Mapeando os Ataques no Espaço Cibernético: a análise descritiva dos principais atores e tendências (2006-2019)

Ana Carolina de Oliveira Assis – Universidade Federal de Pernambuco (UFPE)
Anderson Henrique – Universidade Federal de Pernambuco (UFPE)
Karla Godoy da Costa Lima – Universidade Federal de Pernambuco (UFPE)
Nathalia Viviani Bittencourt – Universidade Federal de Pernambuco (UFPE)

Resumo

Qual é o perfil dos ataques cibernéticos ocorridos no mundo? O presente artigo verifica quais deles foram mais significativos na última década, assim como quais foram os atores envolvidos (criminosos e vítimas) e tipo de ataque. Em termos metodológicos, foi utilizada estatística descritiva e análise de conteúdo, juntamente com a produção de um banco de dados primário a partir das informações obtidas no Center for Strategic & International Studies para o período de 2006 a 2019 e dos conceitos elucidados pela literatura de possíveis atores, Estatais e não-estatais, e tipos de ataques cibernéticos responsáveis pelas ofensivas. Como resultados, foi comprovada a tendência positiva no aumento de investidas ao longo do tempo, principalmente através de Basic Malware, como também que as principais vítimas nesse período foram Governos, Empresas e Associações dos Estados Unidos (EUA), Índia, Coreia do Sul e Ucrânia. Em relação aos atores acusados de cometerem esse tipo de atividade, foi sinalizado que Governos, Hackers Individuais e Organizações Criminosas da China, Rússia, Irã e EUA foram os principais responsáveis.

Palavras-chave: Ciberataque; Guerra Cibernética; Defesa Cibernética; Vulnerabilidade Cibernética; Relações Internacionais.

Abstract

What is the profile of cyber attacks in the world? This article verifies what are the most significant cyber attacks that have occurred in the last decade, as well as who were the actors involved (criminals and victims) and type of attack. In methodological terms, descriptive statistics and content analysis were used, together with the production of a primary database from the information obtained at the Center for Strategic & International Studies for the period from 2006 to 2019 and from the concepts of possible actors, State and non-state, and kinds of cyber attacks that were responsible for the offensives that the literature elucidates. As a result, the positive trend in the increase of attacks over time was proven, mainly through Basic Malware, as well as that the main victims in that period were Governments, Companies and Associations of the United States (USA), India, South Korea and Ukraine. Regarding the actors accused of committing this type of activity, it was pointed out that Governments, Individual Hackers and Criminal Organizations in China, Russia, Iran and the USA were the main responsible.

Keywords: Cyberattack; Cyberwar; Cyberdefense; Cyber vulnerability; International Relations.

1. Introdução

Em 1998, Keohane e Nye escreveram uma matéria na qual afirmaram que a tecnologia informacional seria, provavelmente, um dos recursos mais poderosos do próximo século, seja pelo seu poder de criação, edição e manipulação[1]. Com efeito, a expansão da conectividade em redes e o amplo acesso à *internet* trouxeram diversas oportunidades a indivíduos, empresas e governos, como comodidades relativas à ubiquidade da comunicação, rapidez de transações e vigilância Estatal. Entretanto, o aumento da dependência de serviços básicos ao tráfego das redes no espaço cibernético também trouxe diversos desafios relativos à integridade e confidencialidade das informações disponíveis nesse meio.

Nesse sentido, as vulnerabilidades encontradas nos servidores do espaço cibernético, como *malware* e *spywares*, negação do serviço de dados (*DDoS*), acesso ilegal a segredos comerciais e manipulação indevida de infraestruturas críticas de serviços essenciais passaram a servir como capacidade ofensiva de Estados, organizações criminosas, empresas e até indivíduos. Nota-se, assim, que a evolução do mundo digital e suas comodidades tornaram muitos serviços dependentes da conexão à *internet* e do tráfego de redes de computadores, o que também permitiu o seu mau uso pelas brechas de segurança.

Diante desse cenário, o presente artigo propõe trazer à tona um assunto importante para os pesquisadores das Relações Internacionais: as ameaças e disputas de poder no espaço cibernético. A partir do levantamento de dados da *Center for Strategic & International Studies* para o período de 2006 a 2019, propomos identificar os principais atores e tendências relativas aos tipos de ataques. Com efeito, a partir do momento que as capacidades ofensivas e de defesa cibernética são colocadas como ativos relevantes na busca pelo poder, Governos e outros atores internacionais inserem na agenda doméstica e nas Organizações mundiais um novo tópico de discussões.

Além disso, o fenômeno cibernético e suas idiossincrasias desafiam conceitos tradicionais dos estudos de segurança internacional, na medida em que põem em xeque a forma pela qual percebemos a natureza dos conflitos, o funcionamento da ordem internacional e da balança de poder. Conforme destaca Kello (2013), a evolução do domínio cibernético é disruptiva e desestabilizadora por diversos motivos, dentre eles: a dificuldade de atribuição de responsabilidade, ambiguidade da escalada de conflito e a dominância da capacidade ofensiva sobre a de defesa. Assim, o esta pesquisa busca atender a necessidade da investigação do espaço cibernético no escopo das Relações Internacionais por meio da análise descritiva da ocorrência de ataques nos últimos treze anos (2006 - 2019).

Nessa perspectiva, buscamos responder a seguinte questão de pesquisa: qual é o perfil dos ataques cibernéticos ocorridos no mundo? Para tal, apresentamos quais são os ciberataques mais significativos ocorridos na última década por meio da técnica de análise de conteúdo e estatística descritiva. Produzimos um banco de dados primário a partir das informações obtidas no *Center for Strategic & International Studies* para o período de 2006 a 2019 e dos conceitos elencados pela literatura de possíveis atores Estatais e não-estatais, bem como os tipos de armas cibernéticas responsáveis pelas ofensivas.

Conforme poderá ser verificado, nossos principais resultados identificam o aumento de Estados como atores e vítimas desses ataques, o que sinaliza a consonância com a literatura, a qual aponta para o aumento da securitização no espaço cibernético e formação de ambiente de desconfiança mútua. Dentre os responsáveis pelas ofensivas, notou-se que a China, Rússia, Irã e Estados Unidos (EUA) foram os principais países que empre-

1 Disponível em <https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age> [Acesso em 15 de Maio 2020].

enderam essas armas no espaço cibernético, enquanto que este último, a Índia, Coreia do Sul e Ucrânia foram os principais afetados. Mais uma vez, esses resultados apresentam convergência com a teoria, tendo em vista os diversos interesses políticos e estratégicos que impulsionam essa atividade, como a busca por informação privilegiada, espionagem, retaliação, sabotagem (SANGER, 2018), dentre outras possíveis razões.

Sendo assim, para fins de organização, este artigo está disposto da seguinte forma: na próxima seção apresentamos a revisão de literatura do artigo, que tratará sobre o crescimento da busca pelo monopólio da informação e ascensão do espaço cibernético como ameaça para a segurança nacional. Além disso, trataremos sobre as dificuldades de limitação em relação ao seu território, a complexidade de atribuição da responsabilidade de um crime virtual e acerca das considerações sobre vulnerabilidade de serviços essenciais de países desenvolvidos. Na terceira seção, será apresentada a metodologia aplicada para análise dos dados e variáveis utilizadas. Em seguida, na quarta seção, os principais resultados obtidos através da estatística descritiva. E por fim, apresentaremos as principais considerações finais do estudo.

2. A Securitização do Ciberespaço e sua Fonte de Poder

O desenvolvimento das tecnologias de informação e comunicação (doravante TIC) foi fundamental para acelerar o processo de massificação do uso, processamento e armazenamento de dados. Devido à sua alta capilaridade, relativo baixo custo e grande utilidade para indivíduos, corporações e Estados, a disponibilidade dos sistemas de informação foi, de início, largamente expandida em detrimento da verificação de questões de segurança. Em verdade, conforme assenta Carlin e Graff (2018), as origens das redes de computadores remontam à criação da ARPANET, um projeto desenvolvido na Universidade da Califórnia, em 1969, que tinha como objetivo o mero compartilhamento de informações acadêmicas por pesquisadores e engenheiros nos EUA. O entusiasmo e expansão do seu entorno criaram a mentalidade de que a *internet* seria um ambiente sem fronteiras, descentralizado e aberto a toda coletividade.

De modo semelhante, a conotação do termo espaço cibernético (*cyberspace)* é abstrata e possui diferentes significados com o passar do tempo. Smeets e Shires (2017) apontam que o seu conceito passou de um domínio repleto de possibilidades para um mundo de ameaças e desconfiança mútua. Com efeito, inicialmente, os autores argumentam que a expansão de redes de computadores foi associada com os avanços da democracia, crescimento da interação social e desenvolvimento econômico no mundo globalizado do pós-Guerra Fria. Entretanto, ambos reconhecem que os perigos desenvolvidos pela criação de *softwares* maliciosos capazes de violar, obstruir ou manipular informações no mundo digital tornaram o espaço cibernético um lugar inseguro, anárquico e passível de securitização.

Nessa esteira, Manjikian (2010) aborda que o espaço cibernético passou de "vila global" para "campo de batalha virtual" notadamente após o terror do bombardeio de 11 de setembro de 2001, nos Estados Unidos. A relevância dos atores não-estatais como perigo para a política doméstica e internacional também foi levada em consideração na construção do discurso da *internet* como um ambiente de anarquia e de possível aparato de ação para terroristas. Sendo assim, desenvolveu-se a retórica na qual o mundo digital seria mais uma ferramenta perigosa do que um local essencialmente democrático. Existiria, dessa forma, uma corrida no espaço cibernético pelo monopólio da informação, cujo objetivo seria dominá-la com antecedência para alcançar uma vantagem estratégica sobre o adversário.

A busca na política internacional pela dominância desse meio é descrita como uma competição entre os Estados, especialmente os EUA, China e Rússia, pelo controle da informação, bem como das vantagens da ofensiva nas redes do espaço cibernético (MANJIKIAN, 2010). No que tange a esses dois últimos, foi desenvolvida a alcunha de poder perfurante[2] (*sharp power)* em relação a como a distorção da informação tem sido um projeto estratégico de manipulação do público-alvo para persecução de seus interesses autoritários. O termo foi criado a partir da noção de que o *soft power* desenvolvido por essas nações seria mais agressivo e incisivo (WALKER, LUDWIG, 2017).

Além disso, Hansen e Nissenbaum (2009) explicam a forma pela qual as ameaças no espaço cibernético tornaram-se matéria de segurança nacional através da teoria de securitização (BUZAN et al., 1998) da Escola de Copenhague. Com efeito, as autoras destacam que a temática de segurança cibernética começa a necessitar de proteção do Estado a partir de meados da década de 1990, quando o assunto das ameaças e perigos do mundo virtual passaram a fazer parte da agenda e discurso político. Entretanto, utiliza-se o ataque DDoS na Estônia[3] como estudo de caso e ponto de partida em razão de sua repercussão em todo mundo.

A fim de ilustrar o discurso político que a segurança cibernética passou a ter nos Estados, o trecho da fala do ex-Presidente dos EUA, Barack Obama, quando fez um discurso de alerta para os perigos que os setores estratégicos de países sofrem diante das vulnerabilidades do mundo cibernético, denota a atenção a esse espaço. Nota-se o seu receio para a possibilidade de ataques cibernéticos a estruturas críticas, como os setores de eletricidade, hídrico e financeiro. No discurso, Obama afirma:

> Os sistemas de computação em setores críticos de nossa economia - incluindo as indústrias nuclear e química - estão sendo cada vez mais visados. Em um conflito futuro, um adversário incapaz de igualar nossa supremacia militar no campo de batalha pode procurar explorar nossas vulnerabilidades de computador, derrubando sistemas de bancos estratégicos que podem desencadear uma crise financeira. A falta de água limpa ou hospitais em funcionamento podem desencadear uma emergência de saúde pública. E como vimos nos apagões anteriores, a perda de eletricidade pode paralisar empresas, cidades e regiões inteiras.(OBAMA, 2012, p.1) [4]

Diante dessa conjuntura, Libicki (2007) argumenta que existe uma grande potencialidade de escalada de tensões e disrupturas à medida que os sistemas de informação tornam-se mais difundidos e aplicados de modo generalizado na sociedade. E, como o espaço cibernético[5] tem as suas raízes na informação no formato de *bits* e *bytes,* a corrida pelo seu monopólio torna-se inevitável.

2.1 O Código como Fonte de (In) segurança e de Conflitos

Liff (2012) argumenta que a comunidade acadêmica ainda reluta em situar conflitos cibernéticos como fontes de estudo de segurança em razão da não ocorrência de mortes por ataques cibernético, ou que "*data packets don't hold ground"* (LIFF, 2012, p. 403). Entretanto, o

2 O termo foi criado em 2017 por uma matéria publicada na revista *Foreign Affairs,* e pode ser conferido em <https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power). [Acesso em 19 de Maio 2020].

3 Em 2007, um ataque de negação do serviço de dados (DDoS) desativou as plataformas da *web* do Presidente, Parlamento e diversas agências oficiais, como as mídias de notícias e bancos.

4 Trecho em tradução livre extraído do artigo '*Taking the Cyberattack Threat Seriously*', Wall Street Journal, 19 de julho de 2012. Disponível em <https://obamawhitehouse.archives.gov/blog/2012/07/23/taking-cyberattack-threat-seriously>. [Acesso em 26 de Abril 2020]. Trecho original: "Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill."(OBAMA, 2012, p.1).

5 Kuehl (2009) apresenta uma definição de espaço cibernético que revisa uma miríade de conceitos extraídos de teóricos, ficção científica, dicionários e oficiais de defesa do governo norte-americano, qual seja: cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies (KUEHL, 2009, p.4) .

autor afirma que a guerra realizada no ciberespaço pode ser considerada um evento no qual dois ou mais atores, através de atos hostis e deliberados, induzem ciberataques custosos contra a infraestrutura civil ou militar do adversário com intuito de: exercer coerção e extrair concessões políticas; reduzir a capacidade do adversário de defender-se; retaliação; apoio a ações militares através de ataques contra alvos civis e/ou militares para fins bélicos estratégicos.

Nesse sentido, o autor ainda argumenta que os ataques cibernéticos podem ser mais convenientes do que a força bruta devido ao seu caráter mais econômico e com potencialidade assimétrica de poder em conflito. Essa possibilidade é ilustrada pelas consequências desestabilizadoras da dificuldade existente quanto à atribuição da culpa pelos ataques, a vantagem da ofensiva aos países que tenham capacidade técnica efetiva e a dificuldade de se identificar e proteger contra ataques desse meio. Sendo assim, uma vez adquirindo capital humano e tecnologia suficientes, qualquer país pode executar um ataque pelas redes (LIFF, 2012).

Em contrapartida, Rid (2012) desconfia da alusão à ocorrência de ciberguerra em razão de três fatores: (1) as tecnologias utilizadas no passado e no presente em grandes conflitos foram as mais simples em detrimento das altas tecnologias; (2) a qualidade dos ataques cibernéticos são muito mais importantes do que a quantidade dos ataques, de modo que um país que queira ter vantagens em um possível conflito deverá investir na qualidade de seus ataques; (3) as maiores potências mundiais têm interesse na transparência das organizações quanto seu poderio cibernético para que possam se defender, enquanto que as grandes organizações e até mesmo as grandes potências escondem sua capacidade de ataque (RID, 2012).

Entretanto, Stone (2013), Junio (2013) e Mcgraw (2013) afirmam, a partir de fundamentos teóricos distintos, que a ausência de atrito físico e dos elementos *clausewitzianos* da guerra não impedem que os ataques cibernéticos possam ser considerados ofensivos belicosos, o que acirra o comportamento dos atores internacionais. Nessa esteira, Libicki (2009) afirma que a prática de *deterrence* no espaço cibernético, por exemplo, é possível, porém existem peculiaridades que a distanciam do conceito tradicional[6]. Ao fazer um paralelo com a ação de *nuclear deterrence,* o autor entende que, apesar da dificuldade em se identificar quem executou os ataques, a prática de *cyberdeterrence* por meio da retaliação existe na medida em que seus ataques podem ser uma força beligerante decisiva quando empregada de forma estratégica (LIBICKI, 2009).

Em resumo, Kello (2013) argumenta que o espaço cibernético necessita de mais atenção nos estudos de segurança das Relações Internacionais, na medida em que decisões políticas estratégicas para esse meio precisam ser tomadas. Nesse sentido, o autor alerta para os perigos das lacunas e resistências à análise cibernética, os quais são influenciados pelas dificuldades do entendimento das técnicas computacionais e as características de conflito que se diferem dos estudos tradicionais de Guerra.

2.2 Guerra e Conflitos no Ciberespaço: Aspectos Conceituais

Em um aspecto amplo, a Guerra Cibernética se tornou uma preocupação constante que necessita da adoção de ações protetivas de identificação dos ataques e de respostas eficazes (WENDT, 2011). Segundo Rattray (2009), as características mais relevantes da Guerra Cibernética são: a presença de conflitos no Espaço Cibernético, o anonimato utilizado para ocultação e surpresa, superação de barreiras físicas e geográficas - visto que não existem limites ou distâncias entre os atores durante o

6 Na obra de Libicki (2009), assume-se que *deterrence,* grosso modo, significa qualquer atuação capaz de dissuadir um ataque. Geralmente ela é guiada por duas vertentes: *deterrence* por negação, capaz de frustrar um ataque, e *deterrence* como punição, ou seja, ameaça de retaliação. O autor foca seus argumentos de possibilidade de *cyberdeterrence* nesta última abordagem.

ataque-, e a assimetria de força do ataque devido às diferenças existentes entre as redes que compõem o Espaço Cibernético do inimigo e de quem ataca.

Ademais, Santos e Monteiro (2010) apontam que a Segurança Global segue uma tendência permanente de estar sempre mais vulnerável e exposta devido a busca por eficiente redução da robustez dos sistemas criados. Essa propensão torna os sistemas sujeitos a falhas sistêmicas e alvos de ataques aos seus pontos críticos, os quais podem provocar rupturas em cascata com efeitos em territórios vizinhos[7]. Nesse contexto, apesar de não existir um consenso internacional sobre os conceitos de espaço e Guerra Cibernética, alguns analistas e documentos oficiais de Estados têm apresentado algumas definições. Para o Ministério da Defesa do Governo Brasileiro, Guerra Cibernética:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2015, p. 134).

Para Silva (2014) a definição apresentada pelo Ministério da Defesa brasileiro não abrange todos os tipos e formas de ações que podem ser consideradas como indícios de Guerra Cibernética. Ainda segundo o autor, o Departamento de Defesa estadunidense (DoD), por seu turno, não tem uma definição concreta sobre o que significa Guerra Cibernética, mas, descreve o que é Espaço Cibernético e Operações Cibernéticas. Pelo entendimento desses conceitos, Guerra Cibernética está relacionada com a utilização do conjunto de competências cibernéticas com a finalidade de obter bens ou objetivos militares no âmbito das informações, infraestruturas, redes e Tecnologia da Informação (SILVA, 2014).

No que tange à posição do Estado chinês quanto aos conflitos no ambiente cibernético, ela é a mesma apresentado pelas Nações Unidas, para quem as leis existentes sobre conflitos armados também se estendem ao Ciberespaço, em especial os princípios intitulados como "o não uso da força", a "resolução pacífica de disputas internacionais" e a proporcionalidade do uso da força. A China age em defesa de um Espaço Cibernético pacificado e indica que o Sistema Internacional deveria se opor firmemente à militarização do ciberespaço. Ademais, o país adota o princípio de "não uso inicial" de armas cibernéticas, nem atacar alvos civis, porém ressalta a dificuldade de identificar redes civis e militares (ZHANG, 2012).

Além disso, a potência oriental também acredita ser possível adaptar as regras internacionais existentes para conflitos armados em conflitos cibernéticos, assim como criar novas regras específicas para o Espaço Cibernético, como por exemplo, a identificação e atribuição de um ataque ao agressor e como determinar se o dano causado foi proporcional para que o ato de defesa possa ser caracterizado como legal. Dessa forma, a China se posiciona no sentido de que a comunidade internacional deve revisar e criar leis abordando temas como o controle do uso de armas cibernéticas, o direito à legítima defesa e as obrigações dos atores não-estatais nas suas atuações no Ciberespaço para que se evite ao máximo a ameaça ou o uso da força e uma possível Guerra Cibernética (ZHANG, 2012).

7 O *worm* que havia sido projetado para atacar as centrífugas de enriquecimento de urânio no Irã (Stuxnet) em 2010 foi eventualmente lançado na *internet* e afetou sistemas do Azerbaijão, Índia, Indonésia, Paquistão e dos EUA (TADDEO, 2018). Esse fato ilustra o risco escalado das armas cibernéticas como retaliação por Estados, assim como as suas consequências incalculáveis.

Contudo, os assuntos relativos aos ataques ocorridos no Ciberespaço não acabam no patamar das ameaças à soberania estatal e a possível qualificação como Ciberguerra. Segundo Wendt (2011) existem cinco tipos de ciber conflito que podem ocorrer de acordo com o seu potencial de danos, começando pelo menos danoso até o de mais periculosidade, sendo a própria Ciberguerra, como pode ser observado no Quadro 1.

Quadro 1 - Tipos de Ciber Conflito

Tipo	Características
Cibervandalismo	As ações de hackers são motivadas pelo desafio.
Crime Cibernético	Os atos praticados pelos hackers já acarretam algum tipo de dano à vítima, o que caracteriza crime.
Ciberespionagem	As ações ainda são criminosas, porém as motivações convergem para obtenção de informações comerciais, industriais e governamentais.
Ciberterrorismo	Tem como objetivo ataques virtuais à infraestruturas críticas de uma região ou país capazes de ocasionar colapsos.
Ciberguerra	Os objetivos vão além do ataque à infraestruturas críticas, e afetam a soberania da nação atacada.

Fonte: Elaborado pelos autores (2020), a partir de Wendt (2011).

2.3 As Assimetrias da Vulnerabilidade das Redes e o Retorno do Dilema de Segurança

A crescente dependência dos serviços essenciais (água, eletricidade, produção alimentícia, transações financeiras) a tecnologias da informação e comunicação, ou seja, a natureza interligada das infraestruturas críticas ao funcionamento das redes de computadores tem tornado possível a ocorrência de interrupções e explorações por atividades cibernéticas maliciosas. O grande interesse pela cibersegurança e a precaução em desenvolver resiliência aos ataques que prejudicam essas infraestruturas cresceram significativamente após importantes eventos, como o da Estônia em 2007, Geórgia em 2008 e no Irã, em 2010 (LOBATO, KENKEL, 2015).

Diversos Estados consideram esses acontecimentos citados como causas de grande atenção e muita reflexão no desenvolvimento do campo da Segurança Cibernética. Assim, ataques no ciberespaço não representam perigo apenas para países pequenos e relativamente fracos, já que grandes potências também se preocupam com possíveis ameaças à segurança nacional (LIFF, 2012). Em verdade, nota-se que a crescente corrida por poder no ciberespaço e a alta dependência de tecnologia pelos países desenvolvidos os tornam mais vulneráveis a possibilidade de ataques em redes. Desse modo, enquanto potência militar, os EUA desenvolvem sua Defesa cada vez mais estruturada em redes, o que pode acarretar, como consequência, em um "calcanhar de aquiles" (LIFF, 2012, p. 409), isto é, abertura para novas ameaças cibernéticas.

De outro modo, países que não possuem infraestruturas demasiadamente conectadas podem, por seu turno,

não serem alvos de ataques cibernéticos ou não estarem cientes de que estão sendo atacados. Nesse sentido, salienta-se que um eventual ataque é dificilmente quantificado ou mensurado, já que os efeitos não são necessariamente cinéticos e/ou imediatos, estando muitas vezes escondidos debaixo de inúmeras camadas de rede semânticas e sintáticas. (MEDEIROS et al., 2019).

Nessa perspectiva, McGraw (2013) assevera que existe uma dependência substantiva da sociedade moderna a sistemas informacionais que controlam serviços essenciais, como redes elétricas, finanças e transportes. Isso torna inevitável, para o autor, a tendência de Guerra Cibernética, na medida em que há brechas técnicas nesses sistemas que são exploradas pelos governos, fortes ou fracos, a fim de aumentar o seu poder de barganha na esfera internacional. Desse modo, a alta conectividade exige que as nações reforcem a defesa e segurança cibernéticas como meio de proteção de seus interesses e soberania.

Entretanto, Douzet (2014) destaca que os países mais desenvolvidos que possuem grande parte de sua infraestrutura de serviços conectada a redes de computadores são, de fato, os mais capazes de desenvolver a resiliência a ataques cibernéticos, construindo capacidades ofensivas e aproveitando novas oportunidades oferecidas pelo desenvolvimento da tecnologia para aumentar sua eficácia e poder. Sendo assim, a cibersegurança se torna uma das principais preocupações das relações internacionais em vários sentidos. Trocando em miúdos, os países que são mais dependentes das redes e sistemas de informação também são os mais vulneráveis a ataques cibernéticos, mas também os mais aptos a desenvolver a resiliência de suas redes. Assim, a partir da lógica de aprendizagem, podem construir ainda mais capacidades ofensivas e aproveitar novas oportunidades oferecidas pelas redes para aumentar sua eficácia e poder (DOUZET, 2014).

Devido à rápida disseminação das tecnologias de *hackers*, muitos países e Organizações Internacionais se concentram mais na elaboração de medidas de segurança e no aprimoramento da cooperação multilateral para combater as ameaças cibernéticas, as quais podem ser tão devastadoras quanto os ataques físicos militares (KIM, 2014). Em síntese, Marek Górka (2018) ilustra com acuidade o modo pelo qual os conflitos cibernéticos têm-se tornados fortes ameaças para o Estado moderno, a saber:

> Na última década, as tecnologias da informação foram usadas para melhorar o funcionamento dos governos, aumentar a eficácia militar, desenvolver novos serviços comerciais e produzir bens e serviços de qualidade superior. No entanto, juntamente com esses benefícios, a dependência dessas tecnologias criou novas vulnerabilidades. Se eles permitem monitoramento e controle nacional e global eficientes de infraestruturas críticas, eles também multiplicam os pontos de entrada pelos quais partidos hostis - sejam 'hackers' anarquistas, terroristas transnacionais ou estados hostis - podem atacá-los. (GÓRKA, 2018, p. 14).[8]

Diante do exposto, nota-se que essa conjuntura se assemelha com o conceito tradicional de dilema de segurança[9]. Buchanan (2017) argumenta que o contexto atual de assimetrias, hostilidades e preocupação com a segurança cibernética enaltece a teoria tradicional de Herz (1950) com uma nova roupagem. Dessa forma, as características peculiares do espaço cibernético inovam e enaltecem esse dilema em razão da impossibilidade de os Estados terem acesso à informação concreta sobre todas as capacidades ofensivas e defensivas do opo-

8 Do trecho original: "Over the past decade, information technologies have been used to improve the functioning of governments, increase military effectiveness, develop new commercial services, increase productivity and produce goods and services of superior quality. Yet, along with these benefits, reliance upon these technologies has created new vulnerabilities. If they permit efficient national and global monitoring and control of critical infrastructures, they also multiply the points of entry through which hostile parties – be they anarchist "hackers", transnational terrorists, or hostile states – can attack them." (GÓRKA, 2018,p. 14).

9 O conceito de dilema de segurança aponta que os esforços de um Estado para aumentar o seu aparato de segurança pode acarretar em uma escalada de tensão e conflitos que intensificam o ambiente de desconfiança mútua. Para mais informações ver o artigo de John Herz '*Idealist Internationalism and the Security Dilemma*' em 2011. Disponível em: <https://www.cambridge.org/core/journals/world-politics/article/idealist-internationalism-and-the-security-dilemma/7094783665386FD81A25DF98C7EEC223>. [Acesso em 20 de Abril 2020].

nente. Isso permite que o ambiente de tensão se escale e desenvolva assimetrias únicas.

Sob esse prisma, o presente artigo busca apontar os perfis mais recorrentes que perscrutam os ataques cibernéticos. Diante de suas características ubíquas, sorrateiras e de relativo baixo custo, destaca-se a dificuldade na atribuição de autoria como um dos maiores desafios ao Direito Internacional, sobretudo quando comparado com as hostilidades convencionais. Assim, indagamos: qual é o perfil dos ataques cibernéticos ocorridos no mundo?

3. Metodologia

Esta seção descreve os principais aspectos metodológicos que serão abordados no presente artigo. Portanto, busca-se contribuir com a replicabilidade científica dos dados para a construção de uma ciência transparente e que outros pesquisadores possam chegar aos mesmos resultados encontrados (FIGUEIREDO FILHO et al., 2013; KING, 2015). O quadro 2 abaixo sumariza os principais pontos do desenho de pesquisa do artigo.

Quadro 2 - Informações Gerais do Desenho de Pesquisa

Questão de pesquisa	Qual é o perfil dos ataques cibernéticos ocorridos no mundo?
Unidade de Análise	507 registros de ataques cibernéticos no mundo (evento/ano)
Técnicas	Análise de Conteúdo Estatística Descritiva
Escopo temporal	2006 a 2019
Fonte	Center for Strategic & International Studies

Fonte: Elaboração dos autores (2020).

Procura-se verificar quais são os ciberataques mais significativos ocorridos na última década, assim como, quais foram os atores envolvidos (criminosos e vítimas), tipo de ataque e suas prováveis origens. Este trabalho traz como principal inovação mapear os eventos registrados ocorridos no mundo desde que esses tipos de acontecimentos começaram a ser citados contra nações, empresas, empresas com participação estatal, e outros órgãos, afetados diretamente pelas ações criminosas.

Este esforço justifica-se pela ausência, salvo melhor juízo, de trabalhos empíricos na área de Relações Internacionais e Estudos de Defesa sobre o assunto que compilasse análise descritiva dos dados levando em consideração os eventos criminosos, uma vez que é muito difícil de encontrar informações detalhadas que tratem sobre ataques virtuais. Ademais, segundo o relatório de Riscos Globais de 2020 do Fórum Econômico Mundial, ataques cibernéticos, o colapso da infraestrutura de informações, assim como seu roubo e fraude estão entre os dez maiores riscos globais no que tange à probabilidade de ocorrência e em termos de impacto nos países (WORLD ECONOMIC FORUM, 2020).

O banco de dados original foi elaborado a partir do relatório disponibilizado pelo *Center for Strategic & International Studies* (CSIS), o qual é um *think tank* estadunidense vinculado à Universidade de *Georgetown*[10], que registram eventos de ataques cibernéticos significantes descobertos e divulgados pelos órgãos atingidos. Serão analisados 507 eventos no espaço de tempo de maio/2006 a dezembro/2019, devido à dis-

10 Para mais informações, acesse: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents. [Acesso em 22 de Janeiro 2020]

ponibilidade de dados registrados e serem suficientemente longos para análise.

Para a construção das variáveis do banco de dados foram extraídas informações, em que a unidade de análise é o ataque cibernético ocorrido, de acordo com os dados presentes no relatório acima citado. Para classificação das variáveis *tipo de crime* utilizamos as orientações de Bussolati (2015) e *tipo de ataque* as recomendações de Liff (2012). Por sua vez, as variáveis *tipo de vítima* e *finalidade financeira* foram criadas pelos autores levando em consideração a disponibilidade e relevância da informação.

Em suma, o quadro 3 abaixo apresenta as variáveis, mensuração e respectivas fontes.

Quadro 3 - Descrição das Variáveis

Nome da variável	Mensuração	Fonte da classificação
Ano	Ano em que o evento (ciberataque) ocorreu	-
Mês	Mês em que o evento ocorreu	-
Tipo de Criminoso	Tipo de Criminoso. Para*: 1. Governo; 2. Empresas; 3. Organizações Criminosas; 4.Mercenarios Cibernéticos; 5.Hackitivistas; 6. Hackers Patriotas; 7. Hackers Individuais; 8. NI*	Bussolati (2015) e autores
Tipo de Vítima	Tipo de Vítima. Para*: 1. Governo; 2. Empresas e Associações; 3. Indivíduos; 4. Governo e Empresas; 5. Todos*	Elaboração dos autores
Tipo de Ataque	Tipo de Ataque realizado. Para*: 1. Botnet/DDoS; 2. Basic Malware; 3. Advanced Malware; 4. NI*	Liff (2012)
Finalidade Financeira	Sinaliza a existência de finalidade financeira do ciberataque. *1. Sim(roubo de informações bancárias, crimes contra propriedade intelectual, entre outros); 0. Não (crimes que envolvem apenas a negação de serviço, coleta e divulgação de informações sem a autorização da vítima, e não está ligado a prejuízos econômicos)*	Elaboração dos autores
Origem do Ataque	País de origem do criminoso	Elaboração dos autores
Origem da Vítima	País de origem da Vítima	Elaboração dos autores

Fonte: Elaboração dos autores (2020).

No que tange aos tipos de criminosos, foi utilizada, em parte, a classificação de Bussolati (2015) e adicionada duas categorias elaboradas pelos autores - Governos e Empresas. Optamos por abranger a classificação de atores em: (1) Governos, na medida em que representam ataques promovidos pelo corpo do Estado (Defesa, membros diplomáticos, da inteligência) e com o propósito de buscar informações sensíveis de outra nação ou de indivíduos dissidentes, por exemplo; e (2) Empresas, sendo esta considerada de forma ampla, como corporações e instituições bancárias que atuam com o propósito de roubo de propriedade intelectual, informações comerciais secretas, etc.

Em relação a categorização elaborada por Bussolati (2015), de modo geral, os seguintes perfis mais frequentes de criminosos cibernéticos foram identificados pelo autor, a saber: (3) Organizações Criminosas e (4) Mercenários Cibernéticos. Ambos atuam com finalidade exclusivamente econômica, mas os últimos geralmente vendem suas habilidades técnicas para um propósito específico, enquanto os primeiros são grupos mais permanentes e administram múltiplas atividades ilegais (pornografia infantil, *phishing)* e podem estar vinculados ao Estado.

Os (5) Hacktivistas e (6) Hackers Patriotas, por sua vez, são grupos mais estruturados cujos integrantes têm vínculo ideológico em comum, mas os patriotas possuem forte devoção aos interesses e valores de um país ou nação. Como exemplo, a comunidade *Anonymus* enquadra-se como Hacktivista, ao passo que o Hamas é enquadrado como patriotas. Por último, (7) Hackers Individuais, são indivíduos que possuem conhecimentos e habilidades técnicas para empreender ataques a fim de aferir oportunidades econômicas por meio da caça de *bugs* (*iDefense, Netragard*) e vendê-los ao Estado ou empresas. Esse perfil também inclui pessoas comuns com computadores infectados que acabam transmitindo passivamente malwares para outras máquinas (*botnets* ou zumbis) (BUSSOLATI, 2015).

Por seu turno, os tipos de vítimas foram elencados em: (1) Governos, a partir do objetivo de atingir informações do Estado ou prejudicar infraestruturas críticas; (2) Empresas e Associações, representadas pelas companhias, sociedades, ONGs, Universidades Privadas; (3) Indivíduos, como vítimas de violação de dados pessoais; (4) Governos e Empresas, quando o ataque tem como alvo os dois primeiros; e (5) Todos, quando o ataque consegue atingir múltiplos setores.

Outrossim, no que se refere ao tipo de ataque, utilizamos como base o estudo de Liff (2012). O autor identifica três tipos de ataques a redes de computadores. Os (1) Botnets / Negação de Serviço Distribuída /Ataques (DDoS) que são ataques que inundam de tráfego um grande número de sistemas, alguns deles podendo ter sido sequestrados transformando-se em pequenos robôs projetados para travar ou interromper acesso à rede. Importa destacar que esses ataques têm um custo relativamente baixo, não são complexos, seus efeitos diretos são limitados a interromper o acesso a redes em vez de realizar a destruição dos domínios, bem como podem ocorrer em qualquer rede conectada à Internet.

Nessa esteira, os chamados (2) Malwares básicos (*Basic Malware)* são programas de computador que empregam numerosos meios clandestinos para abrir um ponto de acesso, transmitir dados e / ou perturbar a maneira como os sistemas alvo se comportam. Esses também têm baixo custo, são úteis contra sistemas mal protegidos e usuários não-vigilantes, e são muito comuns na forma de *phishing* e *worms.* Por último, o (3) Malware avançado (*Advanced Malware)*, o qual é capaz de afetar sistemas fortemente defendidos. Esse tipo de ataque requer alto nível de conhecimento para ser projetado e implementado, bem como leva tempo e necessita de

muito recurso financeiro para ser executado. É o caso do *Stuxnet*, cujo potencial para destruir diretamente estruturas físicas ou desativar estruturas críticas específicas é significativo (LIFF, 2012).

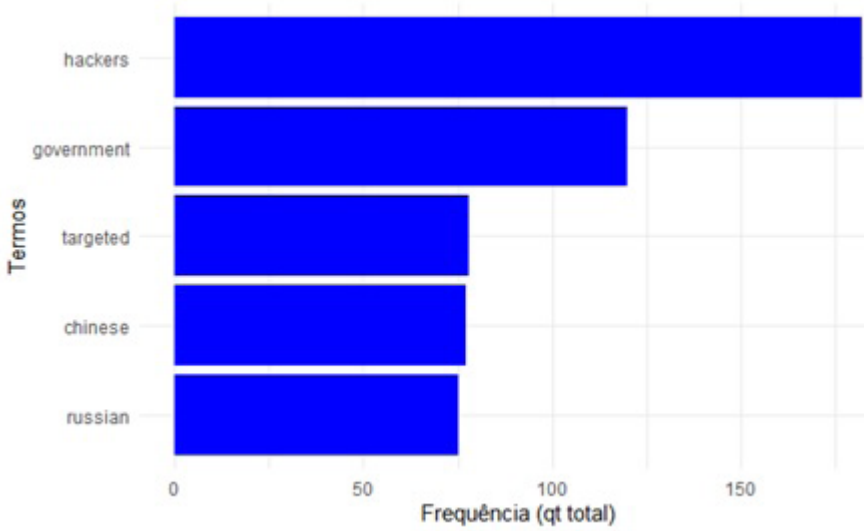
Em relação à análise de dados, optamos por fazer uma análise de conteúdo quantitativa no *software* R do relatório do CSIS, na qual produzimos uma frequência e nuvem de palavras[11]. Essa técnica nos auxilia, de certo modo, a comparar os resultados obtidos pela análise automática do texto com os resultados que foram categorizados para a análise estatística do banco de dados. Assim, nos dando maior embasamento na apresentação e na inferência descritiva dos resultados. A análise de conteúdo com foco quantitativo nos permite atingir resultados sistemáticos na produção de inferência (BARDIN, 1979) e no uso de uma hermenêutica controlada através da dedução (SILVA, FIGUEIREDO FILHO, HENRIQUE, 2015).

Em seguida, analisamos o banco de dados em si, através de estatística descritiva para o mapeamento e identificação das variáveis de interesse do estudo proposto, com auxílio de tabelas e gráficos. Nosso dados foram tabulados no *Microsoft Office Excel* 2016 e analisados no software *Statistical Package for the Social Sciences* - SPSS (versão 24) e no R. Para fins de replicação científica, o banco de dados e o script da análise de conteúdo encontram-se disponível no repositório público OsF[12].

4. Resultados

Esta seção descreve os principais resultados obtidos pela análise descritiva dos dados. Antes de partir para a análise estatística, executamos uma análise de conteúdo, extraindo do arquivo do relatório do CSIS os termos mais comuns ao texto. O gráfico 1 abaixo apresenta os termos mais presentes do relatório.

Gráfico 1 - Frequência dos 5 (cinco) termos mais comuns do relatório '*Significant Cyber Incidents Since 2006*' do CSIS



Fonte: Elaboração dos autores (2020)

Como podemos ver, a análise de conteúdo nos apresenta que: o termo mais comum ao relatório é "*hackers*", totalizando cerca de 182 vezes; seguido pelo termo "*government*" (n=120); pelo verbo em Inglês "targeted" (n=78) e os termos "*chinese*" (n=77) e "*russian*" (n=76). Preliminarmente, essa informação nos revela que o governo é um ator muito frequente no relatório, ou seja, constitui-se como um *player* importante

11 Através do pacote do R "Wordcloud2". Para mais informações, acesse: https://cran.r-project.org/web/packages/wordcloud2/vignettes/wordcloud.html. [Acesso em 27 de Maio 2020] .

12 Disponível em < https://osf.io/sq6he/ > [Acesso em 22 de Março 2021].

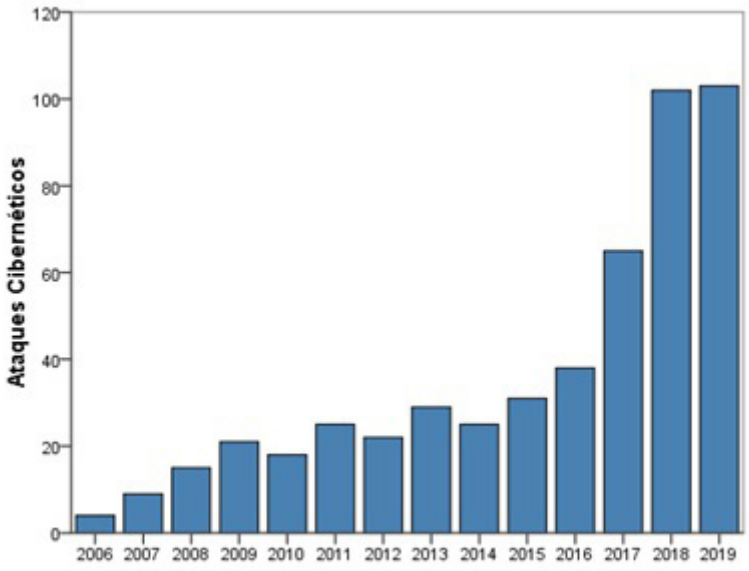
nos ataques cibernéticos, e a indicação que os países com maior frequência envolvidos nos ciberataques são China e Rússia. Desse modo, para uma visualização mais ampla das frequências, a nuvem de palavras abaixo ilustra essa informação com as palavras mais utilizadas no *corpus*.

Figura 1 - Nuvem de Palavras dos Termos mais Comuns do relatório '*Significant Cyber Incidents Since 2006*' do CSIS

Fonte: Elaboração dos autores (2020).

Dada a análise textual do relatório, partimos para análise dos dados em si através da estatística descritiva. O período de análise compreende os anos de 2006 a 2019, e os dados disponíveis no relatório contém 507 casos de ataques registrados. O gráfico 2 abaixo dispõe da frequência de casos de cibercrimes no mundo por ano.

Gráfico 2 - Frequência de Ciberataques no mundo por Ano (2006-2019)

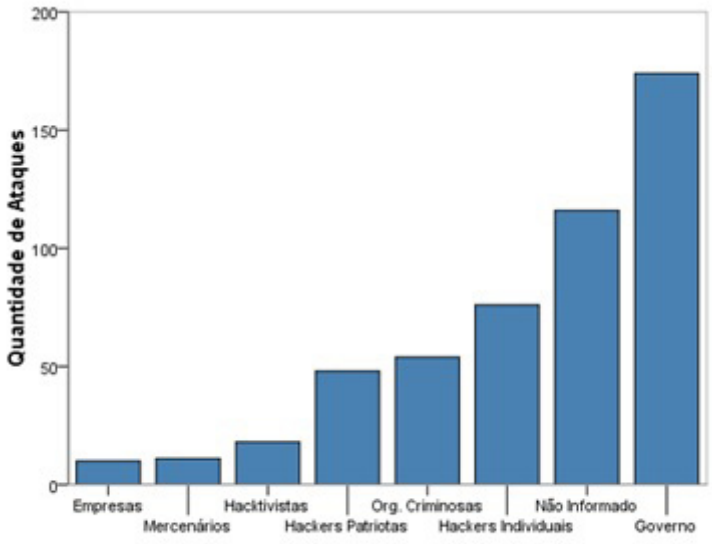


Fonte: Elaboração dos autores (2020).

O gráfico 2 acima apresenta a porcentagem de casos de ciberataques registrados no mundo por ano. Como pode ser visto nos últimos anos, em 2019 (n= 103) e 2018 (n = 102) ocorreram os maiores números registrados, 20,3% e 20,1%, respectivamente, seguidos por 2017 (12,8%) e 2016 (7,5%). É perceptível uma crescente atuação de criminosos ao longo do tempo, que pode ser explicado pela maior conectividade e acesso a ferramentas pelos atores estatais e não-estatais.

O segundo passo foi analisar quais são os tipos de criminosos mais frequentes que atuaram ao longo do período. Para tal, o gráfico abaixo apresenta os possíveis responsáveis pelos ataques à rede.

Gráfico 3 - Frequência dos Possíveis Criminosos Cibernéticos (2006-2019)



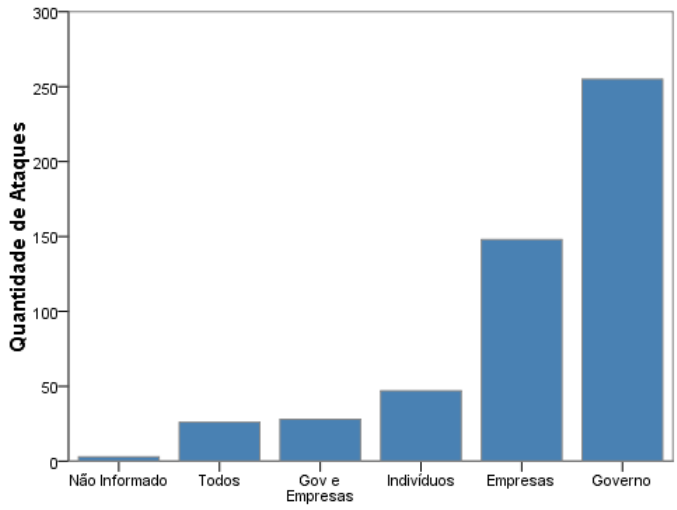
Fonte: Elaboração dos autores (2020).

Temos no gráfico acima a disposição dos possíveis atores com base no relatório do *Center for Strategic & International Studies*. Governo (n=174) aparece com maior número de casos como os principais responsáveis pelos ataques até o momento, contabilizando cerca de 34,2%, seguido pelos casos não informados (n=116), no total de 22,9%, e aos Hackers Individuais o total de 15,%. Por outro lado, os casos menos frequentes foram, respectivamente, Mercenários Cibernético (n=11) com 2,2% e Empresas (n=10) somando 2%.

Acreditamos que os fatores que podem explicar esses resultados relacionam-se com as características do próprio espaço cibernético e das relações internacionais, uma vez que, grande parte dos infratores não puderam ser identificados (caráter furtivo do espaço cibernético) como também a maioria dos países atribui a responsabilidade do crime aos seus principais concorrentes na arena mundial, mesmo sem provas irrefutáveis. Nesse sentido, Kim (2014) ilustra que segurança cibernética é uma preocupação crescente nas relações internacionais, sobretudo pelas tentativas da comunidade de criar uma governança global da *internet,* com o objetivo de fomentar bases para esforços multilaterais de proteção de dados e informações.

Assim como os principais criminosos, se faz pertinente identificar também quais são as principais vítimas das invasões virtuais. A seguir, no gráfico 4, apresentamos as vítimas mais comuns das ações criminosas.

Gráfico 4 - Frequência das Vítimas Identificadas dos Ataques Cibernéticos (2006-2019)



Fonte: Elaboração dos Autores (2020)

As vítimas mais frequentes dos criminosos indicados acima são os Governos (n= 255) contabilizando um total de 50,3%. Ou seja, organismos estatais são os que mais atacam, mas também, os mais afetados entre os criminosos. Seguidos pelas Empresas (n=148) com um percentual de 29,2% e Indivíduos (n=47), que tem seus dados e aparelhos eletrônicos invadidos, somando cerca de 9,3%.

Acredita-se que muitos dos ataques ocorridos possuem algum tipo de finalidade financeira, nos quais os *hackers* buscam vantagem econômica de atores estatais e não-estatais. A tabela 1 abaixo apresenta o percentual de eventos com finalidade financeira encontrados nas ações executadas.

Tabela 1 - Frequência de Crimes com Finalidade Financeira (2006-2019)

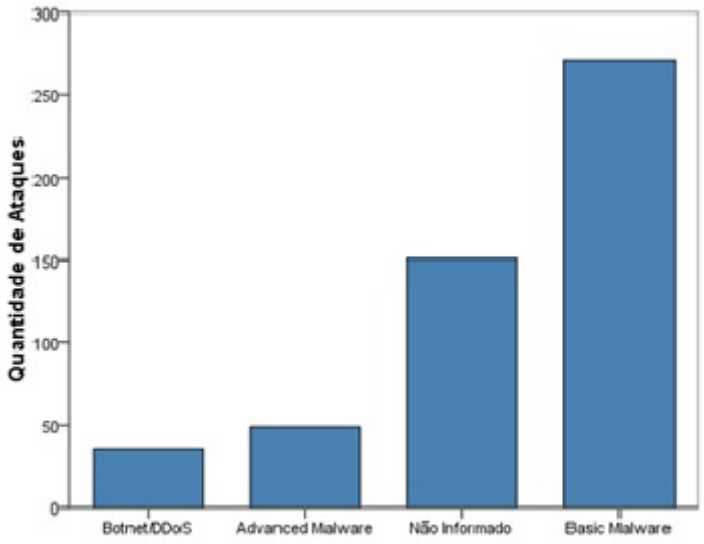
Crime com Finalidade Financeira	N	Percentual (%)
Não	406	80,1
Sim	101	19,9
Total	507	100

Fonte: Elaboração dos Autores (2020).

A tabela 1 acima mostra que, nos ataques cibernéticos registrados até o momento, grande parte deles não apresentam finalidade financeira comprovada (80,1%). Ou seja, eventos com objetivos financeiros e/ou ações empresariais são muito poucos ou não são informados pelos atores envolvidos. Apenas 19,9% das informações disponibilizados tiveram finalidade financeira. Ressalta-se aqui o fato que existe a possibilidade de que os ataques cibernéticos apresentem interesse financeiro velado, o que demonstra outra faceta da dificuldade de traçar o perfil dos ataques cibernéticos.

A seguir, no gráfico 5, apresentamos os tipos de ataques mais recorrentes presentes no banco de dados. Isto é, as táticas mais frequentes utilizadas pelos criminosos para invadir as redes e conseguir atingir seus objetivos.

Gráfico 5 - Frequência dos Tipos de Ataques (2006-2019)



Fonte: Elaboração dos Autores (2020).

A tipificação dos ataques mais comuns utilizados, seguindo a classificação de Liff (2012), até o momento é a de *Basic Malware* (n=271). Esse tipo de ataque contabiliza mais da metade dos registros com 53,5%, seguidos respectivamente por casos que não foram identificados (n=151) contendo 29,8%, *Advanced Malware* (n=49) com 9,7% e *Botnet/DDoS* em último lugar (n=36). Acreditamos que o *Basic malware* foi o mais utilizado, pois ocorrem em maior proporção roubo de dados, abertura de ponto de acesso, transmissão de dados e atividades de ciber-espionagem, que coletam informações de agentes relevantes dos Estados e indivíduos.

Sabe-se que identificar a origem dos ataques é uma tarefa extremamente difícil, uma vez que poucos atores reivindicam as suas autorias, a exemplo dos Hacktivistas. Entretanto, com base nos registro dos eventos disponíveis, encontramos quais foram os países de origem mais frequentes dos ataques. A tabela 2 abaixo apresenta as cinco origens mais frequentes.

Tabela 2 - Frequência dos Cinco Principais Países de Origem dos Ataques Cibernéticos (2006-2019)

País de Origem	N	Percentual (%)
Não Identificado	201	39,6
China	89	17,6
Rússia	80	15,8
Irã	47	9,3
EUA	11	2,2

Fonte: Elaboração dos Autores (2020).

Em razão da dificuldade em identificar a origem dos ataques, grande parte das observações analisadas não foram atribuídas a um Estado em si (n=201) de onde as investidas partiram, totalizando um percentual de 39,6%. Por sua vez, China (n=89) com 17,6% e Rússia (n=80) somando 15,8%, lideram como os países tiveram suas origens descobertas. Isso demonstra, conforme explanado anterior-

mente, a característica furtiva e sorrateira ao novo mecanismo de ataque cibernético.

Apesar de a China apresentar um discurso conciliador no que diz respeito às regras do espaço cibernético como apresentado por Zhang (2012), o país tem trabalhado constantemente para criar uma força moderna e informada capaz de realizar operações cada vez mais informatizadas através do ciberespaço. Desde a década de 1990, esse Estado vem reforçando suas bases militares através da tecnologia da informação para comunicações, inteligência, vigilância e reconhecimento, com o intuito de criar uma capacidade de defesa regional através da cibertecnologia (SPADE, 2012).

Por seu turno, a Rússia tem um histórico de modernização e construção de suas forças para uma possível guerra da informação. O início da experiência russa com ataques cibernéticos começa com a negação de serviço distribuído (DDoS) contra a Estônia, em 2007, que cortou o fluxo de informações da infraestrutura cibernética no país por uma semana. Os próximos ataques notórios também atribuídos à Rússia passam por Geórgia em 2008, com outro ataque DDoS que fez as forças militares da Geórgia não conseguirem manter contato entre si, bem como a Ucrânia, entre 2015 e 2016, através de ataques a empresas de energia distintas, o que se apresentou como uma escalada do uso do cyberpower e da confirmação do poder nacional (SHUYA, 2018).

No que tange ao Irã, Libicki (2015) aponta algumas razões pelas quais o país tem concentrado forças para empreender ataques cibernéticos. Dentre eles, o autor sinaliza que o sistema de governo vigilante, a busca por informação privilegiada e acúmulo de inimigos, a exemplo da Arábia Saudita e notadamente os EUA, são os fatores mais relevantes. Por último, outro país muito sinalizado como responsável por esses tipos de ataques foi a Coreia do Norte. Crawford (2019) argumenta que as capacidades cibernéticas do país são subestimadas pela preocupação da comunidade internacional em relação ao seu poder nuclear. O *Ransomware*[13] *wannacry*, por exemplo, ficou mundialmente conhecido por ter sido bem-sucedido na penetração em computadores que tinham o sistema operacional *Windows* e foi acusado pelos EUA de ter sido promovido pela Coreia do Norte (SANGER, 2017).

Por fim, também é possível mapear quais foram os países que mais sofreram com ataques criminosos no período de 2006 a 2019. A tabela 3 mostra os cinco países mais prejudicados com os ataques cibernéticos

Tabela 3 - Frequência dos Cinco Países Mais Atacados (2006-2019)

País de Origem	N	Percentual (%)
Não Identificado	141	27,8
EUA	135	26,6
Índia	17	3,4
Coreia do Sul	15	3
Ucrânia	14	2,8

Fonte: Elaboração dos Autores (2020).

13 *Ransonware* é um tipo de *malware* que, no caso do ataque *wannacry,* foi capaz de criptografar dados importantes do sistema operacional em troca de vantagem econômica.

Assim como nas origens, os países mais afetados não foram identificados (n=141), o que representa 27,8% dos casos. Devido à complexidade de mensurar os danos em apenas um país ou à falta de elementos comprobatórios, o relatório do *Center for Strategic & International Studies* não consegue identificar o alvo em todos os casos. Em segundo lugar, temos os Estados Unidos (n=135) como a origem mais atacada no período totalizando cerca de 26,6%, o que pode ser explicado pelo fato de ser uma grande potência mundial. Por outro lado, Índia (n=17), Coreia do Sul (n=15) e Ucrânia (n=14) aparecem, respectivamente, com 3,4%, 3% e 2,8% dos casos analisados.

A despeito de não aparecer entre os cinco mais atacados, Zhang (2012) observa que a China também é alvo de graves ataques e que podem ser observados no relatório anual do Centro Nacional de Coordenação da Equipe Técnica de Resposta de Emergência da Rede Nacional de Computadores da China (CNCERT ou CNCERT /CC)[14]. No que tange aos EUA, o país teve destaque tanto como um dos principais ofensores e vítimas desses ataques. Conforme acentuado alhures, esse fenômeno pode estar relacionado com o dilema de segurança aplicado ao espaço cibernético. Com efeito, a anarquia nas relações internacionais torna o ambiente propenso a tensões quando uma nação poderosa passa a armar-se.

Por fim, esse trabalho de cunho descritivo consiste no primeiro passo para conhecimento do objeto de pesquisa e para aprofundamento de trabalhos com inferência causal válidas. Vale salientar que trabalhos descritivos, segundo King, Keohane e Verba (1995), têm um papel central na explicação no processo para inferência sistemática. Além disso, os autores alertam "não é a descrição versus explicação que distingue pesquisa científica de outra pesquisa. E sim, se a inferência sistemática é conduzida de acordo com procedimentos válidos." (KING, KEOHANE, VERBA, 1995, p. 717).

14 CNCERT/CC Annual Report 2012. Disponível em: <https://www.cert.org.cn/publish/english/upload/File/APCERT_Annual2012_CNCERT.pdf>.[Acesso em 27 de Maio 2020].

5. Considerações Finais

A partir dos resultados observados, constatamos que os anos de maior ocorrência de ataques cibernéticos foram 2018 e 2019. Também ficou evidente que o Governo representa o ator que mais empreende ataques no espaço cibernético, assim como o que mais é alvo deles. Identificamos que, assim como os Governos têm papel fundamental no empreendimento de ataques cibernéticos, os Hackers também são personagens muito importantes neste campo já que, entre os atores que puderam ser identificados, estes são responsáveis por grande parte dos ataques. Convergindo, portanto, com a análise de conteúdo textual do próprio relatório que apontava o Governo como um elo central para os ciberataques.

Os ataques cibernéticos foram observados como deveras abrangente, já que as vítimas dos ataques perpassam os Governos, como já citado, Empresas e Indivíduos. Outro aspecto de grande importância é que constatamos que a maior parte dos ataques empreendidos não possuem finalidade financeira que possa ser comprovada.

Outrossim, constatamos que entre as fontes de ataques cibernéticos, os quatro países que mais concentraram essa atividade (China, Rússia, Irã, EUA) coincidem com o mapa de 2009 da *McAfee* da Guerra Fria Cibernética, ao passo que os mais atacados (EUA, Índia, Coreia do Sul, Ucrânia) têm conflitos mais claros no âmbito das relações internacionais nos tempos atuais. Como exemplo, cita-se o conflito Rússia-Ucrânia pela região da Crimeia, China-EUA pela disputa de poder

global e guerra comercial, e Irã-EUA com foco geopolítico e mútuas retaliações. Conforme analisado, as vulnerabilidades das redes podem permitir que segredos de Estado, informações comerciais secretas e dados pessoais sensíveis sejam acessados e violados com relativo baixo custo (MCAFEE, 2009).

No que tange às limitações, observamos que o cibercrime é extremamente difícil de ser mensurado com precisão. O ciberespaço tem dimensões intangíveis, é excessivamente descentralizado para aquilatar, acompanhar e relatar com certeza toda a sua atividade criminosa, tornando-se difícil estimar uma ordem de grandeza da cibercriminalidade. Isso se relaciona ao fato de que os governos não divulgam este tipo de informação por receio de macular a sua reputação internacional (MUGGAH et al., 2014). Ainda sobre esse aspecto, observamos uma grande omissão de dados (ou atores não identificados) referentes aos alvos e os possíveis criminosos, o que pode ser reflexo da não divulgação de dados sobre este tipo de crime por motivos também estratégicos (LIFF, 2012).

É imprescindível pontuar também que nosso estudo possui algumas limitações de cunho metodológico, mas que não impossibilita a compreensão dos resultados aqui apresentados. Primeiro, a construção do banco de dados se deu por caráter manual de cada evento apresentado no relatório do CSIS, que, por ventura, pode apresentar algum tipo erro de categorização. Recomenda-se, para uma versão futura, fazer uma categorização automática por meio de *machine learning* para eliminar ou diminuir qualquer tipo de viés. Segundo, por se tratar de um estudo apenas descritivo, não se pode fazer qualquer tipo de inferência causal mais profunda, assim como, mecanismos causais pela complexidade da identificação do objeto. Por fim, é recomendável a adição de outras fontes ou banco de dados sobre tema para fins de comparação e obtenção de robustez aos resultados.

Apesar das limitações, acreditamos que os resultados são relevantes para colaborar com os estudos de Segurança e Defesa nas Relações Internacionais, na medida em que corroboramos com a literatura acerca do aumento da frequência de crimes cibernéticos ao longo dos anos. Também demonstramos a característica furtiva desses ataques, por meio da categorização dos perfis identificados que participam dessas atividades. Em razão dessa multiplicidade de atores, dificilmente é possível apontar de modo contundente a autoria dos ataques, o que desafia a comunidade internacional em fomentar qualquer arcabouço legal ao seu combate.

Por conseguinte, assim como afirma Muggah et al (2014), os dados sobre ataques cibernéticos podem proporcionar alguma visão das grandes tendências capazes de determinar as prioridades, assim como as questões sobre a alocação de recursos dos governos. Sugerimos, para agendas de pesquisas futuras, que as motivações e resultados destes ataques sejam analisados de forma minuciosa para que possamos compreender a linha de atuação destes países quando se trata de ciberguerra.

Além disso, outro ponto relevante para os próximos estudos refere-se ao aproveitamento de contextos de crise por criminosos virtuais para praticarem ataques. A partir do momento em que as atenções dos governos estão dirigidas para outras áreas prioritárias, a quantidade de crimes cometidos é potencializada decorrente da vulnerabilidade do setor cibernético (SILVA, LOPES, 2020). Assim, a exemplo da atual crise de segurança sanitária decorrente do novo Coronavírus (SARS-CoV-19), no qual houve um aumento em 450% no número de ataques cibernéticos a instituições do governo, empresas, entre outros, contextos de adversidades futuras podem sinalizar o crescimento dos crimes e a necessidade de reforço nas políticas e ações de prevenção, inovação e resiliência para o setor (BREWSTER, 2020).

REFERÊNCIAS BIBLIOGRÁFICAS

BARDIN, Laurance. (1979), *Análise de conteúdo*. Lisboa, Edições 70.

BRASIL. Ministério da Defesa (2015), *Glossário das Forças Armadas.* 5.ed. Brasília, DF.

BREWSTER, Murray. (2020), "*All-volunteer cyber civil defence brigade assembles to fight COVID-19 hackers*", CBC News, 24 de Maio. Disponível em: <https://www.cbc.ca/news/politics/covid19-cyber-companies-1.5508570> Acesso em 27 de Abril de 2020.

BUCHANAN, Ben. (2017), *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.* New York, Oxford University Press.

BUSSOLATI, Nicolo. (2015), "The rise of non-state actors in cyberwarfare". in OHLIN, Jen, GOVERN, Kevin, FINKELSTEIN, Claire(eds). *Cyberwar: Law and Ethics for Virtual Conflicts*. Oxford, Oxford University Press.

BUZAN, Barry, WÆVER, Ole, WILDE, Jaap de. (1998), *Security: A New Framework for Analysis.* London, Boulder.

CARLIN, John, GRAFF, Garrett. (2018), *Dawn of The Code War. America's Battle Against China, Russia and the Rising Global Cyber Threat.* New York, Public Affairs.

CRAWFORD, Ali. (2019), ***Assessing North Korea's Cyber Evolution***. Disponível em:< https://www.realcleardefense.com/articles/2019/11/25/assessing_north_koreas_cyber_evolution_114869.html>. Acesso em: 10 de Maio de 2020.

CSIS, Center for Strategic & International Studies. (2020), *Significant Cyber Incidents*. Washington. Disponível em: <www.csis.org/programs/technology-policy-program/significant-cyber-incidents> Acesso em 20 de Janeiro de 2020.

DOUZET, Frederick. (2014), "Understanding Cyberspace with Geopolitics", *Hérodote* vol. 152-153, no. 1: 3–21.

FIGUEIREDO FILHO, Dalson, PARANHOS, Ranulfo, ROCHA, Enivaldo Carvalho da. (2013), "A importância da Replicabilidade na Ciência Política: O Caso da SIGOBR", *Revista Política Hoje,* vol. 22, no. 2: 213-230.

GÓRKA, Marek. (2018), "Cyberconflicts as a threat for the modern state", *Computer Science and Informal Technology,* vol. 6, no. 1: 11-20.

HANSEN, Lene, NISSEMBAUM, Helen. (2009), "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly,* vol. 53, no. 4: 1155–1175

HARE, Forrest. (2010), "The Cyber Threat to National Security: Why can't we agree?". *Conference on Cyber Conflict. Tallin*, Estonia. 15-18 de Junho. Disponível em: <https://ccdcoe.org/uploads/2018/10/Hare-The-Cyber-Threat-to-National-Security-Why-Cant-We-Agree.pdf> Acesso em 25 de Maio de 2020.

HERZ, John H..(1950). "Idealist Internationalism and the Security Dilemma". ***World Politics***, vol. 2, no. 2: 157-180.

JUNIO, Timothy. (2013), "How probable is cyberwar? Bringing IR Theory back in to the cyber conflict debate". *Journal of Strategic Studies,* vol. 36, no. 1: 125-133.

KELLO, Lucas. (2013), "The Meaning of Cyber Revolution. Perils to Theory and StateCraft". *International Security,* vol. 38, no. 2: 7-40.

KEOHANE, Robert, NYE, Joseph. (1998), "Power and Interdependence in the Information Age". *Foreign Affairs*. Setembro/Outubro. Disponível em: <https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age> Acesso em 02 de Maio de 2020.

KUEHL, Dan. (2009), "From Cyberspace to Cyberpower: Defining the Problem", in KRAMER, Franklin D., STARR, Stuart H., WENTZ, Larry (eds.), *Cyberpower and National Security.* Lincoln, University of Nebraska Press: 24–42

KIM, Sanbae. (2014), "Cyber security and middle power diplomacy: a network perspective". *The Korean Journal of International Studies,* vol. 12, no. 2: 323- 352.

King, Gary, KEOHANE, Robert O., VERBA, Sidney. (1994), *Designing social inquiry: Scientific inference in qualitative research*. Princeton, Princeton University Press.

KING, Gary. 2015, "Replicação, Replicação". *Revista Eletrônica de Ciência Política,* vol. 6, no. 2: 382-401.

LIBICKI, Martin C. (2007), *Conquest in Cyberspace. National Security and Information Warfare.* Cambridge, Cambridge University Press.

_____. (2009), *Cybersecurity and Cyberwar.* Santa Monica, Rand Corporation. Disponível em: <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf> Acesso em 20 de Maio de 2020.

_____. (2015), "Iran: A rising Cyber Power?" *The Rand Blog.* 16 de Dezembro. Disponível em: <https://www.rand.org/blog/2015/12/iran-a-rising-cyber-power.html> Acesso em 20 de Maio de 2020.

LIFF, Adam. (2012), "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War". *Journal Of Strategic Studies,* vol. 35, no. 3: 401-428.

LOBATO, Luisa, KENKEL, Kai Michael. (2015), "A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra". *Contexto Internacional* , vol. 37, no. 2: 629- 660.

MANJIKIAN, Mary M. (2010), "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik". *International Studies Quarterly*, vol. 54, no. 2: 381-401

MCAFEE. (2009), *Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare*. Disponível em: <https://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf> Acesso em 25 de Janeiro de 2020.

MCGRAW, Gary. (2013), "Cyber War is inevitable (unless we build security in)". *Journal of Strategic Studies,* vol. 36, no. 1: 109-119.

MEDEIROS, Breno Pauli, CARVALHO, Alessandra Cordeiro, GOLDONI, Luiz Rogério Franco. (2019), "Uma análise sobre o processo de securitização do ciberespaço". *Coleção Meira Mattos,* vol. 13, no. 46: 45-66.

MUGGAH, Robert, GLENN, Misha, DINIZ, Gustavo. (2014), "Securitização da cibersegurança no Brasil". *Cadernos Adenauer***,** vol. 15, no. 4: 69-109.

OBAMA, Barack. (2012), "Taking Cyberattacks seriously". *Wall Street Journal.* 19 de Julho. Disponível em:<https://www.wsj.com/articles/SB10000872396390444330904577535492693044650> Acesso em 20 de Maio de 2020.

RATTRAY, Gregory J. (2009), "An environmental approach to understanding cyberpower". in: KRAMER, Franklin D., STARR, Stuart H., WENTZ, Larry(eds.), *Cyberpower and National Security.* Lincoln, University of Nebraska Press: 253-274

RID, Thomas. (2012), "Cyber War Will Not Take Place". *Journal of Strategic Studies,* vol. 35, no. 1: 5-31.

SANGER David E. (2017), "U.S. Accuses North Korea of Mounting WannaCry Cyberattack". *The New York Times.* 18 de Dezembro. Disponível em: <https://www.nytimes.com/2017/12/18/us/politics/us-north-korea-wannacry-cyberattack.html> Acesso em 20 de Maio de 2020.

_____. (2018), *The Perfect Weapon. War, Sabotge and Fear in the Cyberspace.* New York, Crown.

SANTOS, Coriolano Aurélio de A. C., MONTEIRO, Renato Leite. (2010), *Estruturas Críticas: o próximo alvo*. São Paulo, OAB/SP.

SILVA, Júlio Cezar Barreto Leite da. (2014), "Guerra Cibernética: A Guerra No Quinto Domínio, Conceituação e Princípios". *Revista Escola de Guerra Naval,* vol. 20, no. 1: 193 – 211.

SILVA, Dáfni Priscila Alves da, FIGUEIREDO FILHO, Dalson Britto, HENRIQUE, Anderson. (2015), "O poderoso NVivo: uma introdução a partir da análise de conteúdo". *Revista Política Hoje* vol. 24, no. 2: 119-134.

SILVA, André Lucas Alcântara da; VILAR-LOPES, Gills. (2020), ***Overview dos casos de ataques cibernéticos durante a pandemia de COVID-19***. Disponível em: https://redectidc.com.br/rede-ctidc-covid-19-overview-dos-casos-de-ataques-ciberneticos-durante-a-pandemia.html. Acesso em: 20 maio 2020.

SHUYA, Mason. (2018), "Russian Cyber Aggression and the New Cold War". *Journal of Strategic Security,* vol. 11, no. 1: 1-18.

SMEETS, Max, SHIRES, James. (2017), *Contesting Cyber.* New York, New America Org.

SPADE, Colonel Jayson M. (2012), *China's Cyber Power and America's National Security*. Carlisle, United States Army.

STONE, John. (2013), "Cyber War Will Take Place!". *Journal of Strategic Studies,* vol. 36, no. 1: 101-108.

TADDEO, Mariarosario. (2018), "How to Deter in Cyberspace". *The European Centre of Excellence for Countering Hybrid Threats,* no. 6: 1–10.

WALKER, Christopher, LUDWIG, Jessica. (2017), "The Meaning of Sharp Power. How Authoritarian States Project Influence". *Foreign Affairs*, 17 de Novembro. Disponível em: <https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power> Acesso em 02 de Maio de 2020.

WENDT, Emerson. (2011), "!Ciberguerra, Inteligência Cibernética E Segurança Virtual: alguns aspectos!". *Revista Brasileira de Inteligência*. vol. 6: 15-26 .

WORLD ECONOMIC FORUM. (2020), *The Global Risks Report 2020*. Suíça, World Economic Forum.

ZHANG, Li. (2012), "A Chinese perspective on cyber war". *International Review of the Red Cross,* vol. 94, no. 886: 801-807.