**CIBERESPAÇO E SEGURANÇA CIBERNÉTICA:** Desafios e Ameaças na era da Informação.

Fernando Henrique Casalunga

O final da grande guerra que culminou na vitória dos aliados ocidentais sobre a ameaça totalitária deixou um grande legado à humanidade, o primeiro domínio artificial inteiramente criado pela ação humana denominado ciberespaço, ambiente anárquico que propeliu nossa sociedade à era da informação. Weiss (2018) define o ciberespaço “o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line [...] Mas o ciberespaço não é puramente virtual. Ele compreende os computadores que armazenam dados, além dos sistemas e infraestrutura que permitem que ele flua”.

Com a chegada do século vinte, a emergência de uma sociedade amplamente conectada ao ambiente virtual fez com que a importância deste domínio para os Estados contemporâneos se tornasse indiscutível e irrevogável, o fracasso na tarefa fulcral de proteger o fluxo do ciberespaço acarretaria problemas substanciais ao funcionamento do comércio, a troca confiável de informações e a estabilidade de infraestruturas críticas que poderiam levar nossa sociedade ao colapso.

Em vista disso, a comunidade acadêmica civil e militar tem se debruçado sobre o problema fundamental da segurança no ciberespaço, a fim de compreender os movimentos da agência no que concerne às estratégias, táticas e operações utilizadas pelos Estados contemporâneos para atuar no ciberespaço. Nesse sentido, Chocri (2012) compreende a segurança cibernética como “a capacidade de um Estado proteger a si e suas instituições contra ameaças, espionagem, sabotagem, crime e fraude, identificar roubo e outras interações e transações eletrônicas destrutivas”.

Na medida em que a comunidade científica buscar forjar chaves conceituais para abrir a caixa de pandora da segurança cibernética, novos desafios teóricos emergem, refletindo a complexidade analítica imposta pela emergência dinâmica e revolucionária do desafio cibernético (KELLO, 2013;2017; WEISS, 2018). Tais distinções analíticas são ferramentas elementares à análise acadêmico-científica que pretende evitar as “ambiguidades das ameaças cibernéticas à segurança nacional” (NYE, 2017) e identificar a realidade fenomenológica da natureza dos problemas de segurança cibernética.

Ao classificar os problemas associados à segurança cibernética, no que se referem aos riscos estruturalmente efetivos e as ameaças à segurança centradas nos atores, Weiss (2018) constrói uma tipologia que auxilia a compreensão objetiva do fenômeno.

Os riscos envolvem perigos associados à vulnerabilidade das infraestruturas críticas que compreendem instalações físicas e lógicas, redes, serviços e bens responsáveis por prover recursos essenciais à vida humana como energia elétrica e água potável, esses sistemas altamente integrados, encontram-se interconectados via ciberespaço, o que aumenta o risco de que uma contaminação por ameaças virtuais como softwares maliciosos possa se espalhar rapidamente por este ambiente. Reduzir os riscos é uma das tarefas dos formuladores de políticas públicas que pode ser analisada pela comunidade acadêmica em termos da efetiva capacidade do Estado em fortalecer a defesa contra riscos potenciais (BECK, 2016).

As ameaças envolvem a análise dos atores que “têm a capacidade de prejudicar a segurança de outros e que são percebidos por seus alvos potenciais como tendo intenções de fazê-lo” (WALLANDER; KEOHANE, 1999; WEISS; 2018). A comunidade acadêmica e empresas especializadas em análise de segurança cibernética as classificam como Ameaças Persistentes Avançadas (APT), em sua origem, o termo remonta à esfera militar, contudo, embora “originalmente usada para descrever invasões cibernéticas contra organizações militares, a APT evoluiu e não está mais confinada às forças armadas” (CHENET; OLSZEWSKI, 2018).

As APT tonaram-se importantes para a projeção de poder dos Estados contemporâneos, “eficazes para a infiltração de sistemas de defesa estrangeiros ou roubo de segredos militares, principalmente devido à relativa facilidade de execução (comparado aos métodos tradicionais de espionagem), bem como um baixo risco de revelar a fonte real e o beneficiário de tal ataque” (GAJEWSKI, 2013). Tratam-se, portanto, de grupos de atores não-estatais, hackers, cibercriminosos, ciberespiões, ciberterroristas que atuam em esquemas altamente organizados, capazes de orquestrar ataques sofisticados sem que sua presença seja notificada até que a ação tenha ocorrido e os danos causados.

Em suma, a proteção do ciberespaço representa uma tarefa árdua para os Estados contemporâneos, a ampla gama de possibilidades oferecidas por este ambiente transcendem fronteiras geográficas e políticas, mas também a distância espacial e temporal (WEISS, 2018). O desafio virtual se materializa em dois problemas distintos da segurança cibernética que podem ser analisados pela comunidade acadêmica civil e militar, riscos e ameaças com potencial para afetar e interromper seriamente a prestação de serviços públicos essenciais.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Beck, U. ( 2016). *The metamorphosis of the world*. Cambridge, UK: Polity.

Choucri, N. ( 2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Crossref | Google Scholar

Kello, L. ( 2013). The meaning of the cyber revolution: Perils to theory and statecraft. *InternationalSecurity*, 38( 2), 7– 40. <https://doi> org.ez16.periodicos.capes.gov.br/10.1162/ISEC\_a\_00138

OLSZEWSKI, Boguslaw. Advanced persistent threats as a manifestation of states’ military activity in cyberspace. Issue SJMULF; 2018; 189 (3): 57-71

Nye, J. S. ( 2017). Deterrence and dissuasion in cyberspace. *International Security*, 41( 3), 44– 71.

<https://doi-org.ez16.periodicos.capes.gov.br/10.1162/ISEC_a_00266>

R. O. Keohane, & C. A. Wallander (Eds.), *Imperfect unions: Security institutions over time and space* (pp. 21– 47). Oxford, UK: Oxford University Press.

Wallander, C. A., Keohane, R. O. ( 1999). Risk, threat, and security institutions. In H. Haftendorn,

WEISS, Moritz. Securing cyberspace: how states design governance arrangements. Volume 32, Issue 2 <https://doi-org.ez16.periodicos.capes.gov.br/10.1111/gove.12368>