**Ataque cibernético como *casus belli*? Impressões sobre a ambiguidade do conceito de guerra cibernética**

Marcus Vinícius Xavier de Oliveira (UNIR)

Gills Vilar-Lopes (UNIFA)

**1 Introdução**

 O “Glossário de Segurança da Informação”, recém-lançado pelo Gabinete de Segurança Institucional da Presidência da República (GSI), assevera, *in verbis*, que ataque (cibernético) é “[...]ação que constitui uma tentativa *deliberada e não autorizada* para acessar/manipular informações, ou tornar um sistema inacessível, não integro, ou indisponível” (BRASIL, 2019, grifo nosso). Mas em que medida tal ataque pode tomar a proporção mais extremada das relações sociais e vir a se constituir, ele mesmo, em um *casus belli*?

No presente *paper* a nossa intenção é a de tentar, brevemente, compreender, desde uma perspectiva interdisciplinar, a ambiguidade conceitual e normativa que giza o conceito de ataque cibernético e aferir, à luz do Direito Internacional contemporâneo – Sistema da Carta –, se ele se ajusta ao conceito de agressão previsto no capítulo VII da Carta das Nações Unidas.

Esse problema se mostra importante pelo menos por dois motivos, a saber: a) existe uma clara lacuna normativa no Direito Internacional acerca do estatuto do ataque cibernético; e b) dessa lacuna, surge a possibilidade de as decisões políticas sobre *casus belli* elevar o atributo da politização estendida que caracteriza o Direito Internacional (PASTOR RIDRUEJO, 2014, p. 48-49). Esse estado de coisas se prostra com claras consequências ofensivas aos princípios da segurança e da paz internacionais tutelados pelo crime de agressão.

Formalmente, a metodologia que encoraja as análises aqui depreendidas apoia-se no estilo qualitativo de pesquisa. Já os métodos decorrentes dessa afiliação dizem respeito à pesquisa bibliográfica, em que pese a interpretação, sobretudo, de fontes primárias – como leis, normas e tratados internacionais – e da recente casuística internacional, que tem eco nas palavras do atual e do último presidente estadunidense e no documento recém-lançado pelo Governo da França.

Diante dessa problemática, o presente trabalho se divide em três partes principais. Na primeira delas, encoraja-se o diálogo entre Direito Internacional e Relações Internacionais. Na segunda, esboça-se como a imprecisão do conceito de guerra encontra eco na epistemologia jurídica e política. E, finalmente, na última parte, avalia-se o ataque cibernético enquanto *casus belli*.

**2** **Relações entre Direito Internacional e Relações Internacionais**

Direito Internacional e Relações Internacionais se constituem em duas disciplinas caracterizadas, desde o seu interior, por aquilo que se pode denominar como “local de encontro” das diversas disciplinas que as conformam e têm por objeto de estudo as relações que transcendem as fronteiras nacionais (BRAILLARD, 1990, p. 82-83), seja internacionais em sentido estrito (relações entre sujeitos do Direito Internacional, em particular os Estados), seja transnacionais (relações entre atores internacionais no contexto das diversas esferas normativas que caracterizam esse campo) (PECEQUILO, 2004, p. 15).

 Para Wengler (1964, p. 1-3), os problemas mais comezinhos que concernem ao Direito Internacional – *e.g.* a relação entre Estado e normas internacionais, ou entre ordenamentos nacionais e Direito Internacional – somente podem ser respondidos a partir de uma perspectiva dialógica entre Direito Internacional e Relações Internacionais. Isso porque os problemas jurídicos internacionais são, antes de qualquer coisa, problemas da política e da sociologia internacionais, não bastando, nesse sentido, a insistência em permanecer na “compulsão legal” e na pureza “técnico-normativa” destituídas do contexto político-sociológico em que as normas internacionais são produzidas e aplicadas, profundamente afetadas pelo elemento político por excelência de qualquer decisão: a preservação do próprio interesse.

 Nesse sentido, mais do que relevante, é essencial que haja um diálogo interdisciplinar entre os campos de estudo, sob pena de ocorrer tanto um empobrecimento da análise produzida como um *gap* na resposta dada ao problema, cujas consequências, no âmbito das relações entre Estados, serão prejudiciais, se não catastróficas.

 Conquanto seja essencial o diálogo interdisciplinar, as disciplinas devem guardar, equilibradamente, suas respectivas autonomias, vez que o Direito, enquanto campo do dever ser, vale e obriga a seus destinatários independentemente de suas adesões morais e/ou políticas acerca das consequências da aplicação da norma e sua sanção, consistindo nisso o atributo da imperatividade. Defende-se, portanto, diálogo, não monólogo, sublimação ou supressão de discursos.

 O problema proposto nesse *paper* se constitui em um tópico privilegiado para se comprovar tanto a necessidade desse diálogo como a de se conservar, com grau mínimo, a autonomia disciplinar, posto envolver, por assim dizer, tema e problema fundamental do Sistema da Carta: a limitação, quase absoluta, do *jus ad bellum*, bem como a formação do *jus contra bellum* no qual vige o *jus in bellum* e o *jus post bellum*, especialmente este último nos campos da responsabilidade internacional dos Estados e dos indivíduos no âmbito Direito Penal Internacional.

 Ora, sendo o *jus ad bellum* subsistente na forma da legítima defesa, individual ou coletiva, perquirir sobre o estatuto jurídico de um ataque cibernético no contexto da lacuna é tarefa pertinente e necessária à chamada Sociedade da Informação (CASTELLS, 1999, *passim*).

**3 Usos e “maus” usos da palavra guerra**

 Mais do que uma questão ontológica, o estudo da guerra perpassa também pela cratologia – “estudo científico do poder e de suas dinâmicas atreladas à área internacional” (CASTRO, 2012, p. 21) – e pelo estudo sociológico da linguagem.

Sampaio Dória – um dos mais destacados constitucionalistas brasileiros pós-Segunda Guerra Mundial e com grande atuação no período que antecedeu a Constituição Federal de 1988 (CF88) – levantou um problema importante acerca da relação entre Direito e linguagem. Para ele, os “[...]homens dissentem mais em virtude da equivocidade da linguagem que usem, do que pelas concepções que tenham das realidades em si[...]”, pelo que o “[...]conhecimento exato dos fenômenos sociais fará mais pela ordem jurídica e pela paz, do que o temor das forças motorizadas[...]” (DÓRIA, 1946, p. 3).

Heidegger, em sua *linguist turn*, já havia afirmado a relação indissociável entre comunidade humana e linguagem, haja vista que o

[...]homem fala. Falamos quando acordados e em sonho. Falamos continuamente. Falamos mesmo quando não deixamos soar nenhuma palavra. [...]A linguagem pertence, em todo caso, à vizinhança mais próxima do humano. A linguagem encontra-se por toda parte. (HEIDEGGER, 2003, p. 7).

 Sendo o direito essencialmente um fenômeno inerente à espécie humana, assim como a natureza desta se manifesta pela linguagem, o mesmo se dá com relação àquela, seja qual forma se adote para tal. Em síntese: a) o direito “é” linguagem, e, onde esta vige, não se busca a “essência” das coisas, mas o “uso” social das palavras, e b) sendo o “uso” linguístico o referencial que se toma para a compreensão e a fixação de normas para o agir humano – a essência é uma consequência do uso linguístico, e não o seu suposto (WITTGENSTEIN, 1922, p. 93-99), o traço mais próprio da linguagem humana é, em nível semântico, a ambiguidade, e que, levado a seu extremo, pode desaguar na inexpressividade, dita anfibologia, caracterizada pela impossibilidade de predicação e de comunicação. Assim, no presente *paper* compreender, a partir de traços mínimos, o que seja, em sentido jurídico, a guerra é condição necessária para, de um lado, afastar a ambiguidade conceitual, bem como se evitar a anfibologia.

 Para o Direito Internacional, *ex vi* dos artigos 39 e 51 da Carta da Organização das Nações Unidas (ONU), em sentido estrito, “guerra” identifica uma agressão mediante ataque armado contra um Estado. Embora a Carta não identifique o agente ativo do ataque armado – se Estado ou outra entidade –, tanto no contexto do Direito Internacional moderno como no contemporâneo, firmou-se a ideia de que ele *deve ser* um Estado. Assim, por exemplo, Rousseau (2007) afirma que:

Não é, pois, a guerra uma relação de homem para homem, mas uma relação de Estado para Estado, na qual os particulares apenas acidentalmente são inimigos [...] como soldados [...] cada Estado não pode ter como inimigo senão outro Estado[...].

 O filósofo suíço evidencia essa máxima, no contexto do Sistema de Vestfália, bem como o faz Oppenheim no contexto da Carta: guerra é “[...]a contenda entre dois ou mais Estados por meio de suas forças armadas, com o propósito de sobrepor um ao outro e impor condições de paz aprazíveis ao vitorioso” (*apud* Dinstein, 2004, p. 5).

 Confirma esses conceitos doutrinários o fato de que os Elementos dos Crimes do Estatuto de Roma (ETPI) define, nesses mesmos termos, o crime de agressão, conforme o artigo 8 *bis*, ensejando, com isso, a persecução criminal dos autores de referido ilícito penal internacional nos termos do artigo 5º do ETPI.

 Em suma, guerra, em sentido técnico-jurídico, é o ataque armado de um Estado contra outro, pelo qual, por sua gravidade e escala, tenha posto em perigo a integridade territorial, a soberania e a independência política do sujeito passivo.

 Qualquer outro uso que se dê a essa palavra será, por definição, uma expressão metafórica para indicar a ocorrência entre dois os mais Estados de uma contenda qualquer – a exemplo da guerra comercial ou tecnológica entre os Estados Unidos da América (EUA) e a China em torno dos equilíbrios de suas balanças comerciais ou da hegemonia empresarial na exploração do 5G –, ou mesmo pelo emprego das forças armadas para o enfrentamento de problemas macrocriminais que ensejariam a cooperação penal e policial entre os Estados, e não de suas forças armadas – guerra às drogas ou guerra ao terror. Os resultados negativos da militarização desses conflitos, por se constituírem em desacordo com o sistema normativo internacional, são muito evidentes.

 Compreensível, entretanto, que as demais disciplinas, frente o grave impacto e a abrangência dos dissensos, use, mesmo que equivocadamente, essa expressão, cuja denotação mais evidente seria a de expressar a sua gravidade. Entretanto, o uso, *per se*, não transforma um conflito de interesses em um conflito armado, posto que, nos termos da Carta, os Estados têm a obrigação “[...]*to settle international disputes by peaceful means and to refrain from threat or use of the force, apply also to non-members states*” (KELSEN, 1951, p. 19).

 Partindo desse pressuposto estatal, seria o ataque cibernético um *casus belli*?

**4 A lacuna e sua supressão legal do ataque cibernético**

 A possibilidade de compreender um ataque cibernético como *casus belli* passa, pelo menos, por três pontos essenciais: 1) a compreensão do significado de espaço soberano; 2) a abrangência do conceito de interesse tutelável pela guerra; e 3) o próprio conceito de ataque cibernético. Da intepretação sistemática desses três elementos, extrai-se, à luz dos artigos 39 e 51 da Carta das Nações Unidas, uma resposta provisória, que é o objetivo deste texto.

 O conceito de espaço soberano, intrínseco ao de território, em Direito Internacional identifica “[...]o espaço no qual a ordem jurídica nacional se aplica, isto é, onde cada Estado exerce válida e permanentemente sua própria autoridade” (ACCIOLY, 2008, p. 157). A expressão espaço empregada por Accioly deve ser compreendida em sua dimensão plural, isto é, espaços, posto que fazem parte do território todas as dimensões em que o Estado, segundo o Direito Internacional, pode exercer a sua soberania: terra, ar, mar, rios etc., inclusive o cibernético ou eletromagnético (GOMES; CORDEIRO; PINHEIRO, 2016, p. 11).

 É fato, entretanto, que a possibilidade de atribuir aos Estados a pretensão de exercer domínio sobre o ciberespaço só se dá com o desenvolvimento tecnológico da rede de computadores, fechada ou interligada mundialmente, um vez que, consoante o Exército Brasileiro, esse espaço abrange “[...]a comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação” (EXÉRCITO BRASILEIRO, 2017, p. 18), cabendo ao Estado, via Forças Armadas, exercer o controle e a defesa de todos os âmbitos em que o Brasil, “[...]como nação soberana, necessita[r] de capacidade para se contrapor às ameaças externas, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no cenário internacional” (Idem, ibidem, p. 13).

Já para a Presidência da República, “[a] Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras” (BRASIL, 2010, p. 13).

 Sob esta perspectiva, compartilhada por todos os demais Estados, o ciberespaço é também onde o Estado pretende o exercício exclusivo de seus interesses inerentes às informações, conhecimento e armazenamentos, gerenciamento de sistemas de interesse geral e/ou sensíveis, de segurança e defesa etc. Nesse sentido, acompanhando as lições de Wengler (1964, p. 7, tradução nossa), pode-se afirmar que se trata de uma pretensão legítima, embora, em razão da lacuna normativa, não se possa atribuir, salvo em juízo meramente apriorístico, certeza a referidas pretensões, na medida em que “os interesses atuais e futuros podem precisar ser ponderados um em relação ao outro”.

 Desde esta perspectiva apriorística, não parece ser indubitável, nem sequer razoável, atribuir a qualquer ataque cibernético o estatuto de *casus belli*, mesmo que, como o faz o Exército Brasileiro, se considerem os diversos meios pelos quais se opera esse ataque como artefato cibernético, assim conceitua todo “[...]equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos [...]” (EXÉRCITO BRASILEIRO, 2017, p. 17).

 Em síntese, assim como somente se pode afirmar em nível metafórico que exista uma “guerra” comercial entre dois Estados, um equipamento ou sistema empregado em um ataque cibernético poderá ser apenas considerado como um artefato de guerra, e por extensão, desencadeador de *casus belli*.

 Se for certa a existência de uma lacuna em torno do conceito de ataque cibernético (UNCSTD, 2014, p. 21) e seu estatuto no campo da defesa e da segurança, ela não pode ser suprida respondendo afirmativamente à possibilidade de atribuir-lhe o estatuto de *casus belli*, mas, antes, em atenção ao princípio da solução pacífica dos conflitos, sustentar que os Estados deverão solver a controvérsia dentre os diversos meio pacíficos que o Direito Internacional contemporâneo lhes põe à disposição.

**Referências**

ACCIOLY, Hildebrando. **Tratado de Direito Internacional Público**. 3. ed. São Paulo: Quartier Latin, 2009. v. 2.

BRAILLARD, Phillipe. **Teorias das Relações Internacionais**. Lisboa: Fundação Calouste Gulbekian, 1990.

BRASIL. Ministério da Defesa. **Manual de Campanha**: Guerra Cibernética. Brasília, DF: Exército Brasileiro, 2017.

\_\_\_\_\_\_. Presidência da República. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da informação. Brasília, DF, Gabinete de Segurança Institucional, 2019.

\_\_\_\_\_\_. Presidência da República. **Livro verde**: segurança cibernética no Brasil. Brasília, DF: Gabinete de Segurança Institucional, 2010.

CASTELLS, Manuel. **A sociedade em rede**. 2. ed. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultura, 1).

CASTRO, Thales. Cratologia e Relações Internacionais: breves notas sobre os fundamentos e a contabilidade do poder na política entre as nações. **Cadernos de Relações Internacionais**, v. 3, n. 4, p. 20-40, 2012.

DINSTEIN, Yoram. **Guerra, agressão e legítima defesa**. 3. ed. Trad. Mauro Raposo de Mello. Baueri: Manole, 2004.

DÓRIA, A. Sampaio. **Curso de Direito Constitucional**. 2. ed. São Paulo: Cia Editora Nacional, 1946. t. 1.

GOMES, Mauro G. F. Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. A guerra cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). **Revista Militar de Ciência e Tecnologia**, v. 33, n. 2, p. 11-18, 2016.

HEIDEGGER, Martin. **A caminho da linguagem**. Petrópolis: Vozes, 2003.

KELSEN, Hans. **The Law of the United Nations**: a critical analysis of its fundamental problems. London: Stevens & Sons Limited, 1951.

PASTOR RIDRUEJO, José Antonio. **Curso de Derecho Internacional Público y Organizaciones Internacionales**. 18 ed. Madri: Tecnos, 2014.

PECEQUILO, Cristina Soreanu. **Introdução às relações internacionais**. Petrópolis: Vozes, 2004.

ROUSSEAU, Jean-Jacques. O contrato social. Trad. Rolando Roque da Silva. 2007. Disponível em: <http://www.dominiopublico.gov.br>. Acesso em: 20 set. 2019.

UNCSTD - UNITED NATIONS INTERSESSIONAL PANEL OF THE COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT. **The mapping of international Internet public policy issues**. Geneva: CSTD Secretariat, 2014. Disponível em: <http://unctad.org/meetings/en/SessionalDocuments/CSTD_2014_Mapping_Internet_en.pdf>. Acesso em: 3 out. 2019.

WENGLER, Wilhel. **Völkerrecht**. Berlin-Heildelberg: Springer-Verlag, 1964.

WITTGENSTEIN, Ludwig. **Tractatus logico-philosophicus**, Londres: Kegan Paul, Trench, Trubner & Co, 1922.