Rússia, China) hoje têm amplas capacidades para conduzir operações cibernéticas e também para defender-se delas, capacidades que os levaram a rever opiniões discretas, e muitas vezes controversas, sobre o papel regulador do direito internacional. Alguns Estados membros mostraram-se relutantes em dar sinais semelhantes, para não se envolverem na disputa e no conflito entre os referidos atores. Trata-se de problemas que os Estados podem evitar se permanecerem em silêncio. Para os outros participantes, a transparência só deveria ocorrer gradualmente, ao longo do tempo, quando os Estados membros tiverem tido mais oportunidades de diálogo e discussão diplomática cuidadosa.

21. Ao mesmo tempo, muitos dos participantes de 23 de junho reconheceram que algumas das razões para o silêncio do Estado eram tanto legais como políticas: vários Estados membros ainda não têm experiência suficiente sobre como o direito internacional pode manifestar-se no contexto cibernético para formularem uma opinião sobre algumas das questões mais atuais e urgentes (e se um Estado não pode formular uma opinião bem-fundamentada, não tem como ser transparente).[28] Um participante explicou de forma sucinta: "ainda não chegamos lá" em termos de estarmos prontos para aplicar o direito internacional ao contexto cibernético.

22. Em terceiro lugar, dados os resultados do questionário e o debate de 23 de junho, o autor gostaria de fazer três propostas concretas para consideração específica da Comissão e da OEA e de seus Estados membros de forma mais ampla.

Proposta 1: A Comissão deveria recomendar que a Assembleia Geral da OEA apoiasse a aplicabilidade do direito internacional às operações estatais e àquelas patrocinadas pelo Estado

23. Como foi observado, a Assembleia Geral das Nações Unidas e várias organizações regionais (ASEAN, UE) endossaram a aplicabilidade do direito internacional à conduta do Estado no ciberespaço. Até hoje, porém, a OEA não o fez. Esse apoio enviaria um sinal claro do compromisso da Organização e da região com o Estado de Direito no ciberespaço. Uma formulação possível para essa declaração seria a seguinte:

> "*A Assembleia Geral da OEA afirma que o direito internacional, incluindo a Carta das Nações Unidas em sua totalidade, a Carta da Organização dos Estados Americanos, o direito humanitário internacional, o direito internacional dos direitos humanos, o dever*

[28] É claro que esses Estados poderiam ser transparentes quanto à sua incapacidade de formular um ponto de vista, mas é compreensível que poucos Estados, se é que haja algum, desejem tornar pública tal concessão.

de não intervenção, a igualdade soberana dos Estados e o direito de responsabilidade do Estado, aplica-se ao uso das tecnologias da informação e das comunicações (TICs) por parte dos Estados e daqueles que são internacionalmente responsáveis".

A região da OEA beneficia-se da aceitação por parte dos Estados membros da aplicação de certos regimes jurídicos internacionais (por exemplo, o direito humanitário internacional) onde ainda não foi possível o consenso global. Incluí também a soberania nessa lista, embora alguns Estados membros possam levantar dúvidas sobre a forma como se aplica. De toda maneira, ao tomar uma posição clara sobre quais normas do direito internacional se aplicam, a OEA poderia contribuir para esse diálogo global e, ao fazê-lo, promover o Estado de Direito.

24. Alternativamente — ou como um passo intermediário — a própria Comissão poderia apoiar a referida formulação em uma de suas resoluções e enviá-la à Assembleia Geral para consideração.

Proposta 2: Manter esse tema na agenda da Comissão e ampliar seu alcance para além dos temas do direito internacional, com vistas à paz e à segurança internacionais

25. Embora o meu mandato termine no final do ano civil, esse tema da agenda certamente mereceria mais atenção por parte da Comissão. Esse é o caso, quer a Comissão (ou a Assembleia Geral) atue ou não sobre a minha primeira proposta. Os participantes do debate de 23 de junho mostraram-se entusiasmados com a possibilidade de novos intercâmbios diplomáticos. Com a ajuda do Departamento de Direito Internacional, a Comissão poderia continuar organizando periodicamente esses intercâmbios diplomáticos. Seus baixos riscos e poucos obstáculos à entrada proporcionariam oportunidades para identificar convergências e divergências nas visões estatais, que podem então ser organizadas contra a ameaça de operações cibernéticas patrocinadas pelo Estado sem regulação apropriada e livres de restrições, como tem sido o caso até agora.

26. Com mais tempo e esforço, poderia ser possível obter mais pontos de vista "oficiais" dos Estados membros para ajudar a cumprir o objetivo geral de melhorar a transparência sobre como o direito internacional se aplica ao ciberespaço. Ao fazer isso, a Comissão também poderia considerar a expansão do escopo de aplicação para cobrir outros temas além da paz e da segurança internacionais, que dominam os processos existentes na ONU. O meu questionário não abordava, por exemplo, o dever de não intervenção, embora vários representantes de Estado tenham pedido mais atenção para o tema nas minhas consultas de 23 de junho. Da mesma forma, vários participantes pediram mais atenção ao papel do direito internacional dos direitos humanos no ciberespaço — tema que a Comissão poderia abordar sozinha ou em concertação com a Comissão Interamericana de Direitos Humanos.

27. Ademais, a Comissão poderia tentar melhorar a transparência sobre como o direito internacional protege o setor da saúde. A pandemia da covid-19 afetou gravemente a região, tanto em termos humanitários como econômicos. Infelizmente, as ameaças cibernéticas correm o risco de causar ainda mais danos, como evidenciado pelos ataques cibernéticos aos hospitais e, mais recentemente, aos esforços de pesquisa de vacinas. A Comissão poderia, portanto, centrar a sua atenção em um tema crucial de interesse atual, que seria de ajuda aos Estados membros e aos seus cidadãos em toda a região.[29]

[29] Para um esforço contínuo de esclarecimento das proteções do direito internacional para o setor de saúde contra as ameaças cibernéticas, consulte Dapo Akande, Duncan Hollis, Harold Hongju Koh e Jim O'Brien, *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector,* JUST SECURITY (21 de maio de 2020) (publicado em OPINIO JURIS & EJILTalk!).

Proposta 3: Apoiar ou empreender esforços adicionais de criação de capacidade legal

28. O CICTE e vários Estados membros já empreenderam esforços significativos e importantes para criar capacidade sobre questões cibernéticas entre os Estados membros, tanto a capacidade de compreender a natureza técnica das TICs e as ameaças que elas representam como a capacidade de compreender e avaliar os problemas legais levantados por essas ameaças. No entanto, tanto as respostas ao questionário como as consultas de 23 de junho deixam claro que ainda há muito por fazer, especialmente no contexto do desenvolvimento da capacidade legal. Os participantes das consultas de 23 de junho falaram longamente sobre a necessidade de desenvolver capacidades adicionais na aplicação do direito internacional no contexto cibernético. Vários Estados membros (por exemplo, Argentina, Canadá e Estados Unidos) expressaram opiniões semelhantes nos seus comentários recentes ao OEWG/GTCA[30]. Por conseguinte, a Comissão parece ter forte apoio se optar por demonstrar a sua vontade de emprestar sua experiência ou recursos aos esforços atuais de criação de capacidade.

29. Como alternativa, a Comissão poderia considerar a possibilidade de apoiar ou empreender seus próprios esforços adicionais (e mais diversificados) de criação de capacidade. Os cursos sobre a aplicação do direito internacional ao ciberespaço poderiam ser complementados por cursos que oferecessem "capacitação técnica" a peritos não técnicos para ajudar os diplomatas estatais e outros representantes a compreender e avaliar com precisão como funcionam as ameaças cibernéticas. Alternativamente, a Comissão poderia usar suas reuniões com os assessores jurídicos do Ministério das Relações Exteriores para "ensaiar, como em um jogo" certos cenários envolvendo ameaças cibernéticas, a fim de dar aos advogados do governo mais oportunidades de aplicar as normas e padrões legais relevantes (e, ao fazê-lo, ajudar a facilitar o desenvolvimento de um Estado sobre sua própria visão de como a lei é aplicada). Por último, a Comissão poderia realizar diálogos periódicos, como os realizados em junho, organizando e moderando debates sobre a aplicação do direito internacional entre os Estados membros (e talvez, em algum momento, com outras partes interessadas relevantes da indústria e da sociedade civil).

30. Em suma, com mais esforços de transparência e criação de capacidade, a Comissão poderia contribuir significativamente para melhorar a aplicação (e a eficácia) do direito internacional como instrumento regulador no ciberespaço. Além disso, poderia fazê-lo sozinha ou em concertação com outras instituições da OEA, certos Estados membros ou outras organizações. O CICV, por exemplo, expressou entusiasmo em apoiar mais esforços de criação de capacidade em direito internacional na região.

31. Para mim foi um verdadeiro privilégio trabalhar nesse tema no período em que estive na Comissão. Acredito realmente que as ameaças cibernéticas, incluindo as operações dos Estados e de seus representantes, criam riscos que têm importantes consequências econômicas, humanitárias e de segurança nacional. O direito internacional proporciona um mecanismo — que o tempo comprovou — para regular as novas ameaças. No entanto, os desafios técnicos, políticos e legais fizeram com que a lei, em geral, e a prática do Estado e a *opinio juris* que compreendem os costumes, em particular, ficassem menos visíveis e, portanto, menos eficazes, até à data. Com mais transparência sobre como os Estados entendem a lei para operar, seria de se esperar uma maior oportunidade de desempenhar um papel regulador muito necessário para restringir comportamentos indesejados e possibilitar maior

[30] Ver, por exemplo, Argentina, *Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security* ("Anteprojeto" do relatório do GTCA sobre a evolução no campo da informação e das telecomunicações no contexto da segurança internacional); Michael Walma, *Canadian Comments on Draft OEWG Report* (6 de abril de 2020); Estados Unidos, *United States Comments on the Chair's Pre-draft of the Report of the U.N. Open Ended Working Group (OEWG)* (6 de abril de 2020). Estas (e outras) declarações nacionais estão disponíveis no Grupo Trabalho de Composição Aberta (GTCA) em https://www.un.org/disarmament/open-ended-working-group/.

assistência e cooperação. Espero que estes relatórios sobre os resultados do questionário e outras discussões dentro da região possam marcar um primeiro e modesto passo para aumentar a visibilidade da aplicação do direito internacional no ciberespaço. Incentivo também a Comissão (e a OEA) a continuarem participando de esforços semelhantes no futuro e espero ver os produtos e processos resultantes de tais esforços.

OEA Mais direitos para mais pessoas

ANEXO A

CJI

COMISSÃO JURÍDICA INTERAMERICANA

COMISSÃO JURÍDICA INTERAMERICANA
Av. Marechal Floriano, 196 - 3º andar - Palácio Itamaraty - Centro - Rio de Janeiro, RJ - 20080-002 - Brasil
Tel.: (55-21) 3172-1474 -

OEA/2.2/14/19

O Departamento de Direito Internacional da Secretaria de Assuntos Jurídicos da Secretaria-Geral da Organização dos Estados Americanos, na qualidade de Secretaria Técnica da Comissão Jurídica Interamericana (doravante designada "CJI"), cumprimenta atenciosamente as missões permanentes e informa que a CJI está realizando um estudo sobre a aplicação do direito internacional no contexto cibernético nos Estados membros da OEA.

Para tanto, a Comissão solicita respeitosamente que as seguintes perguntas sejam respondidas:

1. O seu Governo tornou público algum documento oficial, discurso ou declaração similar resumindo como entende que o direito internacional se aplica às operações cibernéticas? Solicita-se o envio de cópias ou *links* dessas declarações.
2. Os ramos do direito internacional atual (como a proibição do uso da força, o direito de legítima defesa, o direito internacional humanitário e os direitos humanos) aplicam-se ao ciberespaço? Existem áreas em que a novidade do ciberespaço exclui a aplicação de um conjunto específico de direitos ou obrigações legais internacionais?
3. Uma operação cibernética por si só pode constituir um uso de força? Pode constituir um ataque armado que dê origem a um direito de legítima defesa nos termos do artigo 51 da Carta das Nações Unidas? Uma operação cibernética pode ser qualificada como uso da força ou ataque armado sem causar os efeitos violentos que se utilizaram para marcar tais limiares em conflitos cinéticos passados?
4. Fora do conflito armado, quando é que um Estado seria responsável pelas operações cibernéticas de um ator não estatal? Que grau de controle ou participação deve ter um Estado nas operações do ator não estatal para acionar a responsabilidade legal internacional desse Estado?
5. As normas de responsabilidade do Estado são as mesmas ou são diferentes no contexto de um conflito armado tal como definido nos artigos 2º e 3º comuns às Convenções de Genebra de 1949?
6. De acordo com o direito humanitário internacional, uma operação cibernética pode ser qualificada como um "ataque" segundo as normas que regem a condução de hostilidades se não causar morte, lesões ou danos físicos diretos ao sistema informático em questão ou à infraestrutura que suporta? Pode uma operação cibernética que produz apenas uma perda de funcionalidade, por exemplo, ser qualificada como ataque? Em caso afirmativo, em que

casos?

7. Uma operação cibernética que só ataca dados seria regida pela obrigação do direito internacional humanitário de dirigir ataques apenas contra alvos militares e não contra alvos civis?

8. A soberania é uma norma separada do direito internacional que proíbe aos Estados participar de operações cibernéticas específicas? Em caso afirmativo, essa proibição abrange as operações cibernéticas que estão abaixo do limiar de uso da força e que, além disso, não violam o princípio da não intervenção?

9. A devida diligência é uma norma do direito internacional que os Estados devem respeitar no exercício da sua soberania sobre as tecnologias da informação e das comunicações nos seus territórios ou sob o controle dos seus cidadãos?

10. Existem outras regras do direito internacional que o seu Governo considera importante levar em conta ao avaliar a regulação das operações cibernéticas por parte dos Estados ou atores pelas quais um Estado tenha responsabilidade no âmbito internacional?

Mais explicações sobre o questionário podem ser encontradas no relatório da CJI intitulado "*Direito Internacional e Operações Cibernéticas Estatais: Melhoria da Transparência*", documento anexo CJI/doc. 578/19.

As respostas devem ser enviadas até 28 de junho de 2019 para a Secretaria Técnica da CJI, o Departamento de Direito Internacional, aos cuidados de Luis Toro Utillano, por meio eletrônico, para ltoro@oas.org. Também é possível entrar em contato conosco pelo telefone (202) 370-0632 e pelo fax (202) 458-3293.

O Departamento de Direito Internacional da Secretaria de Assuntos Jurídicos da Secretaria-Geral da Organização dos Estados Americanos aproveita a oportunidade para reiterar às missões permanentes junto à OEA os protestos de sua mais alta e distinta consideração.

Washington, D.C., 20 de março de 2019

Luis Toro Utillano

Anexo B

Respostas ao questionário da Comissão Jurídica Interamericana de 14 de fevereiro de 2019 sobre a aplicação do direito internacional nos Estados membros da OEA no contexto cibernético[1]

Pergunta 1: O seu Governo tornou público algum documento oficial, discurso ou declaração similar resumindo como entende que o direito internacional se aplica às operações cibernéticas? Solicita-se o envio de cópias ou links dessas declarações.

1. Essa primeira pergunta solicitava as declarações nacionais feitas sobre o direito internacional e o ciberespaço. A ideia era que a Comissão estivesse ciente das opiniões expressas anteriormente e que os Estados membros não tivessem de responder às perguntas se já tivessem adotado uma posição substantiva pertinente. Contudo, das nove respostas, apenas a dos Estados Unidos dizia que haviam sido feitas declarações e discursos anteriormente sobre a aplicação do direito internacional ao ciberespaço, como os discursos de 2012 e 2016 dos então assessores jurídicos do Departamento de Estado e os textos apresentados pelos Estados Unidos em 2014 e

[1] Sete Estados — Bolívia, Chile, Costa Rica, Equador, Guatemala, Guiana e Peru — responderam formalmente ao questionário. Ver *Nota do Estado Plurinacional da Bolívia, Ministério das Relações Exteriores, Missão Permanente da OEA à Comissão Jurídica Interamericana*, MPB-OEA-NV104-19 (17 de julho de 2019) (contendo respostas do Escritório do Comandante-em-Chefe das Forças Armadas do Estado, Inspetoria-Geral das Forças Armadas, ao questionário da CJI ("Resposta da Bolívia"); *Resposta apresentada pelo Chile ao questionário da Comissão Jurídica Interamericana da OEA* (14 de janeiro de 2020) ("Resposta do Chile"); *Comunicação de Carole Arce Echeverría, Organismos Internacionais, Direção-Geral de Política Externa, Ministério das Relações Exteriores e Culto da Costa Rica, à OEA* (3 de abril de 2019) (à qual se anexa a carta 163-OCRI2019, de Yonathan Alfaro Aguero, Escritório de Cooperação e Relações Internacionais, dirigida a Carole Arce Echeverría, com a resposta da Câmara de Cassação Criminal) (a "instância pertinente")("Resposta da Costa Rica"); *Nota verbal 4-2 186/2019 da Missão Permanente do Equador junto à OEA* (28 de junho de 2019) ("Resposta do Equador"); Nota Of. 4VM.200-2019/GJL/lr/bm, de Gabriel Juárez Lucas, Quarto Vice-Ministro, Ministério do Interior, a Luis Toro Utillano, Secretaria Técnica da Comissão Jurídica Interamericana (14 de junho de 2019) ("Resposta da Guatemala"); *Nota No: 105/2019 da Missão Permanente da Guiana à OEA* (30 de julho de 2019) ("Resposta da Guiana"); *Resposta apresentada pelo Peru ao questionário sobre a aplicação do direito internacional nos Estados membros da OEA no contexto cibernético* (junho de 2019) ("Resposta do Peru").

A resposta dos Estados Unidos dirigiu a Comissão às suas declarações públicas anteriores. *Ver*, Brian Egan, *Remarks on International Law and Stability in Cyberspace* (10 de novembro de 2016), em *Digest of U.S. Practice in Int'l Law* 815 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (outubro de 2016), em *Digest of U.S. Practice in Int'l Law* 823 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (outubro de 2014), em *Digest of U.S. Practice in Int'l Law* 732 (2014); Harold Koh, *International Law in Cyberspace* (18 de setembro de 2012), em *Digest of U.S. Practice in Int'l Law* 593 (2012). Recentemente, o Assessor Jurídico do Departamento de Defesa dos Estados Unidos fez um discurso que também continha opiniões formais sobre a aplicação do direito internacional (embora não esteja claro se estava falando pelos Estados Unidos como um todo ou somente pelo Departamento de Defesa). Ver, por exemplo, Paul C. Ney, "*DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, 2 de março de 2020, em: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/?dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

O Brasil respondeu ao questionário da Comissão com a observação de que utilizaria o Grupo de Peritos Governamentais (GPG) das Nações Unidas sobre "Promoção do comportamento responsável dos Estados no ciberespaço no contexto da segurança internacional" como fórum para abordar esses temas. *Ver* "Resposta do Brasil à CJI da OEA", Nota 2.2/14/19 (1º de julho de 2019).

2016 nas reuniões do Grupo de Peritos Governamentais (GPE) das Nações Unidas sobre os avanços em matéria de informação e telecomunicações no contexto da segurança internacional.[2]

2. Outros Estados respondentes disseram não ter conhecimento de posições anteriores sobre a aplicação do direito internacional no contexto cibernético[3]. Vários aproveitaram a oportunidade para destacar sua ação interna voltada a estabelecer organizações pertinentes ou regimes regulatórios a fim de tratar de assuntos relacionados às tecnologias da informação e das comunicações (TICs)[4].

3. Vários Estados membros utilizaram o Grupo de Trabalho de Composição Aberta sobre Avanços em Matéria de Informação e Telecomunicações no Contexto da Segurança Internacional, patrocinado pelas Nações Unidas, para fazer declarações públicas com referências à aplicação do direito internacional. No entanto, em sua maioria, essas declarações foram expressas em termos muito gerais ou foram adaptadas para abordar aspectos específicos do texto do relatório do Grupo de Trabalho de Composição Aberta. Várias dessas declarações são de Estados que já responderam diretamente ao questionário da Comissão. Contudo, alguns Estados, como Argentina, Brasil, Canadá, Colômbia, México, Nicarágua e Uruguai, fizeram comentários pertinentes ao questionário.[5] Portanto, apresentam-se abaixo referências às declarações nacionais.

---

[2] Para as citações, ver nota 1 *supra*. Deve-se notar, no entanto, que na resposta dos Estados Unidos se dizia que aqueles eram apenas "alguns" dos documentos em que expressavam as suas opiniões. Portanto, pode haver outros que mereçam atenção. Em particular, poderia ser útil saber até que ponto o *Law of War Manual*, do Departamento de Defesa, reflete os pontos de vista dos Estados Unidos como um todo. Ver Office of General Counsel, U.S. Department of Defense, *Department of Defense Law of War Manual* (junho de 2015, atualizado em dezembro de 2016) ("Manual de Direito da Guerra do Departamento de Defesa").

[3] Ver, por exemplo, a resposta do Equador, nota 1 *supra*, em 1 ("Não se tem conhecimento de nenhum documento oficial do Governo do Equador que seja público quanto às operações cibernéticas"); ver também a resposta da Guiana, nota 1 *supra*, em 1 (idem).

[4] Resposta da Bolívia, nota 1 *supra*, em 1 (citando uma nova lei de 2015); resposta do Chile, nota 1 *supra*, em 1 (citando a "Política Nacional de Defesa Cibernética" do Ministério da Defesa, publicada em 9 de março de 2018); resposta da Guatemala, nota 1 *supra*, em 1 (citando a "Estratégia Nacional de Segurança Cibernética" e a nova "Lei contra a Criminalidade Cibernética"); ver também a resposta da Costa Rica, nota 1 *supra*, em 1.

[5] Todas as declarações nacionais podem ser encontradas em Nações Unidas, *Grupo de Trabalho de Composição Aberta,* na página eletrônica https://www.un.org/disarmament/open-ended-working-group/. Ver, por exemplo, Argentina, *Projeto preliminar do Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* ("Comentários da Argentina"); Brasil, *Comentários apresentados pelo Brasil sobre o Projeto Preliminar do Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (8 de abril de 2020) ("Comentários do Brasil"); Michael Walma, *Comentários do Canadá sobre o Projeto Preliminar do Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (6 de abril de 2020) ("Comentários do Canadá"); Colômbia, *Comentários da Colômbia sobre o Projeto Preliminar do Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (16 de abril de 2020) ("Comentários da Colômbia); México, *Comentários preliminares do México sobre o Projeto Preliminar do Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (2020) ("Comentários do México"); Nicarágua, *MINIC-MIS-143-04-2020* (abril de 2020) ("Comentários da Nicarágua"); Uruguai, *Comentários sobre o Projeto Preliminar do Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (2020) ("Comentários do Uruguai").

Para informações sobre os comentários de outros Estados membros, ver Chile, *Comentários do Chile sobre o pré-relatório da Presidência* (2020) ("Comentários do Chile"); Equador, *Comentários preliminares do Equador sobre o Projeto de Relatório do Grupo de Trabalho de Composição Aberta das Nações Unidas sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional*

4. A escassez de declarações oficiais anteriores combinada com a natureza geral das declarações feitas mais recentemente confirma a hipótese subjacente a este projeto: que os Estados têm dito relativamente pouco até agora sobre a forma como o direito internacional se aplica à conduta dos Estados no ciberespaço. Confirma também que a maioria das atividades nacionais relacionadas com a cibersegurança se concentraram até agora em estratégias ou políticas nacionais em matéria de cibersegurança e cibercriminalidade interna, bem como em outros aspectos da regulamentação das TICs.

Pergunta 2: Os ramos do direito internacional atual (como a proibição do uso da força, o direito de legítima defesa, o direito internacional humanitário e os direitos humanos) aplicam-se ao ciberespaço? Existem áreas em que a novidade do ciberespaço exclui a aplicação de um conjunto específico de direitos ou obrigações legais internacionais?

5. Embora uma resolução recente da Assembleia Geral das Nações Unidas[6] pareça indicar que existe hoje um apoio generalizado à aplicação do direito internacional ao ciberespaço, as primeiras tentativas feitas nas Nações Unidas revelaram que alguns Estados tinham profundas reservas quanto à aplicabilidade de certos regimes jurídicos internacionais. De fato, supostamente devido a essas reservas, o GPG da ONU que se reuniu em 2016 e 2017 não produziu um relatório final[7]. Por conseguinte, permanece a necessidade de determinar se a existência de certas áreas do direito internacional em relação ao ciberespaço é um tema controverso e, em caso afirmativo, quais são essas áreas. O objetivo da segunda pergunta era coletar as opiniões dos Estados sobre aspectos do direito internacional que eles consideravam inaplicáveis (ou cuja aplicação poderia ser pelo menos problemática) no contexto cibernético.

6. Em geral, as respostas ao questionário refletem um amplo apoio à aplicação dos campos existentes do direito internacional ao ciberespaço. Como resumido na resposta do Chile, "o direito internacional vigente proporciona o marco normativo aplicável [...], incluindo as normas relativas ao *jus ad bellum*, ao direito internacional humanitário, aos direitos humanos e aquelas que regulamentam a responsabilidade internacional dos Estados"[8]. Outros Estados que confirmaram a aplicação do direito internacional foram o Equador, o Peru e os Estados Unidos[9]. Juntamente com o

---

(abril de 2020) ("Comentários do Equador"); Venezuela (regime de Maduro) *Considerações preliminares da Venezuela sobre o Projeto de Relatório do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (2020) ("Comentários da Venezuela"); Estados Unidos, *Comentários dos Estados Unidos sobre o Projeto de Relatório da Presidência do Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional* (6 de abril de 2020) ("Comentários dos Estados Unidos").

[6] Ver, Resolução 266 da AGNU, UN doc. A/RES/73/266 (2 de janeiro de 2019).

[7] Ver, por exemplo, Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, em *Lawfare* (4 de julho de 2017), em: https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[8] Resposta do Chile, nota 1 *supra*, em 1 (consequentemente, o Chile observa que "o planejamento, a condução e a execução das operações no ciberespaço devem observar estritamente o respeito ao direito internacional público, com especial atenção ao direito internacional dos direitos humanos e ao direito internacional humanitário").

[9] Resposta do Equador, nota 1 *supra*, em 1 ("os ramos do direito internacional aplicam-se ao ciberespaço"); resposta do Peru, nota 1, em 1 ("considerando o papel essencial da Carta na sua relação com outros instrumentos internacionais [...], seria possível considerar que não existam áreas das relações internacionais que estejam à margem dos princípios enunciados. Levando em conta que o ciberespaço se converte em cenário cotidiano de interação internacional, os atores participantes dessas relações são obrigados a respeitar as obrigações maiores do direito internacional, entre as quais estão a proibição do uso da força, o direito à legítima defesa e o respeito aos direitos humanos e ao direito internacional humanitário"); Koh, nota 1 em 594 (onde assinala que os princípios do direito internacional se aplicam ao ciberespaço, que não é uma área "sem lei", onde qualquer pessoa possa conduzir atividades hostis sem restrições e sem aderir a regra alguma).

jus ad bellum e o *jus in bello,* a resposta do Peru enfatiza a validade de vários direitos humanos no ciberespaço, entre eles "o direito à privacidade e à intimidade, a liberdade de informação, a liberdade de expressão, o acesso livre e igualitário à informação, a eliminação do hiato digital, os direitos de propriedade intelectual, o livre fluxo de informação, o direito ao sigilo das comunicações, etc."[10]. Os Estados Unidos apoiam a aplicação do direito internacional dos direitos humanos, ao mesmo tempo que propõem a aplicação do direito internacional como "pedra angular" de sua política para o ciberespaço[11].

7. A Bolívia também dá uma resposta positiva, mas centrada no direito internacional "destinado a ser aplicado em conflitos armados", com opiniões sobre como distinguir entre os casos em que o direito internacional humanitário se aplicaria e aqueles em que não se aplicaria[12]. Portanto, não está claro se a resposta positiva da Bolívia se estende à aplicação de outros subcampos do direito internacional além do *jus ad bellum* e do *jus in bello*.

8. A Guatemala e a Guiana apoiam a aplicação do direito internacional. No entanto, ambos os países formulam reservas no que diz respeito ao alcance universal da aplicação do Direito existente. Sem dar exemplos, a Guatemala observa que poderia haver áreas em que "a novidade do ciberespaço exclua a aplicação de determinados direitos ou obrigações de caráter internacional"[13]. A Guiana, por sua vez, salienta que as operações cibernéticas não se enquadram nos conceitos tradicionais e que há um debate acalorado sobre se os campos do direito internacional existentes se aplicam ao ciberespaço[14]. Tendo em conta o trabalho anterior do GPG, a Guiana afirma que, embora se reconheça que o direito internacional deveria aplicar-se ao ciberespaço, é difícil aplicar alguns princípios existentes, como o uso da força, que tradicionalmente envolve um elemento físico e ataques com algum tipo de arma[15].

9. Portanto, embora a aplicação geral do direito internacional às operações cibernéticas pareça estar firmemente arraigada, as duas últimas respostas parecem indicar a necessidade de mais diálogo. Seria útil indicar *que áreas* específicas de aplicação do direito internacional causam dúvida a alguns Estados e por quê. Isso ajudaria a compreender o grau de convergência (ou divergência) de opiniões sobre a forma como os regimes jurídicos internacionais regem as operações cibernéticas efetuadas ou patrocinadas pelos Estados.

10. Os comentários dos Estados membros ao Grupo de Trabalho de Composição Aberta sobre a Evolução na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional reforçam esses aspectos. Também refletem o amplo consenso de que o direito internacional, incluindo a Carta das Nações Unidas, se aplica ao espaço cibernético. Canadá, Chile, Colômbia, Estados Unidos, México e Uruguai expressaram essa ideia de forma explícita.[16] Alguns

---

[10] Resposta do Peru, nota 1 *supra*, em 1.

[11] Texto apresentado pelos Estados Unidos ao Grupo de Peritos Governamentais (GPG) em 2014, nota 1 *supra*, em 733 (a aplicação do direito internacional é a "pedra angular" das opiniões dos Estados Unidos, dadas as suas características distintivas); Egan, nota 1 *supra*, em 815. Sobre a aplicação dos direitos humanos, ver Koh, nota 1 *supra*, em 598; Egan, nota 1 *supra*, em 820; texto apresentado pelos Estados Unidos ao GPG em 2016, nota 1 *supra*, em 824.

[12] Resposta da Bolívia, nota 1 *supra*, em 2 a 7. A Bolívia indica que o direito internacional humanitário não governaria as operações cibernéticas relacionadas com a segurança nacional, a propaganda, a espionagem, a manipulação da estrutura estratégica crítica, as operações cibernéticas para fins políticos ou a pirataria de sistemas privados que ponha em perigo as operações econômicas e sociais do Estado. *Id*. em 3 a 7.

[13] Resposta da Guatemala, nota 1 *supra*, em 1 e 2.

[14] Resposta da Guiana, nota 1 *supra*, em 1 e 2.

[15] *Id*.

[16] Ver Comentários do Canadá, nota **Error! Bookmark not defined.** *supra*; Comentários da Colômbia, nota **Error! Bookmark not defined.** *supra*; Comentários do Chile, nota **Error! Bookmark not defined.** *supra*; Comentários do México, nota **Error! Bookmark not defined.** *supra*; Comentários dos Estados Unidos, nota 5 *supra*; Comentários do Uruguai, nota **Error! Bookmark not defined.** *supra*.

Estados [por exemplo, Nicarágua e Venezuela (representada pelo regime de Maduro)] questionaram a conveniência do direito internacional vigente no espaço cibernético, mesmo que aceitassem a sua aplicação nesse contexto. [17] Outros comentários acrescentaram um novo nível de preocupação que não foi levantado nas respostas ao questionário da Comissão; por exemplo, se as diferenças na capacidade jurídica poderiam afetar a aplicação efetiva ou a evolução da lei (dado que os Estados com uma infraestrutura avançada em segurança cibernética poderiam contar com a capacidade correspondente para influenciar, de maneira desproporcional, o conteúdo e os limites das normas em matéria de ciberespaço nos Estados que não dispõem dessa capacidade).[18]

Pergunta 3: Uma operação cibernética por si só pode constituir um uso de força? Pode constituir um ataque armado que dê origem a um direito de legítima defesa nos termos do artigo 51 da Carta das Nações Unidas? Uma operação cibernética pode ser qualificada como uso da força ou ataque armado sem causar os efeitos violentos que se utilizaram para marcar tais limiares em conflitos cinéticos passados?

11. A maioria dos Estados, mas não todos, parecem aceitar a aplicação do direito internacional sobre o uso da força (por exemplo, o *jus ad bellum*) às suas operações cibernéticas. O objetivo dessa pergunta era determinar quais são os Estados da região que aderem a essa posição predominante e quais aderem a outras posições. Ao mesmo tempo, surgiram outras questões relativas à aplicação entre os Estados que aceitam o *jus ad bellum* no ciberespaço, em particular a medida em que os limiares para o "uso da força" ou os "ataques armados" exigem que haja efeitos "violentos" semelhantes aos anteriormente considerados como excedentes a esses limiares. A questão agora é como lidar com as novidades na escala ou os efeitos das operações cibernéticas (ou seja, operações que não são semelhantes a operações cinéticas passadas que excederam o limiar do uso da força nem a sanções econômicas ou políticas que não excederam o limiar). Como deve o direito internacional encarar tais operações cibernéticas? Devem ser automaticamente colocadas abaixo ou acima do limiar do uso da força, ou são necessárias mais pesquisas e análises para dividir as operações cibernéticas dessa nova "zona cinzenta" segundo estejam acima ou abaixo dos limiares correspondentes?[19] Assim, com essa pergunta se procurava determinar se os Estados encaram as operações cibernéticas como casos de uso da força (ou ataques armados) inteiramente por analogia com casos anteriores ou se acreditam que é necessário estabelecer uma nova norma para esse fim.

12. Bolívia, Chile, Estados Unidos, Guatemala e Peru entendem claramente que as operações cibernéticas por si só poderiam gerar a proibição do uso da força e o inerente direito de autodefesa para responder a um "ataque armado"[20]. Como explicou a Guatemala:

---

[17] Comentários da Nicarágua, nota **Error! Bookmark not defined.** *supra* (sugerindo que estamos diante de uma "aplicabilidade deficiente" do direito internacional nessa esfera, mas não negando em princípio que o direito internacional se aplica à esfera das tecnologias da informação e das comunicações); Comentários da Venezuela, nota 5 *supra* (reafirmando a necessidade de "adaptar o direito internacional ao contexto das TICs, levando em conta as lacunas legais existentes"). Em seus comentários ao Grupo de Trabalho de Composição Aberta sobre os Avanços na Esfera da Informação e das Telecomunicações no Contexto da Segurança Internacional, a Argentina solicitou que as sugestões do Grupo de Trabalho fossem bifurcadas, a fim de esclarecer a aplicação da proibição do uso da força e do direito internacional humanitário. Ver, Comentários da Argentina, *supra*, nota 5.

[18]Ver, por exemplo, Comentários do México, nota 5 *supra*; Comentários da Bolívia, nota 5 *supra*; Comentários do Equador, nota 5 *supra*.

[19] Ver Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace* , 42 *Yale J. Int' L.* 1 (2017).

[20] Resposta da Bolívia, nota 1 em 2 a 7; resposta do Chile, nota 23 em 1 (o Chile abster-se-á do uso da força "através do ciberespaço" de maneira que transgrida o direito internacional e poderá exercer "seu direito à legítima defesa diante de um ataque armado perpetrado através do ciberespaço"); Resposta da Guatemala, nota 23 *supra*, em 2; resposta do Peru, nota 1 *supra*, em 1 a 3; Koh, nota 1 *supra*, em 595 (apresentando a opinião dos Estados Unidos de que *a)* as atividades cibernéticas poderiam constituir uso da força em

> uma operação cibernética por si só pode constituir um uso de força, já que o uso da força não se refere exclusivamente à força física, mas também aos riscos ou violações que se causem à segurança e à proteção de terceiros. [...] existe o direito de legítima defesa contra um ataque ou operação cibernética que atente contra a soberania de um país[21].

No texto escrito apresentado ao GPG em 2014, os Estados Unidos enfatizaram sua visão de que o direito inerente de legítima defesa poderia aplicar-se ao uso ilegal da força, o que parece indicar um só limiar para ambas as normas[22]. Isso difere da posição dos Estados que consideram que todos os ataques armados constituem uso da força, mas não todos os casos de uso da força constituem ataques armados (os quais envolveriam somente as formas "mais graves" de uso da força)[23]. Os Estados Unidos também afirmaram que podem exercer seu direito inerente de legítima defesa em decorrência de atividades cibernéticas que representem um ataque armado real ou iminente, independentemente de o atacante ser um Estado ou um agente não estatal[24].

13. Em contrapartida, a Guiana expressa dúvidas em sua resposta quanto à aplicabilidade do *jus ad bellum* às operações puramente cibernéticas. Com base na definição de força constante do dicionário jurídico *Black's Law Dictionary* ("poder considerado de maneira dinâmica"), a Guiana aponta que é possível que uma operação cibernética em si não constitua uso da força[25]. Afirma também que um ataque armado implica o uso de armamento e que uma operação cibernética, que não implica o uso de armamento físico, não pode ser considerada como um ataque armado que dê origem ao exercício da legítima defesa[26]. Ao mesmo tempo, a Guiana enfatiza que é possível o uso de operações cibernéticas em conflitos armados, as quais estariam regidas pelo direito internacional humanitário[27].

---

determinadas circunstâncias, no sentido do artigo 2.4 da Carta das Nações Unidas e do direito internacional consuetudinário, e *(b)* as atividades de redes informáticas que representem um ataque armado ou uma ameaça iminente de ataque armado poderiam levar ao exercício do direito nacional de legítima defesa de um Estado, tal como reconhecido no artigo 51 da Carta das Nações Unidas); texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 734; Egan, nota 1 *supra*, em 816 (indicando que a reunião do GPG das Nações Unidas em 2015 referendou o direito à legítima defesa). O Equador também respondeu afirmativamente à pergunta, mas citou a definição de "ataque armado" usada no artigo 92 do Manual Tallinn 2.0, no qual a expressão é definida no contexto de um conflito armado (isto é, *jus in bello*), diferentemente da forma como é usada no artigo 51 da Carta das Nações Unidas e no *jus ad bellum*. Ver a resposta do Equador, nota 1 *supra*, em 1; MICHAEL N. SCHMITT (ED.), *TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS* (2017) ("Tallinn 2.0"); Ver também CICV, *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflict*. Em seus comentários ao Grupo de Trabalho de Composição Aberta, a Colômbia expressou a ideia de que a autodefesa é "essencial para manter a paz e a estabilidade no ambiente das TICs". Comentários da Colômbia, *supra*, nota 5.

[21] Resposta da Guatemala, nota 1 *supra*, em 2; resposta do Peru, nota 1 *supra*, em 3 (citando o CICV e Michael Schmitt, segundo os quais os usos da força não se limitam à força cinética).

[22] Koh, nota 1 *supra*, em 597.

[23] Ver *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)* [1986] ICJ Rep. 14, parágrafos 176 e 191 (27 de junho) (descrevendo os ataques armados como as formas mais graves de uso da força).

[24] Texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 734 e 735. O documento também reitera a prova da falta de vontade ou de capacidade de um Estado para se defender sem o seu consentimento, nos casos em que um Estado territorial não queira ou não possa deter ou impedir um ataque real ou iminente lançado no ciberespaço ou por seu intermédio. *Id*. em 735.

[25] Resposta da Guiana, nota 1 *supra*, em 2.

[26] *Id*.

[27] Ver *id*. em 3 e 5.

14. No que diz respeito à possibilidade de uma operação cibernética cruzar o limiar do uso da força (ou de um ataque armado[28]) sem ter efeitos violentos, as opiniões dos Estados são variadas. A maioria dos Estados respondentes prefere traçar os limiares pertinentes por meio de analogias entre as operações cibernéticas e operações passadas, cinéticas ou não, que reuniam ou não os requisitos para serem consideradas como uso da força ou ataque armado. No entanto, alguns Estados mencionam a possibilidade de não se limitarem a analogias desse tipo. O Chile, por exemplo, aponta que as operações cibernéticas análogas ao limiar de severidade necessário para cumprir os requisitos do direito internacional para serem consideradas um ataque armado podem dar origem ao direito de legítima defesa[29]. Ao mesmo tempo, a resposta do Chile pode deixar margem para definir os ataques armados em termos mais gerais ao indicar que os "ataques cibernéticos dirigidos contra sua soberania, seus habitantes, sua infraestrutura física ou da informação" poderiam cumprir os requisitos para serem considerados ataques armados[30].

15. O Peru admite mais abertamente "a possibilidade de uma operação cibernética que não tenha efeitos violentos ser qualificada como uso da força ou ataque armado"[31]. No entanto, baseia-se na ideia de que, no passado, o armamento cinético também pode ter sido utilizado sem causar efeitos violentos e, mesmo assim, tenha constituído uso da força (por exemplo, o lançamento de um míssil que atravessa o território de outro Estado, mesmo que não caia nesse Estado)[32]. Em geral, o Peru enfatiza a necessidade de distinguir entre "ataques cibernéticos" (que implicam que "se cause dano a um alvo militarmente relevante, que pode ser total ou parcialmente destruído, inclusive capturado ou neutralizado") e uma "interrupção abrupta das comunicações no ciberespaço", ou seja, "as operações cibernéticas que causam inconvenientes, mesmo que extremos, mas não lesões diretas nem mortes, nem destruição de propriedade"[33]. Assim, em sua resposta específica, o Peru enfatiza a determinação da legalidade das operações cibernéticas no contexto do uso da força, levando em conta se elas podem "resultar na morte ou lesão de pessoas ou bens"[34].

16. A Guatemala adota um enfoque diferente em sua resposta e expressa a vontade de repensar o que constitui "efeitos violentos" porque as consequências de uma operação cibernética podem ser "superiores e posteriores, ameaçando setores como saúde e segurança, entre outros"[35]. Indica que, no contexto cibernético, as consequências que produzem "morte, ansiedade, pobreza" devem ser consideradas violentas[36].

17. A Bolívia aponta em sua resposta que poderia ser difícil aplicar o limiar na prática porque "os efeitos dos ciberataques nem sempre serão imediatamente conhecidos", tornando difícil verificar se houve uso da força. Ao mesmo tempo, a Bolívia indica que avaliará o limiar com base em analogias com o contexto cinético, ou seja, que se trataria de um "ataque armado" se "o ataque virtual cibernético utiliza meios não convencionais, mas com o mesmo impacto de um ataque armado"[37].

18. Finalmente, os Estados Unidos não responderam ao questionário em si, mas as suas declarações anteriores lançaram luz sobre suas opiniões. Em seu discurso seminal de 2012, Harold

---

[28] Isso parte do pressuposto de que poderia haver dois limiares diferentes, ao contrário da opinião dos Estados Unidos. Ver as notas 23-25 *supra* e o texto que as acompanha.
[29] Resposta do Chile, nota 1 *supra*, em 2.
[30] *Id*. em 2.
[31] Resposta do Peru, nota 1 *supra*, em 3
[32] *Id*.
[33] *Id.* em 2.
[34] *Id.* em 3.
[35] Resposta da Guatemala, nota 1 *supra*, em 2.
[36] *Id*.
[37] A resposta da Bolívia, nota 1 *supra*, em 2 a 7 (a Bolívia enfatiza que o direito à legítima defesa também engloba a "legítima defesa antecipada", à qual só se pode recorrer quando a ameaça é iminente e a necessidade de se defender é imediata (em oposição a uma represália).

Koh indicou a preferência dos Estados Unidos por uma abordagem contextual para identificar casos de uso da força (embora com a ressalva acima de que a definição usada pelos Estados Unidos também abrange os ataques armados):

> Ao determinar se um evento constituiu uso da força no ciberespaço ou por seu intermédio, devemos avaliar fatores como o contexto do evento, o autor do ato (tendo-se em conta as dificuldades de atribuição no ciberespaço), o alvo e a localização, os efeitos e a intenção, entre outros aspectos possíveis[38].

Ao mesmo tempo, Koh considera claramente que a prova requer uma analogia e pergunta se a lesão física direta e os danos materiais resultantes do evento cibernético se assemelham ao que seria considerado um caso de uso da força se tivessem sido produzidos por armas cinéticas[39]. Também menciona exemplos concretos de operações cibernéticas que constituiriam uso da força: (i) fusão do núcleo do reator de uma usina nuclear causada por um ato cibernético; (ii) operações cibernéticas que abrem uma barragem a montante de uma área povoada e causam destruição; e (iii) uma operação cibernética que inutiliza o controle do tráfego aéreo e causa acidentes de aviação[40]. Na medida em que todos esses exemplos envolvem alguma forma de "violência", parece ser que os Estados Unidos favorecem um limiar para o uso da força análogo ao usado no contexto cinético.

Pergunta 4: Fora do conflito armado, quando é que um Estado seria responsável pelas operações cibernéticas de um ator não estatal? Que grau de controle ou participação deve ter um Estado nas operações do ator não estatal para acionar a responsabilidade legal internacional desse Estado?

Pergunta 5: As normas de responsabilidade do Estado são as mesmas ou são diferentes no contexto de um conflito armado tal como definido nos artigos 2º e 3º comuns às Convenções de Genebra de 1949?

19. Os Estados são responsáveis pela conduta não só dos seus próprios órgãos e dependências no ciberespaço, mas também de todo agente não estatal que apoie ou controle[41]. Na quarta e quinta perguntas indaga-se o que os Estados entendem sobre a atribuição de responsabilidade jurídica internacional por atos de agentes não estatais, em particular o grau de "controle" exigido pelo Estado. Como se sabe, as ameaças cibernéticas podem ser perpetradas não só pelos Estados diretamente, como também por vários agentes não estatais, entre eles, grupos hacktivistas e organizações cibercriminosas. Em alguns casos, os Estados tentam usar esses agentes não estatais como substitutos para realizar várias operações cibernéticas.

20. Rastrear os atos de um substituto e vinculá-los a um autor principal no ciberespaço pode ser bastante difícil do ponto de vista técnico (embora talvez não tão difícil como alguns supunham anteriormente). Ao mesmo tempo, um nexo factual não é suficiente, mas também deve haver uma atribuição jurídica, ou seja, uma conexão suficiente entre um Estado e um agente não estatal para que o primeiro assuma a responsabilidade legal pelos atos do segundo. Por exemplo, um Estado poderia endossar os atos de um agente não estatal *a posteriori* e, dessa forma, assumir a

---

[38] Koh, nota 1 *supra*, em 595 ("as atividades cibernéticas que, de forma direta ou imediata, causam mortes, lesões ou grande destruição provavelmente se considerarão uso de força". Os Estados Unidos têm mantido esse ponto de vista desde então. Ver apresentação ao GPG em 2014, nota 1, em 734. Esse documento foi anexado ao de 2016, o que indica que seu conteúdo continuava sendo válido.

[39] Koh, nota 1 *supra*, em 595.

[40] *Id*.

[41] Ver Comissão de Direito Internacional, *Projeto de artigos sobre a responsabilidade do Estado por fatos internacionalmente ilícitos*, em *Relatório sobre o trabalho realizado em seu Quinquagésimo Primeiro Período de Sessões* (3 de maio a 23 de julho de 1999), UN doc. A/56/10 55 [3]; *Tallinn 2.0,* nota 20 *supra*, regra 15.

responsabilidade legal por eles[42]. Outra possibilidade é que os Estados sejam juridicamente responsáveis pelos atos dos agentes estatais que operam sob seu controle, embora o grau de controle não costume ser claro. No caso da Nicarágua, a Corte Internacional de Justiça (CIJ) indicou que o direito internacional contém uma regra que impõe ao Estado a responsabilidade por atos de agentes não estatais sobre os quais tenha um "controle efetivo" (ou seja, se ordena o ato ou dirige uma operação)[43]. Alguns anos depois, contudo, o Tribunal Penal Internacional adotou para a antiga Iugoslávia uma norma menos estrita de "controle geral" para efeitos do direito internacional humanitário. Segundo o Tribunal, essa prova requer mais do que o mero fornecimento de equipamento, formação militar ou assistência financeira, mas não insiste na emissão de ordens específicas pelo Estado nem em sua condução das operações[44]. Posteriormente, o Tribunal Penal Internacional referendou a norma do "controle geral"[45].

21. No entanto, a CIJ continua insistindo na sua fórmula de "controle efetivo" no contexto do uso da força. Ao mesmo tempo, afirma que a prova do "controle geral" poderia ser apropriada no contexto do direito internacional humanitário, levantando a possibilidade de um consenso sobre o "controle geral" no contexto do direito internacional humanitário e o "controle efetivo" em outros contextos[46]. Em vista disso, perguntou-se no questionário sobre a responsabilidade do Estado, tanto em geral como no contexto do direito internacional humanitário, com base na existência de um conflito armado, da forma como se utiliza a expressão nas Convenções de Genebra.

22. Em sua resposta, vários Estados membros sublinham a dificuldade da atribuição no ciberespaço[47]. Outros se concentram menos na questão da responsabilidade pelos atos de substitutos e mais no dever do Estado de garantir que o seu território não seja utilizado por agentes não estatais para lançar ataques[48]. Nesse sentido, o Peru comenta que "a inércia de um Estado em relação a um ator não estatal que pudesse desencadear um ataque cibernético contra outro Estado e que tivesse condições de controlar poderia fazer com que seu comportamento fosse atribuível ao Estado"[49]. A Bolívia, por outro lado, afirma que os Estados não são responsáveis se lhes faltar a infraestrutura tecnológica necessária para controlar os atores não estatais[50]. Os Estados Unidos observam que "o simples fato de uma atividade cibernética ter sido lançada a partir do território de outro Estado, ou

---

[42] Artigos sobre a responsabilidade do Estado, nota 41 *supra*, art. 11; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* 52 (2012).

[43] *Nicaragua Case*, nota 23 *supra*, par. 115.

[44] *Prosecutor v. Dusko Tadić aka 'Dule'* (Sentença) ICTY-94-1-A (15 de julho de 1999), par. 131 a 145 e 162.

[45] *Prosecutor v. Lubanga*, Processo nº ICC-01/04-01/06, seção de primeira instância, sentença (Tribunal Penal Internacional, 14 de março de 2012).

[46] *Case concerning application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Sentença) [1997] ICJ Rep. 43, 208– 09, par. 402 a 407 (indicando que a prova do controle global poderia muito bem aplicar-se e ser apropriada aos tipos de classificações utilizadas no direito internacional humanitário).

[47] Resposta da Guatemala, nota 1 *supra*, em 3 (afirmando que é "extremamente complicado" determinar uma clara a responsabilidade por um ataque cibernético); resposta do Peru, nota 1 *supra*, em 4 (afirmando que há grande "incerteza na atribuição, e nos níveis de atribuição, da autoria de ataques cibernéticos", o que dificulta a possibilidade de "controle daqueles que usam o ciberespaço para desencadear ataques por internet").

[48] Resposta do Equador, nota 1 *supra*, em 1 ("Os Estados não têm responsabilidade por um ataque de um ator não estatal; entretanto, deveria haver uma forma de colaborar na busca dos responsáveis. Assim, também é responsabilidade do Estado regular/normalizar os serviços a fim de evitar que se possa produzir um ataque a partir do território pertencente a um Estado"); resposta da Guatemala, nota 1 *supra*, em 3 (respondendo a partir da perspectiva da devida diligência do Estado anfitrião e não do grau de controle exercido sobre os agentes substitutos).

[49] Resposta do Peru, nota 1 *supra*, em 4 (citando o artigo 11 dos artigos sobre responsabilidade do Estado).

[50] Resposta da Bolívia, nota 1 *supra*, em 3 a 7. A resposta da Bolívia à pergunta sobre os substitutos é indireta, embora indique a existência de um nexo entre um Estado e os agentes não estatais ligados aos objetivos ou estratégias da política de defesa do Estado em uma situação de conflito armado. *Id*.

ter tido origem de outra forma nesse território, ou ter sido lançada a partir da infraestrutura cibernética de outro Estado é insuficiente, na ausência de outros elementos, para atribuir essa atividade ao Estado"[51].

23. Os Estados que se concentram na questão dos agentes substitutos atribuem grande importância aos artigos sobre a responsabilidade do Estado. Chile, Guiana e Peru baseiam a sua resposta no artigo 8º:

> Um Estado será considerado responsável por uma operação cibernética internacionalmente ilícita quando ela tiver sido cometida por intermédio de algum de seus órgãos, por qualquer pessoa ou entidade que exerça autoridade governamental, ou por uma pessoa ou grupo de pessoas agindo conforme as instruções ou sob a direção ou controle desse Estado[52].

No entanto, os artigos sobre a responsabilidade do Estado não formulam uma opinião sobre o grau de "controle" que o Estado deve exercer, sendo esse um assunto que deve ser avaliado em cada caso[53]. Isso condiz com a opinião dos Estados Unidos, que endossa a responsabilidade do Estado pelas atividades realizadas por meio de "agentes substitutos" que atuam segundo as instruções do Estado ou sob sua direção ou controle, embora diga apenas que o grau de controle exercido deve ser "suficiente"[54]. Os Estados Unidos também reconheceram que um Estado pode reconhecer ou adotar *a posteriori* uma operação cibernética de um agente não estatal como sua própria[55].

24. O Chile, por outro lado, ao expor seu ponto de vista sobre o grau de controle necessário para que haja responsabilidade jurídica, menciona os casos de *Nicarágua* e *Genocídio* e é de opinião que "o grau ou padrão de controle ou participação que um Estado deve ter nas operações de um agente não estatal para desencadear sua responsabilidade internacional é o de controle efetivo"[56]. Acredita também que as normas relativas à responsabilidade do Estado são as mesmas no contexto dos conflitos armados[57].

25. No que diz respeito ao direito internacional humanitário, o Peru adota uma posição semelhante, que favorece uma regra uniforme em relação à responsabilidade do Estado, tanto nos conflitos armados como em outros contextos. Embora reconheça a possibilidade de substituir os artigos sobre a responsabilidade do Estado por uma norma especial, indica que para isso é necessária uma análise minuciosa. Nesse caso, "[n]a revisão das Convenções de Genebra não se identifica uma alteração às normas relativas à responsabilidade internacional previstas no Projeto de Artigos sobre Responsabilidade do Estado por atos internacionalmente ilícitos, motivo pelo qual não se pode sustentar uma mudança no âmbito de aplicação deste projeto"[58] . No entanto, a norma

---

[51] Texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 738.

[52] Artigos sobre responsabilidade do Estado, nota 41 *supra*, art. 8; resposta do Chile, nota 1 *supra*, em 2; resposta da Guiana, nota 1 *supra*, em 3; resposta do Peru, nota 1 *supra*, em 4. As respostas do Chile e do Peru também parecem basear-se no artigo 5º dentre os artigos sobre a responsabilidade do Estado, que atribui ao Estado a responsabilidade pela "conduta de uma pessoa ou entidade que [...] esteja habilitada pelo direito desse Estado a exercer atribuições de poder público, desde que, no caso de que se trate, a pessoa ou entidade atue nessa qualidade". Ver para a resposta do Chile, nota 1 *supra*, em 2, e a resposta do Peru, nota 1 *supra*, em 4.

[53] Artigos sobre a responsabilidade do Estado, nota 41 *supra*, em 48 (comentário ao artigo 8º).

[54] Koh, nota 1 *supra*, em 595; texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 738 (*idem*); Egan, nota 1 *supra*, em 821; texto apresentado pelos Estados Unidos ao GPG em 2016, nota 1 *supra*, em 826.

[55] Egan, nota 1 *supra*, em 821; texto apresentado pelos Estados Unidos ao GPG em 2016, nota 1 *supra*, em 826.

[56] Resposta do Chile, nota 1 *supra*, em 2.

[57] *Id.* em 3.

[58] Resposta do Peru, nota 1 *supra*, em 4 e 5.

sobre responsabilidade enunciada nos artigos sobre a responsabilidade dos Estados refere-se ao "controle" somente de uma forma geral, sem distinguir se deve ser "efetivo" ou "geral".

26. Outros Estados tiveram mais dificuldade em responder à pergunta 5. A Guatemala afirma que "é necessário continuar as discussões em fóruns internacionais sobre os aspectos únicos e diferentes que um conflito no ciberespaço apresentaria, especialmente aspectos como a atribuição e a territorialidade dos ataques"[59]. Outros Estados entenderam que a pergunta se referia às diferenças nas normas em matéria de responsabilidade nos casos de conflitos armados internacionais e sem caráter internacional[60].

Pergunta 6: De acordo com o direito internacional humanitário, uma operação cibernética pode ser qualificada como um "ataque" segundo as normas que regem a condução de hostilidades se não causar morte, lesões ou danos físicos diretos ao sistema informático em questão ou à infraestrutura que suporta? Pode uma operação cibernética que produz apenas uma perda de funcionalidade, por exemplo, ser qualificada como ataque? Em caso afirmativo, em que casos?

27. A sexta pergunta é a primeira de duas que abordam a forma como o direito internacional humanitário (ou *jus in bello*) se aplica às operações cibernéticas. Concentra-se em um assunto que até hoje divide Estados e especialistas: como definir um "ataque" para efeitos do direito internacional humanitário. Grande parte desse ramo do Direito, incluindo os seus princípios fundamentais de distinção, proporcionalidade e precauções, está formulada principalmente do ponto de vista da proibição de certos tipos de "ataques" (por exemplo, os dirigidos contra civis ou alvos civis) e da autorização de outros (por exemplo, os dirigidos contra alvos militares)[61]. Como apontou o CICV recentemente, o tema da interpretação ampla ou restrita do conceito de "ataque" em relação às operações cibernéticas é essencial para a aplicabilidade dessas normas e para a proteção que elas proporcionam à população e à infraestrutura civil[62]. De fato, na medida em que uma operação *não* constitua um "ataque", poderia ser conduzida no âmbito de um conflito armado sem ter em conta a maior parte das normas do direito internacional humanitário[63].

28. De acordo com o direito internacional humanitário, entendem-se por "ataques" no direito internacional consuetudinário (codificado no artigo 49 do Protocolo Adicional I às Convenções de Genebra) "os atos de violência contra o adversário, sejam eles ofensivos ou defensivos"[64]. Além disso, como explicado no Manual Tallinn 2.0, "as consequências, não a sua

---

[59] Resposta da Guatemala, nota 1 *supra*, em 3.

[60] Ver, por exemplo, a resposta da Bolívia, nota 1 *supra*, em 4 a 7, e a resposta da Guiana, nota 1 *supra*, em 3. A resposta do Equador enfatiza simplesmente que "os Estados são responsáveis pelo cumprimento das normas nos conflitos armados, mesmo quando há partes que não fazem parte da convenção" correspondente. Resposta do Equador, nota 1 *supra*, em 2.

[61] Por exemplo, o princípio da distinção apresenta-se normalmente como a proibição de que a população civil seja alvo de ataque. Ver, por exemplo, o Protocolo Adicional às Convenções de Genebra de 12 de agosto de 1949, relativo à Proteção das Vítimas de Conflitos Armados Internacionais (Protocolo I) (8 de junho de 1977), 1125 UNTS 3, art. 5.2 ("Protocolo Adicional I"); o Protocolo Adicional às Convenções de Genebra de 12 de agosto de 1949, relativo à Proteção das Vítimas dos Conflitos Armados Sem Caráter Internacional (12 de dezembro de 1977), 1125 UNTS 609, art. 13 (2); Estatuto de Roma do Tribunal Penal Internacional (17 de julho de 1998), art. 8.2, b, f; Convenção concernente às Leis e Costumes da Guerra Terrestre (H.IV) e seu anexo: Regulamento relativo às Leis e Costumes da Guerra Terrestre (18 de outubro de 1907), 36 Stat. 2277, art. 8.2, b, i-ii; Jean Marie Henckaerts e Louise Doswald-Beck, *Customary International Humanitarian Law* (CICV, 2005), normas 1, 7, 9 e 10.

[62] CICV, *Documento de posición sobre Derecho internacional humanitario y ciberoperaciones durante conflictos armados* (novembro de 2019) em 7 ("Documento de posição do CICV").

[63] Mesmo na ausência de ataques, os Estados devem agir com "cuidado constante" em um conflito armado internacional para "poupar a população civil [...] e os bens de natureza civil". Protocolo Adicional I, nota 61 *supra*, art. 57.1; *Tallinn 2.0* , nota 20 *supra*, em 476.

[64] Protocolo Adicional I, nota 61 *supra*, art. 49.

índole, em geral determinam o alcance do termo "ataque"; a "violência" deve ser considerada no sentido das consequências violentas e não se limita a atos violentos"[65]. O CICV observou que "tem ampla aceitação a ideia de que as operações cibernéticas que se prevê que causem mortes, lesões ou danos físicos constituem ataques em conformidade com o direito internacional humanitário"[66]. No entanto, é sabido que algumas operações cibernéticas (por exemplo, o *ransomware,* ou programa de sequestro de arquivos em troca de resgate) são novidade porque podem perturbar o funcionamento dos alvos sem danificá-los fisicamente[67]. Isso leva à pergunta de se as operações cibernéticas que não produzem efeitos desse tipo (por exemplo, a interrupção da operação de uma estação de tratamento de água sem causar necessariamente um dano físico) podem constituir um ataque. Surgiram opiniões divergentes até à data, até mesmo entre os integrantes do grupo de peritos independentes que elaborou o *Manual Tallinn 2.0*[68].

29. A maioria dos autores do *Manual Tallinn 2.0* é de opinião que, para que haja violência, deve haver algum dano físico que exija, por exemplo, a "substituição de componentes físicos", tais como um sistema de controle[69]. Outros entendem que o dano inclui casos em que não seja necessário substituir componentes físicos e se possa restabelecer o funcionamento mediante a reinstalação do sistema operacional, enquanto alguns especialistas consideram que um ataque poderia consistir na "perda da capacidade de usar a infraestrutura cibernética em si"[70]. O CICV, por sua vez, argumentou que, em um conflito armado, uma operação destinada a desativar um computador ou uma rede informática constitui um ataque ao abrigo do direito internacional humanitário, independentemente de o alvo ser desativado por meios cinéticos ou cibernéticos[71].

30. O objetivo da sexta pergunta era, portanto, determinar se os Estados membros também consideram o limiar para um ataque no contexto do direito internacional humanitário em termos de violência (ou efeitos violentos) ou se consideram que a rubrica de "ataque" poderia ser aplicada a operações cibernéticas com base na perda de funcionalidade, em vez dos conceitos mais tradicionais de dano físico ou destruição.

31. As respostas ao questionário refletem o apoio à aplicabilidade do direito internacional humanitário em geral e à ideia de que as operações cibernéticas podem constituir um ataque nesse contexto[72]. No entanto, há mais variedade nas respostas à pergunta de se uma operação cibernética pode ser qualificada como um "ataque" em conformidade com o direito internacional humanitário, se não causar mortes, lesões ou danos físicos diretos. O Chile, o Peru e os Estados Unidos responderam que não[73]. O Chile cita o artigo 49 do Protocolo Adicional I às Convenções de

---

[65] *Tallinn 2.0*, nota 20 *supra*, em 415.
[66] Ver o documento de posição do CICV, nota 62.
[67] CICV, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, (outubro de 2015) 41 ("Relatório do CICV de 2015").
[68] *Tallinn 2.0*, nota 20 *supra*, em 417.
[69] *Id*.
[70] Relatório do CICV de 2015, nota 67 *supra*, em 41. Ver também CICV, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (novembro de 2019), em 28 ("Relatório do CICV de 2019") ("As normas do DIH que protegem objetos civis só podem, no entanto, proporcionar um escopo completo de proteção legal se os Estados reconhecerem que as operações cibernéticas que afetam a funcionalidade da infraestrutura civil estão sujeitas às normas que regem os ataques nos termos do DIH").
[71] Ver o documento de posição do CICV, nota 62 *supra*, em 7-8, e o Relatório do CICV de 2015, nota 67 *supra,* em 43 (afirmando que o direito internacional deve tratar como ataques as operações cibernéticas que desativem objetos, uma vez que a definição de alvo militar abrange a neutralização, implicando que a neutralização de objetos se enquadra no âmbito do direito internacional humanitário).
[72] Ver, por exemplo, a resposta da Bolívia, nota 1 *supra*, em 3 a 7; *id.* em 4 a 7 (assinalando dois pontos de vista sobre se uma operação cibernética por si só pode levar a um conflito armado sujeito ao direito internacional humanitário); resposta do Chile, nota 1 *supra*, em 3; resposta da Guiana, nota 1 *supra*, em 3; resposta do Peru, nota 1 *supra*, em 1; Koh, nota 1 *supra*, em 595 (opinião dos Estados Unidos).
[73] Resposta da Guiana, nota 1 *supra*, em 4.

Genebra ao insistir que os ataques no contexto do direito internacional humanitário devem envolver "efeitos ou consequências decorrentes do ato em si, que devem ser violentos"[74]. Em particular, indica que, para que o ato possa ser considerado um ataque, o seu resultado deve exigir que "o Estado afetado tome medidas para reparar ou recuperar a infraestrutura ou o sistema informático afetado, porque nesses casos as consequências do ataque são semelhantes às descritas acima, em particular os danos físicos à propriedade"[75]. O Peru responde que, para que haja um "ataque", é necessário que se causem "danos físicos" a "pessoas" ou "bens públicos ou privados"[76]. Os Estados Unidos, entretanto, enfatizaram que o limiar para um "ataque" no contexto do direito internacional humanitário requer a determinação, *inter alia*, de se uma atividade cibernética produz efeitos cinéticos irreversíveis ou efeitos não cinéticos reversíveis sobre a população civil, em alvos de caráter civil ou na infraestrutura civil[77]. Isto implica que, se uma operação cibernética produz efeitos não cinéticos ou reversíveis, não constitui um ataque armado[78], o que pareceria excluir, por exemplo, os programas intrusos de *ransomware* que não sejam cinéticos em si mesmos ou os casos em que os dados que sejam interrompidos possam ser restabelecidos.

32. Em contrapartida, Guatemala e Equador apoiam a ideia de delimitar os ataques com base nas perdas de funcionalidade, e não nas mortes, nas lesões ou na destruição de bens que possam causar. A Guatemala afirma que, entre as operações cibernéticas que podem ser consideradas como um ataque, existem aquelas "que só produzem uma perda de funcionalidade"[79]. O Equador é da opinião que "[uma] operação cibernética pode ser considerada um ataque no caso de deixar sem funcionalidade a infraestrutura crítica do Estado ou outras que ponham em risco a segurança do Estado"[80].

33. As respostas da Bolívia e da Guiana são mais ambíguas. Por um lado, a Bolívia afirma que a definição de ataques ao abrigo do direito internacional humanitário incluiria uma operação cibernética "da qual se espera que possa causar perdas de vidas humanas, lesões a pessoas e danos ou destruição de bens"[81]. Por outro lado, diz que uma operação cibernética "poderia ser considerada como um ataque quando tem o objetivo de desativar os serviços básicos (água, luz, telecomunicações ou o sistema financeiro, etc.) de um Estado"[82]. A Guiana observa que, quando uma operação cibernética resulta em perda de funcionalidade, pode ou não constituir um ataque[83]. Tal como o Chile, refere-se ao artigo 49 do Protocolo Adicional I e vincula o conceito de ataque à necessidade de que haja violência (no que se refere aos meios ou às consequências): "uma operação cibernética que não ocasione mortes, lesões ou danos físicos não pode constituir um ataque" ao abrigo do direito internacional humanitário[84]. Por outro lado, assinala que "as operações cibernéticas que prejudicam o funcionamento dos sistemas e das infraestruturas informáticas necessárias à prestação de serviços e recursos à população civil constituem um ataque". Entre eles

---

[74] Resposta do Chile, nota 1 *supra*, em 3.
[75] *Id*.
[76] No entanto, a resposta do Peru é um tanto ambígua, pois parece basear-se em elementos do *jus ad bellum* para indicar as normas aplicáveis a um ataque no contexto do direito internacional humanitário e menciona a abordagem contextual dos Estados Unidos pela qual Harold Koh expressa preferência. Resposta do Peru, nota 1 *supra*, em 6.
[77] Texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 736.
[78] Egan, nota 1 *supra*, em 818. Egan não mencionou em seu discurso o critério de danos reversíveis ou irreversíveis, mas sublinhou "a natureza e o alcance desses efeitos, bem como a índole da relação, se houver, entre a atividade cibernética e o conflito armado particular em questão". *Id*.
[79] Resposta da Guatemala, nota 1 *supra*, em 3.
[80] Resposta do Equador, nota 1 *supra*, em 3.
[81] Resposta da Bolívia, nota 1 *supra*, em 4 a 7.
[82] *Id*.
[83] Resposta da Guiana, nota 1 *supra*, em 3.
[84] *Id*.

estão "usinas nucleares, hospitais, bancos e sistemas de controle de tráfego aéreo"[85]. Essas respostas parecem indicar a necessidade de aprofundar o diálogo sobre quão imediata deve ser a morte ou destruição após a perda de funcionalidade. Em outras palavras, a perda de funcionalidade de um serviço essencial por si só constitui um ataque ou deve haver concomitância (ou previsibilidade razoável) de mortes, lesões ou danos materiais?

Pergunta 7: Uma operação cibernética que só ataca dados seria regida pela obrigação do direito internacional humanitário de dirigir ataques apenas contra alvos militares e não contra alvos civis?

34. O direito internacional humanitário exige claramente que os Estados "atacantes" façam a distinção entre alvos civis e militares e permite ataques a alvos militares, mas proíbe ataques à população civil e a alvos de caráter civil[86]. No entanto, quando se trata do ciberespaço, nem sempre fica claro o que constitui um "alvo" na aplicação desse princípio. O debate fundamental tem-se centrado nos "dados". Isso significa que os "dados", por sua natureza não física, não são um alvo e que, consequentemente, os militares não precisam fazer a distinção e excluí-los de suas operações cibernéticas? Ou será que pelo menos alguns "dados" deveriam ser considerados como um "alvo" ao qual se aplicam o princípio da distinção e as normas pertinentes do direito internacional humanitário?

35. A maioria dos peritos do grupo independente que elaborou o *Manual Tallinn 2.0* adotou a primeira posição: "O conceito de 'alvo' em conflitos armados não deve ser entendido como incluindo dados, pelo menos no direito atual"[87]. Não obstante, os peritos concordam que uma operação cibernética dirigida contra dados poderia desencadear a aplicação das regras do direito internacional humanitário nos casos em que "seja possível prever lesões, mortes, danos materiais ou destruição de objetos físicos", uma vez que as pessoas e os objetos afetados estariam protegidos pelas regras pertinentes do direito internacional humanitário, como as relativas à distinção[88]. Em contrapartida, o CICV propôs uma definição mais ampla de dados com o termo "dados civis essenciais" (por exemplo, dados médicos, biométricos e de segurança social, registros fiscais, contas bancárias, arquivos de clientes empresariais, cadastros e registros eleitorais). Apontou que "a eliminação ou alteração fraudulenta de dados civis essenciais pode causar mais danos à população civil do que a destruição de objetos físicos"[89]. Embora o CICV reconheça que a questão de saber se os dados podem constituir um alvo civil permanece em aberto, indicou que deve ser resolvida no campo do direito internacional humanitário. Caso contrário, haverá uma grande "lacuna na proteção", incompatível com o objeto e a finalidade do direito internacional humanitário. A sétima pergunta solicitava a opinião dos Estados membros sobre esse importante assunto.

---

[85] *Id*. (citando o artigo 54.2 do Protocolo Adicional I)

[86] Quando um determinado objeto é utilizado para fins civis e militares (os chamados "objetos de dupla utilização"), ele se torna um alvo militar (exceto pelas partes que possam ser separadas). Ver fontes que codificam esse princípio de "distinção" na nota 61 *supra*.

[87] *Tallinn 2.0*, nota 20 *supra*, em 437.

[88] *Id.* em 416.

[89] CICV, Documento de posição, nota 62 *supra*, em 8; Relatório do CICV de 2019, nota 71 *supra*, em 21. (Além disso, os dados tornaram-se um componente essencial do domínio digital e uma pedra angular da vida em muitas sociedades. Contudo, existem diferentes pontos de vista sobre se os dados civis devem ser considerados como objetos civis e, portanto, protegidos ao abrigo dos princípios e normas do DIH que regem a condução das hostilidades. Na opinião do CICV, a conclusão de que esse tipo de operação não seria proibido pelo DIH no mundo atual cada vez mais ciberdependente — seja porque remover ou alterar esses dados não constituiria um ataque na acepção do DIH ou porque esses dados não seriam considerados objetos aos quais se aplicaria a proibição de ataques contra bens de caráter civil — parece difícil de conciliar com o objetivo e a finalidade desse ordenamento jurídico. Em suma, a substituição de arquivos em papel e documentos por arquivos digitais na forma de dados não deve diminuir a proteção proporcionada pelo DIH"); Relatório do CICV de 2015, nota 67 *supra*, em 43.

36. Nenhum dos Estados que responderam a essa pergunta adotou a posição de que os dados civis estão diretamente sujeitos ao princípio da distinção em conflitos armados. De fato, vários Estados mencionam o princípio da distinção sem se pronunciarem sobre a condição dos dados como objeto[90]. Entretanto, a resposta do Chile parece indicar que o princípio da distinção poderia ser aplicado a operações cibernéticas dirigidas contra dados indiretamente com base em suas repercussões. Cita o comentário no Protocolo Adicional I de que um objeto deve ser "visível e tangível", o que significa que, "segundo o direito internacional humanitário vigente, os dados mencionados não se qualificariam como objetos, em princípio, porque são essencialmente intangíveis, sem prejuízo dos elementos físicos em que os dados estão contidos, por exemplo, o hardware"[91]. Ao mesmo tempo, o Chile assinala que "um ataque dirigido exclusivamente contra dados informáticos pode perfeitamente gerar consequências adversas que afetem a população civil". Dá como exemplo a possibilidade de uma operação cibernética que elimine a base de dados de seguridade social de um Estado[92] e conclui que "o princípio da distinção deve ser levado em consideração no contexto de operações cibernéticas, motivo pelo qual um Estado deveria abster-se de atacar dados caso isso possa afetar a população civil, a menos que os referidos dados estejam sendo utilizados para fins militares"[93]. A Guiana responde de forma semelhante. Após assinalar que o ato de eliminar, suprimir ou corromper dados pode ter consequências de grande alcance, concentra-se nos efeitos da operação cibernética, em vez de abordar a questão de se os dados visados podem ou não ser considerados um objeto[94].

37. Em sua resposta, o Peru não aborda a possibilidade de que os dados possam ser considerados como um alvo civil, mas se concentra (de forma afirmativa) na possibilidade de que possam ser considerados como um alvo militar. Indica que certos "dados" (por exemplo, "um software que permite a comunicação entre tropas em um exército em campanha ou sincroniza o arsenal de mísseis de um país ou ajuda a localizar uma aeronave inimiga") são alvos militares legítimos, enquanto outros sistemas de dados usados em conflitos (por exemplo, "um sistema de dados que permite o funcionamento de uma sala de operações de um hospital de campanha onde são tratados feridos de guerra ou civis") não podem ser alvo de ataques[95].

38. Vários comentários dos Estados membros ao Grupo de Trabalho de Composição Aberta afirmaram a importância da aplicação do direito internacional humanitário ao contexto cibernético. Alguns Estados, como o Brasil, salientaram ainda que essa aplicação deve incluir expressamente os princípios fundamentais de "humanidade, necessidade, proporcionalidade e distinção".[96] Contudo, nenhuma das contribuições do Grupo de Trabalho de Composição Aberta abordou a definição de um ataque ou a ideia dos dados como um alvo civil (ou militar).

Pergunta 8: A soberania é uma norma separada do direito internacional que proíbe aos Estados participar de operações cibernéticas específicas? Em caso afirmativo, essa proibição abrange as operações cibernéticas que estão abaixo do limiar de uso da força e que, além disso, não violam o princípio da não intervenção?

---

[90] Ver a resposta da Bolívia, nota 1 *supra* , em 5-7; a resposta do Equador, nota 1 *supra* , em 2; e a resposta da Guatemala, nota 1 *supra*, em 3.
[91] Resposta do Chile, nota 1 *supra*, em 4.
[92] *Id*.
[93] *Id*.
[94] Resposta da Guiana, nota 1 *supra*, em 4 (onde afirma que, no que diz respeito aos dados, deve-se levar em conta se a operação cibernética dirigida contra os dados resultou na referida perda de funcionalidade que possa constituir um ataque).
[95] Resposta do Peru, nota 1 *supra*, em 6 O Peru explica que, no primeiro caso, os ataques causariam "um dano militar significativo às forças da contraparte", enquanto um ataque aos dados no hospital de campanha "não geraria uma vantagem militar legítima". *Id*.
[96] Comentários do Brasil, *supra*, nota 5

39. A soberania é, sem dúvida, a característica estrutural básica do atual ordenamento jurídico internacional, que atribui direitos e responsabilidades aos Estados[97]. É um princípio basilar de algumas das normas jurídicas internacionais mencionadas (por exemplo, a proibição do uso da força, o direito à legítima defesa, a responsabilidade do Estado). Além disso, em certos contextos, a soberania existe não só como um princípio básico, mas também como uma norma independente que regula o comportamento do Estado (por exemplo, uma aeronave que entra no espaço aéreo de outro Estado sem autorização viola a sua soberania)[98]. Contudo, ainda não está claro se a soberania tem qualidade de norma no ciberespaço. O *Manual Tallinn 2.0* assinala que se trata de uma regra que limita as operações cibernéticas de um Estado que não resultam no uso da força nem constituem uma intervenção proibida[99]. Não obstante, em 2018, o Procurador-Geral do Reino Unido considerou que a soberania não era uma norma de direito internacional em si, mas um princípio que servia de base para outras normas[100]. Posteriormente, o Ministério da Defesa da França e o Governo da Holanda manifestaram o seu apoio à soberania como norma autônoma[101].

---

[97] *Island of Palmas (Netherlands v. United States of America)*, 2 R.I.A.A. 829, 839 (1928) ("A soberania nas relações entre os Estados significa independência. A independência em relação à porção do mundo que ocupam é o direito de exercer dentro dela, com exclusão de qualquer outro Estado, as funções de um Estado [...]. A soberania territorial, como já foi mencionado, implica o direito exclusivo de exercer as atividades de um Estado. Esse direito tem como corolário um dever: a obrigação de proteger, dentro do território, os direitos de outros Estados, em particular o seu direito à integridade e à inviolabilidade em tempos de paz e de guerra" [traduzido para português a partir da tradução feita pela CJI]).

[98] Ver, por exemplo, Michael N. Schmitt e Liis Vihul, *Respect for Sovereignty in Cyberspace* , 95 em *Texas L. Rev.* 1639, 1640 (2017). Além da proibição do uso da força enunciada no artigo 2.4, há um amplo acordo no direito internacional sobre o dever de não intervenção que se aplica ao ciberespaço. Ver, por exemplo, *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Jurisdição e Admissibilidade) [2006] ICJ Rep. 6,[46]-[48]; *Nicaragua Case*, nota 23 *supra*, par. 205; Resolução 2625 (XXV) da Assembleia Geral das Nações Unidas, de 24 de outubro de 1970, que contém a Declaração sobre os Princípios do Direito Internacional relativos às Relações Amistosas e à Cooperação entre os Estados, em conformidade com a Carta das Nações Unidas. O GPG de 2015 referendou esse princípio entre as normas do direito internacional que se aplicam ao ciberespaço. Secretário-Geral das Nações Unidas, *Relatório do Grupo de Peritos Governamentais sobre os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional*, U.N. Doc. A/70/174 (22 de julho de 2015) parágrafos 26 e 28, b. A regra 66 do manual *Tallinn 2.0* postula que "um Estado não pode intervir, mesmo por meios cibernéticos, nos assuntos internos ou externos de outro Estado". *Tallinn 2.0*, nota 20 *supra*, em 312 (traduzido para português a partir da tradução feita pela CJI). No entanto, como no caso do uso da força, subsistem dúvidas sobre se esse dever existe no ciberespaço e que operações cibernéticas ele proíbe ou regulamenta.

[99] *Tallinn 2.0,* nota 20 *supra*, regra 4 ["Um Estado não deve realizar operações cibernéticas que violem a soberania de outro Estado" (traduzido para português a partir da tradução feita pela CJI)].

[100] Ver, por exemplo, Jeremy Wright, QC, MP. *Cyber and International Law in the 21st Century* (23 de maio de 2018) em https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("as opiniões do Reino Unido"). ("Alguns tentaram demonstrar a existência de uma norma orientada especificamente para o ciberespaço que se aplica à 'violação da soberania territorial' [...]. É claro que a soberania é fundamental para o sistema internacional baseado em normas, mas não estou convencido de que hoje possamos extrapolar a partir desse princípio geral uma norma específica ou uma proibição de atividades cibernéticas além de uma intervenção proibida. Portanto, a posição do Governo do Reino Unido é que não existe uma norma desse tipo no direito internacional vigente".

[101] Ver Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace* (9 de setembro de 2019), em https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("Opinião do Ministério da Defesa da França") em 6 ("Toda penetração não autorizada de sistemas franceses por um Estado ou todo ato que surta efeitos no território francês por meio de um vetor digital poderia constituir, no mínimo, uma violação da soberania" [tradução inglesa do relator]); *Letter to the parliament on the international legal order in cyberspace* , 5 de julho de 2019, anexo 1 em https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-

40. A finalidade da oitava pergunta era recolher as opiniões dos Estados membros sobre a questão da soberania como princípio em oposição à soberania como norma. A pergunta centra-se na função limitadora da soberania, ou seja, se e como ela limita a capacidade de um Estado de conduzir operações cibernéticas fora do seu território. O interessante é que muitos dos Estados respondentes tomaram a pergunta como um convite para reafirmar a função habilitadora da soberania; por exemplo, de acordo com a autoridade do Estado para regulamentar as TICs dentro de sua própria jurisdição territorial. A Bolívia e a Guiana dizem que a soberania autoriza os Estados a exercerem jurisdição sobre a infraestrutura ou as atividades cibernéticas em seu território[102]. O Equador, por outro lado, questiona a capacidade dos Estados de exercerem sua soberania no ciberespaço em vista de sua "intangibilidade" e, ao mesmo tempo, alega que os Estados têm soberania sobre a "infraestrutura cibernética" e as atividades relacionadas com a referida infraestrutura em seu território[103]. Chile e Estados Unidos também fazem eco do poder que a soberania confere aos Estados sobre as TICs em seu território, mas observam que esse poder deve agir dentro de certos limites. Ambos apontam para a necessidade de os Estados exercerem a soberania de acordo com o direito internacional dos direitos humanos[104]. A Colômbia apoiou este último ponto em seus comentários ao Grupo de Trabalho de Composição Aberta.[105]

41. Sobre a pergunta de se a soberania opera como norma autônoma no ciberespaço, três Estados — Bolívia, Guatemala e Guiana — responderam que sim[106]. A Guiana, por exemplo, afirma que as proteções da soberania "não se limitam às atividades que representem um uso injustificado da força, um ataque armado ou uma intervenção proibida"[107]. Opina que o Estado "não deve realizar operações cibernéticas que violem a soberania de outro Estado", e a existência de uma violação desse tipo depende "do grau de infração e de se houve interferência nas funções do governo"[108]. A Guatemala adota uma posição semelhante, afirmando que "um Estado que participa

---

documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ("Opinião dos Países Baixos") ["Segundo alguns países e juristas, o princípio da soberania não constitui uma norma independentemente vinculante do direito internacional que a separa das demais normas dele derivadas. Os Países Baixos não concordam com esse ponto de vista, pois acreditam que o respeito pela soberania de outros países é uma obrigação em si mesma, cuja violação poderia, por sua vez, constituir um ato ilícito em nível internacional" (traduzido para português a partir da tradução feita pela CJI)]. Uma análise acadêmica recente questiona se a França está claramente do lado da soberania como norma. Ver Gary Corn, *Punching on the Edges of the Gray Zone*: *Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (11 de fevereiro 2020) ("embora o Ministério da Defesa afirme que os ataques cibernéticos, tal como define o termo, contra os sistemas digitais franceses ou qualquer efeito produzido no território francês por meios digitais poderiam constituir uma violação da soberania no sentido geral, em nenhum momento diz, sem sombra de dúvida, que uma violação do princípio de soberania constitui uma violação de uma obrigação internacional. Pelo contrário, os autores do documento, obviamente conscientes do debate, são deliberadamente vagos sobre o assunto e apenas reafirmam o direito da França de responder aos ciberataques com todo o leque de opções que lhe são oferecidas pelo direito internacional").

[102] Resposta da Bolívia, nota 1 *supra*, em 5 a 7; resposta da Guiana, nota 1 *supra*, em 5.

[103] Resposta do Equador, nota 1 *supra*, em 2.

[104] Resposta do Chile, nota 1 *supra*, em 4 e 5 (onde reconhece que a soberania autoriza o Estado a proteger e defender "sua infraestrutura crítica de informação, [...] desde que tais medidas não entrem em conflito com uma norma de direito internacional, como aquelas presentes no direito internacional dos direitos humanos ou no direito internacional humanitário"); texto apresentado pelos EUA ao GPG em 2014, nota 1 *supra*, em 737-738 (observando que o exercício da jurisdição de um Estado territorial não é ilimitado, mas sim deve ser consistente com o direito internacional aplicável, incluindo as obrigações internacionais em matéria de direitos humanos, e mencionando em particular a liberdade de expressão e a liberdade de opinião).

[105] Comentários da Colômbia, nota 5 *supra*.

[106] Resposta da Bolívia, nota 1 *supra*, em 5-7; resposta da Guatemala, nota 1 *supra*, em 3; resposta da Guiana, nota 1 *supra*, em 5.

[107] Resposta da Guiana, nota 23 *supra*, em 5

[108] *Id.*

de operações cibernéticas específicas viola a soberania de um país se, no momento de um ataque cibernético, certas informações são capturadas no ambiente cibernético de outro Estado, mesmo que não causem danos que afetem algum equipamento ou os direitos humanos de alguma ou algumas pessoas"[109].

42. As respostas de outros Estados são bastante ambíguas. O Peru diz simplesmente que a soberania "é um dos pilares fundamentais da sociedade internacional", sem opinar sobre sua condição de norma independente[110]. O Equador indica que a "norma" que autoriza os Estados a controlarem sua própria infraestrutura cibernética "não proíbe um Estado [...] de participar em operações cibernéticas", mas não toma posição sobre se poderia regulamentar a forma como o faz em relação a outros Estados soberanos[111].

43. Em sua resposta, o Chile descreve a soberania como um princípio que "os Estados que realizam operações cibernéticas devem sempre levar em conta"[112]. Por isso, "sempre que um Estado contempla realizar uma operação cibernética, deve ter em consideração não afetar a soberania de outro"[113]. A referência a um "princípio" orientador pode sugerir algo diferente de uma regra concreta, embora o uso do verbo "devem" crie expectativas com um caráter mais vinculante. Por outro lado, o Chile afirma o seguinte:

> cada Estado é obrigado a respeitar a integridade territorial e a independência política dos outros Estados e deve cumprir fielmente as suas obrigações internacionais, inclusive o princípio da não intervenção. Portanto, as operações cibernéticas que impedem o exercício da soberania por parte de outro Estado constituem uma violação da referida soberania e são proibidas pelo direito internacional[114].

A última frase parece indicar que a soberania poderia constituir uma norma autônoma, a menos que a referência à intervenção no exercício da soberania de outro Estado seja entendida como o equivalente ao *domaine resérvé* protegido pelo dever de não intervenção[115].

44. A posição dos Estados Unidos é ainda menos clara. Em 2014, o então assessor jurídico Harold Koh afirmou que "a soberania do Estado [...] deve ser levada em conta na realização de atividades no ciberespaço, mesmo fora do contexto do conflito armado"[116]. No entanto, não está claro se levar em conta a soberania do Estado indica o reconhecimento pelos Estados Unidos da soberania como norma autônoma. Em seu discurso de 2016, o então assessor jurídico Brian Egan deixou claro que "as operações cibernéticas remotas com computadores ou outros dispositivos em rede localizados no território de outro Estado não constituem, por si só, uma violação do direito internacional"[117]. Ao mesmo tempo, admitiu que, "em certas circunstâncias, as operações cibernéticas não consensuais de um Estado no território de outro poderiam violar o direito internacional, mesmo que não atinjam o limiar do uso da força". De toda maneira, Egan indicou que "o momento preciso em que uma operação cibernética não consensual viola a soberania de outro

---

[109] Resposta da Guatemala, nota 1 *supra*, em 3.
[110] Resposta do Peru, nota 1 *supra*, em 6 e 7.
[111] Resposta do Equador, nota 1 *supra*, em 2.
[112] Resposta do Chile, nota 1 *supra*, em 5.
[113] *Id*.
[114] *Id*.
[115] Ver nota 99.
[116] Koh, nota 1 *supra*, em 596 (traduzido para português a partir da tradução feita pela CJI); texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 737; texto apresentado pelos Estados Unidos ao GPG em 2016, nota 1 *supra*, em 825.
[117] Egan nota 1 *supra*, em 818 (traduzido para português a partir da tradução feita pela CJI). Entre outras coisas, Egan disse que os Estados Unidos compilavam informações no exterior e que essas atividades poderiam violar as leis nacionais de outros Estados, mas não eram, por si só, proibidas pelo direito internacional consuetudinário. *Id*.

Estado é um assunto que os advogados do Governo dos Estados Unidos continuam estudando minuciosamente e será finalmente resolvido por meio da prática e da *opinio juris"*[118]. Mais recentemente, porém, o Assessor Jurídico do Departamento de Defesa dos Estados Unidos indicou que "com respeito às operações cibernéticas que não constituiriam uma intervenção proibida ou uso da força [ou seja, aquelas que poderiam estar cobertas por uma regra de soberania], o Departamento acredita que não há uma prática estatal suficientemente difundida e consistente como resultado de um senso de obrigação legal de concluir que o direito internacional consuetudinário geralmente proíbe tais operações cibernéticas não consensuais no território de outro Estado[119].

45. Em um debate entre 16 representantes dos Estados membros realizado de acordo com as "Regras de Chatham House" [120] em 23 de junho de 2020, ficou reforçada a atual diversidade de opiniões sobre a questão da soberania. Vários participantes solicitaram que se afirmasse a opinião da soberania como norma para o ciberespaço, com o que a violação da soberania implicaria uma responsabilidade jurídica internacional. Outros, porém, expressaram maior ceticismo quanto ao valor desse trabalho; um participante sugeriu que poderia haver muitos significados do termo "soberania" para atribuir-lhe o *status* de regra. Outro participante considerou que o "debate sobre a soberania é uma distração", e um terceiro participante sugeriu explicitamente a necessidade de repensar seu significado no contexto cibernético.

Pergunta 9: A devida diligência é uma norma do direito internacional que os Estados devem respeitar no exercício da sua soberania sobre as tecnologias da informação e das comunicações nos seus territórios ou sob o controle dos seus cidadãos?

46. A devida diligência é um princípio do direito internacional segundo o qual um Estado deve responder às atividades que saiba (ou deveria saber) que tiveram origem em seu território ou em outras áreas sob o seu controle e violam os direitos de outro Estado[121]. É uma obrigação de esforço e não de resultado: quando um Estado está ciente da conduta ou deve estar ciente dela, deve usar "todos os meios razoavelmente disponíveis" para corrigi-la[122]. Como princípio, a devida diligência regula atualmente o comportamento do Estado em vários contextos, em particular no direito internacional ambiental, no qual constitui a base da exigência de que os Estados contenham em seu território a poluição que seja fonte de danos transfronteiriços para o território de outros Estados.

47. Assim como acontece com a soberania, existem opiniões divergentes sobre se a devida diligência é uma exigência do direito internacional no ciberespaço. O relatório do GPG de 2015 menciona-a entre as normas "voluntárias" do comportamento responsável dos Estados, em vez de incluí-la nos princípios aplicáveis do direito internacional[123]. Os Ministérios da Defesa dos Países

---

[118] *Id*. em 819

[119] *Ver* Paul C. Ney, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 de março de 2020, em https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/?dod-general-counsel-remarks-at-us-cyber-command-legal-conference. Contudo, não fica claro se Ney estava expressando a opinião dos Estados Unidos na sua totalidade ou se era apenas a posição dos militares americanos, ambiguidade que também existe no que diz respeito às opiniões do Ministério da Defesa francês. Ver nota 101 *supra*.

[120] Chatham House, *A Regra de Chatham House:* https://www.chathamhouse.org/chatham-house-rule (Quando uma reunião, ou parte de uma reunião, é convocada sob a Regra de Chatham House, os participantes têm o direito de usar as informações recebidas, mas não podem revelar a identidade nem a afiliação do orador, ou de qualquer outro participante)

[121] Ver, por exemplo, *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)* [1949] ICJ Rep., par. 22 (9 de abril); *Trail Smelter Case (United States-Canada*), UNRIAA, vol. III, 1905 (1938, 1941).

[122] Ver *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia v. Serbia)* (Sentença) [2007] ICJ Rep. 1, par. 430.

[123] GPG de 2015, nota 1 *supra*, par. 13 e 26 a 28.

Baixos e da França descreveram-na como uma norma jurídica aplicável ao ciberespaço[124]. Contudo, os Países Baixos observam que nem todos os países concordam que o princípio da devida diligência constitui uma obrigação em si mesmo à luz do direito internacional, e se acredita que os Estados Unidos sejam um dos países que questionam essa condição[125]. Portanto, a nona pergunta visava suscitar a opinião dos Estados membros sobre a condição da devida diligência no que se refere às obrigações de um Estado ao abrigo do direito internacional no ciberespaço.

48. Chile, Equador, Guatemala, Guiana e Peru adotam a posição de que o princípio da devida diligência faz parte do direito internacional que os Estados devem aplicar no ciberespaço[126]. Como explica o Chile, "do ponto de vista das operações cibernéticas, um Estado deve exercer a devida diligência para evitar que seu território soberano, incluindo a infraestrutura cibernética sob seu controle, seja utilizado para realizar operações cibernéticas que afetem os direitos de outro Estado ou possam ter consequências adversas para outro Estado"[127]. A Guatemala adota uma posição semelhante e acrescenta que, como "ciberespaço" é um termo muito amplo, agir com a devida diligência pode ser extremamente complicado[128]. Mesmo assim, na medida em que a devida diligência "deriva do princípio de soberania", a Guatemala acredita que "cada Estado deve ter o controle para parar a atividade prejudicial que ocorre a partir de seu território, obrigando-se a tomar medidas preventivas, instituindo uma CERT, adotar políticas de segurança da informação e aumentar a conscientização sobre a segurança da informação"[129].

49. A resposta da Bolívia é mais ambígua. Sem referir-se à condição jurídica da devida diligência, opina que um Estado não pode ser responsabilizado por um ataque cibernético se não tiver a infraestrutura tecnológica para controlar um agente não estatal[130]. Essa opinião poderia ser compatível com o princípio da devida diligência como norma jurídica internacional para as operações cibernéticas, uma vez que geralmente exige que os Estados "tenham conhecimento" das atividades em questão, o que não seria possível para os Estados que não dispõem da infraestrutura

---

[124] Parecer do Ministério da Defesa da França, nota 101 *supra*, em 10 ("De acordo com a obrigação de agir com a devida diligência, os Estados devem assegurar que o seu domínio soberano no ciberespaço não seja utilizado para cometer atos internacionalmente ilícitos. Se um Estado não cumprir com essa obrigação, isso não é motivo para uma exceção à proibição do uso da força, ao contrário do parecer da maioria dos integrantes do grupo de peritos que elaborou o Manual de Tallinn"; parecer dos Países Baixos, nota 101 *supra*, anexo, em 4 ["o princípio da devida diligência exige que os Estados tomem medidas relativamente às atividades cibernéticas realizadas por pessoas em seu território ou para as quais se utilizem redes que se encontrem em seu território ou sob seu controle, que violem um direito de outro Estado e de cuja existência tenham ou devam ter conhecimento" (traduzido para português a partir da tradução feita pela CJI)]. A Estônia, embora não descreva a devida diligência como norma específica do direito internacional, classificou o seu conteúdo como requisito para a conduta do Estado. Kersti Kaljulaid, Presidente da Estônia, *President of the Republic at the opening of CyCon 2019* (maio de 2019), em: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("A opinião da Estônia") ["Os Estados têm de fazer um esforço razoável para garantir que o seu território não seja utilizado com o objetivo de prejudicar os direitos de outros Estados. Devem buscar meios para oferecer apoio quando solicitado pelo Estado atacado, a fim de identificar, atribuir ou investigar operações cibernéticas maliciosas. Essa expectativa depende da capacidade nacional, da disponibilidade de informação e da sua acessibilidade" (traduzido para português a partir da tradução feita pela CJI)].

[125] Opinião dos Países Baixos, nota 101 *supra*, anexo, em 4.

[126] Resposta do Chile, nota 1 *supra*, em 6 e 7; resposta do Equador, nota 1 *supra*, em 2; resposta da Guatemala, nota 1 *supra*, em 4; resposta da Guiana, nota 1 *supra*, em 5; resposta do Peru, nota 1 *supra*, em 7.

[127] Resposta do Chile, nota 1 *supra*, em 6 e 7. O Equador disse simplesmente que "a devida diligência é aplicável ao que acontece nos recursos tecnológicos dentro do seu território nacional". Resposta do Equador, nota 1 *supra*, em 2.

[128] Resposta da Guatemala, nota 1 *supra*, em 4.

[129] *Id*. em 2 e 4.

[130] Resposta da Bolívia, nota 1 *supra*, em 3 a 7.

técnica necessária[131]. Por outro lado, a impossibilidade de "controlar" as atividades cibernéticas das quais se tenha conhecimento poderia indicar que a Bolívia não adere à doutrina da devida diligência no ciberespaço. Sem um esclarecimento da resposta, é difícil chegar a uma conclusão. Além disso, as declarações públicas anteriores dos Estados Unidos não abordaram diretamente a condição jurídica da devida diligência. Deve-se notar, no entanto, que os Estados Unidos tendem a descrever toda obrigação de responder a pedidos de assistência em termos não vinculantes[132]. O fato de os Estados Unidos não terem referendado publicamente o princípio da devida diligência como norma jurídica no GPG ou em outros contextos poderia indicar dúvidas quanto à condição jurídica desse princípio.

50. No debate de Chatham House de junho de 2020, vários Estados membros expressaram seu apoio à devida diligência como norma (importante) do direito internacional no contexto cibernético. No entanto, um representante de um Estado membro manifestou dúvidas quanto ao apoio à devida diligência, dado o risco de incumprimento que poderia ocorrer para os Estados que são incapazes de responder adequadamente a ataques cibernéticos devido à falta de capacidade técnica.

Pergunta 10: Existem outras regras do direito internacional que o seu Governo considera importante levar em conta ao avaliar a regulação das operações cibernéticas por parte dos Estados ou atores pelas quais um Estado tem responsabilidade internacional?

51. A décima e última pergunta pedia aos Estados que indicassem outras áreas do direito internacional nas quais a Comissão deveria se concentrar, a fim de aumentar a transparência no contexto cibernético. As respostas abordam assuntos distintos. A Bolívia pede que seja dada mais atenção à proteção dos "direitos fundamentais de seus cidadãos em qualquer dimensão em que atuem", inclusive no ciberespaço[133]. Algumas respostas concentram-se na criminalidade cibernética e, em particular, na Convenção de Budapeste, elaborada pelo Conselho da Europa[134]; outras destacam a contribuição dos Manuais de Tallinn[135].

52. Dois Estados — Equador e Guiana — indicam que poderia ser necessário um novo direito internacional no contexto cibernético. O Equador enfatiza a necessidade de estabelecer uma forma de regular "os ataques a alvos militares e/ou civis que afetam massivamente a população, como é o caso da infraestrutura crítica, dos hospitais, dos meios de transporte de massa e de outras infraestruturas que afetam a segurança do Estado"[136]. A Guiana diz que seria prudente ter um conjunto de princípios do direito internacional adaptados à índole especial do ciberespaço e observa que os princípios jurídicos atuais foram elaborados para uma época e um contexto diferentes[137].

53. Nas consultas de Chatham House de junho de 2020, vários Estados membros solicitaram que fosse dada maior atenção ao princípio de não interferência (e ao tema de quais atividades cibernéticas constituem coerção). Vários participantes ecoaram o apelo a uma maior atenção aos temas jurídicos "abaixo" do limiar do uso da força estabelecido pela proibição do artigo 2 (4) da Carta das Nações Unidas. Outros sugeriram menos atenção aos temas de paz e segurança

---

[131] Ver *Tallinn 2.0*, nota 20 *supra*, em 40.

[132] Texto apresentado pelos Estados Unidos ao GPG em 2014, nota 1 *supra*, em 739 ("Um Estado *deveria* cooperar, de forma coerente com a legislação nacional e as obrigações internacionais, com pedidos de assistência de outros Estados para investigar crimes cibernéticos, obter provas eletrônicas e mitigar atividades cibernéticas maliciosas em seu território").

[133] Resposta da Bolívia, nota 1 *supra*, em 6 e 7.

[134] Resposta da Guatemala, nota 1 *supra*, em 4; resposta da Bolívia, nota 1 *supra*, em 6 e 7.

[135] Resposta da Costa Rica, nota 1 *supra*, em 2 (expressando o interesse da Costa Rica em aderir à Convenção de Budapeste); resposta da Guatemala, nota 1 *supra*, em 4 (citando a Convenção de Budapeste).

[136] Resposta do Equador, nota 1 *supra*, em 3.

[137] Resposta da Guiana, nota 1 *supra*, em 5 e 6 (indicando que o anonimato é uma dificuldade particular na aplicação do direito atual).

internacional em favor de uma maior atenção à aplicação do direito internacional dos direitos humanos ao ciberespaço. Outros temas que receberam atenção foram o direito diplomático, o princípio da boa fé, as contramedidas e os padrões de prova para a atribuição de operações cibernéticas a um Estado.

54. Finalmente, ao menos um participante solicitou o desenvolvimento de uma perspectiva latino-americana sobre a governabilidade internacional e o marco legal do ciberespaço. O participante observou que a maioria das ideias sobre direito internacional no ciberespaço foram desenvolvidas pelos Estados europeus ou por especialistas do Norte Global. Em vez de duplicar os esforços existentes (por exemplo, GPG das Nações Unidas, Grupo de Trabalho de Composição Aberta das Nações Unidas, etc.), os países latino-americanos poderiam basear-se nesses princípios para elaborar um marco latino-americano, a fim de entender o direito internacional no ciberespaço, orientando-se por uma cultura política comum de instituições democráticas e história ibero-americana. A OEA foi citada como o lugar ideal para coordenar essa visão conjunta.