O ato de guerra e o ataque cibernético: o caso STUXNET na visão de Clausewitz

Amanda Rodrigues Bernardes
Mestranda em Ciências Militares pelo Instituto Meira Mattos/ECEME

Karen Ludmilla Barreto de Ávila
Mestranda em Ciências Militares pelo Instituto Meira Mattos/ECEME

Em 23 de novembro de 2010, autoridades do Irã anunciaram a interrupção do enriquecimento de urânio nas instalações nucleares de Natanz. A decisão foi motivada por um ataque contra as instalações (MELMAN, 2010; ZETTER, 2014). Não se tratava, entretanto, de um ataque militar tradicional. O soldado que havia danificado as instalações era um inimigo invisível: o vírus de computador Stuxnet. Este programa atuava sobre o software que controlava as centrífugas das instalações nucleares, aumentando sua velocidade de rotação a ponto de danificar o equipamento, tornando-o inutilizável (ALBRIGHT, BRANNAN & WALROND, 2010).

Em um pronunciamento à época, o ministro iraniano de indústria e minas, Mahmud Liaii, classificou o ataque do Stuxnet da seguinte forma: "uma guerra eletrônica foi deflagrada contra o Irã" (ANEJA, 2010). De fato, alguns analistas associam o Stuxnet a uma ação deliberada por parte de dois rivais do Irã: Israel e os Estados Unidos (NAKASHIMA, 2012). Evidências disso seriam a sofisticação do vírus, o vazamento do caso no jornal do NYT em 2012 (a ser visto a seguir) e o fato de ele ter sido voltado para prejudicar o programa nuclear do Irã, o qual já havia sido objeto de críticas e sanções por parte dos dois países. De fato, pode-se dizer que, por mais que a autoria do vírus até hoje não tenha sido confirmada, são precisamente estes dois países os maiores beneficiados pelo mesmo.

A forma como as autoridades iranianas responderam à ameaça do Stuxnet motiva a questão sobre se este seria um exemplo de guerra cibernética. Esta questão será analisada por meio da perspectiva Clausewitziana sobre a guerra, filtrada por meio da lente de dois pesquisadores com visões opostas sobre a viabilidade em si de uma guerra cibernética. Dessa forma, na primeira parte deste trabalho, será apresentada a visão de Thomas Rid, contrária à ideia de que ataques cibernéticos são suficientes para caracterizar uma guerra. Na segunda parte, será apresentada a perspectiva de John Stone, que mostra ter uma visão mais abrangente da guerra, capaz de abarcar a guerra cibernética. Em seguida à exposição dessas perspectivas, será feita uma síntese, na qual o conceito de guerras cibernéticas será comparado ao ato de sabotagem e a legislação internacional a respeito do ato de guerra, em um esforço de entender sua relação com o conceito tradicional de guerra conforme elaborado por Clausewitz.

1. A guerra cibernética não ocorrerá: a visão de Thomas Rid

Em seu artigo The Cyber War will not take place, 2011, Thomas Rid retoma a definição Clausewitziana de Guerra como uma aplicação de força, que configure em letalidade, por meio de um ato de violência e com objetivos políticos (RID, 2011, p. 7). De acordo com Rid, ao não preencher adequadamente estes três conceitos – especificamente a necessidade de letalidade e violência, que Rid entende necessariamente como agressão física cometida sobre seres humanos – a guerra cibernética se torna uma contradição em termos. De fato, mesmo com a imprecisão conceitual que caracteriza o termo, até os casos mais frequentemente apontados como atos de guerra cibernética, como o do vírus Stuxnet, ainda se baseiam no uso do ciberespaço para destruir as infraestruturas que dependem desse novo domínio operacional, o que implica na materialidade física do ato. Rid admite que pode chegar o momento em que o mau funcionamento de componentes eletrônicos em virtude de um ataque deliberado pode levar a uma grande perda de vidas humanas, mas o articulista propõe que isso ainda é "ficção científica" (RID, 2011, p. 10). Por essa linha de análise, os exemplos de guerra cibernética a nossa disposição ainda são muito escassos e limitados para que possam ser analisados pela lente Clausewitziana, motivando sua exclusão da categoria "guerra".

2. A guerra cibernética ocorrerá: a visão de John Stone

Escrevendo em resposta a Rid, John Stone adota uma visão mais abrangente de guerra (STONE, 2013). Talvez seu argumento mais persuasivo seja aquele que diz respeito aos objetivos da guerra, tomando como exemplo os bombardeios estratégicos na Segunda Guerra Mundial. De acordo com o autor, estes bombardeios – que ele exemplifica por meio do

64498.011295/2021-11

bombardeio de Schweinfurt, em 1943 – tinham como objetivo na maior parte das vezes destruir infraestruturas críticas para o esforço de guerra alemão; a violência (afinal, esses ataques resultavam em muitas mortes), nesse caso, seria um "efeito colateral" dos ataques, mas não seu objetivo ou sequer o meio principal de se atingi-lo (STONE, 2013, p. 104). De fato, se uma comparação entre o bombardeio de Schweinfurt e o Stuxnet demonstra algo, é que hoje é possível atingir objetivos basicamente semelhantes – a destruição de uma instalação militar estratégica – com número menor ou nulo de perda de vidas humanas e ser considerado um ato de guerra, pois o uso de violência nem sempre terá natureza letal (STONE, 2013).

Stone retoma a frase que talvez sintetize o pensamento de Clausewitz: "a guerra é a continuação da política por outros meios". E, de fato, é difícil de interpretar o Stuxnet como outra coisa senão uma continuação da política norte-americana e israelense com relação ao Irã, que tinha como objetivo negar a este país a capacidade de se dotar da tecnologia para a criação de bombas atômicas.

3.1. Sabotagem e guerra: linhas cinzentas

Fica claro, desse modo, que a forma de entender o caso Stuxnet repousa diretamente sobre a forma como se entende a categoria nebulosa dos ataques cibernéticos – como uma tática similar à espionagem, ou como uma arma de guerra. A tese de Stone, à primeira vista, responde de maneira adequada à principal crítica de Rid – de que a guerra cibernética não corresponde aos parâmetros Clausewitzianos – ao se escorar exatamente nesses parâmetros. E diferente de Rid, que diz que sabotagem não é um ato de guerra e que equipara a guerra cibernética à uma variação da mesma, pois para ele, a sabotagem é realizada por agentes ocultos, enquanto a guerra é necessariamente aberta, ou seja, sempre se sabe que se está combatendo e quem se está combatendo (nem sempre o mesmo ocorre em um ataque cibernético), para Stone, um ato de sabotagem pode sim ser um ato de guerra, já que "os dois não são mutuamente exclusivos" (STONE, 2013, p. 105, tradução própria)[1].

Sendo assim, ao analisar o caso do Stuxnet, mesmo que não tenha tido declaração de autoria do ataque cibernético e possua traços de sabotagem (ZETTER, 2014), o caso poderia ser considerado como um ato de guerra (na visão da guerra limitada da Teoria de Guerra de Clausewitz), pois o ato de força atingiu o seu objetivo, que era retardar a produção de energia atômica (ZETTER, 2014; CLAUSEWITZ, 1984; STONE, 2013).

Em 2012, o jornal New York Times vazou uma conversa do então Presidente Barack Obama - diretamente da Casa Branca – ordenando que as forças armadas norte-americana desferissem sucessivos ataques cibernéticos (ato de força) por meio de worms às infraestruturas críticas do Irã, segue o trecho, "[Obama] secretamente ordenou ataques cada vez mais sofisticados aos sistemas de computadores que administram as principais instalações de enriquecimento nuclear do Irã" (NYT, 2012, tradução própria)[2]. Ou seja, o ciberataque à infraestrutura crítica (Usina Nuclear de Natanz no Irã) possuiu os elementos de guerra de Clausewitz - objetivo político, uso de força e propósito (CLAUSEWITZ, 1984).

3.2. O caso STUXNET perante a legislação internacional

Até hoje nenhum ataque cibernético à uma infraestrutura crítica foi considerada como um ato de guerra pelas organizações internacionais (ONU; OTAN). Mas ao ler os artigos da Carta das Nações Unidas "qualquer ameaça à paz, ruptura da paz ou ato de agressão" (Art. 39 da ONU, 1945) poderá ser considerado um ato de guerra e deverá ser reportado ao Conselho de Segurança da instituição para que essa determine quais ações deverão ser tomadas pela própria ONU ou pelo Estado que esteja sofrendo os ataques.

Para a OTAN, a Organização do Tratado do Atlântico Norte, o Direito Internacional abrange os conflitos cibernéticos, desse modo, acredita que "ameaças cibernéticas à segurança da Aliança estão se tornando mais frequentes, complexas, destrutivas e coercitivas" e afirma que a organização "continuará a se adaptar ao cenário em evolução das ameaças cibernéticas" (OTAN, 2021, tradução própria)[3]. Sendo assim, o caso do Stuxnet poderia ser considerado um ato de guerra, pois o ataque cibernético coordenado pelos Estados Unidos e Israel (NYT, 2012) foi um ato de força/violência contra à infraestrutura crítica do Irã, e um ato de agressão que ameace a paz de um Estado, ameace a sua soberania, destrua suas infraestruturas críticas, prejudique o equilíbrio de poder, interfira na Segurança Internacional e possua a Trindade de Clausewitz, pode ser um ato de guerra (ONU, 2021; OTAN, 1945; DIENSTEIN, 2014; LIBICKI, 2009; STONE, 2013).

[1] [tradução própria]. No original, lê-se: The two are mutually exclusive.

[2] [tradução própria]. No original, lê-se: "President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program".

[3] [tradução própria]. No original, lê-se: "Cyber threats to Alliance security are becoming more frequent, complex, destructive and coercive" (…) "will continue to adapt to the evolving scenario of cyber threats".

Rio de Janeiro - RJ, 30 de agosto de 2021.

Como citar este documento:

BERNARDES, Amanda Rodrigues e ÁVILA, Karen Ludmila Barreto de. O ato de guerra e o ataque cibernético: o caso STUXNET na visão de Clausewitz. **Observatório Militar da Praia Vermelha**. ECEME: Rio de Janeiro. 2021.

Referência:

ALBRIGHT, D; BRANNAN P; WALROND, C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security, 22 dez 2010. Disponível em: https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf. Acessado em 19/06/2021

ANEJA, A. Under cyber-attack, says Iran. The Hindu, 26 Sep 2010. Disponível em: www.thehindu.com/news/international/Under-cyber-attacks-says-Iran/article16048668.ece. Acessado em 19/06/2021

CLAUSEWITZ, C. von; HOWARD, M.; PARET, P. (Eds.). On War. Princeton: Princeton University Press, 1984.

DINSTEIN, Y. War, Aggression and Self-Defence. Editora Cambridge University Press, 2014.

LIBICKI, Martin C. Cyberdeterrence and Cyber War. Santa Monica: RAND, 2009.

MELMAN, Y. Iran Pauses Uranium Enrichment at Natanz Nuclear Plant. Haaretz, 23 nov 2010. Disponível em: https://www.haaretz.com/1.5143485. Acessado em 19/06/2021

NAKASHIMA, E. Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. 2 jun 2012. Disponível em: www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Acessado em 19/06/2021.

NEW YORK TIMES. Obama Order Sped Up Wave of Cyberattacks Against Iran, 2012. Disponível em: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Acessado em 22/06/2021.

OTAN. Cyber Defense, mar. 2021. Disponível em: www.nato.int/cps/en/natohq/topics_78170.htm. Acessado em 20/06/2021.

ONU. Carta das Nações Unidas, 1945. Disponível em: www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm. Acessado em 20/06/2021.

RID, T. Cyber War Will Not Take Place. Journal of Strategic Studies, v. 35, n. 1, 2011. pp. 5-32

STONE, J. Cyber War Will Take Place!, Journal of Strategic Studies, vol. 36, n. 1, 2013. pp. 101-108.

ZETTER, Kim. Contagem Regressiva até Zero Day. Editora Brasport, 2014.