Cyberwar é uma Guerra? Perspectivas Acadêmicas sobre Conflitos Cibernéticos

Ana Carolina de Oliveira Assis

É comum em diversas áreas do conhecimento ocorrerem debates com argumentos e provas distintas. Com a cibernética não é diferente. Um dos principais debates na área gira em torno se o uso de ataques cibernéticos para alcançar objetivos individuais ou coletivos constitui de fato atos de guerra. No campo dos estudos sobre conflito, um artigo seminal que colocou em questionamento essa indagação foi "Cyber War Will Not Take Place" de Thomas Rid (2012). Em seu trabalho, o autor afirma que um ataque cibernético não pode ser considerado totalmente como um ato de guerra, e por consequência, não houve no passado, não existe no presente, nem ocorrerão guerras cibernéticas no futuro.

A afirmação de Rid gira em torno do fato que ataques cibernéticos não abarcam as características fundamentais de um ato de guerra descritas no conceito clássico de guerra de Clausewitz. Para o estrategista clássico alemão, as ações ofensivas ou defensivas para serem classificadas como atos de guerra deveriam obedecer a três premissas básicas: ter caráter violento (causar violência física e/ou letal), apresentar caráter instrumental (meios e fins definidos), e natureza política – ou seja, os atos devem ter um objetivo político e o perpetuador deve transmitir ao adversário suas intenções e vontades políticas (mesmo que de maneira não pública ou direta) (Clausewitz, 1832 apud RID, 2012).

Ao utilizar de fatos históricos, a exemplo da explosão do gasoduto na Sibéria em 1982, do ataque cibernético à Estônia (2007), Geórgia (2008), entre outros, o autor demonstra que os elementos basilares da guerra clausewitziana não estão presentes, o que torna o conceito de guerra no espaço cibernético mais metafórico do que descritivo. Seria possível afirmar apenas que os "atos de guerra cibernética" seriam meras ofensivas, e reduzidas a crimes cibernéticos – a exemplo de versões sofisticadas de espionagem, sabotagem e subversão (RID, 2012).

Próximo à essa perspectiva, Adam Liff (2012) publicou o artigo "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War". O autor foca na questão da dificuldade de ataques a redes de computadores com

objetivos políticos e/ou militares (definição do autor do que poderia ser guerra cibernética) serem usados no futuro como elementos coercitivos. Assim, devido aos obstáculos presentes na tradução de ataques cibernéticos para influência política, a probabilidade de ocorrência de guerra seria baixa - mesmo com a proliferação de capacidades cibernéticas e a diminuição dos custos de utilizarem esses meios (LIFF, 2012).

Essas publicações causaram um impacto significativo para agenda do debate sobre guerra cibernética e não demorou muito para outros pesquisadores responderem às afirmações dos autores. Como resposta a Rid, John Stone publicou o artigo "Cyber War Will Take Place!" no ano seguinte para demonstrar que a guerra cibernética é possível. Segundo o autor, o debate sobre os conflitos cibernéticos serem equivalentes à guerras é complexo devido às perspectivas individuais sobre teoria estratégica, como também à dificuldade de definir ao certo e de maneira única conceitos como letalidade, violência e força (STONE, 2013).

Para comprovar seus argumentos, o autor realiza uma revisão dos conceitos principais debatidos por Rid e extraídos da classificação da guerra por Clausewitz e conclui que atos de guerra não exigem reivindicação nem atribuição. Além disso, a violência, letalidade e força não estão necessariamente conectadas nos conflitos, ou seja, é possível a presença de um dos elementos e a ausência de outros em guerras – como, por exemplo, atos de guerra que envolvem força, mas, não necessariamente violência, caso no qual a guerra cibernética se encaixaria (Ibdem).

Na mesma edição do Journal of Strategic Studies que o artigo de Stone foi publicado, o debate sobre a guerra cibernética foi aprofundado por Timothy Junio (2013). O autor para contrariar o argumento que a guerra cibernética não é possível, utiliza de pressupostos teóricos de Relações Internacionais para demonstrar teoricamente a probabilidade desse evento ocorrer. A perspectiva escolhida pelo autor foi sobre as Explicações Racionalistas da Guerra e o problema agente-principal para avaliar como as atribuições da tecnologia afetam a probabilidade de guerra.

Tendo como base o pressuposto que agente e líderes apresentam incentivos e preferências distintas, o autor analisa os problemas na questão de Comando e Controle (C2) no setor. Assim, chega a conclusão que as operações cibernéticas são diferentes dos outros tipos de atividades realizadas pelos militares, porém, a guerra nesse domínio

é provável uma vez que: em primeiro lugar, as armas cibernéticas são menos letais, o que diminuiria os custos políticos para usá-las em comparação com outros armamentos; em segundo lugar, C2 fracos são condições necessárias na ocorrência de problemas entre agentes e líderes; além disso, o culto a ofensiva na arena cibernética, de países como Estados Unidos e China, é deixado de lado em favor da defesa cibernética, mas no caso de países com baixo controle civil sobre os militares pode ocorrer o oposto. Para ilustrar no sistema internacional um exemplo que une C2 fraco juntamente com o culto a ofensiva, o que favoreceria uma guerra cibernética, o autor aponta para o caso da Coreia do Norte (JUNIO, 2013).

Para enraizar os conflitos cibernéticos como fenômenos bélicos factíveis, Gary Mcgraw (2013) publicou "Cyber War is inevitable (unless we build security in)". O autor retoma também o trabalho de Rid para esclarecer que a guerra cibernética deve ter impacto físico (no mundo real), porém, o efeito cinético não precisa ser convertido em fatalidades de indivíduos, mas pode ocorrer danos à instalações e infraestrutura essencial dos Estados. Um ato de guerra ou ofensiva cibernética envolveria assim, a exploração, penetração e aproveitamento de softwares frágeis para comprometer sistemas de informação essenciais para as sociedades modernas (sistema de distribuição de energia, financeiro, transportes, etc). Consequentemente, decorrente da dependência humana para com esses sistemas, a guerra cibernética é inevitável.

Por fim, muitas questões teóricas e conceituais podem ser extraídas do debate ocorrido no Journal of Strategic Studies entre 2012 e 2013. Mesmo após seis anos, desde a ultima publicação, ainda não foi obtido consenso sobre a questão se a guerra cibernética é possível e constitui-se um novo domínio, ou se as capacidades utilizadas nesse meio são meras armas combinadas e/ou estratégicas de apoio à guerra dita tradicional (TEIXEIRA JÚNIOR, VILLAR-LOPES, FREITAS, 2017).

Referências

JUNIO, Timothy (2013), "How probable is cyberwar? Bringing IR Theory back in to the cyber conflict debate", Journal of Strategic Studies, vol. 36, nº 01.

Liff, Adam (2012), ‘Cyberwar: A New ‘‘Absolute Weapon’’? The Proliferation of Cyberwarfare Capabilities and Interstate War’, Journal of Strategic Studies 35/3, 401–28.

MCGRAW, Gary (2013), “Cyber War is inevitable (unless we build security in)”, Journal of Strategic Studies, vol. 36, nº 01.

RID, Thomas (2012), “Cyber War Will Not Take Place, Journal od Strategic Studies, Vol. 35, n 01

STONE, John (2013), “Cyber War Will Take Place!”. Journal of Strategic Studies. Vol. 36, nº 01.

TEIXEIRA JÚNIOR, Augusto; VILLAR-LOPES, Gills e FEITAS, Marco T. (2017), “As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica”. Revista Carta Internacional, vol. 12, nº 03.