A Guerra Cibernética e o ataque sofrido pela JBS S.A.

Luísa Guimarães Vaz
Mestranda no Programa de Pós-graduação em Ciências Militares

INTRODUÇÃO

Segundo Manuel Domingos (2005), há uma relação direta entre a barbárie e a civilização. Considerando que a guerra nada mais é do que a barbárie ou a violência em seu estado bruto, constatou-se os maiores avanços tecnológicos e procedimentais, nos locais onde houve guerras. Manuel Domingos (2005) tece detalhes adicionais e aponta que uma das funções da guerra é servir de laboratório, pois se não fosse a guerra, não haveria as tecnologias que existem atualmente.

A consequência desses avanços fez com que as tecnologias alcançassem o ciberespaço. Atualmente, percebe-se que há indícios de guerra de 5ª Geração (SANTOS et al, 2019). Nesse sentido, este trabalho propõe uma análise das notícias de mídia sobre o caso do ataque cibernético sofrido pela JBS S.A., no dia 31 de maio de 2021. Para tanto, será utilizada a clipagem como elemento de busca, empregando o conceito de segurança aplicado ao ciberespaço, como lente para a análise do fato.

CIBERESPAÇO E A GUERRA CIBERNÉTICA

O conceito de ciberespaço está em constante evolução. Trata-se de um espaço completamente artificial, possuidor de fronteiras "maleáveis". De acordo com Segal (2016), ciberespaço é um espaço que trouxe novas vulnerabilidades ao sistema internacional, pois é um ambiente que possibilita burlar as leis de várias formas, e por se tratar de um espaço não físico com múltiplos atores envolvidos, também é um ambiente com grande dificuldade de regulamentação. Segal (2016), ainda, afirma que a questão ciber desafia a própria soberania do Estado e ameaça à Segurança e à Defesa.

Diante disso, para fins de análise, o presente trabalho utilizará o conceito proposto por Kuehl (2009), o qual afirma que o ciberespaço é mais do que computadores e informações digitais. Para o autor, o ciberespaço é um domínio global dentro do ambiente de informação, cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas, utilizando tecnologias de informação e de comunicação.

Isto posto, Santos et al (2019) apontam que, atualmente, já se discute o escopo de guerra de 5ª geração, que, dentre todas as características que possui, tomam destaque as seguintes: o emprego massivo da cyber war, existência de elementos de natureza assimétrica, emprego de guerra informacional e traços de guerra híbrida. Dessa forma, é evidente a dificuldade de se elaborar uma teoria que englobe o ciberespaço.

Decorrente dessas incertezas, surgem diversas indagações: Vai atribuí-la a quem? O que constitui um ato de guerra no ciberespaço? E de não guerra? A guerra é necessariamente um ato de violência e que envolve mortes? Mesmo diante de tantas perguntas, pode-se inferir que essas demandas impactam as questões relacionadas à segurança e à defesa cibernética, principalmente por não serem abarcadas por questões ligadas à guerra clássica de Clausewitz.

A par dessas considerações, verifica-se que há uma série de dificuldades para a sociedade compreender essa temática atualmente: 1) na tipificação (da identificação do sujeito e da autoria); 2) no estabelecimento do cenário da competência do direito (quem vai julgar); 3) na definição do alcance do direito; e 4) na determinação se os ataques cibernéticos devem ser considerados atos de guerra, crimes, espionagem ou sabotagem (STONE, 2013).

> *"...a guerra cibernética é possível no sentido de que os ataques cibernéticos podem constituir atos de guerra. Esse ponto só se torna evidente, entretanto, se tivermos clareza sobre o que está englobado pelos termos de "força" e "violência" e sobre sua relação com a questão da letalidade. Atos de guerra envolvem a aplicação de força para produzir efeitos violentos. Esses efeitos violentos não precisam ser letais..." (STONE, 2013 - Tradução própria).*

Para Stone (2013), o fato de não possuir uma estrutura conceitual substancialmente acordada para localizar os ataques cibernéticos é culpa do campo dos Estudos Estratégicos. Diante desse cenário e da dificuldade em regulamentar as ações no ambiente ciber, há a necessidade de pensar a guerra e seu estado de exceção, destinando especial atenção para as particularidades nesse e desse domínio.

Mesmo havendo essas dificuldades, é evidente que os ciberataques são ameaças à Segurança e à Defesa do Estado. Em razão disso, pode-se aplicar a teoria de securitização, visto que não há uma teoria específica para o ciberespaço.

> *"...os recursos inerentes à essas redes têm um grande potencial para afetar o status quo político e estratégico, sendo caracterizado pela inexistência de fronteiras definidas entre o virtual e o real, particularmente em termos de causas e consequências. A arquitetura física e os*

.

> *protocolos de software que moldam o ciberespaço facilita o anonimato. (...) essas características criam um ambiente permissivo para que agentes anônimos - individualmente ou em nome de governos - violem sistemas e redes confidenciais. Essas ações podem ser interpretadas como desafios à soberania do Estado e para a segurança de dados individuais e do setor privado" (BETZ; STEVENS, 2011 apud LOBATO; KENKEL, 2015 - Tradução própria).*

Sendo assim, pode-se definir cibersegurança como:

> *"...é tanto sobre a insegurança criada por e através deste novo lugar/espaço e sobre as práticas ou processos para torná-lo (mais) seguro. Refere-se a um conjunto de atividades e medidas, tanto técnicas quanto não técnicas, destinadas a proteger o ambiente bioelétrico e os dados que ele contém e transporta de todas as ameaças possíveis" (CAVELTY, 2012 apud LOBATO; KENKEL, 2015 - Tradução própria).*

Segundo Lobato e Kenkel (2015), o Manual de Tallin sobre o Direito Internacional aplicável à guerra cibernética (OTAN, 2013) aborda questões como a extensão do Direito Humanitário à realidade virtual, ressaltando aspectos como a frequência e as consequências dos ataques cibernéticos, da mesma forma que aponta a existência de uma preocupação crescente com o alcance econômico, político e social obtido pelos ataques cibernéticos.

ESTUDO DE MÍDIA: ATAQUE À JBS S.A.

A JBS S.A., alvo de ataques cibernéticos no dia 31 de maio de 2021, é uma empresa multinacional de origem brasileira, sendo reconhecida como uma das líderes globais da indústria de alimentos. Segundo o site da própria empresa, a sede está localizada na cidade de São Paulo e está presente em 15 países.

Uma reportagem realizada pelo El País, em 02 de junho de 2021, relatou que a Casa Branca acusou a Rússia pelo ataque cibernético ao frigorífico da JBS, o qual ocasionou a paralisação de sua produção. Neste ataque, os hackers exigiram um resgate para desbloquear os servidores de várias unidades. Segundo o referido jornal, esse resgate é conhecido como ransomware ("programa para resgates"), que nada mais é do que um modus operandi praticado pela delinquência cibernética, no qual consiste em aproveitar as falhas de segurança de um sistema informático para bloqueá-lo, ficando em condições vantajosas para exigir uma quantia em dinheiro para reiniciá-lo (EL PAÍS, 2021). O jornal teceu detalhes adicionais sobre a matéria e acrescentou o seguinte:

> *"...a porta-voz da Casa Branca informou que o Governo do presidente Joe Biden ofereceu assistência à JBS, que o Departamento de Agricultura dos EUA está em contato com a direção da empresa e que o FBI está investigando o incidente em parceria com a Agência de Segurança Cibernética e de Infraestruturas (CISA, na sigla em inglês)" (EL PAÍS, 2021).*

A BBC por sua vez, numa reportagem datada de 02 de junho de 2021, publicou que, dependendo do tempo da paralisação, esse tipo de ataque pode levar à escassez de carne ou aumentar os preços das carnes para os consumidores. Segundo a reportagem, assim que o ataque cibernético foi detectado, a empresa suspendeu todos os sistemas de tecnologia da informação que foram afetados e informou que os seus servidores de backup não foram hackeados (BBC, 2021a).

Uma reportagem publicada em 02 de junho de 2021 pela revista Exame informou que a China poderia ser a mais afetada pela paralisação da JBS após o ataque, pois o país é o maior comprador mundial de carne bovina e responde por quase um terço da receita de exportação da empresa (EXAME, 2021a). Uma outra reportagem da revista Exame, publicada em 03 de junho de 2021, afirmou que a Casa Branca alertou às empresas para reforçarem a segurança cibernética (EXAME, 2021b).

Com relação ao grupo russo, apontado como responsável do ataque pelo FBI, uma reportagem feita pela BBC em 03 de junho de 2021, afirmou que o REvil (também conhecido como Sodinokibi) é um dos grupos cibercriminosos mais lucrativos do mundo e que o FBI está trabalhando para levar o grupo à justiça pelo ataque realizado. Ainda sobre o REvil, essa reportagem expôs que:

> *"...é uma rede criminosa de hackers de ransomware que ganhou destaque em 2019. Acredita-se que a maioria de seus membros residam na Rússia ou em países que antes faziam parte da União Soviética. (...) Se os ataques forem bem-sucedidos para o grupo, os desenvolvedores pegam uma porcentagem da receita obtida e fornecem a outra parte aos afiliados. O grupo ameaça publicar documentos roubados em sites (o que é conhecido como "Happy Blog") se as vítimas não cumprirem suas exigências" (BBC, 2021b).*

Numa reportagem publicada pela revista Exame em 04 de junho de 2021, foi anunciada a retomada integral das operações da empresa JBS, após o ataque sofrido em 31 de maio de 2021. De acordo com essa reportagem, a empresa conseguiu limitar as perdas sofridas para menos de um dia de produção e conseguiu colocar, novamente, todas as suas instalações 100% operacionais (EXAME, 2021c).

Segundo a reportagem do G1 publicada em 09 de junho de 2021, a JBS pagou 11 milhões de dólares pelo resgate, afirmando que o pagamento foi feito para reduzir problemas relacionados à invasão e evitar vazamento de dados. Acrescentou, também, que a maioria de seus frigoríficos estavam em plena operação no momento do pagamento.

Por fim, vale destacar que:

> *"...os ataques cibernéticos, em geral, não são conhecidos publicamente, pois tanto o atacante quanto a vítima, têm motivos para não divulgar detalhes da ação. No caso da vítima, a publicidade do ataque e as suas consequências podem, por exemplo, afetar as medidas de mitigação e forense, além de comprometer a reputação da instituição. No*

.

caso do atacante, a publicidade o impediria de reutilizar artefatos e repetir táticas, técnicas e procedimentos (TTPs) bem-sucedidos" (BRANDÃO; IZYCKI, 2019).

CONSIDERAÇÕES FINAIS

Tendo como base as questões conceituais e teóricas apresentadas nas seções anteriores, pode-se inferir que mesmo o ataque sendo realizado em um "ambiente invisível", ele afetou o mundo físico, real. O ataque cibernético à empresa paralisou sua produção, situação que possibilitou os hackers exigirem um resgate para desbloquear os servidores das unidades atingidas. Não obstante, a gravidade do ataque fez com que o governo norte-americano oferecesse assistência, colocando o FBI para investigar o ataque e a Agência de Segurança Cibernética e Infraestruturas para prestar apoio técnico.

Portanto, pode-se concluir que, tanto o ataque sofrido pela JBS S.A., quanto diversos casos ocorridos no mundo, são uma ameaça à Segurança e à Defesa dos países, pois possuem potencial para provocar a paralisação de sistemas, que podem afetar o mundo físico. Além disso, o ataque em questão descortina as dificuldades relacionadas à competência do direito, haja vista o desafio em apontar o autor e definir o enquadramento legal. Evidencia-se, então, cada vez mais, a necessidade de uma tipificação e de uma teoria para o ciberespaço, a fim de "responder" às indagações levantadas no presente trabalho.

Rio de Janeiro - RJ, 14 de março de 2022.

Como citar este documento:
Vaz, Luísa Guimarães. A Guerra Cibernética e o ataque sofrido pela JBS S.A. **Observatório Militar da Praia Vermelha**. ECEME: Rio de Janeiro. 2022.

REFERÊNCIAS:

BBC. O que se sabe sobre ataque cibernético a JBS investigado pelo FBI, 2021a. Disponível em: https://www.bbc.com/portuguese/internacional-57327955. Acesso em: 22 jun. 2021.

BBC. Ataque de hackers à JBS: o que se sabe sobre grupo russo apontado como responsável pelo FBI, 2021b. Disponível em: https://www.bbc.com/portuguese/internacional -57344706. Acesso em: 22 jun. 2021.

BRANDÃO, José Eduardo Malta de Sá; IZYCKI, Eduardo Arthur. Poder ofensivo no espaço cibernético. In: ANDRADE, Israel de Oliveira Andrade; LANGE, Valério Luiz; MEDEIROS FILHO, Oscar; LIMA Raphael Camargo (Org.). Desafios contemporâneos para o Exército Brasileiro, capítulo 10, p. 241-274. Brasília: IPEA, 2019.

DOMINGOS NETO, M. Os Militares e a Civilização. Tensões Mundiais, vol. 1, nº 1, jul-dez, p. 37-70, 2005.

EL PAÍS. Casa Branca acusa Rússia após ataque cibernético que paralisou produção do frigorífico JBS, 2021. Disponível em: https://brasil.elpais.com/internacional/2021-06-02/casa-branca-acusa-russia-apos-ataque-cibernetico-que-paralisou-producao-do-frigorifico-jbs.html. Acesso em: 22 jun. 2021.

EXAME. China pode ser a mais afetada por parada da JBS após ataque cibernético, 2021a. Disponível em: https://exame.com/exame-agro/china-pode-ser-a-mais-afetada-por-par ada-da-jbs-apos-ataque-cibernetico/. Acesso em: 22 jun. 2021.

EXAME. Casa Branca alerta empresas para reforçarem segurança cibernética, 2021b. Disponível em: https://exame.com/tecnologia/casa-branca-alerta-empresas-para-reforcarem-se guranca-cibernetica/. Acesso em: 22 jun. 2021.

EXAME. JBS anuncia retomada integral de operações após ataque cibernético, 2021c. Disponível em: https://exame.com/negocios/jbs-anuncia-retomada-integral-de-operacoes-após -ataque-cibernetico/. Acesso em: 22 jun. 2021.

G1. JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA, 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-p agou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 22 jun. 2021.

JBS. Quem somos, 2021. Disponível em: https://jbs.com.br/sobre/jbs/. Acesso em: 22 jun. 2021.

KENKEL, K. M.; LOBATO, L. C. Discourses of cyberspace securitization in Brazil and in the United States. Revista Brasileira de Política Internacional, vol. 58, nº 2, p. 23-43, 2015.

KUEHL, D. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, F. D.; STARR, S. S.; WENTZ, L. K. (Eds.). Cyberpower and National Security. Washington: National Defense University, 2009.

SANTOS, Daniel Mendes Aguiar; MALTEZ, Marcelo Monteiro; GOMES, Túlio Endres da Silva; FREITAS, Gerson de Moura; SANDERS, Andrew. A arte da guerra no século XXI: avançando à Multi-Domain Battle. Coleção Meira Mattos, vol 13, nº 46, p. 83-105, janeiro/abril 2019.

SEGAL, A. The Hacked World Order. Nova Iorque: Public Affairs, 2016.

STONE, J. Cyber War Will Take Place! Journal of Strategic Studies, vol 36, nº 1, p. 101-108, 2013.

.