Operações cibernéticas militares e as implicações perante a Lei Internacional

JULIA DORNSBUSCH

■ As operações cibernéticas têm grande importância em uma guerra e desempenham papel significativo nas relações entre os países. Este artigo pretende dar uma visão geral das implicações relevantes perante a lei internacional.

No que se refere a um regime de paz, a pergunta que se faz é em que circunstâncias as operações cibernéticas violam a proibição do uso de força militar contra outro Estado e a proibição de interferir em seus assuntos domésticos. Existe um consenso geral quanto ao fato de que apenas as operações cibernéticas que causam danos físicos podem ser consideradas como uso de força proibida. No entanto, a maioria das operações cibernéticas entre Estados são usadas para angariar informações (incluindo espionagem), o exercício da pressão política com o objetivo de fazer propaganda ou para dar apoio a operações armadas, como diversos exemplos comprovam. Ainda que envolvam um dano material considerável, não causam danos físicos. Com este pano de fundo, o artigo se concentra nas implicações legais de operações cibernéticas em tempos de paz no que diz respeito à interferência proibida em assuntos domésticos dos Estados e a noção de soberania de Estado. Neste artigo, ficará claro que os Estados precisam refinar e chegar a um acordo sobre o entendimento comum do conceito de soberania e outros princípios básicos da lei internacional para regular as operações cibernéticas.

Como as operações cibernéticas militares ganham relevância significativa em tempos de guerra, suas implicações sob a lei em caso de conflito armado não podem ser deixadas fora da equação. Assim, na terceira parte, o texto ilustra o conceito de "ataque", que tem importância crítica para a proteção de civis durante o conflito armado. A interpretação estrita de "ataque" pelos Estados dentro da lei atual será criticada, porque não inclui muitas operações cibernéticas que podem

desencadear consequências humanitárias calamitosas em tempos de guerra. Além do mais, as operações cibernéticas que possibilitam ataques armados (convencionais) e sua regulamentação seguindo as regras do engano em conflitos armados estão sendo contestadas.

O artigo conclui com uma avaliação das medidas defensivas contra operações cibernéticas sob a lei da Responsabilidade do Estado. Dentro deste contexto, destacam-se as obrigações legais dos Estados dentro da lei internacional sobre segurança cibernética e a necessidade urgente da cooperação internacional entre os Estados.

É interessante enfatizar que o artigo não se detém em operações militares por Estados ou, em outras palavras, em ataques cibernéticos que são atribuídos a um Estado dentro da lei de Responsabilidade de Estado. Portanto, em todos os exemplos discutidos, se parte do princípio que a responsabilidade dos Estados pode ser provada.

ATAQUES CIBERNÉTICOS COMO MEIO DE PRESSÃO POLÍTICA, PROPAGANDA E ESPIONAGEM

■ Ao examinar incidentes cibernéticos na prática, fica claro que as operações cibernéticas dos Estados perseguem principalmente os seguintes objetivos: obter informação (espionagem), apoiar ou preparar ataques armados, exercer pressão política e disseminar propaganda. Seria possível questionar porque tamanha determinação dos objetivos subjacentes dos ataques cibernéticos é necessária ou até mesmo útil. Mas entender como e com que propósitos países usam operações cibernéticas nas relações internacionais é essencial para identificar as regras mais adequadas da Lei Internacional para regulamentação, para detectar incertezas legais e desenvolver estratégias adicionais para a garantia da segurança cibernética mundial. Assim, um resumo de alguns incidentes virtuais de grande relevância será apresentado a seguir.

Não há um dia em que os meios de comunicação não informem sobre algum incidente de espionagem cibernética. Há pouco tempo, o governo dos Estados Unidos, especificamente, foi acusado não só de espionar cidadãos estrangeiros, mas também de mirar na comunicação governamental de países estrangeiros. Em geral, esforços para obter dados sensíveis relacionados com as capacidades militares ou econômicas de um Estado parecem ser uma prática generalizada, com uso estendido por vários países. A relevância das operações cibernéticas na espionagem é inegável.

As atividades de engano cibernético são ainda mais importantes para operações militares durante ou imediatamente antes de conflitos armados. Por exemplo, Israel manipulou o Sistema de Defesa Aérea Síria para facilitar a entrada despercebida de seus bombardeiros em território sírio, o que facilitou o ataque a uma instalação nuclear.[1]

O maior incidente cibernético, em termos de escala, e com o objetivo claro de exercer pressão política em um governo estrangeiro, aconteceu na Estônia em 2007. A remoção do Memorial de Guerra Russo do centro da cidade de Talin desencadeou manifestações violentas de cidadãos russos. Durante esse momento de agitação civil, a Estônia enfrentou uma grande variedade de ataques DDoS (Negação de Serviço Distribuído), paralisando websites governamentais e de grandes meios de comunicação e interrompendo os sistemas bancários e instalações de comunicação.[2] O envolvimento do governo russo nunca ficou comprovado, mas essas operações indubitavelmente pretendiam mudar a política do governo estoniano em relação ao deslocamento do Memorial de Guerra. De modo similar, em conjunção com o conflito armado entre a Geórgia e a Rússia em 2008, meios de comunicação georgianos e instituições financeiras do país foram atacados por meios virtuais. Os serviços de comunicação do Governo foram interrompidos e os sites governamentais foram sabotados com objetivos de propaganda. Por exemplo, retratos do presidente da Geórgia foram substituídos por imagens de Adolf Hitler.[3] A relevância dos ataques cibernéticos para a disseminação de propaganda ficou ainda mais evidente na recente crise da Crimeia. Pouco antes do referendo sobre a unificação da Crimeia com a Rússia, os habitantes da Crimeia não apenas ficaram isolados de tudo e recebiam apenas notícias geradas pelos meios de comunicação russos – imprensa e televisão,[4] e também os sites de informação e as redes sociais foram sabotados com mensagens de propaganda e informações errôneas.[5]

Por último, o vírus Stuxnet, que ocasionou efeitos adversos na velocidade do rotor das centrífugas das instalações nucleares iranianas de enriquecimento

1 *Handler, Stephanie Gosnell*, The New Face of Battelfield, 48 Standford Journal of International Law (2012), p. 209-237, 223 (with relevant references)

2 *Tikk, Eneken/Kaska, Kardi/Vihul, Liis*, International Cyber Incidents: Legal Considerations, (2010), p.18-25

3 ibid. p. 69-79.

4 BBC, Crimeans urged to vote against ‚neo-Nazis' in Kiev (13 March 2014), disponível em: http://www.bbc.com/news/world-europe-26552066, last visited: 8 February 2015.

5 BBC, Russia and Ukraine in cyber ‚stand-off' (5 March 2014) disponível em: http://www.bbc.com/news/technology-26447200, última entrada: 8 de fevereiro de 2015.

de urânio de Natanz em 2010 e seu papel especial vai ser mencionado aqui. Stuxnet foi um dos ataques virtuais mais sofisticados que o mundo testemunhou até agora. O vírus auto-replicável foi projetado especificamente para manipular o Sistema de Supervisão de Controle de Aquisição de Dados usado em Natanz de modo que potencialmente pudesse causar danos materiais às centrífugas.[6] Obviamente, esse ataque cibernético também foi usado para aplicar pressão política no Irã e forçar esse país a mudar sua política nuclear. Stuxnet foi a primeira operação virtual que realmente tinha como meta causar destruição material de objetos do mundo real.

Dentro da lei internacional atual, este fato tem particular relevância porque só operações cibernéticas que causam danos físicos ou morte ou lesões corporais são consideradas uma violação da proibição do uso da força armada, algo que discutiremos em detalhes mais adiante, em contraposição à interrupção da infraestrutura essencial dos Estados. Dentro desse cenário, a maior parte dos ataques cibernéticos acarreta implicações para a interpretação de outros princípios ou regras da Lei Internacional, como a proibição de não intervenção ou soberania nacional.

O REGIME DE ÉPOCA DE PAZ

■ Em épocas de paz, a lei internacional, mais especificamente *ius ad bellum*, pretende manter a paz e a segurança internacionais e, portanto, geralmente proíbe o uso unilateral de força (militar) como meio político nas relações entre Estados.[7] Um Estado só pode recorrer à força para repelir um ataque armado, exercendo assim seu direito inerente à autodefesa.[8] Além disso, em função do fato de que a lei internacional é aplicável entre Estados igualmente soberanos, reconhece o direito de todo Estado de escolher seu sistema político, econômico, social e cultura, sem nenhuma interferência de outros Estados.[9] Deveria enfatizar-se que o princípio

6 *Buchan, Russell*, Cyber Attacks: Unlawful Uses of force or Prohibited Interventions?, 17 Journal of Conflict & Security Law (2012), p. 211-227, 219-220 (with relevant references).

7 Art. 2 (4) Carta das Nações Unidas.

8 Art. Carta das Nações Unidas; outra exceção seria a autorização de um Estado pelo Conselho de Segurança da ONU para o uso de medidas violentas de acordo com o Art. 39 e 42 da Carta das Nações Unidas.

9 Declaração dos Princípios da Lei Internacional sobre Relações Amigáveis e Cooperação entre os Estados, de acordo com a Carta das Nações Unidas, Resolução da Assembleia Geral da ONU 2526 anexo (XXV) (24 de outubro 1970), que é considerado direito consuetudinário (doravante: Friendly Relations Declaration); ver Art. 2 (7) da Carta da ONU.

da não intervenção e a proibição do uso da força são aplicados exclusivamente no nível interestatal, isto é, só se aplicam a atos que possam ser atribuídos a um Estado.

Como ficou demonstrado acima, as operações cibernéticas são usadas para propósitos de propaganda, espionagem e para exercer pressão política, o que suscita a pergunta sobre até que ponto essas operações são compatíveis com os princípios declarados da Lei Internacional. Aqui, o princípio da não-intervenção e da soberania do Estado têm interesse especial. Em relação à proibição do uso da força, a perturbação da infraestrutura cibernética, ocasionando meramente uma perda de funcionalidade e não a destruição (parcial) de um objeto, é algo controverso.

INTERRUPÇÃO DA INFRAESTRUTURA CIBERNÉTICA – O USO DA FORÇA

■ Os ataques cibernéticos violam potencialmente o uso da força, se seus efeitos forem comparáveis aos das operações militares convencionais, que são considerados incompatíveis com o Artigo 2 (4) da Carta das Nações Unidas.[10] Afinal de contas, não pode fazer diferença, se pessoas morrem porque uma represa foi destruída por bombardeio aéreo ou porque os portões foram abertos por meio de um ataque cibernético. As consequências típicas (e portanto relevantes aqui) do uso da força militar são a morte ou lesões em pessoas ou danos físicos de objetos. Portanto, os ataques cibernéticos que causam diretamente mortes ou ferimentos em pessoas ou prejuízos materiais, são violações potenciais do Artigo 2 (4) da Carta da ONU, pressupondo que se mantenha um certo grau de severidade.[11] Existe o consenso de que as operações cibernéticas sem consequências na esfera física, por exemplo, a mera manipulação ou furto de dados, não podem ser consideradas como uso de força.[12]

Mais problemática é a classificação legal dos ataques cibernéticos que não têm como resultado algum dano físico, mas que levam à perda da sua funcionalidade. Parece seguro pressupor que a lei internacional não diferencia, por exemplo, se o fornecimento de eletricidade de um Estado for interrompido porque uma central elétrica foi destruída ou porque um ataque virtual prejudicou sua

10 *Schmitt, Michael* (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), Rule 11.
11 ibid. Rule 11, para. 8 + 9 a).
12 *Dinniss, Heather Harrison*, Cyber Warfare and the Laws of War (2012), p.74.

operação. No entanto, a lei atual não parece dar suporte para um tratamento igual nos dois casos. Ainda que as operações cibernéticas que levem à perda de funcionalidade de um objeto com frequência acarretem danos materiais consideráveis, como a paralisação de uma bolsa de valores, elas não violam a proibição do uso da força *de lege lata*.[13] À primeira vista, esta conclusão parece arbitrária, mas a proibição estabelecida no Artigo 2 (4) deve ser interpretada considerando-se seu objetivo e papel dentro do *ius ad bellum*. Primeiro, o esboço do histórico da estipulação reflete a intenção dos Estados, como legisladores da Lei Internacional, de excluir coerção econômica ou política.[14] Além do mais, considerando-se que alguns Estados não distinguem entre um ataque armado que desencadeia o direito de usar força militar em defesa própria, e um uso de força em escala menor, uma interpretação estrita do Artigo 2 (4) da Carta da ONU parece apropriada. Se tivermos em mente o objetivo principal do *ius ad bellum* – geralmente, proibir unilateralmente o uso da força como um meio político nas relações interestatais – o resultado de certa forma ambivalente em relação à operação cibernética que apenas perturba a infraestrutura cibernética, precisa ser aceito por enquanto. Os Estados, como legisladores, precisam considerar se a perturbação da infraestrutura virtual deveria ser incluída na proibição do uso de força no futuro e até que ponto. Uma restrição, por exemplo, para certos objetos de infraestrutura nacional crítica,[15] ou seja, ativos ou sistemas que sejam "essenciais para a manutenção das funções vitais da sociedade, saúde, segurança, bem-estar econômico ou social da população, como por exemplo, centrais elétricas, redes de transporte e redes governamentais,[16] seria algo convincente. Ademais, é evidente que um certo grau de intensidade da perturbação, tornando-a comparável à destruição do objetivo físico seria necessária.[17] A prática de Estado vai mostrar se uma abordagem mais consistente dos ataques cibernéticos e o uso da força em relações internacionais vai prevalecer.

13 *Buchan* (fn. 6), p. 212;

14 *Simma, Bruno/Khan, Daniel-Erasmus/ Nolte, Georg/ Paulus, Andreas* (eds.), Charter of the United Nations - A Commentary, 3ª edição (2012), Vol I, Art. 2 (4), p. 18.

15 ver *Roscini*, *Marco*, Cyber Operations and the Use of Force in International Law (2014), p. 55-63; *Ziolkowski, Katharina*, General Principles of International Law as Applicable in Cyberspace, in: Ziolkowski, Katharina (ed.), Peacetime Regime For State Activities in Cyberspace (2013), p. 135-188, 173

16 Diretiva 2013/40/EU sobre ataques contra sistemas de informação (12 de agosto 2013), Diretiva do Parlamento Europeu e do Conselho, Official Journal of the European Union L 218/8 – 14, p 4.

17 ver *Ziolkowski* (fn. 15), p. 173.

INTERVENÇÃO NOS ASSUNTOS INTERNOS DE UM ESTADO ESTRANGEIRO

■ A Lei Internacional de tempos de paz estipula a obrigação dos Estados de refrear qualquer intervenção nos assuntos domésticos de uma nação estrangeira. O escopo exato e o conteúdo do princípio de não-intervenção é alvo de controvérsia. A lei internacional não proíbe toda e qualquer interferência, mas exige que a intervenção seja de caráter coercitivo e que afete exclusivamente os assuntos nacionais de um Estado.[18]

O significado desses dois elementos qualificadores, porém, não está completamente claro. Em particular, a linha divisória entre assuntos nacionais e internacionais é uma linha tênue,[19]pois a lei internacional cada vez mais se "infiltra" no *domaine réservé* dos Estados.[20] Geralmente, aos Governos é permitido que escolham suas próprias políticas (dentro dos limites da lei internacional) em relação aos temas que a lei internacional deixa para a livre determinação. Para que a intervenção seja considerada ilegal, o Governo afetado precisa ser forçado por uma nação estrangeira a adotar uma determinada política; o nível exato de coerção, porém, não está estabelecido de modo definido.[21] Evidentemente, monitoramento ou subtração de dados de informações sensíveis sobre segurança nacional em si não preenchem o padrão de coerção, já que em nenhum aspecto forçam um Estado a fazer ou deixar de fazer alguma coisa.[22]

Apesar dessas incertezas, as implicações legais dos ataques virtuais em relação ao princípio da não-intervenção podem ser examinadas concentrando-se em alguns tipos de ações reconhecidas como intervenções ilegais sob a lei internacional atual. Essas são ações militares muito próximas do uso da força ou que envolvem a ameaça do uso de força, o apoio de atividades subversivas ou armadas de atores não estatais com o objetivo de derrubar o Governo de outras nações e o impedimento coercitivo do exercício das funções estatais centrais por parte do Governo de outra nação.[23]

---

18 ICJ, Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), Merits, Judgement of 27 June 1986, ICJ Reports p. 14, p. 205 (doravante: Nicaragua case)

19 *Gill, Terry*, Non-Intervention in the Cyber Context, em: Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace, p. 217-238, 217.

20 Especially due to the development of Human Rights and International Criminal law.

21 *Ziolkowski* (fn. 15), p. 165.

22 *Gill* (fn. 19), p. 232.

23 ibid. p. 222.

Em relação ao último fato discutido acima, os ataques cibernéticos que afetam infraestruturas essenciais, mas não causam danos materiais são particularmente relevantes. As perturbações sistemáticas que não sejam de curto prazo de uma infraestrutura crítica têm o potencial de coagir um Estado a mudar sua política e se objetivo era precisamente esse, provavelmente constituem intervenções proibidas. Os ataques de negação de serviço perpetrados contra a Estônia em 2007, que paralisaram sistemas bancários, sites importantes do Governo e páginas de meios de comunicação, atrapalhando a comunicação do Governo com seus cidadãos e também com o mundo exterior, pretendiam sem dúvida mudar a política da Estônia em relação à remoção do Memorial da Guerra da Rússia. Além disso, se estenderam por três semanas, o que deveria ser intensidade suficiente para que se considerassem esses ataques – desde que se pudesse provar a responsabilidade da Rússia – como intervenções ilegais.[24]

Outras ações claramente proibidas pelo princípio da não-intervenção são aquelas que ajudam a atores não estatais, com o objetivo de derrubar o regime de outro Estado por meios violentos.[25] A proibição não engloba apenas assistência financeira ou logística durante uma revolta em ebulição, mas simplesmente a incitação à derrubada violenta do Governo já é proibida. Isso leva à pergunta sobre a disseminação de propaganda por meios virtuais. O espaço cibernético oferece uma grande variedade de possibilidades de disseminação de informações falsas ou propaganda por meio de redes sociais ou e-mails. Além disso, os ataques cibernéticos que desfiguram sites e perturbam ou manipulam a mídia ou sistemas de transmissão ao vivo, ocorreram repetidamente no passado recente, como por exemplo na Crise da Crimeia ou na guerra Rússia-Geórgia em 2008.

Para ser considerada uma violação do princípio da não-intervenção, a propaganda disseminada por uma nação estrangeira precisa ser de natureza subversiva no sentido de instigar o uso da violência para forçar a mudança de Governo ou regime. O mero apoio político a um movimento de oposição ou desaprovação da política externa de outro país não é suficiente para tanto.[26] Considerando esse padrão, campanhas difamatórias, por exemplo, ou a sabotagem de sites governamentais, normalmente não serão consideradas uma intervenção ilegal.[27] De fato,

24 *Buchan* (fn. 6), p. 225-226.

25 Friendly Relations Declaration (fn. 9); Nicaragua case (fn. 18), para. 205.

26 *Gill* (fn. 19), p. 223; *Pirker, Benedikt*, Territorial and Integrity and the Challenges of Cyberspace, in: Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace, p. 189-216, 201.

27 *De Brabandere, Eric*, Propaganda, in: Wolfrum, Rüdiger (ed.), Max Planck Encyclopedia of Public International Law (2012), Vol. VIII, p. 510-511.

os fatos específicos de cada caso precisam ser levados em conta. Em épocas de agitação contínua, será mais provável que a disseminação de propagandas ou de informações enganosas seja definida como campanha subversiva.[28] Na ausência de perturbações civis, a propaganda precisa incitar claramente ao uso da violência porque uma campanha defendendo um regime de paz não seria qualificada como uma intervenção proibida.[29] O conteúdo da propaganda ou da informação disseminada, portanto, é crucial neste aspecto.

Dentro deste contexto, o status especial da propaganda relacionadas com processos eleitorais em outros países deveria ser enfatizado. Mesmo que simpatizar com um movimento oposicionista ou com um partido em geral não seja suficiente para violar o princípio da não-intervenção, campanhas com o potencial de minar o processo eleitoral constituem uma interferência ilegal nos assuntos internos de um Estado, mesmo que não incitem ações violentas.[30] Portanto, ataques cibernéticos que censuram e sabotam sites de meios de comunicação e de mídias sociais com propaganda pró Rússia antes e durante o referendum sobre a secessão da Crimeia e da Ucrânia no dia 16 de março de 2014[31] - desde que a responsabilidade dos russos pelos ataques fique comprovada – deve ser considerada ilegal.

Como já foi demonstrado, na prática muitas operações cibernéticas constituem interferências ilegais em temas nacionais de um país estrangeiro. No entanto, perturbações em pequena escala da infraestrutura cibernética, propaganda que não procure incitar mudanças violentas de regime e a mera intrusão de uma rede, espionagem ou manipulação de dados que não leve ao mau funcionamento ou à perda de infraestrutura não se configuram como violações da proibição, já que não têm natureza coercitiva ou não alcançam o patamar de grandeza que influências semelhantes precisam ter para potencialmente forçar um país a mudar sua política.

28 ver *Gill* (fn. 19), p. 234.

29 *De Brabandere* (fn. 27), p. 509.

30 Respect for the Principles of National Sovereignty and Non-Interference in Internal Affairs of a State in Their Electoral Processes, Resoluções da Assembleia Geral A/RES/44/147 (15 de dezembro 1989); A/RES/45/151 (18 Dezembro1990); A/RES/46/130 (17 December 1991); *Gill* (fn. 19), p. 223.

31 The Telegraph, Ukraine crisis proves cyber conflict is a reality of modern warfare (19 de abril 2014), disponível em: http://www.telegraph.co.uk/technology/internet-security/10770275/Ukraine-crisis-proves-cyber-conflict-is-a-reality-of-modern-warfare.html., última entrada: 10 de fevereiro 2015.

Significa isso, então, que essas atividades cibernéticas não são regulamentadas pela lei internacional de forma alguma? Se considerarmos a noção de igual soberania entre os Estados como o princípio subjacente à ordem legal internacional, esse resultado parece insatisfatório; particularmente quando se leva em conta o impacto adverso que a obtenção de dados sensíveis relacionados às capacidades militares ou econômicas de outro Estado pode ter na segurança nacional (em um sentido amplo) do primeiro.[32] O papel e a importância do princípio de soberania dos Estados nesse contexto vão ser discutidos no próximo parágrafo.

RESPEITO À SOBERANIA DE UMA NAÇÃO ESTRANGEIRA

A soberania dos Estados é, por um lado, o princípio subjacente mais importante da lei internacional. Por outro lado, porém, é também o mais 'obscuro'. O conceito é frequentemente usado com propósitos argumentativos por autoridades governamentais e por tribunais sem que o escopo nem o conteúdo exato do princípio estejam definidos. Para que um ato internacional de responsabilidade de um Estado seja considerado arbitrário, uma obrigação, ou seja, uma regra específica da lei internacional, precisa ser desrespeitada.[33] Portanto, é necessário que se determinem as regras precisas que derivam do princípio de soberania da nação.

A soberania dos Estados sob a lei internacional geralmente é entendida como referência à dimensão territorial, ou seja, a integridade territorial de um país. Além da inviolabilidade das fronteiras nacionais, o Estado tem o direito exclusivo de prescrever e aplicar leis[34] e regulamentar a entrada e o trânsito por seu território. Poder-se-ia pressupor que a soberania não é interessante do ponto-de-vista cibernético, considerando-se que as redes e as atividades virtuais em geral não são interrompidas nas fronteiras territoriais. No entanto, o espaço cibernético não

32 Sobre a relevância da espionagem virtual para a segurança nacional, ver *Ziolkowski, Katharina*, Peacetime Cyber Espionage – New Tendencies in Public International Law, em: Ziolkowski, Katharina (ed.), Peacetime Regime For State Activities in Cyberspace (2013), p. 425-464, 447-450.

33 Art. 2 International Law Commission (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Act, ILC Yearbook 2001, Vol. II, part 2 (doravante: ILC Articles on State Responsibility), p. 26-30; *Gill* (fn. 19), p. 226.

34 A Jurisdição de Estado não se restring ao seu território (solo, mar territorial e o espaço aéreo sobrejacente). Um Estado tem jurisdição sobre seus cidadãos no exterior, sobre aviões e navios registrados e sobre atividades extraterritoriais que ameaçam os interesses do governo central. A aplicação da lei se restringe ao território do país.

pode ser entendido como um domínio comum, livre de soberania.[35] Os Estados têm reafirmado a jurisdição sobre atividades cibernéticas trans-fronteiriças, como os casos em tribunais nacionais e internacionais têm demonstrado.[36] Além disso, os componentes físicos do ciberespaço, por exemplo os servidores, se estiverem localizados no território de um Estado, estão claramente sujeitos à jurisdição do Estado em questão.

Em relação às operações cibernéticas, pode-se dizer que violam a soberania de um Estado quando há um 'efeito físico perceptível'.[37] A lei internacional atual ainda não conseguiu esclarecer se esses efeitos precisam alcançar certo grau de severidade.[38] A necessidade de um certo patamar de gravidade parece algo razoável, considerando-se que a lei internacional não protege um Estado de qualquer impacto negativo que Estados estrangeiros possam ocasionar em seu território. Em um sistema legal de soberanias iguais, a soberania não pode ser absoluta.

Quanto à mera intrusão em uma rede, monitoramento de dados ou manipulação, argumenta-se que a interferência em uma infraestrutura virtual localizada em outro país pode ser equiparada ao exercício de jurisdição em um Estado estrangeiro, o que constituiria uma violação da soberania territorial.[39] Esta interpretação parece convincente na medida em que leva ao tratamento igualitário de dois casos que parecem comparáveis. Por que deveria fazer diferença se um Estado agente está no território de um país estrangeiro, conecta um pen drive e copia dados ou se ele obtém os mesmos dados por meio de *hacking* não autorizado de um computador em cima de uma mesa dentro do seu próprio país? 'O que há de tão especial no cibernético?' A atual lei internacional, porém, trata as duas situações acima de modo diferente. Em primeiro lugar, em função da interpretação (tradicional) do conceito de soberania quando se refere ao território físico de um país.[40] Em segundo lugar, devido ao fato de que espionagem, sem a presença física no território estrangeiro não está regulamentada pela lei internacional; não existe uma proibição geral, nem uma regra permissiva.[41] Alguns países, como os EUA, parecem ter uma visão ampla e consideram uma mera intrusão da suas redes

35 *Heintschel von Heinegg, Wolf,* Territorial Sovereignty and Neutrality in Cyber Space, 89 International Law Studies US Naval War College (2013), p. 123-156, 133.
36 Por exemplo: França LICRA v Yahoo (2000); ECJ, Google v Espanha (2014).
37 *Ziolkowski* (fn. 32), p. 485.
38 *Heintschel von Heinegg* (fn. 35), p. 129.
39 ibid. p. 128.
40 ver *Buchan* (fn. 6), p. 222-223.
41 *Ziolkowski,* (fn. 32), p. 445-446.

como uma violação da sua soberania.[42] Não existe, porém, nenhum acordo oficial dos Estados sobre este tópico.

Essas dúvidas deixam claro que os Estados, ao refinar e até mesmo reinterpretar o conceito de soberania, podem esclarecer como e até que ponto as operações cibernéticas estão regulamentadas pela lei internacional. O reverso da compreensão tradicional, estritamente territorial da soberania parece útil.[43] Curiosamente, a Alemanha se refere a 'soberania tecnológica' (sem nenhum esclarecimento adicional) na sua Estratégia de Segurança Cibernética.[44] De acordo com o Plano de Ação do Canadá para a Estratégia de Segurança Cibernética, 'resguardar de modo efetivo os sistemas [do governo] e os dados contidos neles, é […] um assunto de segurança nacional e soberania.'[45] Cabe aos Estados proporcionar padrões internacionais claros para as operações cibernéticas e suas implicações na soberania das nações.

O REGIME DE TEMPOS DE GUERRA

■ Embora muitas operações cibernéticas que buscam exercer pressão política e disseminar propaganda sejam ilegais em tempos de paz, essas operações frequentemente estarão em conformidade com a lei internacional durante tempos de guerra. O fato não surpreende, se considerarmos os diferentes objetivos que o *ius ad bellum* e o *ius in bello* perseguem. O primeiro pretende possibilitar a coexistência pacífica dos Estados, enquanto o segundo se aplica quando os países estão em 'guerra' e usam força militar uns contra os outros. O *ius in bello* ou

42 The President of the United States of America, International Strategy for Cyberspace -Prosperity, Security, and Openness in a Networked World (Maio de 2011), p.12 ff, disponível em: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 5.Fev. 2015; *Heintschel von Heinegg,* (fn. 35), p. 129; *Ziolkowski* (fn. 32), p. 459, fn. 193.

43 *Joyner, Christopher/Lotrionte, Catherine*, Information Warfare as International Coercion: Elements of a legal Framework, 12 European Journal of International Law (2001), p. 825-865, 843-845; see also *Buchan* (fn. 6), p. 222-223; stressing the potential need for reinterpretation of principles under international law with regard to cyber operations: *Heintschel von Heinegg* (fn. 35), p. 127.

44 German Ministry of Internal Affairs, Cyber-Sicherheitsstrategie für Deutschland (February 2011) p. 12, available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, last vistited: 5 February 2015.

45 Canada's Action Plan on Cyber Security Strategy (2010-2015), p. 5, available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx, last vistited: 5 February 2015.

Lei Internacional de Conflito Armado (LOAC em inglês) não regulamenta se e quando a força pode ser usada, mas estipula como pode ser usada, tentando limitar as calamidades da guerra[46] enquanto permite o combate armado efetivo. Em relação às operações virtuais durante um conflito armado, a noção de 'ataque' no Artigo 49 do Primeiro Protocolo Adicional das Convenções de Genebra (API) é de particular importância: desencadeia a aplicação dos princípios centrais e regras da LOAC no que diz respeito à proteção de civis e de objetos civis. Além disso, em um conflito armado, os ataques cibernéticos podem ser usados para fins de distração, possibilitando ataques armados convencionais.

ACIONANDO A PROTEÇÃO – DEFINIÇÃO DO ATAQUE

■ Um dos princípios cardinais da LOAC é o princípio da distinção, que obriga os Estados a distinguir entre objetivos civis e militares. Além disso, a LOAC estabelece regras específicas para proteger a população civil, como a proibição de atacar objetivos indispensáveis à sobrevivência da população civil.[47] Atos hostis durante um conflito armado estão sujeitos apenas a estas regras, se constituem um ataque segundo a definição que está no Artigo 49 API, por exemplo, um ato de violência, tanto de ofensiva quanto de defesa. Para determinar se as operações cibernéticas se qualificam como um ato de violência, as consequências pretendidas e as reais devem ser comparáveis às consequências de um ataque com meios de guerra convencionais.[48] Afinal de contas, as regras em questão pretendem proteger civis dos efeitos generalizados das hostilidades (tanto quanto o permitem as necessidades militares), então não pode fazer diferença se meios convencionais de guerra ou operações cibernéticas são usadas, se levam exatamente ao mesmo resultado.[49] Fica portanto aberto o debate sobre que efeitos um ato precisa ter para ser considerado um ataque. Claramente, (mais uma vez) operações cibernéticas que previsivelmente ou diretamente tenham como resultado morte ou lesão de pes-

46 Preâmbulo da Declaração de São Petersburgo (1868).

47 Art. 54 (2) API.

48 *Turns, David*, Cyber Warfare and the Concept of Attack under International Humanitarian Law, em: Saxon, Dan (ed.), International Humanitarian Law and the Changing Technology of War, 41 International Humanitarian Law Series (2013), p. 209-227, 225-226; *Schmitt, Michael*, Cyber Operations and the Jus In Bello, 41 Israel Yearbook on Human Rights (2011), p. 113-135, 118-120.

49 Uma justificativa convincente e detalhada desta abordagem e sua inerência em LOAC, *Schmitt,* ibid. p. 118-119.

soas ou em danos materiais[50] de objetivos constituem ataques segundo o Artigo 49 API.[51] A questão particularmente interessante aqui é o nível de imediatismo e objetividade que as consequências precisam ter para serem relevantes para a determinação da existência de um ataque. Sob a lei atual, os efeitos secundários, mesmo que sejam previsíveis até um certo ponto, e consequências de longo prazo, não são incluídos no teste. Por exemplo, as consequências de uma interrupção prolongada do fornecimento de eletricidade, como o impedimento de produção de comida e de armazenamento de comida, não são levados em conta, embora possam – em casos extremos -- acarretar risco de vida. Realmente, o objetivo da LOAC não é proteger a população civil de qualquer inconveniência durante conflitos armados.[52] No entanto, o autor não está convencido de que uma abordagem mais inclusiva (*de lege ferenda*), contradiga o objetivo principal e a praticabilidade da LOAC.[53] É inegável que atos que não têm potencial de risco de vida e não têm efeitos posteriores observáveis no mundo real, para além de espalhar o medo e o horror, como a mera desconfiguração de websites ou manipulação de dados ou comunicações, deveriam ser excluídos. No entanto, a privação de eletricidade ou água por um período mais prolongado, tem previsivelmente consequências humanitárias calamitosas.[54] Outrossim, como o conceito de ataque precisa ser entendido dentro do contexto do objetivo das regras às quais se aplica – a proteção da população civil dos efeitos das hostilidades – os Estados deveriam adotar uma abordagem mais inclusiva.

Além disso, uma interpretação ampla de 'ataque' parece oportuna quando consideramos a importância de operações baseadas em efeito para a Lei (moderna) de seleção[55]. Ao contrário dos meios de guerra tradicionais, que se concentravam em enfraquecer progressivamente as forças militares dos oponentes, as operações baseadas em efeito são lançadas contra alvos em função dos efeitos

50 A interpretação de 'dano' é suscetível a controvérsia, para uma interpretação extensa: *Dörmann, Knut*, The Applicability of the Additional protocols to Computer Network Attacks: ICRC Viewpoint, em: Byström, Karin, 2004 International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law (2005), p. 139-153, 142-143; para uma interpretação estrita *Schmitt*, (fn. 48), p. 121.

51 *Schmitt*, ibid. p. 120.

52 ibid. p. 121.

53 Arguing a devaluation of the law and its objectives, *Turns*, (fn. 48), p. 227.

54 *Geiß, Robin*, War and Law in Cyberspace, American Society for International Law Proceedings 2010, p. 371-374, 373.

55 Em geral *Henderson, Ian*, The Contemporary Law of Targeting (2009), p.125-146; *Schmitt, Michael,* Targeting and Humanitarian Law: Current Issues, 80 International Law Studies, p. 151-194.

sistemáticos que a destruição ou interrupção desses alvos têm no comportamento do oponente. Isso 'pode levar à tentação de atacar alvos que não sejam de natureza militar'.[56] Além disso, na moderna arte de guerra objetivos de uso dual ou até mesmo objetivos civis são mais prováveis de serem atacados. Um entendimento amplo do conceito de ataque, desencadeando a aplicação das regras de proteção mencionadas acima, garantem uma proteção efetiva da população civil durante um conflito armado.

Além disso, um desvio para uma abordagem mais humanitária da definição de ataque não necessariamente diminuiria a efetividade ou praticabilidade da LOAC, porque a qualificação de um ato como um ataque não leva automaticamente à proibição. Se for dirigido contra um objeto militar, ou se os padrões de proporcionalidade forem seguidos, esses ataques são considerados legítimos.[57] Consequentemente, uma definição abrangente pode atender às realidades da guerra e permitir uma guerra efetiva.

OPERAÇÕES CIBERNÉTICAS QUE PERMITEM ATAQUES ARMADOS (ENGANO)

■ Operações cibernéticas militares frequentemente são usadas como uma preparação para medidas de apoio que possibilitam ataques armados (convencionais). Por exemplo, o bombardeio de uma central nuclear elétrica por Israel em 2007 teve o auxílio da perturbação do sistema de defesa aéreo sírio através de meios virtuais para possibilitar a entrada não detectada de aeronaves de combate em espaço aéreo sírio. Hoje, as regras quanto à trapaça na guerra, que valem independentemente da existência de um ataque,[58] são particularmente relevantes. A operação israelense citada acima precisa ser qualificada como uma estratagema de guerra permitida, que devem distinguir-se de atos de perfídia, proibidos. Atos pérfidos são caracterizados como atos que buscam despertar a confiança do oponente, para levá-lo a acreditar que existe uma situação em que estão sendo aplicadas as regras de proteção da LOAC, com a intenção de trair a confiança conquistada.

O espaço cibernético permite uma extensa gama de usos das operações enganosas. A origem da atividade cibernética pode ser facilmente dissimulada

56 *Dinniss* (fn. 12), p. 25.
57 ver *Geiß*, (fn. 54), p. 373.
58 Art. 37 API; *Roscini* (fn. 15), p. 217.

usando táticas como os *botnets*[59], por exemplo.[60] No contexto militar, a manipulação das comunicações das forças inimigas é altamente relevante. Pouco antes da invasão em 2003, os EUA *hackearam* o sistema de e-mails do Ministério de Defesa iraquiano 2003 e enviaram mensagens encorajando os funcionários iraquianos a largar as armas e reforçando a ideia de que os EUA pretendiam apenas tirar Saddam no poder e não tinha intenção de prejudicar as forças armadas locais.[61] Aqui, o conteúdo da mensagem é o critério crucial para delimitar a fronteira entre perfídia e estratagemas de guerra. As mensagens para os funcionários iraquianos são estratagemas legítimos, já que não implicavam em estar em conformidade com as regras protetoras sob a LOAC. Em comparação, operações cibernéticas que, por exemplo, fingem ter status civil ou fingem a rendição do inimigo, seriam ilegais, desde que incluam outros requisitos da proibição ou perfídia. Não apenas é necessário demonstrar a busca de confiança, mas também a intenção de traí-la. Além disso, o ato pérfido precisa ter como consequência a captura, a morte ou a lesão de uma pessoa. Dado o estreito escopo de interpretação da aplicação da proibição ou da perfídia, as regras que definem o uso impróprio dos emblemas reconhecidos no Artigo 38 API parecem ter maior relevância prática.

O último proíbe o uso inadequado dos sinais de proteção e afirma que endereços de domínio como 'icrc.org', desde que essa ideia seja aprovada pela prática futura do Estado, estão englobados na proibição.[62] Realmente, endereços de domínio em determinados níveis 'mais baixos' são ativos que podem ser obtidos no mercado livre e portanto mudam seus usuários com frequência. No entanto, em função da governança do ICANN – Corporação da Internet para Atribuição de Nomes e Números, especialmente os domínios de segundo nível sob os domínios genéricos do 1º nível, como por exemplo 'icrc.org', são atribuídos exclusivamente à instituição em questão e, portanto, funcionam como uma função de identificação comparável a emblemas.

---

59 Uma botnet é uma rede de computadores comprometidos, 'the bots', controlados remotamente por um intruso, o 'botherder', usado para conduzir operações ou crimes cibernéticos. Não há limite prático para o número de bots que pode ser 'recrutado'para entrar em uma botnet. *Schmitt* (fn. 10), Glossário, p. 257.

60 *Pool, Phillip*, 47 International Lawyer (2013), p. 299-323, 309; *Roscini* (fn. 15), p. 215;

61 *Gervais, Michael*, Cyber Attacks and the Laws of War, 30 Berkeley Journal of International Law (2012), p. 525-579, 547.

62 *Boothby, Bill*, Cyber Deception and Autonomous Attack – Is There a Legal Problem?, Podins, Karlis /Stinissen, Jan/Maybaum, Markus (eds.), 5th International Conference on Cyber Conflict (2013), p. 245-261, 256; *Dinniss* (fn. 12), p. 265.

E por último, assim como em tempos de paz, a compilação de informações por meios cibernéticos – espionagem cibernética – como preparação para atos hostis durante conflito armado também carece de um arcabouço regulatório. Não existe nenhuma proibição de espionagem e a LOAC aborda a espionagem exclusivamente em relação à presença física do espião em território controlado pelo oponente.[63]

CONCLUSÃO

Obrigações dos Estados quanto à Segurança Cibernética

■ Como foi definida anteriormente aqui, a soberania igualitária é o princípio subjacente da lei internacional. Assim, a soberania de uma nação só pode chegar até onde a soberania de outro país não seja infringida. E, principalmente, a lei internacional também fornece obrigações positivas dos Estados para protegerem mutuamente as respectivas soberanias. O princípio da prevenção é particularmente interessante no âmbito do espaço cibernético.

De acordo com o princípio da prevenção, 'cada Estado tem a obrigação de não deixar, intencionalmente, que seu território seja usado para atos contrários aos direitos de outros Estados'[64]. Além disso, um Estado precisa tomar todas as medidas necessárias disponíveis para interromper operações virtuais em curso contra uma nação estrangeira originadas em seu território, a partir do momento em que o país fique ciente dessas operações adversas ou onde uma situação impõe esse conhecimento. No entanto, essa obrigação se aplica apenas às operações virtuais que causem prejuízos significativos em outro Estado.[65] Aqui, mais uma vez não fica claro se o prejuízo não perceptível no mundo real, como o monitoramento ou manipulação de dados, está incluído ou não.

Mas os países também são obrigados a adotar medidas para impedir que uma infraestrutura cibernética em seus territórios sejam usadas para ataques cibernéticos que causem prejuízos significativos a outro país. Essas medidas podem ser de

63 Art. 46 API , sobre o status de prisioneiro de guerra para espiões.

64 ICJ, The Corfu Channel Case, (United Kingdom v Albania), Merits, Judgement of 9 April 1949, ICJ Reports 1949, p. 4, 22.

65 Ver Trail Smelter Arbitration (United States v Canada) (1938/1941), Reports of International Arbitral Awards, Vol. III p. 1905-1982, p.1965; ICJ, Case concerning Pulp Mills on the River Uruguay (Argentina v Uruguay), Judgement of 10 April 2010, ICJ Report 2010, p. 14, para. 101; ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities (2001), ILC Yearbook 2001, Vol. 2, Part 2, p. 148-170, Art 1.

natureza regulatória, legal, administrativa, política ou técnica.[66] Por exemplo, a adoção de leis criminais e o estabelecimento de mecanismos de monitoramento são algumas possibilidades. É importante o fato de que as nações precisam se certificar de que essas medidas estejam em concordância com as obrigações de direitos humanos sob a lei internacional ou nacional, como o direito à privacidade, liberdade de expressão e de informação. E a extensão até onde um Estado é obrigado a adotar medidas preventivas permanece em aberto. Como a obrigação está restrita às medidas disponíveis para o país em questão e as capacidades tecnológicas dos países diferem, o padrão vai variar de acordo com isso. Com frequência debate-se se há uma obrigação de maior alcance da *'due diligence'* dos Estados para preservarem a segurança cibernética.[67] Podem ser estabelecidos paralelos para o princípio da precaução, desenvolvido na área da lei internacional ambiental. De acordo com este princípio, os Estados ainda precisam adotar medidas preventivas, mesmo que não exista ainda uma certeza científica em relação aos potenciais efeitos adversos de uma determinada atividade para o meio ambiente.[68] 'Se traduzirmos' o conceito para a esfera virtual, os Estados não apenas seriam obrigados a impedir prejuízos significativos, mas também seriam, de modo geral, solicitados a identificar potenciais ameaças à segurança cibernética e adotar medidas de prevenção.[69] O enfoque preventivo, no entanto, está sujeito a controvérsias quanto à sua natureza, sua base normativa e seu conteúdo exato.[70] Portanto, ser parte do direito consuetudinário é questionável. Mesmo enfatizando o alto potencial que esse enfoque preventivo possa ter para a regulamentação das atividades cibernéticas no futuro,[71] não há

66 Para exemplos dessas medidas, ver *Ziolkowski* (fn. 15), p. 169.

67 *Heintschel von Heinegg*, *Wolf,* Legal Implications of Territorial Sovereignty in Cyberspace, in: Czosseck, Christian/ Ottis, Rain/Ziolkowski, Katharina (eds.), 4th International Conference on Cyber Conflict (2012), p. 7-19, 17-18.

68 Por exemplo

: Principle 15 Rio Declaration (1992), Art. 3.3 UN Framework Convention on Climate Change (1992), Preamble of the Convention on Bio Diversity (1992), Art 1 Stockholm Convention of Persistent Organic Polluters (2001).

69 *Marauhn*, *Thilo,* Customary Rules of International Environmental Law - Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?, em: Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace (2013), p. 465-484, 475-476

70 Com relação à natureza, não está claro ainda se a precaução é um princípio ou apenas um enfoque. Além disso, ainda está em aberto a questão sobre se é um princípio de direito consuetudinário ou um princípio geral dentro do significado do Artigo 38 (1)(c) do Estatuto. Em relação ao conteúdo, se debate se leva a uma mudança do ônus da obra ou se é uma obrigação stricto sensu, *Dupuy, Pierre-Marie/ Viñuales, Jorge E.*, International Environmental Law: A Modern Introduction (publicado em Abril 2015), capítulo 3.

71 *Marauhn,* (fn. 69), p. 475.

evidências suficientes de que a segurança virtual internacional seja (já) considerada um interesse jurídico da comunidade internacional como tal, como acontece com a preservação do meio ambiente. As diferentes iniciativas (políticas), como as resoluções da Assembleia Geral da ONU,[72] em relação à segurança cibernética demonstram que essa visão está evoluindo. Porém, pressupor que há um princípio operando normativamente que obrigará os Estados a proteger a segurança cibernética internacional como tal, parece algo prematuro.

No entanto, o princípio da prevenção obriga os países a adotarem medidas disponíveis para impedir prejuízos significativos no território de outro Estado causados por operações cibernéticas geradas a partir de infraestrutura dentro do seu território. Outrossim, os Estados têm deveres processuais, por exemplo, informar outro país quando tiver conhecimento de atividades cibernéticas sendo iniciadas em seu território, realizar avaliações de impacto e cooperar com o país em questão.

Contramedidas eficazes contra Operações Cibernéticas

■ Se as violações da lei internacional forem cometidas, um conjunto de regras internacionais secundárias, – a lei de responsabilidade de Estado – fornece contramedidas ao país ofendido, que deverão induzir o 'Estado-perpetrador' a retornar ao comportamento legalizado. Como já se mencionou aqui, o chamado ato iníquo deve ser uma violação de uma regra específica da lei internacional. Além disso, os organismos de um Estado precisam ter cometido o ato ou ele precisa ser atribuído a um Estado.[73] A lei de responsabilidade de Estado determina os critérios para uma atribuição semelhante e fornece os requisitos e limites das medidas defensivas.

No ambiente acadêmico, já foi enfatizado que os critérios de atribuição, sob a lei internacional atual, foram elaborados de modo muito estreito e portanto não estão adequados à esfera virtual.[74] Realmente, a maior parte dos incidentes

72 Por exemplo: Creation of a global culture of cybersecurity, UN General Assembly resolution 57/239 (20 Dec 2002); Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, UN General Assembly resolution 64/211 (21 Dezembro de2009).

73 Para os critérios de atribuições de atos (de atores não-Estado) para um Estado, ver Art. 4-11 ILC Articles on State Responsibility (fn. 33).

74 *Heintschel von Heinegg, Wolf,* Cyberspace- Ein völkerrechtliches Niemandsland, em: Schmidt-Radefeldt, Roman/Meissler, Christine (eds.), Automatisierung und Digitalisierung des Krieges, p. 159-174, 172.

cibernéticos na prática não podem ser atribuídos a um Estado sem que haja sombra de dúvida. O ciberespaço proporciona uma extensa gama de possibilidades para tornar anônima ou ocultar a autêntica fonte das atividades cibernéticas. No entanto, até agora, os Estados não concordaram em um padrão diferente, especial de atribuição para atividades cibernéticas maliciosas. De modo geral, o problema de atribuição parece ter uma natureza mais técnica do que legal.

Mesmo que seja possível identificar o Estado responsável, medidas defensivas sob a lei de responsabilidade de Estado não necessariamente constituem ferramentas efetivas para repelir operações cibernéticas porque é preciso também cumprir com os requisitos de necessidade e proporcionalidade.[75] As investigações de incidentes cibernéticos frequentemente continuam por longo tempo após a cessação da atividade cibernética ilegal. No entanto, depois que o estado de legalidade é restaurado, as contramedidas, que perseguem o único objetivo de induzir o comportamento legal, e não contemplam punição, talvez não cumpram com o padrão exigido de necessidade sob a lei internacional.[76] Dado esse escopo restrito da aplicação (temporária) das contramedidas e os problemas relacionados com a atribuição de atividades cibernéticas a um país, uma abordagem mais preventiva da segurança cibernética parece oportuna. Os Estados precisam especificar suas obrigações sob o princípio da prevenção e desenvolver fóruns e procedimentos para possibilidade a cooperação.

Necessidade de Cooperação no desenvolvimento de padrões aceitos para a Segurança Cibernética

■ A análise das implicações das operações cibernéticas sob a lei internacional (feita acima) deixa claro que existe a necessidade de esclarecimentos adicionais ou até mesmo da reinterpretação dos princípios e regras legais. Os princípios subjacentes da ordem legal internacional, como o princípio da não-intervenção, o conceito de soberania de Estado e o princípio da prevenção geralmente são aplicados às operações virtuais, mas muitas incertezas ainda permanecem. Para fechar essas "brechas" as nações precisam se reunir e chegar a um acordo sobre os entendimentos comuns dos princípios fundamentais da lei internacional, que a longo prazo poderia possibilitar a formulação de obrigações específicas dos Estados no tópico segurança cibernética.

75 Art. 51-52 ILC Articles on State Responsibility (fn. 33).
76 Art. 49 (1) and Art. 52 (3) ILC Articles on State Responsibility (fn. 33).

A ênfase deveria estar em determinar as medidas que um Estado deve ser solicitado a adotar para impedir atividades cibernéticas adversas originadas de infraestrutura virtual sobre o seu controle. Afinal, o escopo e a extensão das obrigações sobre o princípio da prevenção não podem variar segundo o critério individual de cada Estado. Os países precisam chegar a um acordo não apenas sobre um padrão mínimo, mas sim preparar um catálogo de medidas preventivas. Uma revisão periódica desse catálogo pelos Estados permitiria que se incluíssem respostas a novos desenvolvimentos tecnológicos. Adicionalmente, as diferentes capacidades tecnológicas dos Estados deverão ser levadas em consideração. Seguindo os exemplos de tratados de leis meio-ambientais, nos quais os países em desenvolvimento são submetidos a obrigações menos estritas,[77] os Estados poderiam ser submetidos a diferentes padrões de acordo com seu *know-how* tecnológico. Em linhas gerais, se deve oferecer suporte aos países com menos capacidade tecnológica.

No entanto, uma regulamentação assim tão detalhada, em forma de um tratado de segurança cibernética, parece muito distante da realidade. Os Estados relutam em compartilhar suas conquistas tecnológicas relacionadas com a esfera virtual, em função dos potenciais benefícios de ataques cibernéticos durante conflitos armados e em ações de política de dissuasão.

Além disso, os países não compartilham um entendimento comum dos temas mais básicos e dos conceitos legais. Será que a segurança cibernética é um interesse legal em comum dos Estados ou apenas um objetivo político? Como a segurança virtual se relaciona com a soberania? A soberania deveria ser entendida para além da questão meramente territorial? Esclarecimentos adicionais também são necessários no que diz respeito à relação entre direitos humanos e segurança cibernética, como a liberdade de informação e de expressão e o direito à privacidade. A Rússia, por exemplo, tem uma interpretação peculiar de 'segurança de informação', que inclui o direito de um Estado à censura, o que aparentemente contradiz os padrões de direitos humanos nas democracias ocidentais.[78] Considerando as extensa competências da ASN no quesito monitoramento de dados, os EUA parecem ser da opinião de que as preocupações com a segurança (virtual) justificariam amplas restrições do direito à privacidade, o que não se encaixa nos padrões de proteção garantidos em outros países.

77 Por exemplo: o Protocolo de Kioto para a Convenção do Marco das Nações Unidas para Mudanças Climáticas (1998) ou o Protocolo Montreal para Substâncias que afetam a Camada de Ozônio (1987).

78 *Schaller, Christian*, Internationale Sicherheit und Völkerrecht im Cyberspace, 18. Studie der Stiftung Wissenschaft und Politik (2014), p. 28.

Todas as inconclusões em relação à aplicação das normas internacionais e as diferentes interpretações dos conceitos legais mais amplos expõem a necessidade urgente de que se intensifiquem as consultas e a cooperação entre os Estados no tema de segurança cibernética. O trabalho da Assembleia Geral da ONU em relação ao assunto é um ponto de partida proveitoso, como bem ilustra a adoção de uma resolução 'O direito à privacidade na era digital[79] em 18 de dezembro de 2014, introduzida pelo Brasil e pela Alemanha.

Julia Dornsbusch é Pesquisadora Assistente do Institute for International Peace and Security Law, da Universidade de Colônia.

79 Resolução da Assembleia Geral das Nações Unidas A/RES/69/166 (18 de Dezembro 2014).