revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

O mercado global das empresas militares privadas e operações cibernéticas: elementos para atribuição de responsabilidade estatal[1]

The global market for private military companies and cyber operations: elements for attributing state responsibility

Luciano Vaz-Ferreira
Doutor em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul, com período de pesquisa na American University (EUA). Professor do Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea. Professor da Universidade Federal do Rio Grande. E-mail: lvazferreira@gmail.com.
Filipe Bach Rodrigues
Mestre em Direito e Justiça Social pela Universidade Federal do Rio Grande. E-mail: bachfilipe@gmail.com.

Resumo
O objetivo do presente artigo é analisar a expansão do mercado global de empresas militares privadas na área de operações cibernéticas e refletir sobre a possibilidade de responsabilidade dos Estados por ações destes atores não estatais. Sob o aspecto metodológico, o trabalho possui uma natureza exploratória, pois se trata de tema ainda pouco analisado na literatura. A técnica utilizada envolverá uma revisão bibliográfica, com base em artigos acadêmicos e documentos internacionais. O artigo é dividido em duas partes. Na primeira serão demonstrados a expansão na utilização de tecnologias de comunicação e informação e o surgimento de empresas militares privadas na área da cibersegurança. Na segunda parte serão discutidas as possibilidades de responsabilização de Estados por operações cibernéticas conduzidas por empresas militares privadas. Como resultados parciais, observou-se a emergência de um mercado global de empresas militares na área de cibersegurança. A atribuição de responsabilidade estatal em caso de operações cibernéticas realizadas por atores privados pode ser analisada em três perspectivas: técnica, política e jurídica. Em relação à jurídica, a literatura aponta divergências entre a aplicação das teorias do controle efetivo e do controle geral.
Palavras-chave: Empresas Militares Privadas, Operações Cibernéticas, State Responsibility.

Abstract
The aim of this article is to analyze the expansion of the global market of private military companies in the field of cyber operations and to reflect on the possibility of State responsibility for the actions of these non-state actors. From a methodological point of view, the research has an exploratory character, since it deals with a topic that has been understudied in the literature. The technique used includes a bibliographic review based on academic articles and international documents. The article is divided into two parts. The first part highlights the expansion of the use of communications and information technologies and the emergence of private military companies in cybersecurity. The second part discusses the possibilities of holding states accountable for cyber operations conducted by private military companies. As a partial result, the emergence of a global market of private military companies in cybersecurity could be observed. The attribution of state responsibility in the case of cyber operations conducted by private actors can be analyzed from three perspectives: technical, political, and legal. As for the legal perspective, the literature points to divergences between the application of the theories of effective control and overall control.
Keywords: Private Military Companies, Cyber Operation, State Responsibility.

[1] Recebido para Publicação 22/07/2022. Aprovado para Publicação em 01/09/2022.
DOI https://doi.org/10.5281/zenodo.7236757

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Introdução

A sociedade moderna é extremamente dependente da utilização das tecnologias de comunicação (TIC). Quanto mais a sociedade utiliza-se destas tecnologias, mais exposta fica a riscos de segurança, visto que são noticiados diariamente incontáveis incidentes ao redor do mundo, atribuídos a ataques cibernéticos.

Observa-se que, nos últimos anos, os Estados têm investido na utilização de atores não estatais, na forma de empresas militares privadas, para conduzirem operações cibernéticas. Assim, o objetivo do presente artigo é analisar a expansão do mercado global de empresas militares privadas na área de operações cibernéticas e refletir sobre a possibilidade de responsabilidade dos Estados por ações destes atores não estatais. Sob o aspecto metodológico, o trabalho possui uma natureza exploratória, pois se trata de tema ainda pouco analisado na literatura, especialmente no contexto nacional. A técnica utilizada envolverá uma revisão bibliográfica, com base em artigos acadêmicos sobre os temas correlatos e documentos internacionais, como tratados internacionais, decisões de tribunais internacionais e trabalhos técnicos realizados por comissões internacionais de especialistas.

O artigo é dividido em duas partes. Na primeira parte serão demonstradas a expansão na utilização das tecnologias de comunicação e informação (TIC) e a presença de novas vulnerabilidades cibernéticas. Neste contexto é que surgem as empresas militares privadas na área da cibersegurança, formando um novo mercado global. Na segunda parte serão discutidas as possibilidades de responsabilização de Estados por operação cibernética conduzida por atores não estatais, mais precisamente as empresas militares privadas. Como resultado, serão analisadas as principais normas internacionais aplicadas neste cenário.

Cibersegurança e Empresas Militares Privadas

É notável que nos últimos anos existiu um crescimento exponencial da utilização de tecnologias de comunicação e informação (TIC). Conforme União Internacional de Telecomunicações (UIT), em 2005, apenas 17% da população mundial utilizava da internet; em 2019, este número correspondia a 51% da população. Nye (2011, p. 153) chama este fenômeno de “Revolução da Informação”, baseada nos “rápidos avanços tecnológicos em computadores, comunicações e softwares”. Neste contexto, a sociedade moderna está cada vez mais dependente dos serviços digitais, que incluem ferramentas de comunicação, trabalho, entretenimento, sistemas industriais ou comerciais complexos, serviços públicos, entre outros. As TICs também são de grande importância para os sistemas militares e de defesa dos países, oferecendo um apoio logístico e comando global de forças, além do fornecimento em tempo real de inteligência (LYNN, 2010, p. 98). A estratégia miliar contemporânea não pode ser colocada em ação sem sistemas eletrônicos e redes de TIC (UESSELER, 2008, p. 168).

Além dos benefícios que proporciona, o uso das TICs também representa uma desvantagem, pois estas tecnologias também podem ser utilizadas para fins ilícitos (CEPIK; CANABARRO; BORNE, 2014, p. 161).

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Atualmente, o acesso a certas ferramentas de TICs pode ser realizado em um custo relativamente baixo, o que facilita o seu uso com objetivos espúrios. Em contrapartida, seu desenvolvimento não levou em consideração esta variável, visto que em seus primórdios ninguém imaginava que a internet seria utilizada por outros públicos além de acadêmicos e cientistas bem-intencionados (CLARKE; KNAKE, 2015, p. 93). Pouca reflexão costuma ser dedicada à segurança dos sistemas eletrônicos (NYE, 2011, p. 165). Como resultado, as cyber vulnerabilidades são constantemente exploradas e mercantilizadas.

Neste contexto é que surgem os cyber threat actors (CTA), atores que promovem ameaças cibernéticas e representam possíveis perigo à segurança da sociedade, pois podem, a um custo extremamente baixo, produzir efeitos relevantes em estruturas tecnológicas de natureza civil ou militar. Os CTAs podem ser indivíduos ou grupos pequenos, de natureza não estatal ou estatal (SHELDON, 2019). Alguns são ideologicamente motivados, outros ingressam neste tipo de atividade apenas por realização pessoal e prestígio. Há, ainda, aqueles que oferecem os seus serviços de maneira paga para conduzirem operações em benefício de seus contratantes.

Uma expressão que tem emergido nos últimos anos é a de “mercenários cibernéticos”. Noor (2014) define estas figuras como sendo um indivíduo ou um grupo de especialistas que podem oferecer suas habilidades a qualquer um que lhes pague uma boa quantia em dinheiro. Para Pedron e Da Cruz (2020, p. 03), são atores intermediários com capacidades cyber ofensivas que atuam ilegalmente no comércio de inteligência hackeada, explorações de software, ou conhecimentos técnicos em troca de ganhos financeiros ou ideológicos.

Em virtude do deslocamento de várias funções do Estado para a iniciativa privada, por conta da difusão do modelo neoliberal, atores privados estão proliferando na área da segurança cibernética, responsável por neutralizar os ataques dos CTAs (PATTISON, 2020, p. 239). Empresas de cibersegurança utilizam-se de “tecnologias, medidas, processos e práticas destinadas a proteger redes, dispositivos, programas e dados contra ataques, danos ou acesso não autorizado” (MAUER; HOFFMAN, 2019, p. 03). Dependendo da sua atuação, estas organizações também podem ser caracterizadas como private military companies (empresas militares privadas), ou de maneira eufemística security or military contractors (contratantes de segurança ou contratante militares). Seus serviços podem incluir apoio material e técnico às forças armadas, planejamento estratégico, inteligência, investigação, treinamento e outras atividades relacionadas (MAUER; HOFFMAN, 2019, p. 03).

Como resultado, um mercado global está sendo formado e novos fornecedores com perfis diversos estão surgindo (GASSER; MALZACHER, 2020, p. 53). Empresas militares privadas tradicionais, que costumam fornecer soldados, apoio logístico, equipamento militar e treinamento (como as que atuaram no Iraque e Afeganistão) estão criando suas próprias equipes de segurança cibernética ou adquirindo empresas menores do ramo (MAUER; HOFFMAN, 2019, p. 05). Da mesma forma, empresas de consultoria empresarial e tecnologia, sem background militar, estão ingressando neste mercado (GASSER; MALZACHER, 2020, p. 53). Recentemente, a ManTech, empresa de tecnologia, fechou um contrato de 125 milhões de dólares com o governo dos EUA para preparar a “próxima geração de guerreiros digitais para o Departamento de Defesa” (MAURER, 2018, p. 74). O interesse destas organizações está relacionado aos custos relativamente baixos destas atividades comparados a outras áreas de operações militares e de segurança, visto que é necessário apenas recursos humanos adequados e acesso a computadores (MAUER; HOFFMAN, 2019, p. 05).

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Governos contratam estas novas empresas militares privadas por diversos motivos. Primeiro, ao utilizar atores privados, os Estados mantêm a aparência de negação e neutralidade, pois permitem que se envolvam em um conflito com um adversário sem se vincularem diretamente. Assim, são evitadas as baixas de guerra, custos e possíveis repercussões sociais (PEDRON; DA CRUZ, 2020, p. 08).

Segundo, os meios de recrutamento e formação militar tradicionais podem não ser eficientes em lidar com tecnologias avançadas e de rápida transformação (ESTEVES, 2013, p. 69). O manuseio e manutenção de sistemas eletronicamente ligados entre si demanda pessoal altamente especializado, o que traz a necessidade de suporte de profissionais da iniciativa privada (UESSELER, 2008, p. 161-164). A experiência destas organizações costuma ser superior às divisões cibernéticas militares de alguns países (PEDRON; DA CRUZ, 2020, p. 08). Este cenário dificilmente mudará nos próximos anos. É pouco provável que os Estados desenvolvam conhecimentos técnicos ou capacidade de defesa plenas contra ameaças cibernéticas, visto que esta tecnologia de ponta não está nas mãos do Estado, mas em empresas privadas (PATTISON, 2020, p. 244).

Responsabilidade dos Estados em Operações Cibernéticas Conduzidas por Empresas Militares Privadas

Conforme Maurer (2018, p. 22) a mídia frequentemente refere-se, de maneira descompromissada, que operações cibernéticas conduzidas por atores privados foram patrocinadas por algum Estado. Contudo, a atribuição de responsabilidade internacional no ciberespaço é um dos elementos mais complexos sobre o tema, sendo objeto de intenso debate no campo das relações internacionais e do direito internacional.

Até o presente momento, é extremamente difícil identificar claramente os perpetradores de operações cibernéticas e de determinar se a sua conduta é imputável a Estados (DELERUE, 2020, p. 50). Conforme relatório do grupo de especialistas constituídos pela ONU para estudar o comportamento responsável dos Estados no ciberespaço (Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security – GGE) “os incidentes envolvendo a utilização maliciosa das TIC pelos Estados e intervenientes não estatais aumentaram em alcance, escala, severidade e sofisticação” (GGE, 2021).

“Atribuir” significa identificar o responsável pela ação. Em outras palavras significa quem, na realidade, realizou a operação cibernética (DELEURE, 2020, p. 50; RID; BUCHANAN, p. 04). Com o conhecimento da atribuição, é possível tomar as devidas medidas preventivas (defensivas) ou repressivas (contramedidas). A atribuição de operações cibernéticas envolve questões técnicas, políticas e jurídicas (DELERUE, 2020; SCHMITT, 2021; TSAGOURIAS, 2012; GGE, 2021).

A atribuição técnica refere-se à utilização de tecnologia para identificar o perpetrador de uma operação cibernética (SCHMITT, 2021; NOOR, 2014, p. 06). Tais atividades necessitam de um humano que possua conhecimento sobre o espaço cibernético e de uma máquina tecnológica ligada ao sistema em rede, que recebe comandos deste humano para que uma operação seja realizada. O objetivo, então, é identificar de maneira precisa o indivíduo e a máquina ligada ao ataque cibernético, para ser possível definir

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

relacionamentos com grupos, organizações ou um determinado Estado (CARTER; ENOIZI, 2021, p. 13). Observa-se que mesmo em processos automatizados, há sempre uma participação humana. Identificar o computador de onde originou o ataque pode auxiliar na definição de identidade do agressor, porém nem sempre resolve plenamente a questão da atribuição.

É comum o uso de "computadores zumbis" para ataques, controlados pelos agressores sem a vítima ter conhecimento, o que mascara a real origem da operação cibernética (CARTER; ENOIZI, 2021, p. 13). O objetivo é cobrir as próprias pistas e envolver terceiros em países não relacionados ao ataque cibernético (DELERUE, 2020, p. 72). Esta prática tem sido constantemente utilizada por atores não estatais, como no caso Ghostnet, em que um grupo se infiltrou em estruturas governamentais e empresas em todo mundo sem ser possível identificar a origem do ataque (NOOR, 2014). Nos casos Gucciger 2.0 e Cyber Caliphate, há indícios de perpetradores que mascaram a sua nacionalidade (MAUER, 2018, p. 23). A constante evolução e transformação da tecnologia tornam os procedimentos de investigação de atribuição rapidamente obsoletos, visto que são desenvolvidas de maneira paralela técnicas de rastreamento e de encobrir rastros cibernéticos (TSAGOURIAS, 2012, p. 234).

A atribuição política envolve um ou mais Estados acusando o outro de conduzir uma operação cibernética hostil ou estar ligado à atuação de atores não estatais (SCHMITT, 2021). Possui um efeito estratégico, pois envolve a utilização do discurso diplomático e análise das consequências políticas. Uma acusação pública pode trazer consigo o reconhecimento das vulnerabilidades do Estado vítima. Por conta disso, muitos Estado preferem manter os incidentes em segredo para evitar constrangimento e perder credibilidade (KATAGIRI, 2021, p. 05). Neste contexto, optam por manter indícios sobre atribuição registrados em suas agências de inteligência, de modo a orientar possíveis políticas de cibersegurança no futuro. O sigilo destas informações dificulta que sejam tomadas ações coordenadas no campo internacional, de modo a incrementar a segurança coletiva (RID; BUCHANAN, 2015, p. 28). O GGE (2021, p. 20) entende que o exercício de transparência e troca de informações sobre incidentes de segurança das TICs é importante para construir confiança e previsibilidade no ambiente internacional, reduzindo possíveis interpretações erradas e escalamento do conflito. Segundo Banks (2017, p. 1504-1511), uma articulação de opiniões a respeito das operações cibernéticas auxiliaria maior previsibilidade e estabilidade na área da cibersegurança.

A atribuição jurídica de operações cibernéticas gira em torno da responsabilidade internacional dos Estados, um dos temas mais importantes do direito internacional. Como se sabe, os Estados são considerados, pelo menos sob o ponto de vista formal e jurídico, como iguais nas relações internacionais (princípio da igualdade). O direito internacional, composto por normas criadas pelos próprios Estados com objetivo de regular suas condutas, propõe oferecer certeza e estabilidade a estas relações. O descumprimento destas normas gera consequências, na forma de responsabilidade internacional.

Até o momento, os Estados não foram capazes de criarem um tratado internacional dispondo sobre normas gerais de responsabilidade. Porém, em 2001, a Comissão de Direito Internacional da ONU (International Law Commission), composta por juristas indicados pelos Estados-Membros, produziu um trabalho que é considerado como a principal norma sobre o tema (Draft Articles on Responsibility of States for Internationally Wrongful Acts). Apesar de não possuir natureza vinculativa, foi endossado pela Assembleia Geral da ONU em 2012 e tem sido citado repetidamente em tribunais internacionais e outros órgãos internacionais (BANKS, 2017). Neste contexto, o Draft Articles tem sido considerado como fonte de

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

direito internacional (NGUYEN; DAILLIER; PELLET, 2003). Outro documento importante é o Tallinn Manual 2.0, um trabalho elaborado por um grupo de pesquisadores internacionais com objetivo de mapear a aplicabilidade do direito internacional em operações cibernéticas (BANKS, 2017; SCHMITT, 2017). Apesar de não se tratar de uma norma jurídica, a sua pesquisa compila e codifica as normas existentes, inclusive sobre responsabilidade, aplicando-as no contexto do ciberespaço.

Três elementos compõem a responsabilidade internacional. Primeiro, deve haver uma violação de uma norma internacional. Segundo, o ato ou omissão deve ser atribuível a um Estado responsável, estabelecendo um nexo causal. Terceiro, exige-se a comprovação de dano moral ou patrimonial causado a um Estado ou particular (MELLO, 2000, p. 500; SHAW, 2010, p. 572).

Operações cibernéticas podem ser classificadas de modo geral como sendo uma interferência indevida na soberania de um Estado e violação do princípio da não intervenção em assuntos domésticos (BANKS, 2017). Dependendo da escala e do efeito também podem ser consideradas como um ataque armado, que seria uma violação do princípio do uso da força (Artigo 2, § 4º da Carta das Nações Unidas). Uma situação de gravidade envolve, por exemplo, perda de vidas ou extensa destruição de propriedade, com efeitos similares a um ataque cinético convencional (OORSPRONG; DUCHEINE; PIJPERS, 2021). É o caso, por exemplo, de um ciberataque dirigido a uma usina nuclear capaz de causar uma explosão e resultar em danos maciços ao seu entorno.

Sabe-se que o Estado é um ente artificial, logo, ele age por meio de indivíduos (ou grupo de), que podem praticar atos ilícitos. Um fator importante é definir se trata de um ato de Estado ou praticado exclusivamente no interesse do indivíduo que conduzir a ação (CRAWFORD, 2013, p. 113). De acordo com o Draft Articles, é de responsabilidade dos Estados qualquer ato de órgão do Estado, independentemente de sua posição na organização (Artigo 4º). Estão incluídas também pessoas ou entidades que exercem atribuições do poder público (Artigo 5º). O Tallinn Manual 2.0 estabelece que as operações cibernéticas praticadas por órgãos de um Estado, ou por pessoas ou entidades autorizada pelo direito interno para exercer elementos de autoridade governamental são atribuíveis a Estados (Regra 15). Uma parte das operações cibernéticas são realizadas diretamente pelos Estados, por órgãos militares, de segurança ou de inteligência (DELERUE, 2020, p. 15). Neste caso, não há problemas jurídicos de atribuição.

A controvérsia maior é quando acontece uma operação praticada por um ator não estatal, como as empresas militares privadas, atuando em favor de um determinado Estado. Neste caso, ainda que não sejam oficialmente um órgão de Estado, esta responsabilidade pode ser atribuída em determinadas circunstâncias. O Artigo 8º do Draft Articles considera ato de Estado quando um indivíduo ou um grupo de pessoas estão agindo sob instrução, sob controle ou sob direção de um Estado ao executar a conduta (CRAWFORD, 2013, p. 126). Em sentido similar, o Tallinn Manual 2.0 estabelece que as operações cibernéticas conduzidas por um ator não estatal são atribuíveis a um Estado quando: a) são realizadas seguindo instruções ou sob a sua direção ou controle; b) o Estado reconhece e aceita a operação como sendo sua (Regra 17).

Uma dificuldade enfrentada é determinar o parâmetro desta “instrução, direção ou controle” exigido para que o ato possa ser imputado a um Estado. A resposta está na jurisprudência de dois tribunais internacionais, a Corte Internacional de Justiça (CIJ), ligada à ONU e responsável por julgar as controvérsias jurídicas entre Estados, e o Tribunal Internacional Penal para Ex-Iugoslávia (ICTFY), uma Corte estabelecida

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

de maneira ad hoc com objetivo de julgar indivíduos pela prática de crimes internacionais durante a Guerra da Iugoslávia na década de 90.

No Caso Nicarágua, julgado pela CIJ em 1986, os Estados Unidos foram acusados de patrocinarem rebeldes contra o governo. Na ocasião, a CIJ decidiu que o financiamento, organização, treinamento, suprimento de grupos não estatais não era o suficiente para atribuir responsabilidade por violação de normas aplicáveis aos conflitos armados, necessitando de um "controle efetivo" (effective control) (CIJ, 1986, p. 62). Neste contexto, deveria ser comprovado que os rebeldes deveriam estariam atuando em nome dos americanos e sendo controlados em uma operação militar específica, agindo como se fossem órgãos estatais de fato.

O Caso Tadic, julgado pelo ICTFY em 1999, refere-se ao processamento de um guarda de campos de concentração na Bósnia Herzegovina, que foi acusado de crimes de guerra e crimes contra a humanidade. Uma discussão que surgiu em caráter preliminar foi sobre uma possível responsabilidade da República da Iugoslávia por violação de direito internacional praticada por indivíduos que compõem uma organização hierarquicamente estruturada, tal como uma unidade militar, bandos armados irregulares ou de rebeldes (ICTFY, 1999). Na ocasião, a Corte da Apelação da ICTFY entendeu que a atribuição de responsabilidade a um Estado acontece quando ele possui o papel não apenas de financiar, treinar, equipar ou providenciar apoio operacional, mas organizar, coordenar ou planejar operações militares. Serão considerados atos de Estado independentemente de qualquer instrução específica do controlador estatal referente ao cometimento das ações violadores de direito internacional (ICTFY, 1999). Neste contexto, entende-se que o "controle geral" (overall control) é mais frouxo que o "controle efetivo" previsto no Caso Nicarágua, bastando demonstrar uma influência geral do Estado em atos de organização, coordenação e planejamento, sem a necessidade de se relacionar à condução de uma operação específica (CASSESSE, 2007).

No campo das operações cibernéticas, as duas teorias podem ser aplicadas. O Tallinn Manual 2.0 adota a teoria do "controle efetivo" (SCHMITT, 2021). Um ponto importante diz respeito quando os atores não estatais agem além da autoridade e das instruções do Estado (ultra vires acts), o que não poderia acarretar responsabilidade estatal. É o caso, por exemplo, de um Estado que instrui o desenvolvimento de um malware para ser enviado a um Estado rival, porém a empresa opta por usar a mesma tecnologia para atacar também um terceiro Estado (BANKS, 2017). Roscini (2014, p. 38) entende que o objetivo principal da teoria do "controle efetivo" é evitar que os Estados sejam acusados maliciosamente.

Se o "controle geral" for utilizado como base, seria imputável a um Estado um ataque cibernético realizado por um grupo de hackers, em uma situação em que há apoio técnico ou organizacional de um determinado Estado, mesmo que não possa ser comprovado o seu envolvimento em uma operação específica (TSAGOURIAS, 2012, p. 238). Shackelford (2009, p. 233-234) entende que exigência do "controle efetivo" seria rigorosa demais nas situações envolvendo cibersegurança, favorecendo a irresponsabilidade dos Estados, que continuaram utilizando atores não estatais para esconderem suas ações.

Observa-se que esta discussão ainda se limita no campo teórico. Conforme visto, não há uma norma específica que trate sobre a imputação de responsabilidade em operações cibernéticas praticadas por atores não estatais, devendo-se valer de normas gerais que muitas vezes possuem dificuldade de adaptação. Não existe consenso para produção de novas normas internacionais nesta área no futuro (BANKS, 2017, p. 1444; GGE, 2021, p. 08). A prática dos Estados e declarações sobre o tema ainda é ambígua. De fato, as acusações

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

internacionais limitam-se no campo da retórica, visto que os Estados evitam fazer referências ao direito internacional quando acusam a responsabilidade por um determinado ato (KATAGIRI, 2021, p. 03).

Considerações Finais

Com o crescimento da utilização da TICs, é inegável que a sociedade moderna está cada vez mais dependente de serviços digitais. De outro lado, ampliam-se as possibilidades de exploração das cyber vulnerabilidades, por meio de ataques dos CTAs. Como resultado, empresas militares privadas estão investindo em oferecer serviços de cibersegurança aos Estados, inclusive na área militar e de defesa. O interesse destas organizações está na exploração dos custos baixos destas atividades, que exigem apenas recursos humanos e acesso a computadores. Os Estados, por sua vez, optam por contratar empresas militares privadas por diferentes razões: custos, experiência e capacidade técnica destas empresas, além de manter a aparência de negação e neutralidade na ocorrência de uma operação cibernética. Assim, um mercado global de empresas militares privadas de cibersegurança está emergindo.

A atribuição de responsabilidade a Estados por operações cibernéticas conduzidas por empresas militares privadas envolve questões técnicas, políticas e jurídicas. Sobre a atribuição técnica, o objetivo é identificar com precisão a pessoa e a máquina responsável pelo ciberataque, para poder verificar uma possível responsabilidade estatal. Trata-se de um grande desafio, visto ser comum a utilização de "computadores zumbis" e estratégias de encobrir rastros cibernéticos. A atribuição política também possui seus obstáculos, pois é comum que muitos Estados vítimas optem por manter em segredo tais operações, com medo de demonstrar vulnerabilidade. Esta prática acaba por dificultar possíveis ações internacionais coordenadas.

Por fim, a atribuição jurídica busca no direito internacional uma resposta, porém também apresenta seus problemas e controvérsias. Atualmente, não há uma norma internacional que disponha especificamente sobre operações cibernéticas e a possibilidade de sua elaboração no futuro é improvável. Um dos pontos mais importantes diz respeito ao grau de proximidade entre o ator não estatal e o Estado a ser responsabilizado. Aqui, a literatura divide-se em duas teorias: a do controle efetivo, em que se exige instrução, direção ou controle em relação a uma operação específica; e a do controle geral, que comporta uma influência geral do Estado em atos de organização, coordenação e planejamento, sem necessitar a vinculação a uma operação específica. Ambas as teorias implicam diferentes perspectivas para a atribuição jurídica de responsabilidade estatal, podendo gerar casos de imputação equivocada ou irresponsabilidade.

REFERÊNCIAS

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVIII | Volume XIX | Nº 37| Janeiro/Junho 2022 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

BANKS, William. State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. Texas Law Review, [s. l.], v. 95, n. 7, 2017.

CARTER, Rachel Anne; ENOIZI, Julian. Mapping a Path to Cyber Attribution Consensus. 2021. Disponível em: <https://www.genevaassociation.org/sites/default/files/cyber-attribution_web_final.pdf>. Acesso em: 30 set. 2022.

CASSESSE, Antonio. The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. The European Journal of International Law, [s.l.], v. 18, n. 4, p. 649-668, 2007.

CEPIK, Marco Aurélio Chaves; CANABARRO, Diego; BORNE, Thiago. A Securitização do Ciberespaço e o Terrorismo: uma Abordagem Crítica. In: MELLO E SOUZA, André; NASSER, Reginaldo Mattar; MORAES, Rodrigo Francalossi (Org.). Do 11 de Setembro de 2001 à Guerra ao Terror: Reflexões sobre o Terrorismo do Século XX. Brasília, Ipea, 2014, p. 161-186.

CLARKE, Richard A.; KNAKE, Robert K. Guerra Cibernética: a Próxima Ameaça à Segurança e o que Fazer a Respeito. Rio de Janeiro, Brasport, 2015.

CRAWFORD, James. State Responsibility: The General Part. Cambridge, Cambridge University Press, 2013.

DELERUE, François. Cyber Operations and International Law. Cambridge, Cambridge University Press, 2020.

ESTEVES, João Amorim. Privatização da Guerra Perante a Redução das Atribuições do Estado na Hora da Globalização. Lusíada Direito, Lisboa, n. 7–8, p. 45–74, 2013.

GASSER, Martina; MALZACHER, Mareva. Beyond Banning Mercenaries: The Use of Private Military and Security Companies Under IHL. In: HEFFES, Ezequiel; KOTLIK, Marcos; VENTURA, Manuel J (Org.). International Humanitarian Law and Non-State Actors. The Hague: T.M.C. Asser Press, 2020, p. 47-77.

GROUP OF GOVERNMENTAL EXPERTS ON ADVANCING RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY (GGE). Report of the Group of goGovernmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. [S. l.: s. n.], 2021. Disponível em: <https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf>. Acesso em: 30 set. 2022.

INTERNATIONAL COURT OF JUSTICE (ICJ). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). 1986. Disponível em: <http://www.icj-cij.org/docket/%0Afiles/70/6503.pdf>. Acesso em: 30 set. 2022.

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGUSLAVIA (ICTFY). Case n. IT-94-1-A. Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction 1999. Disponível em: <http://www.icty.org/sid/7537>. Acesso em: 30 set. 2022.

INTERNATIONAL LAW COMMISSION. Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries. 2001. Disponível em:

<https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf> Acesso em: 30 set. 2022.

KATAGIRI, Nori. Why International Law and Norms do Little in Preventing Non-State Cyber Attacks. Journal of Cybersecurity, [s. l.], v. 7, n. 1, p. 01-09, 2021.

LYNN, William. Defending a New Domain: The Pentagon's Cyberstrategy. Council on Foreign Relations, [s. l.], v. 89, n. 5, 2010. Disponível em: < http://www.jstor.org/stable/20788647>. Acesso em: 30 set. 2022.

MAURER, Tim. Cyber Mercenaries: The State, Hackers, and Power. Cambridge, Cambridge University Press, 2018.

MAURER, Tim; HOFFMAN, Wyatt. The Privatization of Security and the Market for Cyber Tools and Services. Genebra, Geneva Centre for Security Sector Governance, 2019.

MELLO, Celso de Albuquerque. Curso de Direito Internacional Público. Rio de janeiro: Renovar, 2000.

NGUYEN, Quoc Dinh; DAILLIER, Patrick; PELLET, Alain. Direito Internacional Público. Lisboa, Fundação Calouste Gulbenkian, 2. ed, 2003.

NOOR, Sitara. Cyber (In) Security: A Challenge to Reckon With. Strategic Studies, [s. l.], v. 34, p. 1–19, 2014.

NYE, Joseph. The Future of Power. 1. ed. [S. l.]: PublicAffaris, 2011.

OORSPRONG, F. M. E.; DUCHEINE, P. A. L.; PIJPERS, B. M. J. Armed Attack in Cyberspace: Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands´ Right of Self-Defense. Amsterdam Law School Legal Studies Research Paper No. 2021-29. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3934417>. Acesso em: 29 set. 2022.

PATTISON, James. From Defence to Offence: The Ethics of Private Cybersecurity. European Journal of International Security, [s. l.], v. 5, n. 2, p. 233–254, 2020.

PEDRON, Stephanie Mae; DA CRUZ, Jose de Arimataeia. Cyber Mercenaries: A New Threat to National Security. International Social Science Review, [s. l.], v. 96, n. 2, p. 1–33, 2020.

RID, Thomas; BUCHANAN, Ben. Attributing Cyber Attacks. Journal of Strategic Studies, [s. l.], v. 38, n. 1–2, p. 4–37, 2015.

ROSCINI, Marco. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014.

SCHMITT, M. N. Terminological Precision and International Cyber Law. [s. l.], 2021. Disponível em: <https://lieber.westpoint.edu/terminological-precision-international-cyber-law/> Acesso em: 30 set. 2022.

SCHMITT, M. N. (Org.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, Cambridge University Press, 2017.

SHACKELFORD, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkley Journal of International Law, [s. l.], v. 25, n. 3, 2009.

SHAW, Malcom. Direito Internacional. São Paulo, Martins Fontes, 2010.

SHELDON, John B. The Rise of Cyberpower. In: BAYLIS, John; WIRTZ, James J; GREY, Colin (Org.). Strategy in the Contemporary World: An Introduction to Strategic Studies. Oxford, Oxford University Press, 2019.

TSAGOURIAS, Nicholas. Cyber Attacks, Self-defence and the Problem of Attribution. Journal of Conflict and Security Law, [s. l.], v. 17, n. 2, p. 229–244, 2012.

UESSELER, Rolf. Guerra como Prestação de Serviços a Destruição da Democracia pelas Empresas Militares Privadas. São Paulo, Estação Liberdade, 2008.

UIT, União Internacional de Telecomunicações. Estatística Utilização da Internet. [S. l.], 2019.