UNIVERSIDADE FEDERAL DO PAMPA
CAMPUS SANTANA DO LIVRAMENTO
BACHARELADO EM RELAÇÕES INTERNACIONAIS

ELISA MARIA WOEHL DE ANDRADE

SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DAS CONSEQUÊNCIAS GERADAS POR ATAQUES *HACKERS* DENTRO DO SISTEMA INTERNACIONAL

Santana do Livramento
2023

ELISA MARIA WOEHL DE ANDRADE

SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DAS CONSEQUÊNCIAS GERADAS POR ATAQUES *HACKERS* DENTRO DO SISTEMA INTERNACIONAL

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Federal do Pampa, como requisito parcial para a obtenção do Título de Bacharel em Relações Internacionais.

Orientador: Prof. Dr. Renatho José da Costa.

Santana do Livramento

2023

ELISA MARIA WOEHL DE ANDRADE

SEGURANÇA CIBERNÉTICA: UMA ANÁLISE DAS CONSEQUÊNCIAS GERADAS POR ATAQUES *HACKERS* DENTRO DO SISTEMA INTERNACIONAL

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Federal do Pampa, como requisito parcial para a obtenção do Título de Bacharel em Relações Internacionais.

Trabalho de Conclusão de Curso defendido e aprovado em 27 de novembro de 2023.

Banca Examinadora:

Prof. Dr. Renatho José da Costa

(Orientador)

UNIPAMPA

Prof. Dr. Flávio Augusto Lira Nascimento

(Membro da Banca)

UNIPAMPA

Prof. Dra. Leticia Britto dos Santos

(Membro da Banca)

UNIPAMPA

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

A553 Andrade, Elisa Maria Woehl de
Segurança cibernética: uma análise das consequências geradas por ataques hackers dentro do sistema internacional / Elisa Maria Woehl de Andrade.
92 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, RELAÇÕES INTERNACIONAIS, 2023.
"Orientação: Renatho José da Costa".

1. ataques cibernéticos. 2. hard power. 3. neorrealismo. I. Título.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer aqueles que, sem eles, nada disso seria possível. Helena e Sebastião, meus pais, que me fizeram a pessoa que sou hoje, que sempre trabalharam muito duro para que eu pudesse estar onde estou hoje. Obrigada por tudo que vocês sempre fizeram por mim, obrigada por confiarem em mim, obrigada por me proporcionarem estudar tão longe do ninho familiar e evoluir como pessoa, obrigada por toda a minha vida, amo vocês. Também gostaria de agradecer ao Nikolas, meu namorado, por me acompanhar durante esses anos e me dar forças em momentos difíceis, sempre me apoiando. À Heloise, minha irmã do coração, agradeço por todas as conversas que me fizeram ficar mais confiante com o meu processo, e por todas as experiências compartilhadas nesses anos. Ainda, uma pequena dedicatória à minha cachorrinha, que nos deixou após treze anos, mas que com todo o amor que só um cachorro pode proporcionar, ela sempre esteve presente, pronta para encher meu coração de alegria.

Dentro da Unipampa, por esses anos, estive em contato com diversas pessoas, e agora, agradeço àqueles amigos que marcaram presença nesse tempo, e que pretendo levar para a vida. Ana e Jéssica, agradeço por todas as risadas e longas conversas que sempre fizeram meu dia melhor, espero poder estar com vocês durante outras fases da vida. À Jociely, pelas idas ao mercado, churros e sorvete na praça e pela parceria nos trabalhos. À Maria Fernanda, pela cumplicidade nessa jornada e àqueles outros, Irina, Carolina e Gabriel que estiveram juntos comigo durante essa jornada. Também gostaria de agradecer aos professores do curso, que me proporcionaram uma bagagem grande de conhecimento, que vou levar para a vida. Ao meu orientador, que me ajudou durante todo esse processo, que sempre esteve disposto a sanar as minhas dúvidas e que me ajudou a colocar o tema deste trabalho em prática. À Unipampa pela estrutura que me proporcionou chegar até aqui, a um passo da conclusão do curso de Relações Internacionais.

RESUMO

A presente pesquisa visa estabelecer a relação entre ataques cibernéticos e o poder do Estado, isto é, analisar se ataques cibernéticos podem alterar o status quo de um Estado no sistema internacional "tradicional" de forma que seu *hard power* seja superado. Para tal, fez-se uso da teoria neorrealista de Kenneth Waltz de maneira a estabelecer um modelo para o entendimento de sistema internacional "tradicional", assim como, no intuito de compreender alguns conceitos existentes dentro do meio cibernético, procurou-se explicar e definir a cibersegurança e o ciberespaço, baseando-se em diversos autores da área, de modo que possa ficar claro a interação existente no meio cibernético. A partir desses referenciais, analisou-se os impactos de ataques cibernéticos em três casos, o caso ocorrido na Estônia em 2007, outro que aconteceu no Irã em 2010 e, por fim, um caso mais recente ocorrido na Costa Rica em 2022. Essa análise objetivava compreender a extensão dos danos dos ataques cibernéticos apresentados e, por conseguinte, se estes danos poderiam reverberar de modo a alterar o status quo dos Estados alvejados. Com isso, pôde-se testar a hipótese levantada, qual seja, de que status quo dos Estados não é alterado, pois o poder se baseia no *hard power*, e este não é afetado em ataques ocorridos no meio cibernético. Para a realização da pesquisa optou-se pela metodologia qualitativa, utilizada de forma a aprofundar os conhecimentos sobre as organizações hackers. Também, optou-se por uma pesquisa de caráter exploratório, na qual busca-se estabelecer familiaridade com a problemática apresentada e estabelecimento de hipóteses. Com base nessa problemática e metodologia, o trabalho chegou à confirmação da hipótese levantada, onde compreende-se que o *hard power* de um Estado não é superado pelos ataques cibernéticos, assim como este último não apresentou riscos efetivos e alterações significativas para a soberania territorial dos Estados analisados.

Palavras-chave: ataques cibernéticos; *hard power*; neorrealismo.

ABSTRACT

This research aims to establish the relation between cyber attacks and a State's power, that is, analyze if cyber attacks can alter a State's status quo within the international system to the point of overcoming its hard power. For such, Kenneth Waltz's neorealist theory was used in a way to establish a model of the international system, as well as cyber concepts such as cyberspace and cybersecurity so the cyber leveled interaction could be comprehended. From these references, the impact of cyber attacks were analyzed considering three cases, the estonian attack in 2007, the iranian attack in 2010, and the most recent cyber attack in Costa Rica, which happened in 2022. This analysis aimed to understand the damage extension of the presented cyber attacks and therefore, if these damages can modify the affected States status.Therewith, the hypothesis of this research could be raised, and that is, a State's status cannot be altered by cyber attacks, but only through hard power. Thus, to carry out this research, the chosen methodology was qualitative, so the knowledge about hackers could be deepened. Also, the character of this research was exploratory, in which seeked to establish familiarity with the presented problematic, as well as setting hypotheses. Based on the problematic and methodology established before, this research confirmed the hypothesis, and therefore, the obtained results show that cyber attacks are not capable of surpassing the three analyzed State's hard power, nor presented effective risks for these State's territorial sovereignty.

Keywords: cyber attacks; hard power; neorealism.

LISTA DE GRÁFICOS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

APT - Advanced Persistent Threat

APWG - Anti-Phishing Working Group

CERT - Computer Emergency Response Team

CSNU - Conselho de Segurança das Nações Unidas

DDoS - Distributed Denial of Service

DoS - Denial of Service

IAEA - Agência Internacional de Energia Atômica

IP - Internet Protocol

JCPOA - Joint Comprehensive Plan of Action

OTAN - Organização do Tratado do Atlântico Norte

PIB - Produto Interno Bruto

RaaS - Ransomware as a Service

SaaS - Software as a Service

SQL - Structured Query Language

TNP - Tratado de Não-Proliferação Nuclear

SUMÁRIO

1 INTRODUÇÃO

Os Estudos de Segurança Internacional, com sua ênfase no pós-Segunda Guerra Mundial, acabaram por focar a perspectiva militar, enfatizando temas como o Estado, autoridade, política e soberania. No entanto, ao longo do tempo, os Estudos de Segurança Internacional se expandiram e, atualmente, englobam outros fatores como meio ambiente, saúde, economia e a tecnologia (BUZAN; HANSEN, 2009). Apesar da ampliação do escopo analítico, a Segurança Cibernética tornou-se um ramo da segurança internacional que, diferentemente de outros temas atuais, somente foi incorporada à sua agenda a partir do século XXI. Portanto, além de tratar-se de um tema atual, a cibersegurança também necessita de constantes revisões e atualizações, devido às novas tecnologias que vão surgindo ao longo do tempo (MESQUITA, 2019). Ainda, a cibersegurança "abrange uma ampla gama de aspectos técnicos, organizacionais e de governança. [...] Ela vai muito além dos detalhes da criptografia, *firewalls, software,* antivírus e ferramentas técnicas de segurança" (Veale; Brown, 2020, p. 2, tradução nossa).

Desse modo, as últimas décadas são um período importante de se analisar para entender seu impacto nas guerras mais recentes. Diferentemente dos armamentos e das guerras tradicionais, a ciberguerra não está restrita a determinados atores do sistema internacional, uma vez que a capacidade de ataque a estruturas críticas no meio cibernético pode ser realizada por quaisquer atores. Logo, com a dependência da tecnologia, ataques cibernéticos podem ser capazes de paralisar sociedades inteiras (Greathouse, 2014). Dessa forma, ao adentrar ao mundo da cibersegurança, encontra-se o ciberespaço, que é um ambiente de informações, onde elas podem ser armazenadas, compartilhadas e criadas e, dessa forma, configura um espaço quase abstrato, onde a noção geral de espaço como algo físico se dissolve (SINGER; FRIEDMAN, 2014). Além disso, já se observa possíveis implicações políticas relacionadas ao ciberespaço, uma vez que é um ambiente sem limites territoriais, também se observa que é um espaço sem exato controle de quem transmite, e sobre o que está sendo transmitido nesse ambiente (CHOUCRI, 2012). Desse modo, dentro desse espaço criam-se comunidades, ou seja, atores reais que se relacionam através do ciberespaço. No entanto, ao afunilar essas organizações, encontram-se os grupos de *Advanced Persistent Threat (APT),* onde, através de um alvo específico e com intenções específicas, ataques são demoradamente planejados, consistindo em várias fases e demasiada preparação. Em geral, os ataques são direcionados a grandes alvos e seus *malwares* são bastante sofisticados, podendo gerar danos consideráveis a um país (SINGER;

FRIEDMAN, 2014). Destacam-se três casos nos quais ataques *hackers* APT são bem exemplificados, o caso iraniano Stuxnet (2010), o caso estoniano em 2007, e um caso recente na Costa Rica (2022).

No caso iraniano, um *worm* intitulado Stuxnet foi introduzido nos computadores da instalação nuclear de Natanz, causando rapidamente a falha das centrífugas e, como consequência ao Estado iraniano, um atraso considerável em seu programa nuclear (COLLINS; McCOMBIE, 2019). Já no caso da Estônia, o país sofreu uma série de ciberataques em 2007, fazendo com que os sistemas governamentais ficassem fora do ar, gerando diversas consequências ao país (HERZOG, 2011). Por fim, há o caso mais recente, em 2022, da Costa Rica, no qual, através de um *ransomware*, instituições públicas governamentais foram infectadas, gerando caos e crise, em um país que sempre se amparou na paz e na tranquilidade (CANO, 2022).

O estudo da segurança cibernética e o ciberespaço, assim como o que acontece nesse meio, se fazem necessários pelo fato de a internet ter se tornado, de modo não convencional, um novo campo de batalha. Desse modo, o equivalente de armamentos dentro do ciberespaço se encontra em diversos códigos maliciosos que têm o poder de danificar ou falhar aparatos tecnológicos de uso dos Estados (MARTINS, 2012). Além disso, necessita-se conhecer e entender de maneira mais aprofundada o espaço no qual se dão esses conflitos, uma vez que são questões bastante novas e atuais, ou seja, havendo demasiado desconhecimento sobre esse novo campo. Portanto, no que diz respeito às relações internacionais, se configura um tema importante de modo que torna-se uma variável crucial quando há a necessidade de tomada de decisões por parte dos atores internacionais, assim como para a política internacional contemporânea (MESQUITA, 2019).

Em relação a metodologia, de acordo com Gerhardt e Silveira (2009), a pesquisa qualitativa preocupa-se em aprofundar a compreensão de um grupo social ou organização, visto neste trabalho através do esquadrinhamento de organizações *hackers* e sua dinâmica com os Estados e o sistema internacional. Também é de caráter qualitativo a "hierarquização das ações de descrever, compreender, explicar" (p. 32). Além disso, Gerhardt e Silveira, ao falar sobre a pesquisa, apontam também a natureza da mesma, e então, este trabalho seguirá a natureza básica, que de acordo com os autores, "objetiva gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática prevista" (2009, p. 34). Outrossim, essa pesquisa tem objetivo de caráter exploratório, que, segundo Gil (2002), são pesquisas que buscam maior familiaridade com

um problema de modo a construir hipóteses. Portanto, será através do método de procedimento bibliográfico, onde dar-se-ão pela busca das bibliografias disponíveis, tanto primárias quanto secundárias. Então, o método científico irá tratar-se do hipotético-dedutivo, que contribuirá para a pesquisa através da comprovação ou do falseamento da hipótese apresentada no trabalho.

Sendo assim, o problema de pesquisa apresentado para esse trabalho é: os ataques cibernéticos promovidos por organizações *hackers* não estatais poderiam fragilizar um Estado de modo a superar seu *hard power* e mudar a sua dinâmica de poder dentro do sistema internacional tradicional? Para tal, trabalhar-se-á com a hipótese de que esses ataques cibernéticos que advém de organizações *hackers* não teriam a capacidade de alterar o *status* de um Estado no sistema internacional tradicional, portanto, a dinâmica de poder de um Estado estaria condicionada ao seu *hard power*, isto é, onde os embates entre os Estados se dão de modo mais efetivo, e que, somente ali poderiam ocorrer danos à soberania territorial de um país. Além disso, objetivar-se-á neste trabalho analisar as ações de organizações *hackers* dentro do meio cibernético e quais as suas implicações para a soberania estatal, assim como compreender o papel dos atores estatais no sistema internacional tradicional a partir da perspectiva neorrealista de Kenneth Waltz. Ademais, também é previsto entender como as organizações *hackers* se inserem no contexto internacional e se tornam um risco para o Estado. Desse modo, entende-se que os três casos que serão descritos irão auxiliar o cumprimento da pergunta, hipótese e objetivos apresentados. Para testar a hipótese apresentada e alcançar os objetivos propostos, o trabalho se encontra dividido, em um primeiro momento, pela parte teórica, onde utilizar-se-á da teoria neorrealista de Waltz para que possa ser estabelecido um modelo para o sistema internacional, além da explicação de conceitos relacionados ao mundo cibernético. Desse modo, o trabalho segue com a apresentação dos três casos de ataque cibernético, para que, através desses exemplos, seja possível verificar a veracidade das consequências desses ataques para os Estados no sistema internacional.

2 NEORREALISMO E CIBERSEGURANÇA

2.1 A estrutura do Sistema Internacional neorrealista de Kenneth Waltz

Em sua obra Theory of International Politics, Kenneth Waltz traz diversos aspectos relacionados a teorias e estruturas políticas. Dessa forma, abordar-se-á neste ponto a Teoria Sistêmica proposta por Waltz e suas observações a respeito do assunto.

Desse modo, ele inicia as suas próprias reflexões acerca de leis e teorias. Para Waltz, uma teoria é "uma imagem, formada mentalmente, de um reino limitado ou domínio de uma atividade"[1] (Waltz, 1979, p. 8, tradução nossa). Portanto, em uma teoria, uma área é isolada de todas as outras para que possa ser feita sua análise e, esse isolamento é requisito fundamental para que uma teoria seja, de fato, uma teoria. Além disso, um isolamento de uma área precisa ser útil e não tão somente realista. Para Waltz (1979), as teorias relativas à política internacional são fracas, onde são utilizados os mesmos termos para se referir a questões diferentes e, desse modo, tornando a compreensão limitada.

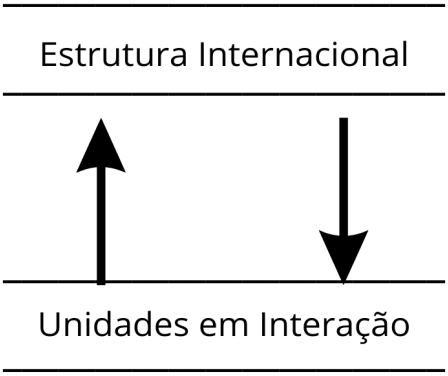
Também, ao falar de diferentes abordagens teóricas, Waltz (1979) compreende que caminhar através de outras teorias é necessário de modo a entender o porquê de o modelo sistêmico ser melhor encaixado. A partir disso, têm-se as teorias reducionistas, onde pode-se entendê-la através do "esforço feito para entender a política internacional por meio de estudos sobre as burocracias nacionais particulares"[2] (Waltz, 1979, p. 18, tradução nossa). Portanto, a falta de capacidade das teorias de política internacional em apresentar boas explicações e orientações mais úteis, tendem a tornar a busca pela abordagem reducionista maior. No entanto, as teorias com abordagens reducionistas não seriam ideais para o estudo da política internacional, o que não implica que essa abordagem não possa ser utilizada e, também, isso não significa que o geral deve ser explicado sem ter como referência às condições internas (Waltz, 1979).

A análise se estende também às abordagens sistêmicas contidas em certas teorias da política internacional. Para tal, necessita-se uma breve explicação sobre sistema, que é tido como um conjunto de unidades que estão em interação. Desse modo, "um sistema consiste em uma estrutura, e a estrutura é o componente a nível de sistemas que torna possível pensar nas unidades

[1] A theory is a picture, mentally formed, of a bounded realm or domain of activity.
[2] The effort to understand international politics by studying national bureaucrats and bureaucracies.

formando um conjunto distinto do que uma mera coleção”[3] (Waltz, 1979, p. 40, tradução nossa). Portanto, em uma teoria sistêmica a intenção é mostrar como dois níveis interagem entre si, para que uma unidade A possa afetar ou ser afetada por outra unidade B, elas precisam estar totalmente distintas uma da outra. Dessa forma, para que uma abordagem ou teoria possa ou não ser considerada sistêmica, se faz necessário que dentro dessa explicação esteja contida a distinção entre o nível dos sistemas e o nível das unidades em interação. Também se faz necessário que as definições da estrutura não abriguem questões relativas à interação entre as unidades. Para que uma abordagem sistêmica seja transformada em uma teoria são necessárias melhores especificações, como a relação entre forças e efeitos podem mudar de um sistema para o outro, também expressar quais unidades estão compreendidas dentro do sistema. A figura 1 demonstra como uma abordagem sistêmica vê o sistema internacional político.

Figura 1 – Abordagem Sistêmica



Fonte: Waltz (1979, tradução nossa).

Desse modo, embora as teorias reducionistas e as teorias sistêmicas trabalhem com vários níveis de eventos, o que as define como uma ou outra é, é a forma que seus materiais são organizados. Então, o que as teorias reducionistas usam para a explicação dos resultados internacionais vem de elementos que estão localizados a níveis subnacionais ou nacionais. No entanto, “não dá para concluir a condição política internacional a partir da composição interna dos Estados”[4] (Waltz, 1979, p. 64, tradução nossa). Além disso, o comportamento dos Estados e de seus líderes não pode ser previsto, ou seja, é indeterminado. Desse modo, como poderiam

[3] A system consists of a structure, and the structure is the systems-level component that makes it possible to think of the units as forming a set as distinct from a mere collection.
[4] One cannot infer the condition of international politics from the internal composition of states.

teorias dentro da política internacional serem construídas, haja vista que deve-se analisar comportamentos que não são possíveis de determinar? Para Waltz, chegar a essa possível resposta pode ser possível através da Teoria Sistêmica. Dessa forma, nas ciências sociais deve-se assumir que as explicações e as previsões contidas em uma teoria serão gerais.

Uma estrutura é vista como um conceito estático e quase vazio. Na verdade, uma estrutura pode parecer estática por, geralmente, ser muito duradoura e, mesmo que continue exatamente a mesma, ainda existem dinâmicas dentro dela. Dessa maneira, as dinâmicas de uma estrutura alteram o comportamento dos atores e, alterando seus comportamentos, elas afetam o resultados das suas interações. Além disso, "dentro de uma estrutura durável, torna-se fácil negligenciar os efeitos estruturais porque são sempre os mesmos. Portanto, é esperado que sempre se obtenha a mesma variedade de resultados como consequência das ações dos Estados estando em uma condição anárquica"[5] (Waltz, 1979, p. 70, tradução nossa). Todavia, isso não representa uma falta de importância das mudanças que, de fato, ocorrem fora do que é esperado, afinal, algo que é recorrente ajuda a identificar e explicar os padrões e as características que a política internacional concentra. Além disso, o conceito de estrutura como algo vazio está ligado à sua falta de detalhes, mas, essa falta de especificidade traz consigo o auxílio no estudo de algo maior e mais geral. No entanto, uma estrutura, mesmo sendo estabelecida e duradoura, pode mudar. Essas mudanças que podem ocorrer em uma estrutura estão ligadas a revoluções, e essas revoluções podem ou não ser violentas. Ademais, uma mudança estrutural significa novos caminhos que podem ser produzidos em consequência de como as unidades irão interagir. Uma administração de política internacional tem êxito somente se as estruturas políticas estão bem explicadas de modo que os efeitos na estrutura, provocado por ações casuais, possam ser notados. Também, uma fração da explicação dos comportamentos e dos resultados é encontrada na própria estrutura do sistema, então, como explicado por Waltz "uma estrutura política está ligada a um campo de forças na física: interações dentro de um campo tem propriedades diferentes daquelas que ocorrem fora desse campo, e como o campo afeta o objeto, o objeto afeta o campo"[6] (Waltz, 1979, p. 73, tradução nossa). Apesar disso, o sistema como um todo não possui ação, mas, a sua estrutura afeta os agentes de maneira

[5] Given a durable structure, it becomes easy to overlook structural effects because they are repeatedly the same. Thus one expects the same broad range of outcomes to result from the actions of states in an anarchic condition.
[6] A political structure is akin to a field of forces in physics: Interactions within a field have properties different from those they would have if they occurred outside of it, and as the field affects the objects, so the objects affect the field.

indireta. Esses efeitos, para Waltz, são produzidos através da socialização e da competição. Portanto:

> A primeira forma pela qual as estruturas trabalham seu efeito é pelo processo de socialização que limita e molda comportamentos. A segunda forma é através da competição. Nos setores sociais onde são livremente organizados ou segmentados, a socialização acontece dentro de segmentos e a competição ocorre dentro desses segmentos. Socialização encoraja similaridades de atributos e comportamentos. A competição também. A Competição gera uma ordem cujas unidades ajustam suas relações por meio de suas decisões e atos autônomos[7] (1979, p. 76, tradução nossa).

Os mesmos resultados podem ocorrer mesmo que as estruturas sejam diferentes e as interações entre as unidades sejam variadas. Isso porque a estrutura pode determinar resultados que independem de mudanças ao nível das unidades. Dessa forma, causas similares podem ter consequências diferentes, assim como diferentes coisas podem produzir os mesmos efeitos.

Ao falar sobre estrutura, Waltz também indica como definições sobre estrutura devem deixar de lado questões como comportamento, interação e as características das unidades. Isso se deve ao fato de que para o estudo em questão, se faz necessário separar as variáveis que se encontram no nível das unidades e as variáveis a nível de um sistema. Dessa forma, ao se abstrair das questões relativas às unidades, entende-se que essas são de bastante importância, mas essas relações de interação se encontram no nível das unidades, e para se estudar a estrutura, deve-se tratar de questões a nível sistêmico, como por exemplo, a disposição das unidades. Portanto, a estrutura não é sobre as instituições políticas, mas pela disposição delas. Desse modo, o princípio ordenador de um sistema revela uma informação inicial sobre como as partes estão relacionadas umas às outras. Além disso, as capacidades relativas também afetam a disposição das unidades dentro de um sistema, de modo que, no desempenho de suas funções, as agências podem perder ou ganhar capacidade. Essa relação mostra que, mesmo que as funções específicas se mantenham inalteradas, as unidades acabam encarando diferentes relações entre si por conta das mudanças que ocorrem em relação às capacidades relativas. Sendo assim, os efeitos resultados de uma estrutura, entre um país e outro, podem ser identificados pela percepção de comportamentos similares nas políticas de estruturas semelhantes e então, estruturas semelhantes produzem efeitos semelhantes.

---

[7] The first way in which structures work their effects is through a process of socialization that limits and molds behavior. The second way is through competition. In social sectors that are loosely organized or segmented, socialization takes place within segments and competition takes place among them. Socialization encourages similarities of attributes and of behavior. So does competition . Competition generates an order, the units of which adjust their relations through their autonomous decisions and acts.

Os sistemas internacionais são descentralizados e anárquicos, diferentemente de sistemas domésticos, onde se destacam a hierarquia e a centralização. A estrutura de um sistema nasce da coexistência dos estados. Por conseguinte, nenhum Estado, por si, deseja ser constrangido por uma estrutura. No entanto, sistemas políticos internacionais são gerados espontaneamente e de maneira não intencional. Além disso, o sistema político internacional é de autoajuda, isto é, as unidades dependem de si próprias para garantir sua sobrevivência. Ademais, deve-se manter em conta que, as predições relativas à política internacional são premissas e, portanto, essas premissas são feitas de modo a ser possível a construção da teoria. Então, sobre a garantia da própria sobrevivência, Waltz apresenta

> Por além do motivo da sobrevivência, os objetivos dos Estados são infinitamente variados; eles podem partir da ambição de conquistar o mundo, até o desejo de ser deixado sozinho. [...] O motivo da sobrevivência é tido como base de ação em um mundo onde a segurança dos Estados não é assegurada, em vez de uma descrição realista do impulso que está por trás de cada ação de Estado. A suposição permite o fato de que nenhum Estado age exclusivamente a fim de assegurar sua sobrevivência. Permite o fato de que alguns Estados possam buscar incansavelmente por objetivos que valorizem mais do que a sobrevivência[8] (1979, p. 91-92, tradução nossa).

A anarquia do sistema implica uma relação de coordenação entre as unidades, isso implica em uma mesmice. Também, enquanto a anarquia perdurar, os Estados permanecem como unidades. Além disso, os Estados não são os únicos atores internacionais, mas as estruturas de um sistema são definidas pelos atores predominantes. Ao colocar os Estados como unidades, "é falar que cada Estado é como todos os outros ao ser uma unidade política autônoma. É outra forma de falar que os Estados são soberanos"[9] (Waltz, 1979, p. 95, tradução nossa). Lembrando que soberania não garante livre ação aos Estados, uma vez que eles podem ser pressionados e constrangidos. Portanto, a soberania dos Estados é tida como a liberdade que esses possuem de fazer suas escolhas na cooperação interna e externa, podendo ser constrangida por diversos fatores como a busca por assistência internacional. Desse modo, os Estados são parecidos, mas diferentes, e a diferenciação deles vem com as suas capacidades. As capacidades são maneiras de

---

[8] Beyond the survival motive, the aims of states may be endlessly varied; they may range from the ambition to conquer the world to the desire merely to be left alone.[...] The survival motive is taken as the ground of action in a world where the security of states is not assured, rather than as a realistic description of the impulse that lies behind every act of state . The assumption allows for the fact that no state always acts exclusively to ensure its survival . It allows for the fact that some states may persistently seek goals that they value more highly than survival.

[9] To call states '1ike units" is to say that each state is like all other states in being an autonomous political unit. It is another way of saying that states are sovereign.

estimar o poder, e as variações na estrutura vêm com as distinções entre os Estados em relação às suas capacidades (Waltz, 1979).

Ao dialogar sobre a anarquia, Waltz coloca que "entre os Estados, o estado de natureza é um estado de guerra"[10] (1979, p. 102, tradução nossa). Porém, essa declaração vem em um sentido de que, pelos Estados agirem por si próprios, uma guerra pode iniciar a qualquer momento. Apesar de a anarquia do sistema ser vista como um estado de ameaça e de um meio violento e inseguro, é fácil esquecer como questões relacionadas à manutenção do poder e ao estabelecimento da ordem podem ser mais sangrentas que as próprias guerras. Portanto, há períodos mais violentos e outros menos violentos, onde a insegurança se torna maior ou menor. Dessa forma, através do sistema de autoajuda, as unidades do sistema utilizam parte de seus esforços para que possam se auto-proteger de outras unidades. Essa constante preocupação molda o comportamento dos Estados que, por meio da insegurança em relação às outras unidades, podem evitar cooperações e integrações. Além disso, a divisão desfavorável de possíveis ganhos e o receio de tornar-se dependente através de esforços de cooperação e a troca de bens e serviços, são formas pelas quais a estrutura da política internacional limita a cooperação entre os Estados.

Ademais, a interdependência afeta uns estados mais que outros. Desse modo, Estados menores e com menos capacidades são menos aptos a frear a interdependência aos seus moldes. No entanto, nenhum Estado coloca-se deliberadamente em uma situação em que a dependência aumenta constantemente. Também, os Estados podem lamentar a falta de oportunidades que possuem de melhorar o bem-estar da sua população por conta da constante despesa relativa à própria defesa. Dessa forma, fica ainda mais claro como a estrutura provoca ações, e que essas ações desdobram-se em consequências que não eram pretendidas. Além disso, um Estado não provoca mudanças na estrutura somente por sua própria vontade de alterar o curso de algo, mudanças nos resultados de uma estrutura somente são atingidas por mudanças na estrutura.

Portanto, dentro do sistema internacional, um Estado torna-se vulnerável se não se preocupa com a constante evolução de seus esforços internos e externos. Logo, é citada por Waltz a teoria da balança de poder, ou, equilíbrio de poder. Segundo ele, a teoria expõe os resultados que são produzidos a partir de ações desordenadas vindos dos Estados. Para Waltz, a teoria acaba assumindo os motivos e interesses do Estados, e não os explicando. No entanto, o autor também reflete que essa teoria pode ser vista como um desenvolvimento vindo da teoria sistêmica das

[10] Among states, the state of nature is a state of war.

relações internacionais. Nesse sentido, quanto maior for a participação de um Estado na disposição das capacidades dentro do sistema internacional, as possibilidades de ele ser constrangido são menores. Além disso, encontra-se segurança no sistema internacional através da assimetria entre suas unidades e, dessa forma, contribuindo para uma situação em que há equilíbrio de poder.

"Uma teoria sistêmica requer que alguém defina estruturas parcialmente através da distribuição de capacidades pelas unidades"[11] (Waltz, 1979, p. 131, tradução nossa). Desse modo, os Estados precisam utilizar as suas capacidades combinadas para a sua manutenção em um sistema de autoajuda. A partir de questões como tamanho da população e do território, estabilidade política, capacidade econômica e força militar, é como um Estado irá se destacar dentro da estrutura. São muitas combinações possíveis dessas capacidades, e, portanto, difíceis de mensurar e comparar. Dessa forma, um desequilíbrio de poder pode ser perigoso, visto que, Estados ambiciosos podem promover atividades arriscadas em prol da extensão de seus poderes. Portanto, cada Estado dentro da balança de poder deveria ter um mínimo de capacidade de manter sua integridade, como se em um sistema igualitário. Todavia, o que predomina no sistema é a desigualdade entre as unidades. Dessa maneira, poucos Estados ao longo da história coexistiram possuindo capacidades proporcionais uns aos outros. Portanto, os Estados agem de acordo com seus interesses nacionais, isto é, procuram atender às necessidades de segurança que lhes são necessárias. Além disso, vinculado a esses interesses próprios, há questões militares e diplomáticas que precisam atender a planos cuidadosos de modo a não colocar o país em risco (Waltz, 1979).

Através de uma explicação econômica, Waltz traz alguns pontos para o texto a explicação em relação à quantidade de grandes poderes que deveriam coexistir dentro do sistema internacional

> (i) Economistas concordam que, mais que qualquer outro fator relativo ao tamanho determina a sobrevivência das firmas. Firmas que são grandes em comparação com a maioria da sua área, tem mais capacidade de cuidar e proteger a si próprias de outras grandes firmas. [...] (ii) A estabilidade dessas grandes firmas é promovida futuramente, através da dificuldade que novas firmas têm, de operar em mercados já consolidados. [...] Poucas firmas significam firmas maiores, e firmas maiores significam maiores barreiras para a entrada nesse mercado. [...] (iii) Os custos de barganha crescem em um nível acelerado conforme o número de partes se torna maior. Conforme o número de partes cresce, cada parte precisa barganhar com outras mais. [...] (iv) Conforme um grupo cresce, cada membro tem menos incentivo para suportar os custos de barganha. Cada membro de um par espera conseguir metade do benefício, cada membro de um trio,

[11] A systems theory requires one to define structures partly by the distribution of capabilities across units.

> um terço e assim por diante. (v) Conforme um grupo encolhe, cada membro restante consegue uma parte maior dentro do sistema e obtém mais incentivo para sua manutenção. (vi) Os custos esperados do cumprimento de acordos, e da coleta de ganhos que esses acordos oferecem, aumentam desproporcionalmente conforme o grupo cresce. (vii) A diversidade de partes aumenta a dificuldade de chegar em acordos, e a diversidade aumenta conforme esse número cresce. (viii) Por conta dos resultados de um acordo e a possibilidade de manutenção do mesmo poder mudar com o tempo, é necessário que todas as partes estejam vigilantes. [...] (ix) Aumento da dificuldade de detectar um acordo feito em desvantagem própria (1979, p. 135-136, tradução nossa).[12]

Para Waltz (1979), esses nove pontos são argumentos que apontam fortemente para a conclusão de que menor é melhor. Sistemas que são menores são mais estáveis. Assim, a conclusão obtida não quer dizer que o menor número possível em um sistema (dois), é a melhor opção. Dentro do sistema internacional, com os tipos de armamento atuais, a estabilidade é de grande importância para que o sistema se mantenha pacífico. Desse modo, se um Estado agressivo se torna forte, outros sofrerão. No entanto, a taxa de "mortes" de Estados dentro do sistema internacional é baixa.

Além disso, a interdependência não necessariamente traz paz, uma vez que ela provoca maior contato e isso aumenta uma possível chance de conflito. Também, para que o conflito ocorra, é necessário que suas partes estejam de alguma forma envolvidas. Para Waltz (1979), dentro de um sistema bipolar, a interdependência é menor. Ademais, a interdependência é um conceito antes de ser um fato. O conceito popular de interdependência não traz a questão da desigualdade econômica e política. A interdependência é uma relação entre iguais, e é reduzida conforme o aumento da disparidade nas capacidades nacionais. Dessa forma, em qualquer sistema internacional alguns Estados são mais independentes e outros menos. No entanto, se a interdependência é maior ou menor dentro de um sistema, está relacionada à dependência dos Estados em relação aos grandes poderes. Economicamente, conforme materiais brutos se

---

[12] Economists agree that more than any other factor relative size determines the survival of firms. Firms that are large in comparison to most others in their field find many ways of taking care of themselves-of protecting themselves against other large firms. [...] Stability is further promoted by the difficulty newcomers have in competing with large and experienced firms operating in established markets. [...] Fewer firms means bigger ones, and bigger firms means higher barriers to entry. [...] The costs of bargaining increase at an accelerating rate as the number of parties becomes larger. As numbers increase each has to bargain with more others. [...] As a group grows, each member has less incentive to bear the costs of bargaining. Each member of a pair expects to get about one-half of the benefits of a bargain made; each member of a trio, about one-third, and so on. As a group shrinks, each remaining member acquires a larger stake in the system and has more incentive to help to maintain it. The expected costs of enforcing agreements, and of collecting the gains they offer, increase disproportionately as the group becomes larger. The diversity of parties increases the difficulty of reaching agreements, and expected diversity increases as numbers grow. Because the effects of an agreement and the desirability of maintaining or amending it change over time, surveillance of all parties by each of them is called for. [...] And so does the difficulty of predicting and detecting deals that other parties may make to one's own disadvantage.

tornarem escassos, a interdependência entre os Estados para o mercado internacional aumentará. Assim sendo, Estados que são grandes economicamente também podem ser fracos em termos militares. Dessa forma, Estados podem ser grandes influências políticas mesmo não possuindo grandes forças militares ou econômicas. Portanto, as capacidades políticas, militares e econômicas se separam da habilidade de ação de um Estado. Mesmo assim, em um mundo onde as nações são bastante desiguais, são poucos Estados que detém grandes condições de escolha e uma enorme quantidade de influência. Sendo assim, "Atualmente, o mito da interdependência obscurece as realidades da política internacional e afirma uma crença falsa sobre as condições que promovem a paz" (Waltz, 1979, p. 159, tradução nossa).[13]

Para que seja possível dizer que um sistema é estável, é necessário que isso signifique duas coisas: que o sistema permanece anárquico e que não há variações substanciais no número das partes que o constituem. No entanto, nem todas as mudanças de número são mudanças no sistema. Dessa forma, claramente há diferenças em sistemas multipolares e bipolares, a mais crucial seria o balanceamento. Em um sistema bipolar, os desbalanceamentos que ocorrem devem ser corrigidos através de ações internas. Já em um sistema multipolar, as mudanças de alinhamento entre os Estados precisam de mais de um tipo de ajuste. Então, a noção de que o sistema precisa de um balanceador, um sistema de três, cinco grandes poderes, é uma generalização histórica.

Em se tratando de sistemas multipolares, as ameaças contidas dentro desse modelo são incertas, os cálculos relativos à ação dos Estados são mais difíceis de se fazer. Portanto, em um sistema com mais de dois grandes poderes, a diplomacia é acionada, de modo que alianças possam ser feitas, mas, também, de maneira que os próprios planos estejam em concordância com a satisfação de seus aliados. Essas alianças são formadas pelo medo dos Estados em relação aos outros. Além disso, as tensões também podem ser geradas pelas interações entre dois Estados que compõem alianças diferentes. Ademais, um Estado é constrangido para que consiga adequar suas próprias estratégias às desconfianças e objetivos de seus parceiros de aliança. Dessa forma, mesmo que um sistema esteja dividido em dois grandes blocos de aliança, isso não o torna bipolar. Ao trazer a questão das capacidades militares, Waltz (1979) menciona que, em sistemas bipolares, a dependência militar se baseia em si próprio, sendo os próprios dois grandes poderes quem devem resolver o balanceamento dessa questão internamente. Já em sistemas multipolares,

[13] Today the myth of interdependence both obscures the realities of international politics and asserts a false belief about the conditions that promote peace.

outros Estados compõem o sistema de modo que dependam uns dos outros. Desse modo, retorna-se à questão da interdependência, que em sistemas multipolares há maior entrelaçamento entre os Estados. Portanto, em sistemas bipolares há menos desconfiança pois já se obtém um Estado oposto muito claramente. Não há periferias em mundos bipolares, qualquer ocorrência dentro do sistema é, em alguma instância, de preocupação de um dos dois grandes poderes. Também, em um mundo bipolar

> A competição se torna mais compreensiva assim como mais amplamente extensa. Não são somente preparações militares, mas também crescimento econômico e desenvolvimento tecnológico são questões de intensa e constante preocupação. A auto-dependência das partes, a clareza dos perigos, e a certeza sobre quem precisa enfrentá-los são as características de uma política de grande potência em um mundo bipolar (Waltz, 1979, p. 171-172, tradução nossa).[14]

Além disso, a barganha entre Estados se torna mais eficaz se feita entre apenas dois. Também, essas relações bipolares são mais simples e de bastante pressão, tornando os posicionamentos dos Estados, conservador. Para que estes resultados possam ser explicados, deve-se observar as ações, as capacidades, a interação entre os Estados, assim como também deve ser notada a estrutura em que estão inseridos.

Ao longo da história, Waltz percebeu o quão pouco as posições dos Estados no sistema se modificaram. Também alterou-se a percepção compensadora das armas nucleares que outrora se teve, pois essa capacidade não altera as bases econômicas do poder de uma nação, somente as reitera. Além do mais, as capacidades militares de nações menores, se forem lentas em seu desenvolvimento, podem se tornar obsoletas. No entanto, armas nucleares, como dito anteriormente, não possuem contribuições nesse sentido, além de não ser capaz de desestabilizar um sistema bipolar, mas de limitar o escalonamento de tensões. Portanto, as capacidades e forças militares de uma nação são úteis em situações em que elas não são necessárias para ação, mas para a dissuasão. Dessa forma, armas e armamentos são menos custosos quando não são utilizados. Ainda assim, poderio militar não traz consigo controle político sobre outrem, tornando-se obsoleto em relação à definição estrutural de um sistema. Apesar da força ainda ser útil na manutenção do *status quo*, não o altera.

---

[14] Competition becomes more comprehensive as well as more widely extended. Not just military preparation but also economic growth and technological development become matters of intense and constant concern. Self-dependence of parties, clarity of dangers, certainty about who has to face them: These are the characteristics of great-power politics in a bipolar world.

Sobre o poder, Waltz elenca quatro pontos

> Primeiro, o poder proporciona os meios de manutenção da autonomia diante da força que outros exercem. Segundo, grandes poderes permitem maiores margens para ação, enquanto deixam os resultados das ações incertos. Terceiro, o mais poderoso se aproveita de margens maiores de segurança na tratativa com os menos poderosos, e tem mais poder de previsão quanto a quais e como os jogos serão jogados. [...] Quatro, um grande poder dá ao seu possuidor uma boa aposta no sistema e a habilidade de agir pelos seus próprios interesses (1979, p. 194-195, tradução nossa).[15]

Como sistemas autorreguladores operam dentro somente de ordens planejadas, o gerenciamento das relações entre as nações de um sistema clama por ajuda. No entanto, os custos de uma guerra ou da chance de guerra são maiores. Ainda assim, as ações em grupo por partes dos Estados, com a finalidade de um bem geral comum, são difíceis de serem atingidas em um sistema anárquico. Dessa forma, pode ser complicado empreender projetos internacionalmente devido à resistência que um ou alguns Estados podem vir a ter em relação a determinados projetos. Portanto, sistemas são mantidos ou transformados, e as entidades principais das quais constituem um sistema são também, seus gerenciadores. Assim sendo, guerras que eliminam grandes poderes são guerras que transformam um sistema. Além disso, a mudança de é um grande projeto histórico, que, no entanto, nunca encontrou seu sucesso.

Contando com dois grandes poderes, o esperado é que ambos ajam em prol da manutenção do sistema. Os Estados colocam bastante esforço na manutenção da sua autonomia e, por isso, em um mundo multipolar podem ocorrer conflitos ocasionais. Também, deve-se esperar em um mundo bipolar que haja um maior gerenciamento uma vez que a atenção é focada em somente dois grandes poderes. Assim sendo, os grandes Estados também agem pelo bem comum, ao invés de somente pelo seu próprio. No entanto, as definições sobre o bem comum variam e entram em conflito entre si. Dessa forma, as nações do mundo requerem certo nível de regulamento em termos militares, econômicos e políticos e, para Waltz (1979), os Estados Unidos exercem função reguladora no mundo desde a Segunda Guerra Mundial. Portanto, um sistema, mesmo que bipolar, irá requerer projetos para o bem comum, onde dependerão de mais de um Estado, assim como os custos dessas e outras ações, tendem a ficar concentrados nos grandes

[15] First, power provides the means of maintaining one's autonomy in the face of force that others wield. Second, greater power permits wider ranges of action, while leaving the outcomes of action uncertain. Third, the more powerful enjoy wider margins of safety in dealing with the less powerful and have more to say about which games will be played and how. [...] Fourth, great power gives its possessors a big stake in their system and the ability to act for its sake.

poderes, afinal, Estados líderes executam os papéis de líderes dentro da manutenção das relações mundiais internacionais.

2.2 Segurança Cibernética

2.2.1 O ciberespaço

O termo *cyberspace*[16] é derivado da palavra *kyber* em Grego, e tem como significado "navegar" (Dodge; Kitchin, 2017). Então, no início da década de 1980, quando o ciberespaço ainda era algo separado do mundo físico, William Gibson, autor de ficção científica, levou a palavra *cyber* para uma nova etapa ao forjar o conceito de ciberespaço em um de seus livros. Portanto, a partir desse uso ficcional, o ciberespaço se tornou largamente utilizado em nível acadêmico e profissional (Ottis; Lorents, 2010). Portanto, o ciberespaço e a tecnologia da informação ocasionaram mudanças substanciais na maneira pela qual as pessoas levam suas vidas e o modo como trabalham. Sendo assim, na atual era da informação, há um mundo tridimensional onde estão entrelaçados o mundo físico, a sociedade e o mundo da informação (ciberespaço) (Huanguo et al, 2015). Em comparação ao seu início, o fenômeno do ciberespaço obteve grandes mudanças e forte expansão global, o que pode ser difícil de conceituá-lo (Singer; Friedman, 2014). Dessa forma, pode-se citar a definição do Departamento de Defesa dos Estados Unidos para o ciberespaço, que trata de "um domínio global dentro do ambiente de informação que consiste na rede interdependente de infra-estruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores embutidos" (Dictionary of Military and Associated Terms, 2010, p.58, tradução nossa).[17]

Em vista disso, dentro do que se entende por ciberespaço estão contidas informações que são criadas, armazenadas e compartilhadas e, por isso, causa uma dificuldade na métrica de sua dimensão. Como exposto anteriormente, não é um espaço exclusivamente virtual, uma vez que há máquinas através das quais as informações irão fluir. Além disso, essas máquinas estão atreladas a um espaço geográfico e, por consequência, ligadas a um Estado soberano. Portanto, não é um espaço livre de Estados, suas leis e políticas (Singer; Friedman, 2014). Desse modo, em uma

[16] Ciberespaço.
[17] A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

entrevista para o *Harvard International Law Journal*, o coronel Brown[18] esclarece que as leis internacionais também são aplicadas no ciberespaço, mesmo que seja um ambiente no qual questões legais tendem a ser contraditórias. Para tanto, Brown expõe que "o ciberespaço não é uma zona livre de leis onde qualquer um pode conduzir atividades hostis sem regras ou restrições" (2012, p. 3, tradução nossa)[19]. Para que um ataque possa ser, de fato, identificado e julgado como um crime, a lei já deve existir. No entanto, os ataques acontecerão mesmo que não haja leis para qualificá-los (Ghernaouti, 2013). Também, o próprio ciberespaço e a sua arquitetura podem agir como reguladores de comportamento. Os códigos, os *hardwares* ou os *softwares* que tornam o ciberespaço da maneira que é, podem constituir restrições a quem o utiliza (Ku, 2020).

Sendo assim, obtêm-se quatro elementos base do ciberespaço: instalação, dados, funções e operações

> Instalação: [...] pode ser entendido como as formas de todos os tipos de transportadoras que transportam todos os tipos de cargas úteis (sinais, dados, informações e assim por diante) estão certas na instalação, porque os atributos apresentados por essas instalações no ciberespaço são idênticos, todos eles mostrado como a característica de "carregar". [...] Mostra a característica de liderança da rede na soberania do ciberespaço.
> Dados: se refere à sinais digitais que expressam informações como luz, eletricidade, som, magnetismo, quântico, e assim por diante dentro do ciberespaço, e é correspondente a *payload* na definição de *network*. [...] A instalação e os dados pertencem ao nível tecnológico, que refletem os atributos de uma rede. [...]
> Funções: se refere a todos as funções e usuários no ciberespaço. No ciberespaço, humanos são funções; Além do mais, organizações, equipamentos, *softwares*, *websites,* robôs, equipamentos de rede e assim por diante, também são funções capaz de produzir informações. [...]
> Operações: se refere a vários dados de atividades e comportamentos no ciberespaço, e é substancialmente todos os comportamentos de processamento de dados. As funções e as operações pertencem ao nível social (Fang, 2018, p. 28-29, tradução nossa).[20]

---

[18] Foi parte da força aérea norte-americana e atuou com política ciber e como analista estratégico para o Departamento de Defesa dos Estados Unidos. Atualmente, é professor de Direito Cibernético na faculdade de informação e ciberespaço, da Universidade Nacional de Defesa.

[19] Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.

[20] The "Facility": [...] it can be understood that the forms of all types of carriers for carrying all kinds of payloads (signals, data, information and so on) are right the "Facility", because the attributes presented by these facilities in Cyberspace are identical, all of which are shown as the characteristic of "carrying". [...] shows the characteristic of "leading the net" in cyberspace sovereignty. The "Data" of the four elements refers to digital signs expressing such informations as light, electricity, sound, magnetism, quantum (and even smaller particles that may appear in the future) and so on in the cyberspace, and it is corresponding to "Payload" in the definition of "Network". [...] "Facility" and "Data" belong to the technology level, reflect the attributes of "Network". The "Roles" of the four elements generally refers to all roles and users in the Cyberspace. In the cyberspace, humans are roles; besides, organizations, equipments, softwares, websites, virtual humans (robots), network equipments (Router) and so on may also be the main body roles capable of producing information. The "Operations" of the four elements refers to various data activities and behaviors in the cyberspace, and is substantively all kinds of behaviors of processing data. Both "Roles" and "Operations" belong to the social levels.

A tecnologia da informação está prosperando quando se trata de suas aplicações industriais, no entanto, a segurança da informação torna-se cada vez mais em evidência. Assim, ações hostis através de ataques *hackers*, crimes informáticos, violações de privacidade e *softwares* maliciosos são grandes ameaças à segurança da informação (Huanguo et al, 2015). Desse modo, os ciberataques podem ser referidos como armas militares. Portanto, também se transformou em um espaço de tratativas políticas e econômicas, um campo de batalha para essas questões. Todavia, ciberataques criminais embora sirvam de arma, não são necessariamente, em sua totalidade, relacionados ao terrorismo ou a guerras. Em tese, qualquer indivíduo com uma conexão à internet poderia utilizar-se de informações vazadas como uma forma de ataque a qualquer outra máquina, independentemente de ser estatal ou privada. Desse modo, mobilizações da população podem se tornar realidade, como nos eventos relacionados à Primavera Árabe[21], em que a articulação ocorria no ciberespaço, mas reverberava nas ruas. Outro exemplo de ação diz respeito aos vazamentos de informações confidenciais pelo grupo *Anonymous*[22]. Devido às características dos vazamentos, o grupo foi capaz de mobilizar a opinião pública, no que pode ser chamado de *hacktivism*[23]. Portanto, como não há protocolos ou tratados a respeito de ataques cibernéticos que sejam adotados universalmente, cada Estado torna-se livre para tratar dessas questões de acordo com seu conjunto de leis e regulamentos internos, no entanto, um Estado deve preocupar-se em prevenir e não apoiar a perpetuação de ciberataques a outras nações, para que não seja coautor desses atos (Ghernaouti, 2013).

2.2.2 A cibersegurança

O termo cibersegurança se tornou popular no final da primeira década do século XXI, quando o então presidente dos Estados Unidos, Barack Obama, declarou a importância da cibersegurança, entrelaçando-a com o termo segurança nacional do país (Schatz; Bashroush; Wall, 2017). Dessa forma, a cibersegurança, ou segurança cibernética, pode possuir variadas definições, de acordo com que as escreve. Mas antes, dar-se-á uma simples explicação para as palavras que compõem o termo, isto é, ciber e segurança. Segundo o dicionário de Oxford, a

[21] Marcada por uma série de protestos populares que aconteceram em mais de dez países do Oriente Médio e Norte da África, com o intuito de se revoltar contra as ditaduras desses países.
[22] Coletivo hacker famoso, que atua em prol de causas específicas, através de ataques cibernéticos criminosos.
[23] Ataques cibernéticos promovidos por atacantes que se auto declaram ativistas políticos e sociais.

palavra *cyber* significa "estar conectada com redes de comunicação eletrônicas, especialmente a internet" (2023).[24] Desse modo, a palavra ciber é uma contração da palavra cibernética (Craigen; Diakun-Thibault; Purse, 2014). Por isso, pode-se definir cibernética como "o estudo científico de como a informação é comunicada em máquinas e aparelhos eletrônicos" (Cambridge Dictionary, 2023, tradução nossa).[25] Já a palavra segurança encontra-se relacionada não somente à situação de estar livre de perigos, mas também, relaciona-se com a existência de um adversário. Desse modo, um problema de ciber somente se transforma em um problema de cibersegurança se o adversário em questão pretende obter ganhos através da sua atividade de maneira ilegítima (Singer; Friedman, 2014). Portanto, entre as várias definições encontradas, pode-se citar por exemplo, "A habilidade de proteger ou defender o uso do ciberespaço de ciberataques" (Cnss, 2010, p. 22, tradução nossa).[26] Também, "o estado de proteção contra o uso criminoso e não-autorizado de dados, ou as medidas tomadas para conseguir isso" (Collins, 2023, tradução nossa).[27] Além disso, ela também pode ser definida como "a organização e coleção de recursos, processos e estruturas usadas para proteger o ciberespaço e os sistemas habilitados para o ciberespaço, de ocorrências que desalinham os direitos de propriedade reais dos direitos de propriedade percebidos" (Craigen; Diakun-Thibault; Purse, 2014, p. 17, tradução nossa).[28]

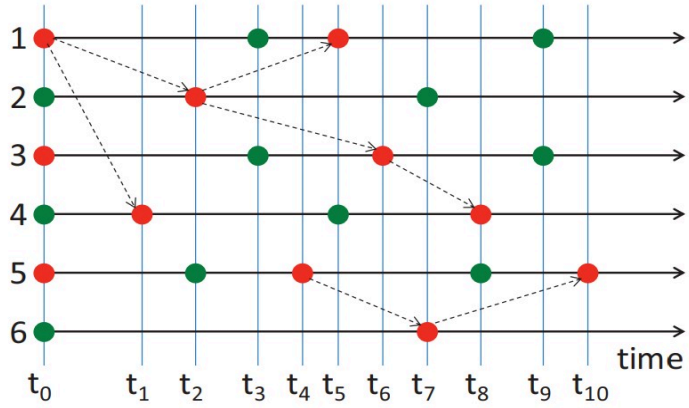
Desse modo, a cibersegurança evoluiu demasiadamente, levando uma disciplina técnica para um conceito estratégico e, portanto, de preocupação nacional. Ataques cibernéticos não são um fim, mas um meio significativo para atingir uma grande variedade de fins (Geers, 2011). Portanto, tem crescido a sua importância no dia a dia, nos negócios e para os governos de cada nação (Veale; Brown, 2020). No entanto, a cibersegurança não se encaixa em problemas comuns de segurança e, por isso, o processo de construção de políticas para a segurança cibernética é mais dispendioso (Harknett; Stever, 2011). Além do mais, com a pandemia da COVID-19, o uso das tecnologias se elevou, e trouxe consigo maior pesquisa e investimento para a área, além de evidenciar a falha das nações mundiais em obter planejamentos e programas voltados para a questão. Então, a expectativa em relação aos ciberataques é de aumento, uma vez que os métodos de ataque transformam-se ao longo do tempo, e se tornam mais sofisticados (Aldaajeh et al,

[24] Connected with electronic communication networks, especially the internet.
[25] The scientific study of how information is communicated in machines and electronic devices.
[26] The ability to protect or defend the use of cyberspace from cyber attacks.
[27] The state of being protected against the criminal or unauthorized use of electronic data.
[28] Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.

2022). A base da segurança da informação tem sido estabelecida desde o final da década de 1970 através da tríade de conceitos utilizadas pela CIA[29], são elas: confidencialidade, integridade e disponibilidade. Esses são pontos que nortearam os estudos da segurança da informação por décadas (Veale; Brown, 2020).

Sendo assim, o estudo da dinâmica da cibersegurança também se faz necessário para que se possa entender algumas questões dentro de um sistema. Desse modo, para melhor ilustrar um sistema cibernético, a figura 2 representa, em pequenas proporções, um modelo relativo a sistemas cibernéticos. Portanto, composto por seis bolinhas, onde cada um deles simboliza um computador, mas poder-se-á analisar, mesmo que de maneira superficial e simplificada, a fragilidade de um conceito de segurança dentro do meio cibernético (Xu, 2014).

Figura 2 – Modelo de Sistema Cibernético



Fonte: Xu 2014.

Logo, as bolinhas verdes representam um computador seguro e as vermelhas, um computador comprometido. No entanto, os computadores que estão seguros, não necessariamente estarão seguros de maneira irreversível, e assim sendo, os que estão comprometidos podem ser remediados. Essas mudanças podem ocorrer livremente ao longo do tempo (t). Além disso, mesmo que um computador não tenha sido atacado, ele ainda pode ser comprometido através de ameaças vindas do interior (Xu, 2014). No entanto, há engano em pensar que o termo cibersegurança está direto e exclusivamente relacionado ao uso de códigos e em conexão com a

[29] Central Intelligence Agency. Agência de Inteligência dos Estados Unidos.

internet, uma vez que a segurança física de máquinas e a utilização da engenharia social[30] também são aspectos importantes relacionados ao tema (Veale; Brown, 2020).

2.2.3 Ameaças, vulnerabilidades e infraestruturas críticas

As ameaças podem ser propositais ou acidentais e, em ambos os casos, elas possuem potencial para possíveis prejuízos. Desse modo, o elo mais fraco nas arquiteturas de segurança dentro do ambiente cibernético são as pessoas. No entanto, também pode-se ter ameaças não humanas, que são influenciadas pelo exterior, como desastres naturais (Ferreira, 2021). Além disso, no mundo atual há um bombardeio de ataques *hackers*, causando danos a sistemas e informações sensíveis, além do impedimento do acesso do usuário à sua máquina. Para além dessas opções, os ataques *hackers* podem ser gerados e utilizados das mais diversas maneiras. Logo, é necessária uma boa segurança dos sistemas de uma nação ou de uma organização, afinal, há ataques diretamente focados em atingir Estados soberanos e roubar suas informações. Todavia, também se têm ataques com alvos não-estatais, isto é, privados, que são direcionados geralmente a indivíduos. Desse modo, ao sofrer ciberataques, um governo ou instituição privada deve atuar de modo a responder essas ameaças e, portanto, a possibilidade de resposta às ameaças se dá das seguintes formas

> Resposta Governamental: a resposta do governo à ameaça cibernéticas se dá de maneira legal ou organizacional. No mundo atual um governo, por si próprio, não consegue eliminar ameaças cibernéticas mas, alguns Estados têm se saído muito bem ao lutar contra essas ameaças. [...]
> Setor Privado: se as respostas do governo podem ser ditas como *ad hoc*[31] das do setor privado, respostas não podem ser ignoradas. No mundo atual a força econômica de uma nação não pode ser ignorada e, uma vez que o setor privado fornece essa força à nação, sua segurança não pode ser tratada de maneira leviana (Patel; Chudasama, 2021, p.13, tradução nossa).[32]

Assim sendo, um governo deveria trabalhar em conjunto com o setor privado para que possa haver a construção de uma série de padrões relacionados à segurança cibernética. Ainda

[30] Técnica utilizada por atacantes cibernéticos para induzir usuários desavisados a fazer o envio de dados confidenciais ou abrir links infectados, de modo a infectar o computador.
[31] Expressão latina de tradução “para isto”, normalmente utilizada em contexto jurídico como “para um fim específico”.
[32] Government Response- The government responses to cyber threats in either legal ways or by the organizational way. In today’s world no government alone can eliminate the cyber threats but some countries have done some pretty good to fight against cyber threats. [...] Private Sector Responses – If the government responses can be said ad hoc than the private sector, responses cannot be ignored. In today’s world the economic strength of a nation cannot be ignored as private sector provides economic strength to the nation and its security cannot be taken easily.

assim, o ciberespaço promove um entrelaço profundo entre as nações, de modo que estão todas conectadas e, além disso, os ciberataques somente têm crescido e, portanto, tornado Estados com menos capacidades cibernéticas demasiadamente frágeis, podendo estar vulneráveis a sérias ameaças à segurança dos mesmos (Patel; Chudasama, 2021).

De fato, os *hackers* buscam por vulnerabilidades em seus alvos para que possam obter vantagens a partir dessas brechas (Ferreira, 2021). Essas vulnerabilidades "são falhas em um sistema ou no seu design que permite um atacante executar comandos maliciosos, acessar dados não-autorizados e conduzir diversos ataques de negação de serviço" (Humayun et al, 2019, p. 3173, tradução nossa). Assim, há alguns tipos de vulnerabilidades que são mais comuns: *denial-of-service*, *malware*, *phishing*, *SQL injection*[33].

A primeira, *denial-of-service (DoS)*, é um tipo de ataque que tem como objetivo tornar uma máquina ou rede inacessível para seus usuários. Desse modo, qualquer evento que interrompa a capacidade de uma rede de funcionar normalmente, está encaixado nessa vulnerabilidade (Humayun et al, 2019). Ataques desse tipo podem ter diferentes durações, além de poderem ter mais de um alvo ao mesmo tempo (NCSC, 2016). Outra vulnerabilidade é o *Malware*, onde o atacante implanta programas de *software* maliciosos para que, dessa forma, possa obter acesso a um sistema de computador através das suas brechas de segurança. Também, a técnica de *phishing* pode ser citada. Essa atividade ilegal faz uso de engenharia social para que possa ser feita a coleta de informações sensíveis (Humayun et al, 2019). A técnica, se traduzida, significa 'pesca', o que é uma boa definição para esse tipo de atividade. Através das informações acessadas, o atacante pode obter vantagens de vários tipos, como por exemplo, financeiras (TRE-SE, 2022). Entre seus meios de aplicação do ataque, são utilizados emails, páginas da web e mensagens instantâneas. Além disso, também citar-se-á o ataque por *SQL injection*, que é onde a linguagem de programação SQL é utilizada de modo que o atacante possa inserir uma *string*[34] na aplicação a fim de alterar ou manipular a declaração SQL em vantagem de si próprio. Esse ataque é arriscado pela possibilidade de perda ou mau uso dos dados (Humayun et al, 2019).

Entre os danos que a exploração dessas vulnerabilidades pode causar estão danos econômicos, constrangimento social e a perda de informações valiosas. Desse modo, a vulnerabilidade é o meio pelo qual uma ameaça se faz efetiva. (Ferreira, 2021). Sendo assim, a comunidade cibernética possui a iniciativa de encorajar os fornecedores de tecnologias a

[33]

[34]Na programação, sequências de caracteres usados para a manipulação de textos.

reportarem sobre a vulnerabilidade de seus produtos, uma vez que isso colabora com a garantia de segurança por parte dos usuários de um produto ou tecnologia. Logo, se uma vulnerabilidade não é reportada, ela não pode ser consertada (Herrmann; Pridöhl, 2020).

Em se tratando de vulnerabilidades, pode-se citar as infraestruturas críticas, que se refere à tecnologia de sistemas de informação físicas, redes, serviços e ativos, que se interrompidos podem causar grandes danos à economia e no bem-estar dos cidadãos de um país (Berg; Kuipers, 2022). Além disso, é possível comparar infraestruturas críticas com o corpo humano, uma vez que são necessárias que todas as partes funcionem bem, assim como nas infraestruturas críticas (Viganó; Loi; Yaghmaei, 2020). São consideradas infraestruturas críticas: sistemas de energia elétrica, telecomunicações, bancos, transportes, sistemas de abastecimento de água, sistemas de saúde, entre outros (Moteff; Copeland; Fischer, 2003). Segundo o presidente dos Estados Unidos Bill Clinton, em 1996, "algumas infraestruturas nacionais são tão vitais que sua incapacidade ou destruição teriam um impacto debilitante na defesa ou segurança da economia dos Estados Unidos" (The Daily Journal of the United States Government, p. 37347, tradução nossa).[35] Desse modo, a cibersegurança ameaça explorar a crescente complexidade e a conexão entre sistemas de infraestruturas críticas (Nist, 2018).

Assim, embora redes de computadores sejam vulneráveis, infraestruturas críticas não precisam necessariamente ser. Além disso, essas infraestruturas possuem consideráveis capacidades de se autodefender de ataques cibernéticos, além de ataques físicos. No entanto, isso não quer dizer que deve-se subestimar a cibersegurança, afinal, conforme as redes de computadores aumentam, as vulnerabilidades contidas nelas também seguem o mesmo movimento (Lewis, 2006). Sendo assim, ligando infraestruturas críticas à conectividade cibernética, tornou estas mais eficientes e, ao mesmo tempo, as deixou abertas a diversos tipos de riscos (Berg; Kuipers, 2022). Além do mais, os oponentes enfrentados por um Estado podem tirar mais proveito tendo como alvo a armazenagem de dados, do que causar um terror físico em uma nação (Lewis, 2006). Essa grande possibilidade de riscos faz com que as infraestruturas críticas estejam em lugar prioritário nas agendas políticas dos países (Berg, Kuipers, 2022).

2.2.4 A cibersegurança e o Estado

[35] Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

Precauções relativas à segurança nacional cibernética já estavam em ação nos anos 1960 pelos Estados. Desse modo, foi necessário que a segurança em relação à cibernética desse um passo, e então, passou de uma questão tática, para uma de estratégia (Geers, 2011). Dessa forma, o papel estatal dentro da cibersegurança está relacionado com a segurança dos sistemas federais e, na assistência da proteção de sistemas que não são federais (Fischer, 2017). Portanto, os desafios encontrados pelas nações quando tratando-se de cibersegurança serviram para que houvesse uma necessidade de estruturar melhor as pesquisas e iniciativas na área. Desse modo, embora ainda haja a falta de mão de obra para tratar dessas questões, ela aumentou consideravelmente (Aldaajeh et al, 2022).

Dessa forma, ao tratar de planejamento estratégico nacional de cibersegurança, a colaboração entre doze parceiros, entre eles a *Microsoft* e a *NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE),* resultou na criação de um guia que pudesse ajudar as nações a desenvolverem suas estratégias nacionais cibernéticas (Aldaajeh et al, 2022). De modo geral, o guia aponta sete pilares para esse planejamento, que serão brevemente explicados a seguir.

O primeiro pilar é a Governança, onde é necessário que seja delineada uma série de papéis e, recursos, responsabilidades e processos que possam guiar o desenvolvimento, além da implementação do plano nacional estratégico de cibersegurança. O segundo pilar consiste no Gerenciamento de Riscos, que é focado em identificar uma abordagem de gestão de risco e categorizar perfis com riscos setoriais. Chegamos ao terceiro pilar, que é a Preparação e a Resiliência, e fornece uma visão mais geral de boas práticas "que apoiam o estabelecimento e a sustentabilidade de capacidades nacionais efetivas para que estas possam estar preparadas para prevenir, mitigar e responder grandes incidentes cibernéticos e aumentar a resiliência geral da área cibernética de um país" (Guide to Developing a National Cybersecurity Strategy, 2021 p. 39, tradução nossa).[36] O quarto pilar é sobre Infraestrutura e serviços essenciais, onde o foco é implementar planos efetivos de modo que a infraestrutura crítica do país venha a ser protegida, assim como seus serviços. Já o quinto pilar concentra-se nas capacidades e na aptidão, além do aumento do conhecimento. Desse modo, o foco é aumentar as habilidades profissionais para garantir a proteção às infraestruturas críticas da nação. Em seguida, o sexto pilar é focado na

[36] This focus area provides an overview of good practices that support the establishment and sustainability of effective national capabilities to prepare for, prevent, detect, mitigate and respond to major cybersecurity incidents, and to improve a country's overall cyber-resilience.

legislação e no regulamento. Portanto, ele trata de um país assegurar que os crimes cibernéticos possam ser combatidos, e para isso, são necessárias leis e regulamentos que tratam do assunto. Por fim, o sétimo pilar vem a ser a cooperação internacional, isto é, engajar internacionalmente no combate aos crimes cibernéticos, de maneira que a política nacional possa estar alinhada com as políticas internacionais (Guide to Developing a National Cybersecurity Strategy, 2021).

Dessa forma, os Estados desenvolvem seus próprios planos relativos à estratégia cibernética. Os Estados Unidos, por exemplo, estabeleceram algumas prioridades em relação a esse plano, como a proteção de ativos críticos, garantia de grandes inovações, e extensão da influência estadunidense de modo que o ciberespaço possa se tornar um ambiente mais seguro (Aldaajeh et al, 2022). Assim, em 2023, os Estados Unidos construíram em seu plano estratégico, um grande papel para a regulamentação, nunca antes obtido em grandes proporções. Desse modo, o governo Biden deseja a construção de uma série de regulamentações relativas à segurança cibernética (Washington Post, 2023).

Além disso, há o conceito de ciber espionagem, que pode ser definido como "o uso intencional de computadores ou comunicações digitais em um esforço para obter acesso à informações sensíveis sobre um adversário, de modo a ser recompensado financeiramente, ou de forma que possa se obter vantagem" (Weissbrodt, 2013, p. 370-371).[37] Portanto, a espionagem tradicional não é enquadrada como uso de força internacionalmente, no entanto, se os espiões das nações forem apreendidos sob jurisdição internacional, eles podem responder criminalmente. Desse modo, a espionagem também é um risco para um Estado. Todavia, os espiões ligados à ciber espionagem correm menos riscos de apreensão, uma vez que suas atividades podem ser feitas a partir de seu país de origem. Além disso, é argumentado que a espionagem cibernética deve ser tratada de maneira mais severa que a tradicional, visto que possui capacidade de obtenção de dados em larga escala, além de ter a possibilidade de ser efetuada por um ator não estatal. Também, discute-se a necessidade de novas leis e normas voltadas exclusivamente para a ciber espionagem (Weissbrodt, 2013).

Através do princípio de soberania territorial, o Estado tem total autoridade sobre o seu território, ou seja, cada Estado soberano tem o poder de executar suas regras e leis dentro do seu território, assim como controlar os acessos a ele. Contudo, o ciberespaço coloca essa questão em

[37] Cyber-espionage is defined as the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward.

evidência, pois sua utilização vinculada à soberania é quase antitético, afinal, o ciberespaço é uma área de anonimidade e ubiquidade. Ainda que haja o debate premente de que o ciberespaço não foge à soberania territorial de um país, as normas e leis de uma nação possuem aplicabilidade diferente quando se trata do mundo cibernético. Todavia, os Estados, em conjunto, podem chegar a uma interpretação comum da lei internacional relativa ao ciberespaço. Através disso, forjar-se-ia um consenso entre as nações, de modo que surgisse um padrão a ser seguido internacionalmente quanto às questões relativas ao ciberespaço (Heinegg, 2013).

Dessa maneira, todos os conflitos atuais desenvolvem-se também dentro do espaço cibernético, isto é, os acontecimentos ocorridos no mundo físico são, também, espelhados no mundo cibernético (Geers, 2011). Em vista disso, um exemplo bastante atual dessa ligação entre o espaço cibernético e os conflitos no mundo real, é o caso da guerra entre a Rússia e a Ucrânia. Em seu início, em 2022, autoridades já alertavam para possíveis ataques cibernéticos. O *National Cyber Security Centre*, que é parte do governo britânico, aconselhou as organizações do país a reforçarem suas estruturas cibernéticas, de modo que pudessem estar mais protegidas contra ameaças e ataques, visto que estas estavam em aumento no início do conflito (NCSC, 2022). Além disso, uma matéria publicada em 2023, pela BBC, expõe os exércitos *hackers* contidos na linha de frente ucraniana. Desse modo, ao mesmo tempo que a guerra se iniciava no mundo físico, uma guerra cibernética também era travada. Além de profissionais militares atuando dentro do meio cibernético, também há diversos ativistas *hackers* trabalhando a partir dos seus lares. Um destes *hackers* serviu de fonte sobre o funcionamento do conflito. Ao ser entrevistado, informou que ele e o seu time de *hackers* atacaram um serviço de autenticação russo que era responsável por todos os produtos produzidos no país. O ataque foi feito através do método de distribuição de negação de serviço (Distributed Denial-of-Service - DDoS) visto no subtópico anterior deste capítulo. Também é relatado que esses ativistas se sentem úteis para seu país desta maneira, gerando um sentimento de pertencimento ao grupo militar do país (BBC, 2023).

Portanto, a crescente importância do ciberespaço o colocou em posição de grande evidência quando trata-se de políticas nacionais e internacionais. Desse modo, a cibersegurança entra em pauta para que a questão cibernética seja tratada como de interesse nacional. Além disso, neste capítulo foi explorado que as nações estão sujeitas a ameaças cibernéticas, portanto, suas estruturas e planejamentos devem ser fortificadas. Essas ameaças podem tornar-se ataques e afetar as infraestruturas críticas de um Estado, de maneira que venha a gerar caos e prejuízos aos

alvos. Também, no cenário internacional, os conflitos e a espionagem ganharam espaço dentro do meio cibernético, elevando essas questões a um novo patamar, gerando novos riscos e novas medidas de proteção. Em suma, o ganho de espaço conquistado pela segurança cibernética é considerável, acarretando novas medidas de proteção e novos meios pelos quais um Estado pode ser afetado, sem necessariamente estar relacionado a conflitos e embates físicos.

3 AMEAÇA HACKER

Os ataques cibernéticos existem desde que a internet é ativa e, portanto, evoluíram de maneira constante e abundante até os dias atuais (Chen; Desmet; Huygens, 2014). Desse modo, os números relativos às atividades criminosas são altos, afinal, o cibercrime ganha espaço devido à baixa possibilidade de ser descoberto e de ser levado a um processo jurídico. Portanto, pode-se dizer que ao longo do tempo construiu-se uma verdadeira indústria de crimes cibernéticos. Dessa forma, em âmbito virtual, todas as empresas podem sofrer ameaças ou ataques às suas redes, sendo também um ambiente onde o próprio governo de um país pode ser afetado, e as espionagens são um exemplo dessa sensibilidade presente dentro de um Estado (Ghafir; Prenosil, 2014). Além disso, o Fórum Econômico Mundial de 2023 colocou a cibersegurança entre os dez riscos globais atuais e futuros, uma vez que os custos do cibercrime estão estimados em US$10.5 trilhões até o ano de 2025 (Ene, 2023).

3.1 *Advanced Persistent Threat (APT)*

O termo *Advanced Persistent Threat* foi inicialmente introduzido no meio militar, quando em 2006 a Força Aérea dos Estados Unidos adentrava em uma discussão com civis especialistas sobre o assunto acerca dos ataques sofridos por eles, ao mesmo tempo em que eles não podiam revelar a autoria dos ataques, tampouco poderiam considerar as invasões como ataques simples e comuns e, desse modo, criou-se então o termo APT. Dentro do que compõe o termo, cada palavra traz consigo sua relevância. Dessa forma, *Advanced* foi pensado de maneira a tirar a simplicidade do ataque, então serve para referir-se à invasões e ações mais elaboradas que as normais (Steffens, 2020). Também, refere-se à grande habilidade que o autor possui de modo que possa passar despercebido dentro do sistema alvo. Em seguida, o termo *Persistent* faz alusão a uma ação de longo prazo, e a dificuldade de detecção da ameaça por todo um período de tempo (Ando, Itoh, 2022). Então, mesmo que alguma técnica seja falha, esse tipo de ataque, ao invés de desistir do alvo, se adapta a ele para novas futuras tentativas de ataque. Sendo assim, o termo *Threat* indica que o atacante é relevante, isto é, um APT se refere à motivações estratégicas e a quem está por trás, não a classe de *malwares* que é utilizada. Portanto, na época em que foi criado, o termo era referido a ataques específicos de certos autores dentro da esfera militar, no

entanto, ao longo do tempo, o termo APT ganhou relevância e adentrou às esferas tecnológicas e civis (Steffens, 2020).

De maneira geral, grupos que produzem ataques cibernéticos APT carregam consigo a ideia de ciber espionagem, logo, é considerada uma ação que necessita de meios para que possa ser efetivada, como por exemplo, um bom financiamento (Sharma et al, 2023). Dessa forma, pode-se categorizá-los como organizações financiadas por um Estado, ou como resultado de uma junção entre as esferas pública e privada (Ando; Itoh, 2022). Sendo financiados por Estados e grandes empresas, esses grupos apresentam uma considerável ameaça a outros Estados e empresas. Outra questão envolvendo ataques APT é a sua detecção, uma vez que, normalmente, não são utilizadas vulnerabilidades conhecidas, então, são exploradas as chamas *zero-day exploits*, onde falhas de *software* ainda não conhecidas publicamente são utilizadas (Ghafir; Prenosil, 2014). Dessa forma, os ataques APT são compostos por um variado número de etapas e, a seguir, utilizar-se-á da proposta da Lockheed Martin[38] para apresentar como se dá um ciclo de vida de um ataque APT (figura 3).

[38] Criadora do conceito *Cyber Kill Chain* e uma das maiores produtoras aeroespaciais do mundo.

Figura 3 - O ciclo de vida de um ataque APT

Fonte: Lockheed Martin, 2023, tradução nossa.

3.2 *Malwares*

Malware é um termo geral utilizado para se referir a *softwares* indesejados. Portanto, sua composição enquanto palavra vem da abreviação de duas outras palavras, *malicious* e *software*, isto é, um programa malicioso. Os *malwares* englobam vários tipos de programas maliciosos: vírus, *ransomware*, robôs, *rootkits*, *spyware*, *trojans,* entre outros. Desse modo, os *malwares* têm sido utilizados ao longo do tempo como armas nas mãos de cibercriminosos para lançar ataques, comprometer computadores e roubar informações confidenciais (Ye et al, 2017).

Portanto, para melhor elaborar, vale citar a evolução de camuflagem que os *malwares* obtiveram ao longo do tempo. Dessa forma, a primeira técnica utilizada a fim de encobrir um malware foi a criptografia, onde é basicamente criptografar e descriptografar. Nesse vírus, as chaves de criptografia são alteradas, enquanto que aquela referente à descriptografia permanece sendo a mesma. Sendo assim, nesse tipo de camuflagem, devido a chave para descriptografar permanecer a mesma, é um vírus que pode ser detectado. No entanto, esta é uma forma de camuflagem que pode contribuir ao oferecer um atraso nas investigações de ataques. Além desse, há também o oligomorfismo, que sinalizou uma evolução em relação ao primeiro método. Dessa maneira, no oligomorfismo, a chave de descriptografia é alterada a cada ataque. Todavia, as chaves para descriptografar utilizadas nesse tipo de camuflagem, vêm de uma lista, sendo portanto, detectável. Ainda, representando outra evolução para a camuflagem de um *malware*, há o vírus Polimórfico, onde observa-se uma combinação do oligomorfismo e da criptografia. Contudo, é um vírus muito mais complexo que os anteriores, cuja aparência altera-se a cada cópia, tornando-se de difícil detecção, além de que as suas possibilidades de gerar chaves de descriptografia não são limitadas como o vírus anterior. Já na camuflagem de Metamorfismo, a criptografia não é parte desse vírus, uma vez que no metamorfismo o conteúdo do *malware* é alterado, não sendo necessária uma criptografia. Assim como o polimorfismo, há mutações, no entanto, essa mutação ocorre em toda a sua estrutura, e não somente na alteração da descriptografia (Tahir, 2018). Logo, pode-se referir que "a ideia básica é que a sintaxe é alterada a cada nova mudança, enquanto que a semântica permanece a mesma"[39] (Tahir, 2018, p. 23, tradução nossa). A seguir, serão aprofundados alguns tipos de ataques de *malware*, de maneira a explicar mais detalhadamente aqueles ataques considerados mais relevantes ao propósito deste trabalho.

[39] The basic idea is the syntax change on each new copy while semantics remains the same.

3.2.1 *Phishing*

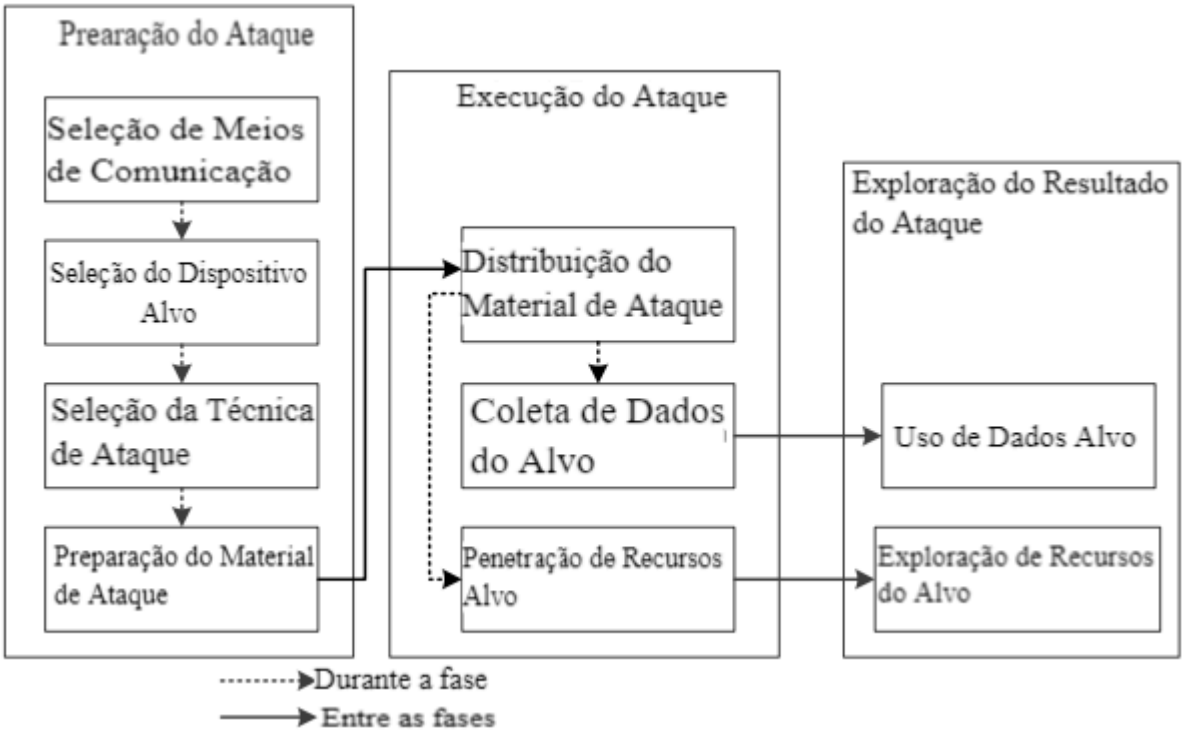
A definição de *phishing* pode ser encontrada como "um tipo de ataque cibernético que comunica mensagens socialmente projetadas para humanos através de canais eletrônicos de comunicação de modo a persuadir eles a realizar determinadas ações que beneficiarão o atacante"[40] (Khonji; Iraqi; Jones, 2013, p. 2092, tradução nossa). O termo *phishing* vem da palavra *fishing*, e que traz o sentido da utilização de uma isca para pescar, isto é, ao fazer uso de ferramentas da engenharia social, o atacante rouba informações pessoais das vítimas (Khonji; Iraqi; Jones, 2013). Os ataques de *phishing* exploram as vulnerabilidades humanas, ao utilizar truques psicológicos de modo que a vítima possa realizar as ações necessárias para que o ataque se complete. No geral, as tentativas de *phishing* são consideradas simples quando em comparação com outras técnicas (Aleroud; Zhou, 2017). Além disso, é importante ressaltar que os atacantes não restringem seus ataques somente ao roubo de informações pessoais, uma vez que também podem ser utilizadas técnicas que, não necessariamente, sejam necessárias as informações pessoais das vítimas para obter seus acessos. Também, as contas roubadas via *phishing* já foram usadas como moeda de troca entre os *hackers*, para que estes as trocassem por softwares de *hackers*. Desse modo, atualmente, os ataques de *phishing* também têm como alvo funcionários técnicos de empresas provedoras de serviço, podendo utilizar de técnicas mais avançadas em suas ações. Portanto, há diversos motivos que impulsionam um ataque de *phishing*, podendo-se elencar alguns, como ganhos financeiros através do roubo de credenciais bancárias, a venda de identidades a outros *hackers* e também, por reconhecimento e fama (Khonji; Iraqi; Jones, 2013).

De modo a reconhecer e detectar o uso de *phishing* pelos usuários, pode-se considerar o uso de treinamentos para reconhecimento desse tipo de ataque e também o melhoramento dos *softwares*. No entanto, educar as pessoas em geral sobre o reconhecimento de *phishing* pode ser dificultoso, uma vez que essas pessoas podem ter grandes dificuldades em absorver as informações a respeito do assunto, acabando por ser necessária a repetição do processo de treinamento de maneira constante. Além disso, os softwares, mesmo que melhorados, ainda necessitam que o usuário acate suas notificações de alerta e sejam cautelosos com seus cliques, fazendo com que o seu melhoramento não seja fator único para o sucesso da detecção de *phishing* (Khonji; Iraqi; Jones, 2013).

[40] Is a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit.

Portanto, dentro do processo de *phishing* (figura 4), elenca-se algumas fases: preparação, execução e a exploração dos seus resultados. Desse modo, possui-se um antes, durante e depois do ataque, que incluem diversos fatores como a sua escolha em relação a qual tipo de comunicação o atacante irá utilizar, sejam e-mails, aplicativos de celular, redes sociais e mensagens instantâneas. Também, obtêm-se o tipo de ataque e constrói-se o seu material de ataque, por exemplo, ao optar por email, é necessário construir esse email falso. Sendo assim, durante a execução do ataque, é preciso que a vítima execute as ações necessárias para que a coleta de dados possa ser iniciada. Logo, assim que esse roubo de dados é executado, o atacante personifica, isto é, torna-se online, a sua vítima (Aleroud; Zhou, 2017).

Figura 4 - As fases de *phishing*



Fonte: Aleroud; Zhou, 2017, tradução nossa.

Dentro das possibilidades de ataque através das mídias de comunicação, pode-se citar algumas como e-mails, *websites,* blogs e plataformas móveis (Aleroud; Zhou, 2017). Na figura 5, é mostrado um exemplo de *phishing* através do email, onde, em um primeiro momento pode parecer bastante real, mas ao analisar melhor pode-se detectar algumas características que o tornam suspeito, como por exemplo, o pedido que o email traz para que o usuário clique em um

determinado link de modo a atualizar seus dados de pagamento. Além disso, o cumprimento genérico também pode significar a falta de veracidade do email. (Federal Trade Comission, 2022)

Figura 5 - Falso Email

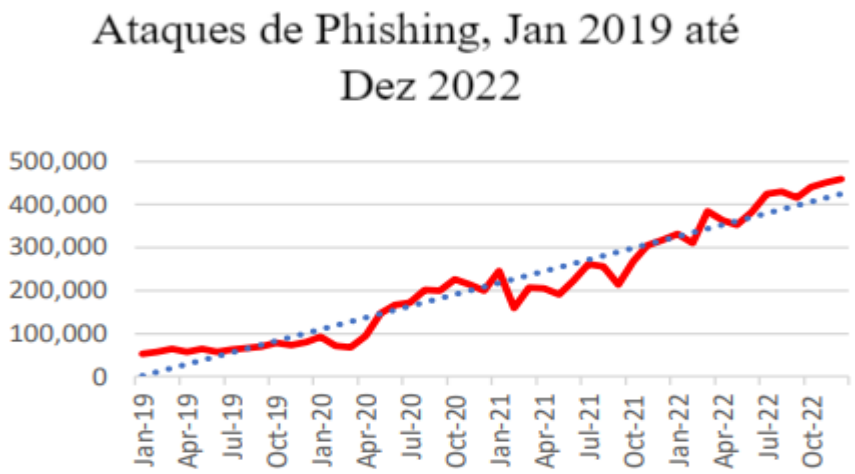
Fonte: Federal Trade Comission, 2022, tradução nossa.

Outro ponto relevante para ressaltar é o *phishing* em aparelhos móveis, afinal, a interface dos usuários é constrangida pelo tamanho da tela dos aparelhos celulares. Desse modo, "Em particular, os sistemas operacionais e navegadores móveis carecem de indicadores seguros de identidade de aplicativos. Um usuário não pode dizer definitivamente qual aplicativo móvel ou site com o qual ela está interagindo"[41] (Felt; Wagner, 2012, n.p, tradução nossa).

Dessa maneira, segundo o *Anti-Phishing Working Group (APWG)*[42], o ano de 2022 marcou um recorde para os ataques de *phishing*, com o registro de mais de 4.7 milhões de ataques, resultando em um crescimento de mais de 150% por ano desde 2019 (Gráfico 1)

[41] In particular, mobile operating systems and browsers lack secure application identity indicators. A user cannot definitively tell what mobile application or web site she is interacting with.
[42] Associação sem fins lucrativos focada em eliminar o roubo e fraude de identidades que são resultado de um crescente problema que é o *phishing*.

Gráfico 1 - Ataques de *phishing* no período 2019 - 2022



Fonte: APWG, 2023, tradução nossa.

Além disso, seguindo os dados mais recentes encontrados no site do APWG, no último trimestre de 2022 (período entre outubro e dezembro), foi encontrada a maior porcentagem de ataques de *phishing* àquelas direcionadas ao setor financeiro com 27,7% dos ataques. Também pode-se ressaltar a alta que o setor de logística e transporte sofreu, marcando 9% do total (gráfico 2).

Gráfico 2 - As indústrias mais afetadas no último trimestre de 2022

Fonte: APWG, 2023, tradução nossa.

3.2.1 Ransomware

O ataque por *ransomware* é um ataque onde a vítima é impedida de acessar seus dados, porque eles ficam criptografados. Portanto, o *ransomware* é um *malware* que ao limitar o acesso da vítima, é cobrado um valor pelo resgate do seu computador e seus dados (Richardson; North, 2017). A primeira demonstração de ataque por *ransomware* aconteceu em 1989, onde o atacante utilizou-se de uma criptografia de chaves simétricas, isto é, a mesma chave utilizada para criptografar, é a chave utilizada para descriptografar. Portanto, essa primeira realização tinha um ponto fraco, uma vez que a chave para descriptografar ia embutida no ransomware (O'Kane; Sezer; Carlin, 2018). Esse ataque imbuído à extorsão existe desde, pelo menos, 2005, e ao longo do tempo, as moedas virtuais, tal como o *bitcoin*, puderam facilitar esse tipo de esquema. Além de computadores, os ataques por *ransomware* também afetam aparelhos celulares. Desse modo, há dois modelos básicos de ataques, aqueles que encriptam os dados e arquivos da vítima e aqueles que bloqueiam o acesso ao aparelho ou computador da vítima. Dito isso, no segundo caso, muitas vezes, os dados contidos no computador, não são afetados, no entanto, isso torna esse método muito menos eficaz que o primeiro em relação ao sucesso no pagamento do resgate. Além disso, antes do surgimento do *bitcoin*, esse tipo de ataque era consideravelmente mais arriscado, isso porque era possível rastrear o atacante através do pagamento. No entanto, a partir do *bitcoin*, tornou-se bastante difícil, ou até mesmo impossível rastrear o atacante e, portanto, colaborou com a manutenção da anonimidade do atacante (Richardson; North, 2017). Dessa forma, em relação ao dinheiro do resgate, são utilizadas algumas maneiras para que este possa ser tornar-se limpo:

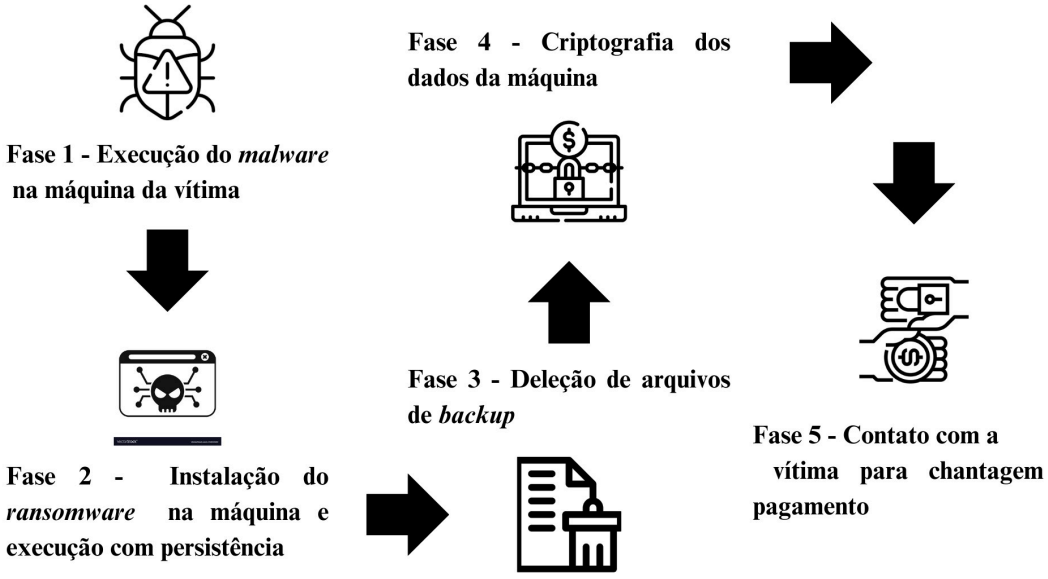
> Os métodos utilizados para a lavagem do dinheiro dependem do tipo de *ransomware*. Ransomwares de bloqueio que tendem a usar sistemas de pagamentos em *vouchers* como resgate, fazem a utilização de serviços de apostas online em uma variedade de jurisdições legais que aceitam os códigos de voucher como pagamento. Então, o dinheiro é transferido para um cartão de débito pré-pago e *money mules*[43] são usadas para fazer o saque desse dinheiro. Já os pagamentos em *bitcoin* podem ser usados de maneira direta devido à privacidade da criptomoeda. No entanto, muitos criminosos preocupam-se com a aplicação das leis e, como resultado, variados serviços de lavagem de *bitcoins*

[43] Pessoa que recebe/saca dinheiro de terceiros e transfere ou entrega esse dinheiro para terceiros.

> tornaram-se disponíveis para uso desses criminosos[44] (Richardson; North, 2017, p. 11, tradução nossa).

Os ataques por ransomware tem se tornado, ao longo do tempo, um negócio, e um negócio lucrativo. Desse modo, nota-se a expansão das suas ambições ao realizar seus ataques. Portanto, o que antes afetava usuários individuais e empresas pequenas, cada vez mais tem afetado grandes organizações mundiais e afetado dados sensíveis. Ataques de ransomware também utilizam a técnica de *phishing* (citada anteriormente) nas fases iniciais de seus ataques (Brewer, 2016). Dessa maneira, apresentar-se-á em cinco fases, um ataque de ransomware, demonstrados na figura 6.

Figura 6 - Fases de um ataque *ransomware*



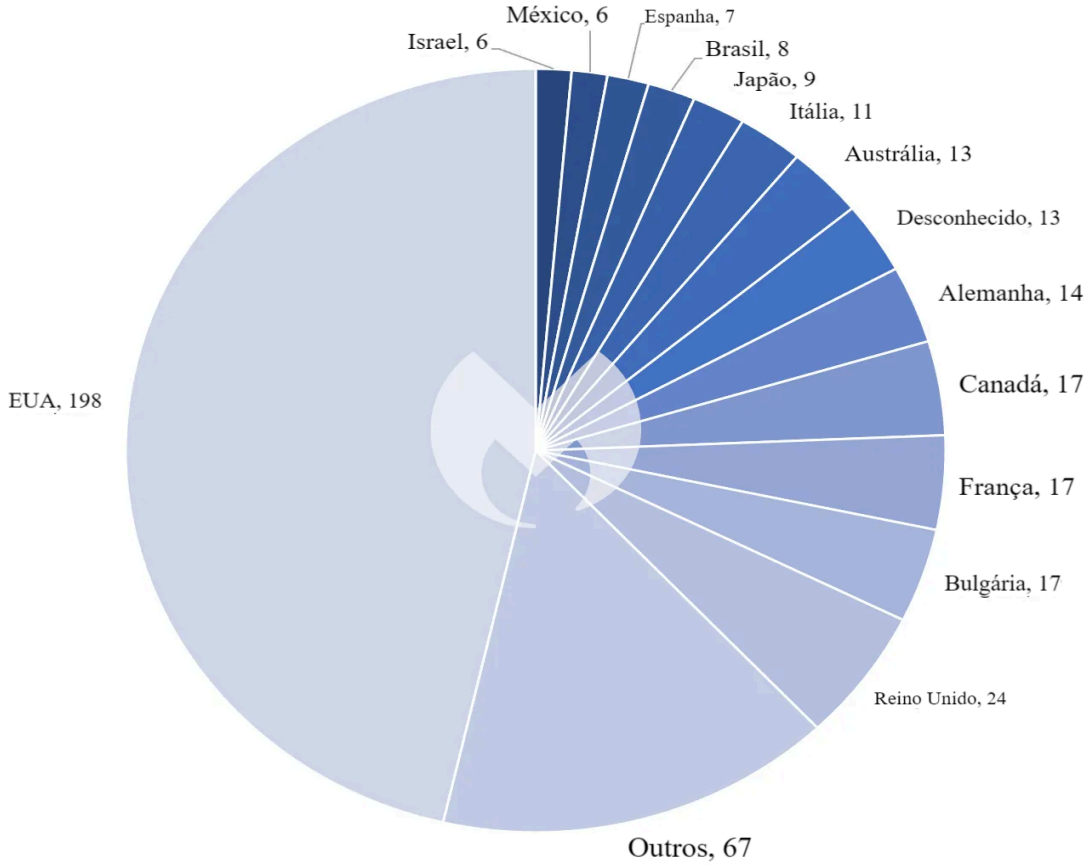
Fonte: Brewer, 2016, tradução nossa.

A fim de entender o panorama geral, os ataques direcionados à empresa, voltadas ao setor de infraestrutura e indústria tiveram seus números dobrados desde o segundo trimestre de 2022. Além disso, nos dois primeiros trimestres de 2023 já foram notados consideráveis aumentos,

[44] The methods used to laundry the ransom depend on the type of ransomware. Locking ransomware, which tend to use payment voucher systems, use online betting services in a variety of legal jurisdictions that accept the voucher codes as payment. The money is then transferred to prepaid debit cards and “money mules” are used to withdraw cash (Savage, Coogan, & Lau, 2015). Payments in Bitcoin can be used directly due to the privacy of cryptocurrency. However, many criminals are worried about law enforcement. As a result, a number of Bitcoin-laundering services have become available for criminals to use.

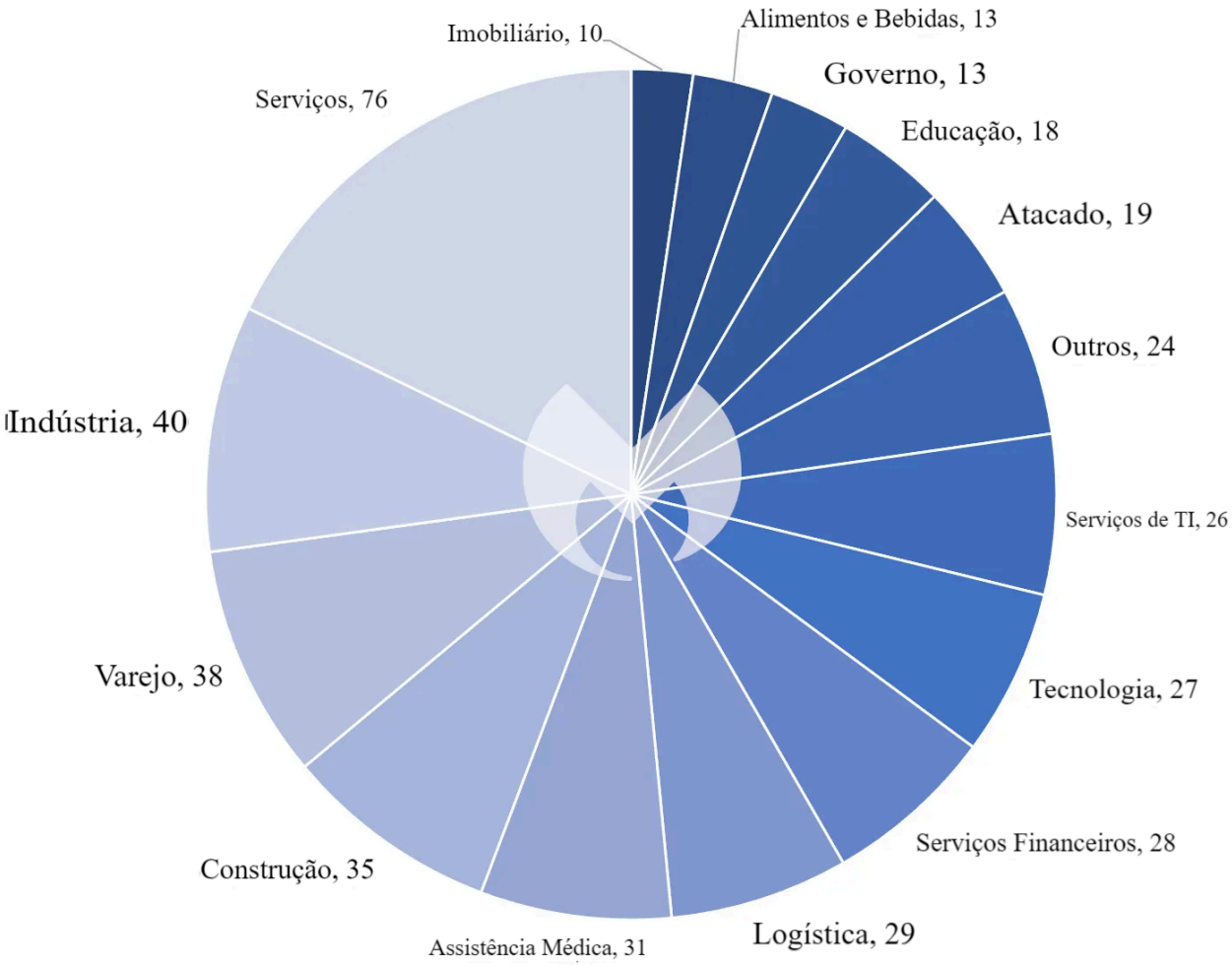
sendo este 18% entre o primeiro e o segundo trimestre. Ainda em 2022, notaram-se algumas quedas em certos momentos, como no segundo trimestre quando o grupo *hacker* Conti teve suas operações interrompidas. Dessa forma, o crescimento em relação a quantidade de ataques pode estar conectado com a queda na receita dos grupos atacantes, isto é, proporcional a recusa das vítimas em pagar os resgates requeridos pelos *hackers* (CisoAdvisor, 2023). Ademais, de acordo com os dados mais recentes obtidos, constatou-se que, em setembro de 2023, 427 ataques por ransomware foram registrados, tendo o grupo *hacker Lockbit* dominado os gráficos. Ainda, foram constatados oito ataques por ransomware no Brasil (gráfico 3), além dos mais diversos setores terem sido atacados (gráfico 4) (Malwarebytes, 2023).

Gráfico 3 - Países Atacados



Fonte: MalwareBytes, 2023, tradução nossa.

Gráfico 4 - Setores Afetados pelos Ataques



Fonte: MalwareBytes, 2023, tradução nossa.

4 ESTUDOS DE CASO

4.1 O caso da Estônia

4.1.1 O Estado da Estônia

A República da Estônia está localizada no continente europeu e ao norte do Mar Báltico, com 45.340km² de território. Ainda, sua capital é Tallinn, e o país tem suas fronteiras ligadas com a Letônia e com a Rússia (figura 7). Dentro do seu território, possui em torno de 1.345.000 milhões de habitantes. Além disso, a sua moeda adotada é o euro e o seu idioma oficial é o Estoniano, mas o Russo também ocupa o segundo lugar entre os habitantes, tendo em torno de 27% de falantes no país (Dados Mundiais, 2023).

Figura 7 - Mapa da Estônia

Fonte: Mapas do Google 2023.

A incorporação dos Estados Bálticos à União Soviética em 1940, se deu sem considerável resistência, embora a sua população como um todo tenha recebido essa assimilação com pouco ânimo. Portanto, esse processo se deu através dos próprios governos de cada um dos países

bálticos, que decidiram ceder à pressão soviética para a ocupação ‘pacífica’ desses países. (Smith, 1996).

Os países do báltico conquistaram a sua independência do Império Russo logo após a Revolução Russa, portanto, os conflitos existentes na Rússia durante a sua revolução possibilitaram um enfraquecimento do seu controle territorial. Desse modo, em 1918, a Estônia declarou a sua independência do Império, entrando em conflito e saindo vitoriosa e, sendo assim, passou a ser internacionalmente reconhecida como um Estado soberano (Rosevics, 2012).

No entanto, anos depois, em 1939, houve um encontro entre os ministros das relações exteriores tanto da Alemanha quanto da União Soviética e, nesse encontro, foi feito um acordo de não agressão entre os dois países, acordo esse que foi nomeado como Pacto Molotov-Ribbentrop. Nesse acordo, havia cláusulas secretas, que faziam uma divisão do leste Europeu em zonas de influências alemãs e soviéticas, determinado que os países bálticos estariam sob a égide soviética. Contudo, esse pacto vigorou até a invasão dos alemães ao território soviético, em 1941. Dessa maneira, essas zonas de influências foram tiradas da influência soviética entre os anos de 1941 e 1944, ocasião em que esse cenário se transformou em palco de batalha durante a Segunda Guerra Mundial. Além disso, durante o tempo de controle da região, a população desses países cooperou com ações nazistas, mantendo esperanças de que seu território lhes seria devolvido ao final da guerra. Todavia, a União Soviético venceu a guerra, e com a sua vitória, retomou os territórios do Báltico e os incorporou novamente à União Soviética. (Rosevics, 2012).

Dessa maneira, durante seus anos independentes, a Estônia teve diversos monumentos erguidos em homenagem à própria independência, mas, uma vez que a ocupação soviética tomou conta, esses monumentos símbolo do país foram destruídos. Sendo assim, em 1945, soldados soviéticos mortos na guerra foram enterrados pela segunda vez em *Tonismägi* (uma praça) com um simples memorial feito em madeira. No entanto, no ano seguinte (1946), ele foi demolido por duas meninas, como forma de vingança pelos memoriais demolidos pelos soviéticos na ocupação da Estônia. Ainda, no ano em que se seguiu (1947), outro monumento foi construído no exato lugar do anterior, este era um soldado de bronze (figura 0), que viria tornar-se o memorial de guerra mais representativo da cidade de Tallinn, na Estônia (Ehala, 2009). No entanto, o soldado de bronze representava a vitória dos soviéticos aos russos, e para muitos estonianos, representava os vários anos de repressão soviética, tornando a existência deste monumento, uma questão de debates (Melchior; Visser, 2011).

Figura 8 - O Soldado de Bronze

Fonte: DW, 2007.

Após a dissolução da União Soviética, foi esperado que a questão relativa à população russa dentro da Estônia seria resolvida por si, através da emigração. Todavia, até o fim da década de 1990, ficou claro que o "problema" da população russa não seria resolvido sozinho e, dessa forma, o Estado deveria certificar-se de que haveria integração entre esses grupos étnicos dentro do país (Raun, 2009). Portanto,

> O objetivo oficial era uma Estônia multicultural onde cada grupo étnico poderia manter seu idioma nativo e sua cultura, mas também, uma sociedade onde o estoniano seria a base para que pudesse ser estabelecido uma identidade comum e uma cidadania que pudesse comunicar-se facilmente uns com os outros. Além disso, um sistema educacional totalmente reformado estava programado para desempenhar um papel fundamental nesta transformação. O elevado prestígio do estoniano como língua oficial e reconhecimento das conquistas políticas e econômicas do país encorajou um estudo mais sério do estoniano em todos os níveis de ensino. Dessa forma, outros grupos étnicos passaram a matricular seus filhos em colégios estonianos. Ainda assim, havia muita resistência em relação ao idioma e faltava recursos ao Estado para que esses números aumentassem[45] (Raun, 2009, p. 532, tradução nossa).

[45] The official goal was a multicultural Estonia in which each ethnic group would be able to retain its native language and culture but also a society in which a functional command of Estonian, the privileged state language, served as the basis for establishing a common civic identity and an informed citizenry that could readily communicate with each other. A fully reformed educational system was slated to play a key role in this transformation. The heightened prestige of Estonian as the state language and recognition of the country's political and economic achievements did encourage more serious study of Estonian at all levels of education, and some Russian and other non-Estonian parents began to enroll their children in Estonian Language schools from the first grade. Nevertheless, much

Desse modo, não havia muitas aberturas para que essas integrações acontecessem na prática, isto é, o passado de ocupação soviética, para os estonianos, e o presente da perda de seu país para os russos, representavam muitas resistências para a integração étnica (Raun, 2009).

É importante ressaltar o Dia da Vitória, que é comemorado na Rússia no dia 9 de maio de cada ano, em representação à vitória da União Soviética contra os nazistas. Este é um importante feriado para os russos, que simboliza o orgulho nacional e homenageia aqueles mortos na Segunda Guerra Mundial (Bilefsky; Troianovski; MacFarquhar, 2023). Essa comemoração também era feita na Estônia pelos russos residentes no país, mesmo após a dissolução da União Soviética. No entanto, em 2006, no Dia da Vitória, um estoniano nacionalista estava posto em frente ao soldado de bronze, segurando a bandeira de seu país e gritando em direção ao monumento, acusando-o de ocupar o seu país e deportar o seu povo. Esse protesto foi feito em meio a vários russos que se encontravam ali para deixar flores referentes ao Dia da Vitória. Como resultado, o manifestante foi levado pela polícia, acentuando a percepção de que a bandeira da Estônia não era suportada ali, diferentemente da bandeira russa. De modo geral, a questão não agradou à população estoniana. A partir daí, gerou-se uma grande insatisfação com aquele monumento e a situação foi escalando rapidamente. Portanto, entre ataques ao monumento de um lado e a garra para protegê-lo, do outro, a polícia acabou isolando a estátua para evitar confusões e possíveis confrontos (Juurvee; Mattiisen, 2020). Então, iniciou-se o processo legal para a remoção daquela estátua da praça, com o Parlamento da Estônia aprovando a Lei de Proteção aos túmulos de guerra, onde, para fins de esclarecimento, pode-se citar o artigo 8:

> Com base nesta lei os restos mortais estão sujeitos a um novo enterro se o túmulo estiver localizado em um lugar inadequado, em particular, praças e outras áreas verdes e prédios e edifícios em áreas densamente povoadas áreas fora dos cemitérios também como lugares onde eventos de massa são organizadas ou as construções não relacionados aos túmulos estão localizados e outros locais que impeçam tratamento digno de um túmulo de guerra são lugares inadequados para um túmulo de guerra [...][46] (Diário Estadual, 2023, tradução nossa).

resistance to learning Estonian remained, and the state clearly lacked the resources—both human and material—to dramatically raise the quality of Estonian-language instruction in Russian schools.

[46] On the basis of this Act the remains are subject to reburial if a war grave is located in an unsuitable place. In particular, parks, other green areas and buildings within densely populated areas outside cemeteries as well as places in which mass events are organised or the constructions not related to the graves are located and other places which preclude dignified treatment of a war grave are unsuitable places for a war grave.

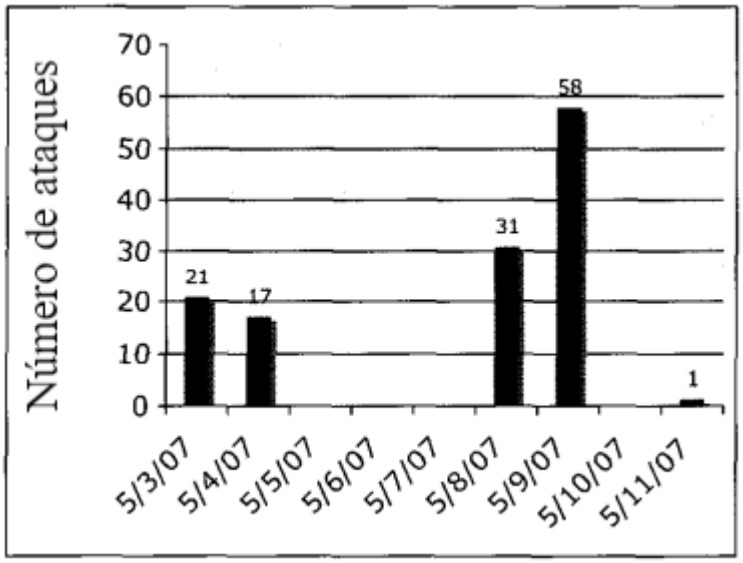
Com a lei aprovada, houve resposta por parte da Rússia, isto é, a Duma Federal[47]. Então, no dia 17 de janeiro de 2007, foi feita uma declaração rejeitando as ações do governo estoniano, criticando a lei aprovada e associando o governo da Estônia a um caminho para a glorificação do nazismo (Juurvee; Mattiisen, 2020). Sendo assim, instaurou-se um clima de tensão entre os estonianos e os russos que viviam no país. Logo, o governo da Estônia tomou a decisão de mover a estátua de bronze da praça para um cemitério militar, e essa mudança provocou grande comoção pelas ruas estonianas (Herzog, 2011). Além disso, a embaixada da Estônia na Rússia foi atacada pelos manifestantes, que atiraram pedras na fachada do prédio, quebrando algumas janelas. Esse protesto na Rússia demandava um pedido de desculpas aos russos, pela mudança da estátua de bronze (Lowe, 2007). Também, o Estado estoniano já havia discutido a mudança de local com o governo russo, no entanto, este último além de condenar o ato, também avisou que teriam consequências caso a mudança fosse efetivada (Barletta, 2017).

4.1.2 O ataque cibernético

No dia 27 de Abril de 2007, iniciou-se na Estônia uma série de ataques cibernéticos. Esses ataques coincidiram com os protestos ocasionados pela mudança de local da estátua do soldado de bronze. Eles se deram através de ataques de negação de serviço distribuído (DDoS) (Barletta, 2017). Um ataque DDoS possui como objetivo impedir completamente o funcionamento de um recurso da *Web* e, portanto, é uma completa negação de serviço (Kaspersky, 2023). Em um primeiro momento, os sites que estavam sob ataque foram do Parlamento, do primeiro-ministro, do presidente e dos principais partidos políticos. Além disso, a natureza desses ataques mostra que a inundação de dados foi feita de modo a "aleijar" o sistema de administração pública do país, além de objetivar que a confiança da população em relação ao governo e às instituições governamentais fosse deteriorada. Nos dias que se seguiram, diversos ataques continuaram a ocorrer, como pode ser visto no gráfico 5 (Barletta, 2017).

[47] Câmara baixa da Assembleia Federal da Rússia.

Gráfico 5 - Comparação Entre o Número de Ataques



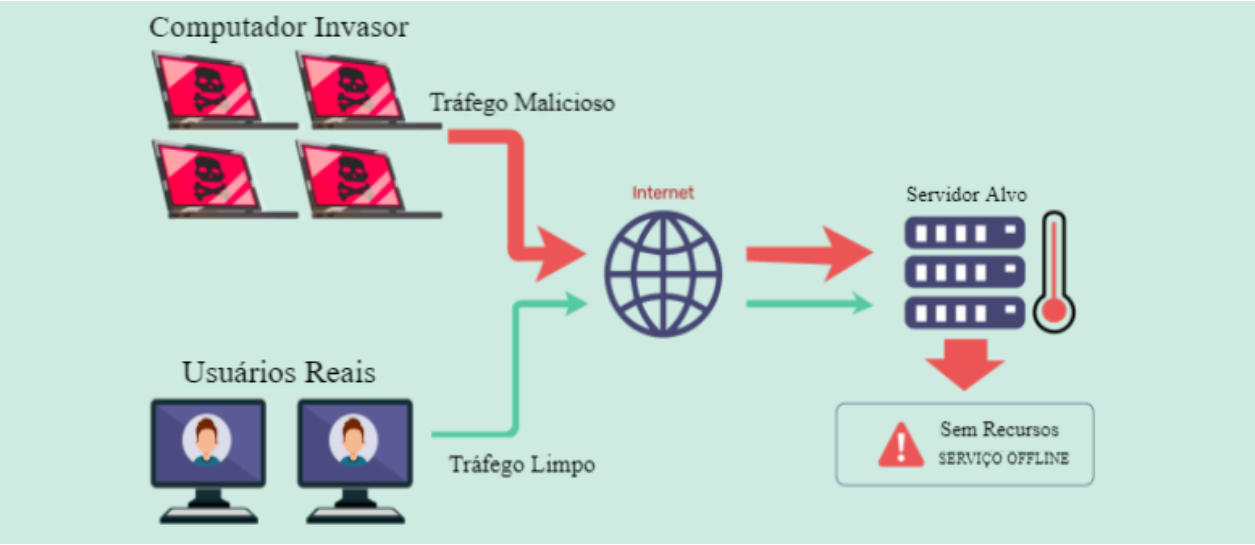
Fonte:Barletta, 2017, tradução nossa.

Portanto, esses ataques iniciaram-se com uma simples desconfiguração de sites e, conforme os dias passaram, transformaram-se em ataques DDoS nas diversas plataformas governamentais (Barletta, 2017). Esse ataque ficou registrado como o primeiro ataque cibernético direcionado à segurança nacional de um Estado. Também, o ataque ao país báltico limitou-se a gerar caos dentro do país (Greathouse, 2014). Além disso, a Estônia já era, na época, o exemplo de um futuro com a tecnologia, isso porque o país já havia informatizado, em 2007, seu sistema de educação, as eleições, sua segurança e até mesmo as operações bancárias. Desse modo, é visto que um Estado que incorpora a tecnologia nas suas infraestruturas nacionais deve estar ciente das diversas vulnerabilidades que sua estrutura pode sofrer, assim como as consequências que os ataques cibernéticos podem trazer à infraestrutura do país (Ashmore, 2009). Os ataques tiveram uma duração de três semanas, sendo a sua primeira leva muito menos elaborada e sofisticada do que a segunda parte. Mais especificamente, houve um pico desses ataques no dia 9 de maio de 2007, data em que é comemorado o Dia da Vitória pela Rússia, também houve um abrupto corte de ligações ferroviárias eram comercialmente importantes para ambos os países – o motivo alegado foi “manutenções”. Dessa forma, a Estônia enfrentou diversas consequências, como por exemplo, a baixa na produtividade e “a aquisição de alojamentos da *web* alternativos, possuindo taxas de emergência estimada em vários milhões de euros” (Pamment et al, 2019, p. 53, tradução

nossa). Ademais, o ataque afetou a população estoniana, de modo que, de imediato, tornou-se impossível acionar uma ambulância ou os bombeiros no país (Shaheen, 2014). Portanto, para melhor entender o ataque que atingiu a Estônia, far-se-á uma breve explicação de como funciona um ataque DDoS.

Ataques do tipo de negação de serviço (DDoS) são bastante comuns no meio cibernético. As vítimas desse modelo de ataque são impossibilitadas de acessar um serviço ou um site, isto é, tem seus serviços da internet interrompidos. Desse modo, o ataque DDoS fará esse trabalho de interromper um *website* através da inundação desse site com tráfego indesejado de diversos computadores. Logo, para que haja sucesso, o atacante espalhará *softwares* maliciosos para máquinas vulneráveis, geralmente através do uso de *phishing*. Então, essas máquinas infectadas irão criar uma rede de *bots*, chamada de *botnet*. Ao formar essa rede de *bots*, o atacante pode controlá-la e dar comandos à ela, comandos esses que intencionam a inundação de um site, causando a sua queda (Mercer, 2017). Na figura 9 obtém-se a compreensão gráfica desse tipo de ataque cibernético.

Figura 9 - Ataque DDoS



Fonte: Indusface, 2023.

Também, pode-se observar na linha do tempo a seguir (figura 10), a ordem em que os ataques aconteceram:

Figura 10 - Linha do Tempo dos Ataques Cibernéticos

Fonte: Pamment et al, 2019, tradução nossa.

Os ataques cibernéticos promovidos contra a Estônia em 2007 consistiram em ataques direcionados, isto é, quando os atacantes têm um alvo específico e direcionam seu ataque com um fim específico. Portanto, os riscos relacionados a ataques direcionados são mais altos, uma vez que são movidos a objetivos que podem ir além de dinheiro e buscam dados mais específicos. Desse modo, ao diagnosticar um ataque direcionado, o foco é a priorização das áreas que podem proporcionar uma reação mais rápida (SEI, 2021). Ainda assim, a Estônia conseguiu equipar-se de uma boa defesa em relação a esses ataques. Essa defesa se deu através de especialistas de segurança, além de contar com *Internet Service Provider*[48] em vários lugares do globo, tais como Estados Unidos e Israel. Também, os ataques não danificaram permanentemente as infraestruturas governamentais afetadas (Barletta, 2017).

[48] Empresa que fornece acesso à internet.

4.1.3 Origem dos ataques cibernéticos

Não há nenhuma prova de que os ataques ocorridos na Estônia foram feitos pelo governo da Rússia, embora endereços de IP relacionados aos ataques tenham vindo de endereços russos (McGuinness, 2017). Também, o governo russo negou qualquer envolvimento com os ataques. Além disso, os atacantes utilizaram-se de uma rede bastante grande de *bots* no seu ataque e, portanto, isso também inclui diversos países do globo, isto é, não há origem em somente um país (Barletta, 2017). Ainda assim, vale ressaltar alguns discursos proferidos por membros do governo de ambos os países na época dos ataques. O então presidente estoniano, Toomas Hendrik, declarou no mês seguinte aos ataques:

> De qualquer forma, foi mais do que um crime comum. Alguém pagou muito dinheiro para poder pagar o serviço de criminosos da Internet. Se você observar o curso dos ataques, notará que eles pararam exatamente à meia-noite. Perguntei ao CERT[49] o que isso significava. E me disseram: Bem, foi quanto pagaram pelo ataque naquele dia. Foi assim que foi organizado, e certamente não por um louco sentado em São Petersburgo que quer irritar a Estónia[50] (Frant'furter Allgemeine, 2007).

Além do presidente da Estônia, no dia 9 de maio daquele ano, também houve um breve discurso por parte do presidente Vladimir Putin, da Rússia: "Aqueles que tentam hoje, corromper os monumentos feitos a heróis de guerra estão insultando seu próprio povo, semeando discórdia e desconfiança entre Estados e pessoas" (Pamment et al, 2019, p. 58, tradução nossa). Outrossim, cabe ressaltar que os ataques seriam um bom teste para as armas cibernéticas russas, de maneira a entender o campo cibernético em uma região da qual a Rússia é bem ativa (Pamment et al, 2019.

4.1.4 Efeitos

A Estônia sofreu diversas complicações devido aos ataques ocorridos em 2007, sendo algumas de imediato e curto-prazo, e outras que somente puderam ser sentidas a longo-prazo. Portanto, de imediato, os efeitos que foram sentidos estavam relacionados ao impacto direto que

---

[49] Organização responsável pelo gerenciamento de incidentes de segurança.

[50] Es war jedenfalls mehr als gewöhnliche Kriminalität. Jemand hat sehr viel Geld bezahlt, um sich den Service von Internetverbrechern leisten zu können. Wenn man sich den Verlauf der Angriffe anschaut, fällt auf, dass sie exakt um null Uhr Mitternacht aufhörten. Ich habe CERT gefragt, was das zu bedeuten hat. Und mir wurde gesagt: Naja, so lange haben sie an dem Tag für den Angriff eben bezahlt. Es war also organisiert, und sicherlich nicht von einem Verrückten, der in Sankt Petersburg sitzt und Estland ärgern will.

os ataques tiveram tanto no governo, quanto no país. Já em se tratando de longo prazo, pode-se citar a relação do país com a Rússia, que se manteve estremecida e tensa. Todavia, embora a grande dependência do país o tornava vulnerável para ataques cibernéticos capazes de paralisar o país, este ataque não causou grandes danos às infraestruturas cibernéticas da Estônia (Joubert, 2012). Além disso, após a recuperação dos ataques, a Estônia tornou-se referência dentro da segurança tecnológica (Ashmore, 2009). Também, a partir do ataque que ocorreu no país, evidenciou-se as novas possibilidades dentro da esfera tecnológica, sendo entre elas, a violência digital. Dessa maneira, a resposta internacional para esses incidentes ocorridos na Estônia foi rápida, tendo o país uma considerável rapidez na sua reconstrução. Então, entre os auxílios recebidos, destaca-se a ajuda da Organização do Tratado do Atlântico Norte (OTAN), da qual a Estônia é membro desde 2004 (Herzog, 2011). Ademais,

> O conceito de Segurança Nacional, que foi atualizado e aprovado em maio de 2010, representa a segunda maior política de resposta à cibersegurança do governo estoniano. Ele reconhece a crescente confiança em tecnologias de informação e comunicação (ICT) junto com o aumento das ameaças representadas por terroristas e grupos do crime organizado. O cibercrime deveria receber atenção especial, assim como soluções devem ser encontradas em conjunto com agências a níveis nacionais e internacionais (Warren, 2013, p. 77, tradução nossa).

Recentemente, em 2022, a Estônia registrou outra onda de ataques cibernéticos, sendo estes dessa vez reivindicados pelo grupo *hacker Killnet* que possui a sua base na Rússia. Esses novos ataques foram, assim como aqueles em 2007, ataques DDoS. Além disso, foram afetados órgãos governamentais, serviços de pagamento e bancos e serviços públicos. Os rumores em torno desse novo ataque relacionam as recentes ofensivas contra a Estônia com a remoção de um tanque russo, que era tido como um monumento à Rússia, em uma cidade na fronteira leste do país. Além disso, o diretor executivo da CERT Estônia alegou que os ataques cibernéticos contra a Estônia dobraram após o início da guerra russo-ucraniana. Apesar disso, a Estônia possui uma grande infraestrutura cibernética e de defesa cibernética, ocupando o terceiro lugar no *ranking* mundial, estando atrás somente dos Estados Unidos e Arábia Saudita (CisoAdvisor, 2022).

4.2 O caso do Irã

4.2.1 O Estado do Irã

A República Islâmica do Irã é um país que se encontra situado entre o Mar Cáspio e o Golfo Pérsico, e possui fronteira direta com vários países, sendo estes: Afeganistão, Iraque, Turcomenistão, Turquia, Armênia, Azerbaijão e Paquistão (figura 11). A sua capital é Teerã e seu idioma oficial é o Persa (ou Farsi). Além disso, sua moeda é o Rial iraniano e o país conta com uma população de 88,551 milhões e uma área territorial de 1.745.150 km² (Dados Mundiais, 2023).

Figura 11 - Mapa do Irã

Fonte: Google Maps 2023.

Durante a Guerra Fria, dentro do contexto bipolar, o Irã se posicionava como aliado dos Estados Unidos e de Israel (Jacinto, 2023). No entanto, a Revolução Iraniana em 1979 transformou o panorama internacional para o Irã, uma vez que a sua relação com os Estados Unidos ficou deteriorada e o país inseriu-se internacionalmente de maneira anti-imperialista e contestadora, além de incorporar a religião às suas relações internacionais (Do Espírito Santo; Baldasso, 2017). No entanto, após a Guerra Fria, ao analisar o panorama regional da época, Israel enxergou o fim do mundo bipolar como uma abertura para o Irã colocar-se como uma potência na região, impondo a sua própria ordem. No entanto, esse receio por parte do Estado israelense se devia à sua própria vontade de tornar-se uma potência regional (Jacinto, 2023).

Portanto, de maneira estratégica, em 1992, Israel apresentava o Irã como uma ameaça através do fundamentalismo religioso na tentativa de fazer os Estados Unidos adotarem essa narrativa (Jacinto, 2023). Dessa forma, os norte-americanos adotaram uma política de contenção em relação ao Irã, esse endurecimento teve influência da forte presença de israelenses na política interna do país. Desse modo, durante os dois mandatos do presidente estadunidense, Bill Clinton (1993-2001), os Estados Unidos adotaram políticas duras em relação ao Irã, sob a justificativa de que o país financiava grupos terroristas e desenvolvia armas de destruição em massa. Essa contenção se refletiu em ações como sanções econômicas, banimento de transações comerciais e a punição, pelos Estados Unidos, a outros países que fizessem investimentos no Irã acima de US$40 milhões. No entanto, com a eleição do presidente Khatami, em 1997, que destacava-se pelas mudanças anunciadas no Estado iraniano, houve avanços na política estadunidense em relação ao Irã e com o encerramento do governo de Clinton, algumas sanções aos produtos iranianos foram retiradas (Cunha, 2021).

A partir da administração de George W. Bush (2001-2009) e dos ataques do 11 de setembro de 2001, as expectativas do governo de Khatami não se concretizaram, e o Irã foi incluído na lista dos países que faziam parte do "Eixo do Mal" – apoiadores do terrorismo –, por isso deveriam ser combatido. Dessa maneira, para o governo estadunidense, o Irã tornou-se um Estado indigno de confiança, que viabilizava o fundamentalismo religioso e que, secretamente, procurava um mecanismo nuclear para promover ameaças regionais e mundiais (Carneiro, 2018).

Com base nessa alegação dos estadunidenses, faz-se necessário apresentar o histórico do programa nuclear iraniano, de modo que se compreenda sua estrutura e seus objetivos. Assim, em 1953, o então presidente estadunidense, Dwight Eisenhower, sugeriu a criação de uma agência atômica para que o uso da energia nuclear pudesse ser regulado. A partir dessa premissa, houve a criação da Agência Internacional de Energia Atômica (IAEA). Portanto, através de outra iniciativa promovida por Eisenhower, o projeto "Átomos para a paz", que propunha que os Estados Unidos disponibilizariam o conhecimento e tecnologia necessários para que houvesse um desenvolvimento pacífico da energia nuclear, em 1957, os Estados Unidos firmaram um acordo com o então presidente iraniano, Mohammed Reza Pahlevi, para o uso pacífico da energia nuclear. Então, em 1967, dez anos após o acordo, chegou ao Irã um reator nuclear com a finalidade de pesquisa (Rocha, 2022). Ainda, em 1970, entrou em vigor o Tratado de Não-Proliferação Nuclear (TNP) que objetiva o desarmamento nuclear total, assim como o

fomento ao seu uso pacífico. Neste tratado, países que, de fato possuem armas nucleares, não fazem parte dele e, portanto, não estão submetidos aos seus dispositivos (Brasil, 2022).

Todavia, o programa nuclear do Irã, após a Revolução Iraniana de 1979, foi considerado não importante pelo aiatolá Khomeini, Líder Supremo do país e que se impunha aos demais Poderes estatais. Desse modo, o programa somente voltou a obter mudanças após a morte de Khomeini. No entanto, seu sucessor, aiatolá Ali Khamenei, já tinha outra postura em relação à política exterior do país, se mantendo na neutralidade e dando mais liberdade ao presidente. Assim, em 1997, durante a presidência de Mohammad Khatami, o programa nuclear iraniano passou por razoável melhora no seu desenvolvimento (Lima, 2016). Na mesma época o programa já era visto com desconfiança e como uma ameaça à ordem internacional, portanto, em dezembro de 2002, os Estados Unidos divulgaram imagens de satélite de instalações nucleares iranianas, em Natanz e Arak, evidenciando o empenho do Irã em desenvolver sua capacidade de produção de armas nucleares.

Diante de tais acusações por parte do governo estadunidense, o presidente Khatami declarou que era signatário do TNP e que em suas instalações não se desenvolviam armas nucleares. Contudo, uma equipe da AIEA visitou as instalações nucleares iranianas para fins de inspeção, e de fato, encontraram irregularidades em relação ao TNP, mas também impressionaram-se com o avanço que o programa tinha obtido até ali (Carneiro, 2018). Ainda, depois dessa visitação de inspeção

> o país recebeu então um ultimato da agência para que revelasse toda atividade do seu programa nuclear até uma data no mesmo ano. Destacando que, como participante do Tratado de Não Proliferação Nuclear, o Irã precisaria avisar a Agência Internacional de Energia Atômica, 180 dias antes de introduzir qualquer material nuclear (Rocha, 2022, p.33-34).

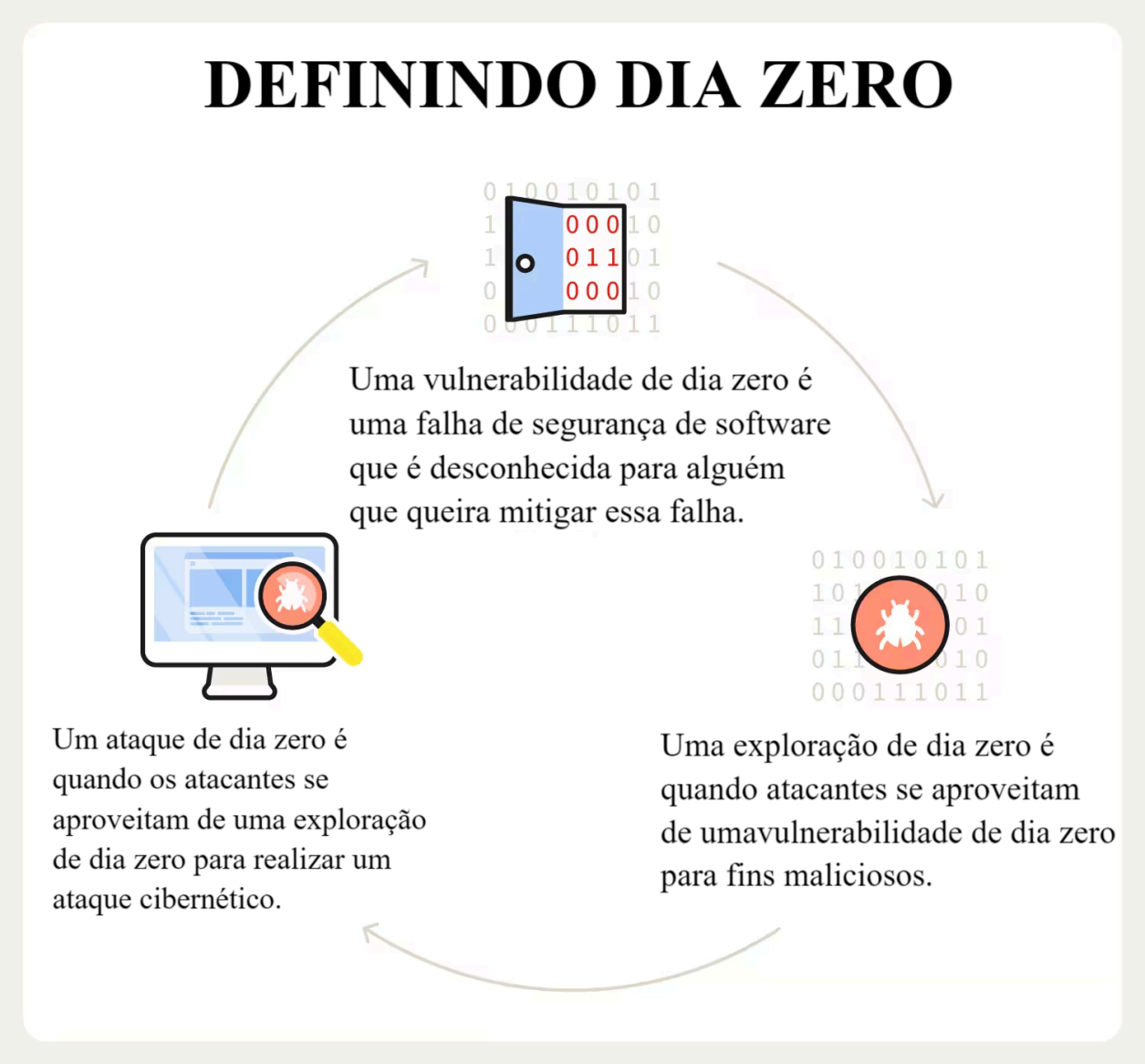
Dessa maneira, o Irã recebeu acusações de que seu programa buscava o enriquecimento do urânio para fins militares. Essa desconfiança se fundamentava no fato de que, para a geração de energia elétrica, somente são necessários até 5% de enriquecimento de urânio, ao passo que o governo iraniano estava enriquecendo o urânio a 20%. Ainda assim, para que armas nucleares possam ser desenvolvidas, são necessários 90% de enriquecimento de urânio e, embora o país não estivesse atingindo esse nível, os 20% indicava que os 90% não eram inatingíveis (Rocha, 2022). Consequentemente, o Conselho de Segurança das Nações Unidas (CSNU) solicitou ao Irã

que este seguisse as regras determinadas pela AIEA, para que assim, pudesse comprovar que o seu programa nuclear era desenvolvido para fins pacíficos. Além disso, ainda foi pedido ao Irã que suspendesse temporariamente o enriquecimento de urânio. No entanto, o governo iraniano não acatou essas resoluções, não aceitando a exigência do CSNU. Logo, com o descumprimento das exigências feitas pelo CSNU, foram lançadas diversas sanções ao Irã, que se intensificaram conforme o programa nuclear iraniano se desenvolveu. Ademais, é interessante ressaltar que todos os membros permanentes do CSNU são potências nucleares (Caetano, 2014). Desse modo, de fato as sanções enfraqueceram o desenvolvimento do programa nuclear do Irã, uma vez que estas têm impactos consideráveis na economia do país. Ainda, os Estados Unidos a partir da administração Obama (2009), passou a ter uma posição mais dura em relação ao programa iraniano, visto que o Irã estava mantendo-se firme contra as investidas estadunidenses no que se refere ao seu desenvolvimento nuclear (Caetano, 2014).

4.2.2 Stuxnet

No início de 2010, foi notado um funcionamento anormal das centrífugas de enriquecimento de urânio nas instalações nucleares de Natanz, parte do programa nuclear do Irã. Havia crescido o número de substituições de centrífugas em um encurtado período de tempo. No entanto, até ali, ninguém conseguiu distinguir exatamente o que estava acontecendo que estava levando as centrífugas a falharem (Rocha, 2022). Contudo, quando um dos computadores da instalação nuclear começou a se reiniciar sozinho em *looping*, uma empresa de antivírus da Bielorrúsia foi contatada a fim de verificar o que estava errado. Dessa forma, a empresa detectou um *worm* de tamanho e complexidade surpreendentes, o Stuxnet. O *worm* Stuxnet foi introduzido através de uma *zero-day vulnerability*, ou seja, uma vulnerabilidade no sistema que ainda não era do conhecimento humano (figura 12). Além disso, levou tempo para que a estrutura do Stuxnet fosse compreendida mas, enfim, chegou-se a uma constatação: uma vez que o *worm* estivesse dentro do sistema de controle, ele causaria um descontrole nas centrífugas de enriquecimento de urânio, acabando assim por destruí-las (Collins; McCombie, 2019).

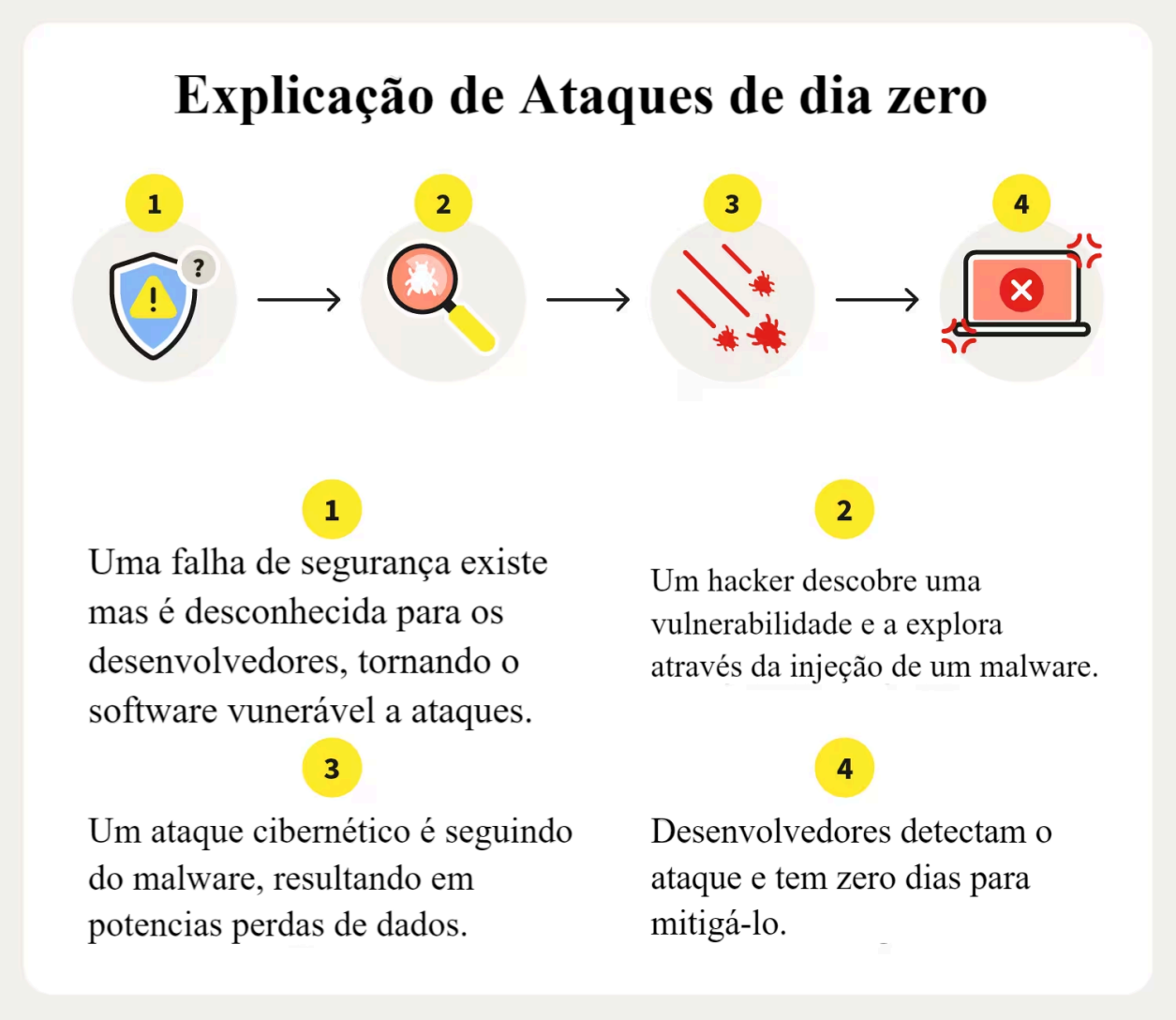
Figura 12 - Definição de Dia Zero



Fonte: Stouffer 2023, tradução nossa.

Os *malwares* relacionados aos ataques cibernéticos considerados *zero-day-attacks* podem envolver a táticas de engenharia social ou podem aplicar o método de *phishing* (Stouffer, 2023). Esse tipo de ataque está graficamente explicado na figura 13.

Figura 13 - Ataques de Dia Zero



Fonte: Stouffer 2023, tradução nossa.

O *worm* Stuxnet foi estruturado sobre variadas linguagens de programação e utilizadas quatro *zero-day vulnerabilities*, isto é, um *worm* complexo e que estima-se ter requerido um grande time de especialistas, além de um considerável financiamento e bons recursos (Baezner; Robin, 2017). Além disso, o Stuxnet é capaz de se autocopiar em *drives* removíveis. Assim, uma vez dentro de uma rede, ele pode se autocopiar para outros computadores que fazem parte dessa mesma rede (Grayson, 2011). Ademais, especialistas constatou-se que um *worm* com a estruturação do Stuxnet, além do seu nível de financiamento, só poderia ser um feito vindo de um

Estado. Portanto, o ataque à instalação iraniana pode ter sido proposital, uma vez que os criadores obtinham um largo conhecimento a respeito da estrutura das instalações nucleares do Irã (Baezner; Robin, 2017).

Desse modo, a proliferação do Stuxnet pelo mundo, que fugiu do controle das autoridades e profissionais que o criaram, poderia ter gerado como consequência, a utilização desse *worm* como ferramenta para grupos terroristas, muito embora essa possível consequência fosse uma ameaça da qual não foi concretizada devido à complexa estrutura que a compõe e, dessa forma, para alguém utilizá-la para fins pessoais, seriam necessários recursos que não estão disponíveis para qualquer ator (Baezner; Robin, 2017). Portanto, o *worm* Stuxnet foi um marco importante para o que compõe a ciberguerra. Embora já tivessem existido outras formas de ataques anteriores ao Stuxnet, esse se coloca como o primeiro na história a, de fato, conseguir afetar algo fisicamente. Dessa forma, o Stuxnet representou um passo muito além para a segurança cibernética, uma vez que a partir dele pôde-se enxergar como a ciberguerra pode ter impactos estruturais, além de econômicos (Rocha, 2022).

4.2.3 Origem do ataque

O Irã acusou o Ocidente ou, mais especificamente, a Organização do Tratado do Atlântico Norte (OTAN), de estar por trás do ataque. De fato, especialistas apontaram que as condições direcionavam a autoria aos Estados Unidos e a Israel, tendo muito mais dúvidas em relação à participação do Estado israelense. À vista disso, o jornalista do *The New York Times,* David E. Sanger relatou em seu livro que os Estados Unidos teriam conduzido uma operação cibernética secreta, de nome *Operation Olympic Games* (Operação Jogos Olímpicos) (Baezner; Robin, 2017). Portanto, Sanger, em seu texto intitulado *Obama Order Sped Up Wave of Cyberattacks Against Iran,* expõe que houve uma operação do governo dos Estados Unidos que teria começado no Governo Bush e teve sua continuidade no Governo Obama, cuja finalidade foi promover uma série de ataques cibernéticos contra as instalações nucleares iranianas, a fim de atrasar o processo de desenvolvimento das mesmas. Além do mais, mesmo quando o *worm* Stuxnet acabou, por um descuido, vazando para fora do alvo (Irã), a operação ainda teria continuado ativa e destruiria muitas outras centrífugas, gerando prejuízos de tempo e dinheiro ao Estado iraniano (Sanger, 2012). Além de o jornal *The New York Times*, pode-se citar também, o *The Washington Post*

como outra mídia estadunidense que expôs os Estados Unidos e Israel como autores dos ataques (Nakashima; Warrick, 2012).

4.2.4 Efeitos

O Irã denunciou o ataque Stuxnet como um ato de ciberguerra e, embora tenha efetuado tentativas de remoção do *worms* das suas redes, não foi possível uma vez que ele possui a capacidade de sofrer mutações enquanto continua se espalhando. Em decorrência desse fato, no fim de 2010 as autoridades iranianas anunciaram que levariam diversos meses para que o *worm* viesse a ser totalmente removido dos seus sistemas, sendo necessária, então, a paralisação das suas atividades (Buxton, 2022). Ainda, o ataque atrasou o programa nuclear iraniano, inviabilizando, ainda que temporariamente, o possível desenvolvimento de armas nucleares, mesmo que não haja informações a respeito de o país estar de fato, neste caminho (Jorge, 2012).

Além disso, em 2015, cinco membros do CSNU juntamente com a Alemanha, aceitaram retirar as sanções relacionadas ao programa nuclear iraniano em troca da cooperação do Irã em desacelerar seu programa nuclear, isto é, manter seus trabalhos somente para fins comerciais, industriais e médicos, alinhando-se com o TNP (G1, 2017). Esse acordo, que foi chamado de *Joint Comprehensive Plan of Action* (JCPOA), foi implementado efetivamente a partir de Janeiro de 2016. Sendo assim, a AIEA verificou a implementação, por parte do Irã, das principais medidas do acordo (U.S Department of State, 2015). Dessa forma, entre as medidas acordadas, o Irã concordou em manter seu enriquecimento de urânio em moldes específicos e até somente 3.67% de enriquecimento, assim como também aceitou não alterar os modelos de centrífugas utilizados (JCPOA, 2015). No entanto, em 2018, o então presidente dos Estados Unidos, Donald Trump anunciou a saída do país do acordo nuclear feito com o Irã, afirmando que o país asiático era o principal país patrocinador do terrorismo. Como resposta, o presidente iraniano, Hasan Rouhani, afirmou que permaneceria no acordo caso as questões acordadas nele (retirada de sanções) permanecesse (G1, 2018). Todavia, as sanções foram impostas novamente pelos Estados Unidos e, portanto, na falta de seguimento às medidas do acordo, o Irã começou a descumprir os compromissos firmados (BBC, 2019). Atualmente, após a retirada estadunidense do acordo feito em 2018, o Irã violou as regras do acordo e continuou desenvolvendo seu programa nuclear, houve uma tentativa de reatar esse acordo, no entanto, fracassou repetidamente. Ainda assim, ao

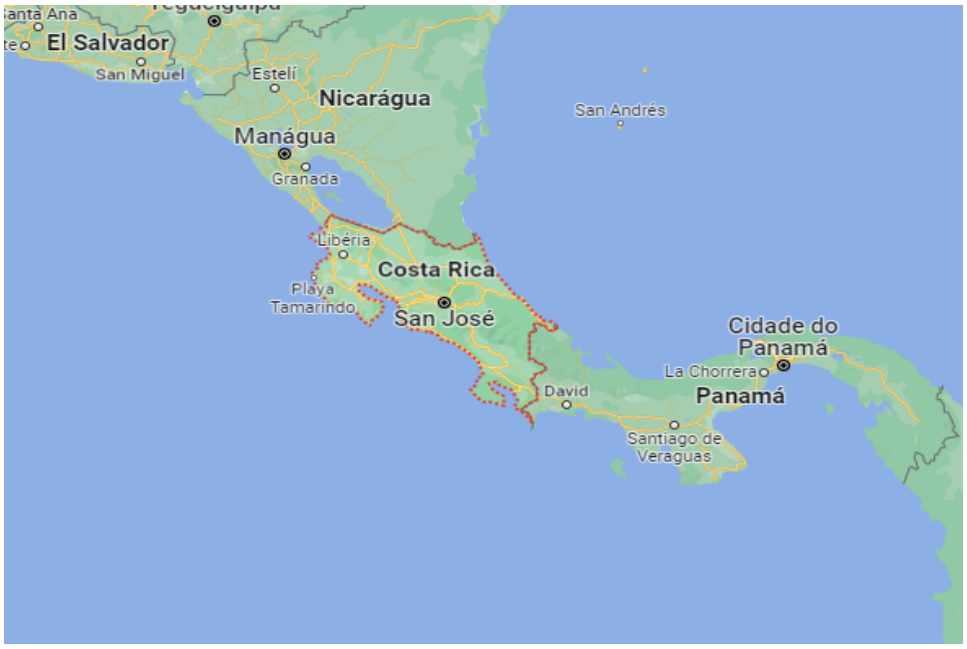
utilizar Omã como intermediário, as discussões acerca desse assunto voltaram a ser feitas. Dessa forma, o governo do atual presidente dos Estados Unidos, Joe Biden, alegou que estaria disposto a impedir que o Irã tivesse poder suficiente para uma bomba nuclear através de meios diplomáticos. Sendo assim, os Estados Unidos aprovaram a transferência de US$2,7 bilhões de fundos para bancos iranianos, sendo esta medida uma possível construção de confiança nas relações entre os dois países (CNN, 2023).

4.3 O caso da Costa Rica

4.3.1 O Estado da Costa Rica

A República de Costa Rica é um país da América Central banhado pelo mar do Caribe ao leste e pelo oceano Pacífico a oeste. O país faz fronteira com o Panamá ao sul e com a Nicarágua ao norte (Figura 14). Sua capital é San José, possui o idioma espanhol como oficial e sua moeda é o colón costarriquenho. Além disso, possui uma população de aproximadamente 5,181 milhões, distribuídos em sua área total de 51.100 km² (Dados Mundiais, 2023).

Figura 14 – Mapa da Costa Rica



Fonte: Mapas do Google 2023.

No ano de 1948 houve uma corrida presidencial na Costa Rica, onde o candidato da oposição, Otilio Ulate, venceu as eleições daquele ano, derrotando o então atual presidente do país, Rafael Angel Calderón. No entanto, o partido comunista, *Vanguardia Popular*, juntamente do seu presidente, anularam os resultados daquela eleição. Desse modo, a resposta da oposição veio em forma de luta armada, todavia, os rebeldes (oposição) conseguiram derrotar as forças governamentais e seus aliados. Desse modo, o líder dessa revolução, José Figueres, estabeleceu na Costa Rica uma junta revolucionária que governaria o país durante dezoito meses, sendo após esse período, dada a oportunidade a Ulate de cumprir seus quatro anos de mandato. Sendo assim, a Revolução de 1948 foi uma ruptura no padrão costarriquenho de relações sociais e políticas pacíficas (Longley, 1993). Outra característica distinta da revolução foi proclamada no dia 11 de outubro de 1948, e oficializada na Constituição através do artigo 12, nele constava a abolição das forças armadas. Essa medida foi incorporada após a vigência do governo provisório (Sarmento, 2023).

Além disso, cabe expor a relação do país latino-americano com os Estados Unidos na revolução de 1948, onde, dado o cenário do pós-Segunda Guerra Mundial, o Estado norte-americano, em busca de minar a influência soviética e o surgimento de movimentos comunistas dentro do continente americano, buscou-se criar um sistema interamericano. Desse modo, a Costa Rica tornou-se o primeiro teste do que viria a ser uma política de contenção do comunismo no território latino-americano. Ainda em 1945, o governo dos Estados Unidos já estava preocupado com a infiltração soviética na América Latina, portanto, adotou um posicionamento rígido em relação a *Vanguardia Popular*, ligando o partido ao movimento comunista internacional. Ao longo dos anos que se seguiram, o governo norte-americano manteve-se alerta em relação ao partido comunista e as suas ações. No entanto, conforme crescia a tensão e a pressão da Guerra Fria, os Estados Unidos realocaram o seu embaixador na Costa Rica, visto que este simpatizava com o governo do partido comunista que estava no poder. Mais tarde, no ano da revolução, oficiais estadunidenses na Costa Rica reportaram que o número de propagandas anti-Estados Unidos e pró-União Soviética aumentaram consideravelmente, então, quando irrompeu o conflito, os Estados Unidos tomaram ações que ajudaram a garantir a vitória rebelde no país. Ainda assim, nenhum plano foi formado pelo governo Truman para que a vitória rebelde fosse garantida no país centro-americano, no entanto, quando a oportunidade se

apresentou, os Estados Unidos não hesitaram em agir de modo a ajudar na vitória da oposição (Longley, 1993).

Sendo assim, a Costa Rica se fez presente como uma exceção em sua região geográfica, isto porque é uma área de constantes tentativas de intervenções militares, oposto ao que acontece em território costarriquenho. Desse modo, a Costa Rica tem níveis de bem-estar acima da média latino-americana e, liga-se isso à possibilidade de maior investimento em educação e saúde em consequência do processo de desmilitarização (BBC, 2022). Portanto, nos primeiros vinte e cinco anos da desmilitarização, os investimentos destinados à educação foram de 15% para 35%, assim como o aumento também se refletiu na área da saúde, que recebeu 29% do PIB (EL País, 2018). Ainda assim, o atual presidente da Costa Rica é o economista Rodrigo Chaves, eleito em 2022, em uma eleição que bateu recordes de abstenção, sendo essa de 43% e grande polarização política (BBC, 2022).

Foi a partir dos anos 1970, quando a Costa Rica abandonou certos dogmas da Guerra Fria. O país livrou-se das tensões e abriu as suas relações diplomáticas a todos os países, inclusive os socialistas (Facio, 2015). Agora, em termos de segurança nacional, o país encontra-se prejudicado, visto que se o Estado que não possui forças armadas, em tese, não necessita de um plano de segurança nacional. Desse modo, se faz necessário um plano de ação de modo a garantir os interesses nacionais. Além disso, as ameaças à integridade de um Estado não advêm somente de outros Estados, atores não estatais também podem se configurar em um risco. Nesse contexto, a Costa Rica foca sua política de segurança na ausência de forças armadas. Por conseguinte, os costarriquenhos possuem a tendência de alinhar as suas políticas exteriores de acordo com o governo em exercício, não constituindo uma política de Estado para o setor, o que gera prejuízo a longo prazo (Zamora, 2012).

Contudo, retomando o tópico das suas relações com os Estados Unidos, a Costa Rica recebe assistência norte-americana para o seu combate ao tráfico de drogas e em relação a crimes transnacionais. Além disso, a assistência por parte dos Estados Unidos também engloba o suporte ao desenvolvimento econômico costarriquenho e a segurança na América Central. Portanto, desde 2018, o Departamento de Estados dos Estados Unidos e a Agência para o Desenvolvimento Internacional, já alocaram cerca de $347 milhões para assistência à Costa Rica (U.S Department of State, 2023).

4.3.2 O ataque de ransomware

Os ataques por *ransomware* não são técnicas recentes, é uma expressão evolutiva do *malware*, onde são aproveitadas ações como o ato de abrir um email ou o clique para exibir uma imagem, para permitir que um programa malicioso possa ser ativado de maneira silenciosa, de modo que passe despercebido. Portanto, na segunda-feira do dia 18 de abril de 2022, o Ministério de Finanças da Costa Rica foi vítima de um ataque de *ransomware*. O ato teve início com os perpetrantes do ataque tendo acesso às credenciais de login de funcionários do governo, que nada detectaram, mesmo quando a ação já migrava para outros sistemas do governo. Esse ataque foi provocado pelo grupo Conti. Assim, dois sistemas governamentais principais foram afetados, a Administração Virtual de Impostos e o Sistema de Informação Aduaneira, além de vários servidores e diversos arquivos relativos aos impostos do país.

Sendo assim, O grupo Conti utilizou-se de uma conta anônima em uma rede social para mandar informações ao governo costarriquenho e, entre as postagens feitas pelo grupo, havia detalhes de como o grupo agiu e os tipos de dados que roubaram, assim como o valor requerido para a devolução dos dados e do acesso aos sistemas governamentais. Na figura 15, é mostrada a mensagem inicial do grupo ao governo da Costa Rica (Datta, 2023). Cabe ressaltar que na data em que os ataques iniciaram, Carlos Alvarado ainda era o presidente da Costa Rica, uma vez que Rodrigo Chaves, vencedor das eleições presidenciais no país, somente assumiria seu cargo no dia 8 de maio de 2022. Desse modo, Alvarado alegou que os ataques às plataformas governamentais da Costa Rica possuíam o objetivo de desestabilizar o país enquanto este passava por uma transição. Ainda, ele afirmou que especialistas já estariam trabalhando nos danos feitos pelos *hackers*, e que o país não pagaria nenhum tipo de resgate ao grupo (Ciso, 2022).

Figura 15 - Mensagem Inicial do Grupo Hacker

Fonte: Security Affairs 2022, tradução nossa.

Além disso, também cabe ressaltar o fato de que o governo costarriquenho nunca inventariou seus sistemas ou seus dados em relação à sensibilidade que eles carregavam, ou em relação às suas necessidades operacionais e, portanto, de maneira geral, não havia um planejamento de segurança relacionado à área cibernética (Datta, 2023). Logo

> Meses antes do ataque, *WizardSpider*[51] juntou-se em várias redes sociais do governo da Costa Rica e fez amizade com os profissionais funcionários do governo costarriquenho, redes essas onde os usuários solicitavam e distribuíam conselhos. Nessas comunidades virtuais profissionais, o *WizardSpider* tinha como alvo aqueles usuários que lamentavam abertamente sobre o seu trabalho para que eles pudessem aprender mais rapidamente sobre as falhas, desorganização de dados e outros problemas operacionais das redes governamentais. Sendo assim, o *WizardSpider* forneceu as informações obtidas para o grupo Conti para que o grupo pudesse então esquematizar sua estratégia para o ataque de *ramsonware*[52] (Datta, 2023, p. 7, tradução nossa).

Dessa forma, há dois tipos de abordagens em ataques *hackers* e o grupo Conti fez uso das duas abordagens simultaneamente para efetuar o seu ataque à Costa Rica. Primeiro, espelhou-se em uma abordagem de acesso e exfiltração, tendo como objetivo a liberação desses dados de

[51]Afiliado do grupo Conti.

[52]Months before the attack, WizardSpider had joined multiple Costa Rican government social networks and befriended Costa Rican government employees' professional groups where users requested and dispensed advice. In these virtual professional communities, WizardSpider targeted users that openly bemoaned about their work to quickly learn about process failures, data disorganization, and other operational problems such as lack of transparency and approvals. They fed that information to Conti, providing Conti information as ammunition to strategize on their ransomware attack vector and attack surface.

maneira gradativa, tendo como consequência a exposição das vítimas e o dano causado à integridade da fonte. A segunda abordagem utilizada consistiu na violação dos sistemas, tornando os dados de origem criptografados, e, na sequência, passou a ser requisitada uma quantia específica em dinheiro para que a vítima pudesse receber a chave para descriptografar seus dados. Nessa segunda situação, torna-se inviável que os dados sejam acessados, tornando seu funcionamento impossível. Na figura 16, apresenta-se uma linha do tempo de como os acontecimentos se deram durante os ataques sofridos pelo governo da Costa Rica, (DATTA, 2023). Desse modo, o governo da Costa Rica passou por grandes dificuldades, uma vez que produziu danos significativos às plataformas governamentais. Portanto, um exemplo dessa dificuldade foi quando o país precisou pedir para a sua população que fizesse as contas de seus impostos à mão e que realizasse os seus pagamentos pessoalmente nos bancos (Greig, 2022).

Figura 16 - Linha do Tempo

DATA	INCIDENTE	RESPOSTA
Domingo, 17/04	Servidores do Ministério de Finanças são comprometidos.	Dia 0: Sem resposta.
Segunda, 18/04	Grupo Conti posta exfiltração de dados fiscais.	Dia 1: Ministério das Finanças reporta problemas técnicos mas sem referência ao ataque ou nota de resgate.
Terça, 19/04	Grupo Conti ameaça a vazar/vender dados e pede resgate de U$S10 milhões.	Dia 2: Devido a várias páginas do governo estarem no mesmo servidor, todo o servidor foi desconectado sem recuperação, deixando todas as comunicações no escuro.
Quarta, 20/04	Os servidores de e-mail do tesouro da Costa Rica e do provedor de serviços de Internet estatal são violados.	Dia 3: Preocupado com a escalada de vulnerabilidades, o governo tenta desconectar todos os sistemas de internet possíveis, enquanto negava a comunicação sobre o ataque para o público da Costa Rica. O governo pede ajuda à Microsoft e países como Israel, EUA e Espanha.
Quinta, 21/04	Conti ataca os servidores do Ministério do Trabalho e Segurança Social, junto com o Serviço Social para roubar e-mails e dados de pensão.	Dia 4: O presidente em exercício anuncia publicamente a não intenção do governo em pagar o resgate.
Sexta, 22/04	----------	Dia 5: O governo da Costa Rica declara emergência nacional devido a um ataque cibernético.
23 de Abril - 10 de Maio	Conti viola uma concessionária de eletricidade estatal da Costa Rica e criptografa seus dados.	Dia 6: A partir daí, respostas ou pagamentos desconhecidos do setor privado, se houver.
Última semana de Maio	Outra ramificação de ransomware, Hive (ligado ao Conti) ataca 30 servidores pertencentes ao CCSS (Serviço Social da Costa Rica) e os infecta com ransomware roubando dados de saúde pública e exigindo US$5 milhões em Bitcoins. Sistemas do hospitais são bloqueados.	Costa Rica recorre ao modo manual, seus hospitais recorreram a documentos e dados físicos.
Sábado, 11/06	----------	Nenhum resgate é pago. Finalmente, depois de 2 meses do ataque, os serviços são reestruturados.

Fonte: Datta 2023.

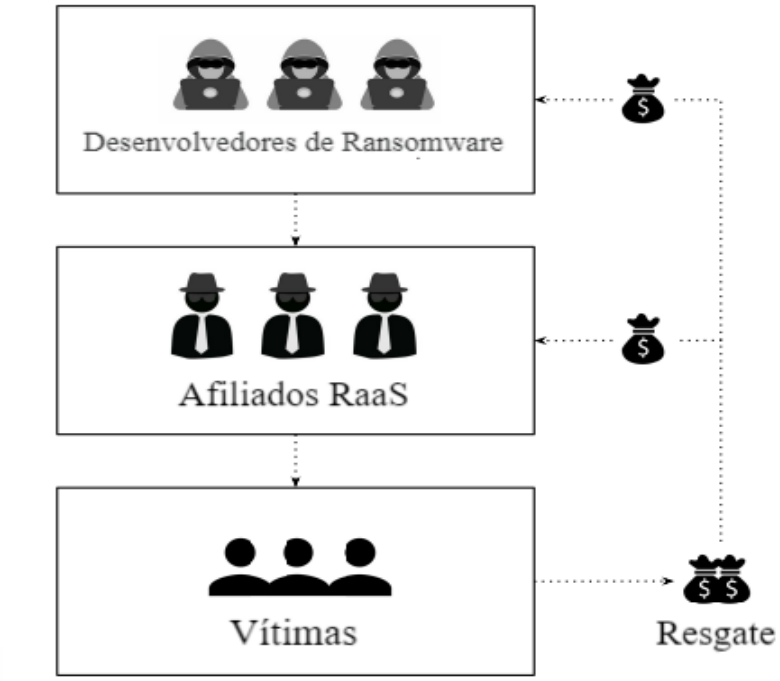
Os ataques por *ransomware* não são técnicas recentes, é uma expressão evolutiva do *malware*, onde são aproveitadas ações como o ato de abrir um email ou o clique para exibir uma imagem, para permitir que um programa malicioso possa ser ativado de maneira silenciosa, de modo que passe despercebido. Além do Ministério de Finanças, outras áreas governamentais também foram afetadas pelo ataque como O Ministério da Ciência, Inovação, Tecnologia e Telecomunicações; O Ministério do Trabalho e Segurança Social; O Fundo de Desenvolvimento Social e Benefícios Familiares; O Instituto Nacional de Meteorologia; O Fundo de Segurança Social da Costa Rica; A Sede Interuniversitária de Alajuela (Cano, 2022). Além disso, o grupo ofereceu a devolução dos dados por uma quantia de $20 milhões, no entanto, o governo costarriquenho se recusou a pagar a quantia requisitada. Ao invés disso, o presidente Rodrigo Chaves declarou estado de emergência no país e iniciou uma busca por supostos traidores, além de escorar-se em fortes aliados como os Estados Unidos e a Espanha de modo que pudesse ser amparado (Murray; Srivastava, 2022).

4.3.3 O grupo Conti

Tendo surgido no final de 2020, o grupo *hacker* Conti é um ator relativamente novo dentro do mundo do cibercrime. No entanto, apesar de novo, o grupo já se fez bastante presente de maneira agressiva, mas sofisticada. O modo de atuação desse grupo baseia-se, majoritariamente, nas suas diversas formas de uso de *ransomwares*, geralmente encriptando dados de suas vítimas e, posteriormente, exigindo pagamento pela recuperação do acesso desses dados. Além disso, o grupo é conhecido pelas altas quantias exigidas às vítimas em seus ataques, assim como por utilizar métodos combinados de extorsão, como a criptografia de dados e o roubo de informações sensíveis (Sayegh, 2023). Ademais, o grupo *hacker* Conti compõe uma nova tendência dentro do espectro dos *ransomwares*, onde há um espelhamento do *Software as a Service* (SaaS) onde um serviço é oferecido como produto. Esta nova tendência, conhecida como *Ransomware as a Service* (RaaS), "permite que qualquer um possa utilizar ferramentas pré-criadas de *ransomwares* para lançar um ataque"[53] (Alzahrani; Xiao; Sun, 2022, p. 100178). Desse modo, aqueles afiliados RaaS obtêm seu lucro a partir da divisão de um percentual em cada pagamento de resgate bem sucedido (Figura 17) (Alzahrani; Xiao; Sun, 2022).

[53] Allows anyone 26 to use pre-created ransomware tools to launch a ransomware attack.

Figura 17 - Modelo simplificado de um negócio RaaS



Fonte: Alzahrani; Xiao; Sun, 2022.

O grupo opera a partir de países do leste europeu e da Rússia, e estima-se que tenha apoiado a invasão russa à Ucrânia (Sayegh, 2023). Ainda, Jeimy Cano[54], para o *Global Strategy,* sugeriu um possível patrocínio do governo russo ao grupo Conti (2022). Dessa forma, o grupo anunciou seu apoio à invasão russa à Ucrânia, em fevereiro de 2022, e também ameaçou tomar medidas de forma a retaliar infraestruturas críticas caso ataques cibernéticos fossem efetuados contra os russos. No entanto, uma conta com nome de *ContiLeaks* em uma rede social, deu início a uma série de vazamentos de informações a respeito da comunicação interna do grupo, inclusive, vazando o código fonte para o *ransomware* criado pelo grupo e que leva o mesmo nome, Conti (Alzahrani; Xiao; Sun, 2022). Portanto, nos meses seguintes, o *website* do grupo não estava mais disponível, e, desse modo, "a abordagem metódica e empresarial do Conti desintegrou-se, embora ainda tenha efetuado ataques, como o da Costa Rica" (Vickers, 2023).

4.3.4 Efeitos

[54] Professor Universitário e Consultor Internacional em Cibersegurança e Ciberdefesa. Doutor em Administração e Doutor em Educação. Professor em diversos cursos de pós-graduação em segurança da informação, segurança cibernética e crimes cibernéticos na Colômbia.

O presente caso da Costa Rica evidencia os riscos que um sistema de segurança cibernética fraco pode trazer para a infraestrutura tecnológica de uma nação. Na época dos ataques, o presidente Chaves culpou a administração anterior pela omissão das verdadeiras extensões dos danos, além de comparar a situação com terrorismo. Desse modo, os ataques também debilitaram o sistema de saúde do país por alguns meses, provocando casos que chamaram a atenção pela sua gravidade, como a mulher que possuía deficiência mental e teve seu tratamento atrasado devido à falta de acesso dos médicos aos exames anteriores dela (Murray; Srivastava, 2022). Também, o ataque prejudicou o comércio internacional, devido ao dano no sistema de impostos, além de afetar diretamente os salários de seus servidores (BBC, 2022).

Ainda, o presidente da Costa Rica chegou a sugerir que o motivo pelo qual o grupo Conti teria atacado a infraestrutura do país seria por conta de Chaves ter sido o primeiro chefe de estado da américa latina a condenar a invasão russa à Ucrânia, chamando-a de criminosa. Portanto, segundo o presidente, o ataque *hacker* tenha partido da Rússia. Outrossim, o presidente também afirmou que esses ataques alertaram o país em relação às suas defesas cibernéticas.

A Costa Rica faz parte da Iniciativa Contra-Ransomware, promovida pela administração de Joe Biden dos Estados Unidos, onde é reiterada a aplicação das leis e da cooperação diplomática, em busca da não-exploração da moeda virtual (Ciso Advisor, 2023). Além disso, em março de 2023, os Estados Unidos anunciaram o fornecimento de $25 milhões de modo a fortalecer a segurança cibernética da Costa Rica contra ameaças de atores maliciosos. Esse financiamento também irá fornecer suporte para operação de treinamento de cibersegurança, assim como a capacitação a longo prazo. Cynthia Telles, embaixadora dos Estados Unidos na Costa Rica, declarou que “The United States values our longstanding and close relationship with Costa Rica as we work together to make the region more democratic, prosperous, and secure” (Us Embassy, 2023).

5 CONSIDERAÇÕES FINAIS

Antes de iniciar as considerações finais, é importante relembrar quais os objetivos estabelecidos no início deste trabalho, assim como a sua pergunta e hipótese. Portanto, o presente trabalho pretendeu analisar as ações de de organizações *hackers* dentro do meio cibernético e quais as suas implicações para a soberania estatal, como também, entender o papel dos atores estatais dentro do sistema internacional tradicional partindo da perspectiva neorrealista de Waltz. Além do mais, procurou-se entender como as organizações *hackers* se inserem no contexto internacional. Então, estabeleceu-se o seguinte questionamento: se os ataques cibernéticos promovidos por organizações *hackers* não estatais poderiam fragilizar um Estado de modo a superar seu *hard power* e mudar a sua dinâmica de poder dentro do sistema internacional tradicional? Sendo assim, a hipótese estabelecida foi de que os ataques cibernéticos promovidos por organizações *hackers* não teriam a capacidade de alterar o *status* de um Estado no sistema internacional tradicional, e portanto, a dinâmica de poder de um Estado estaria condicionada ao seu *hard power*.

Como estabelecido por Waltz, dentro de uma estrutura durável, é comum subestimar os efeitos estruturais, pois eles tendem a permanecer constantes. Logo, é esperado obter resultados semelhantes devido às ações dos Estados dentro de um contexto anárquico. Além disso, o cientista político também menciona que a soberania não garante a livre ação dos Estados. Embora estes possuam liberdade de escolha na sua cooperação interna e externa, ainda assim, podem ser constrangidos. Outro ponto relevante diz respeito às capacidades dos Estados, pois, sendo esta a forma de estimar o poder, consequentemente, as variações na capacidade refletem em variações na estrutura. Dessa forma, Waltz alega que quanto maior a disposição de capacidades de um Estado, menor sua possibilidade de ser constrangido pela estrutura. Ademais, o teórico também evidenciou que as posições dos Estados dentro do sistema internacional pouco se alteram, assim como a utilidade do poderio militar de um Estado está mais associado à sua capacidade de dissuasão do que a sua capacidade de ação efetivamente.

Portanto, revisados alguns pontos relativos à teoria de Kenneth Waltz, pode-se entender que, por mais que o meio cibernético traga um novo tipo de relação entre os Estados, a estrutura do sistema internacional os constrangem, isto é, a estrutura em si não é alterada, mesmo que a relação entre os Estados (unidades em interação) tenha-se elevado a um novo patamar, o meio cibernético. Além disso, através dos casos expostos, também foi possível elucidar que um Estado pequeno necessita do auxílio de potências, mesmo que independente. Também, esse

constrangimento exercido pelo sistema não está aplicado, de maneira tão assertiva, nas potências às quais os Estados precisam recorrer e, dessa forma, essas potências possuem mais liberdade ao transitar entre as suas capacidades e em relação ao uso delas, isto é, os possíveis Estados autores dos ataques efetuados apresentados, como os Estados Unidos e a Rússia, obtêm autonomia sobre como esses ataques impactaram a sua posição dentro do sistema internacional.

Outrossim, como recém mencionado, a posição ocupada pelos Estados dentro do sistema internacional não é alterada de maneira geral, sendo mantidas as potências já previamente estabelecidas. No entanto, embora a manutenção do *status* seja pouco ou nada alterada quando nos referimos às potências dentro do sistema, àqueles Estados menores afetados e, consequentemente com menos capacidades, tendem a sentir mais o constrangimento estrutural do sistema. Portanto, entre os casos analisados neste trabalho, pode-se evidenciar no caso iraniano, que ao ter seu desenvolvimento nuclear atrasado, também teve o seu *status* levemente alterado dentro do sistema internacional, ao passo que suas capacidades diminuíram e o constrangimento da estrutura foi mais sentido.

Agora, ao tratar-se de poderio militar, é notório que ataques cibernéticos compõem um novo desafio aos Estados, uma vez que esses tipos de ataque pouco relacionam-se com o poderio militar de um país, e sim com seu poderio cibernético, ou seja, a capacidade de defesa e ataque de um Estado no meio cibernético. Desse modo, ao tratar-se de um assunto recente, pouco se mencionam as consequências reais que esse tipo de interação pode trazer para um Estado. Sendo assim, os casos expostos neste trabalho servem para evidenciar os efeitos "no mundo real" que ataques cibernéticos podem carregar consigo e o quão facilitador esse meio tornou-se para a promoção de ofensivas entre Estados, afinal, é um tipo de ataque com custo consideravelmente menor que o tradicional.

Assim, cada caso mostra diferentes consequências e maneiras de ataque. Dessa forma, o ataque ocorrido na Costa Rica coloca em pauta a utilização do meio cibernético como uma fonte de enriquecimento, visto que, ao criptografar e roubar dados importantes do governo do país, os atacantes possuem em mãos, uma forte moeda de troca. Além disso, esse caso mostrou como, em um mundo cada vez mais informatizado, as consequências de um ataque cibernético podem ser sentidas diretamente pela população de um país. Também, no caso iraniano já mencionado, nota-se que o intuito do ataque tinha motivações diferentes do ocorrido na Costa Rica, isto é, o foco estava na desestabilização do programa nuclear do Irã e possível redução de risco para os

países opositores ao regime iraniano. Então, pode-se observar que, neste caso, as motivações eram políticas e direcionadas ao enfraquecimento do poderio nuclear do iraniano, de modo que este não pudesse mais, temporariamente, desenvolver seu programa nuclear e a avançar para uma posição de maior, ou equivalência, às potências.

Todavia, ao analisar o caso da Estônia, pôde-se observar diferentes consequências, uma vez que o Estado estoniano obtinha melhores condições de defesa quando recebeu o ataque. Portanto, neste caso observa-se as poucas consequências reais sentidas, de forma que este ataque teria sido um desestabilizador dos sistemas do país, e não um imobilizar do Estado. Além disso, a Estônia combateu os ataques com mais facilidade do que o observado nos outros países, isto porque seu sistema de defesa cibernética apresentava, no momento do ataque, melhor estruturação. Desse modo, para combater a vulnerabilidade de sistemas governamentais informatizados, o foco deve manter-se na estruturação e investimento em uma boa política de defesa. Para tal, é necessário reconhecer os efeitos reais que um ataque cibernético pode oferecer, removendo a possibilidade de ameaças do plano "abstrato" e incorporando-as entre as ameaças concretas que um país pode enfrentar.

Um ataque cibernético pode, além de gerar caos, danificar as infraestruturas críticas de um país de modo a paralisar as suas funcionalidades e afetar diretamente a população de um Estado, como em casos de ataque a bancos e hospitais. Ainda assim, um ataque cibernético não explora as consequências físicas da maneira que aqueles produzidos pelo meio bélico. Então, um Estado não irá alterar, de maneira abrupta, a sua posição e a sua dinâmica de poder dentro do sistema internacional ao considerar somente ataques cibernéticos. Portanto, indo de encontro à hipótese apresentada inicialmente para este trabalho, certamente, o *hard power* se sobressai quando se mencionam consequências físicas produzidas por um ataque, contudo, isso não significa que ataques cibernéticos não possuem qualquer tipo de efeito físico, pois como apresentado nos casos explorados neste trabalho, este tipo de dano pode ocorrer e afetar diversas áreas. Por fim, danos territoriais não são observados em casos de ataques cibernéticos, sendo esse tipo de perda ou ganho condicionado ao poderio militar dos Estados, isto é, seu *hard power*.

REFERÊNCIAS

ALDAAJEH, Saleh et al. **The role of national cybersecurity strategies on the improvement of cybersecurity education**. Computers & Security: v. 119, 2022. Disponível em: <https://doi.org/10.1016/j.cose.2022.102754>. Acesso em 19 jun 2023.

ALEROUD, Ahmed; ZHOU, Lina. **Phishing environments, techniques, and countermeasures: A survey.** Computers & Security, v. 68, p. 160-196, 2017. Disponível em:<https://doi.org/10.1016/j.cose.2017.04.006>. Acesso em: 27 out 2023.

ALZAHRANI, Saleh; XIAO, Yang; SUN, Wei. **An Analysis of Conti Ransomware Leaked Source Codes.** IEEE Access, v. 10, p. 100178-100193. Disponível em:<10.1109/ACCESS.2022.3207757>. Acesso em: 23 out 2023.

APÓS Protestos, a transferência. DW, 2007. Disponível em:<https://www.dw.com/pt-br/monumento-controverso-%C3%A9-transferido-para-cemit%C3%A9rio-na-capital-est%C3%B4nia/a-2462505>. Acesso em: 3 nov 2023.

ASHMORE, William C. **Impact of Alleged Russian Cyber Attacks.** Baltic Security & Defence Review, v. 11, 2009. Disponível em:<https://www.baltdefcol.org/files/files/BSDR/BSDR_11_1.pdf>. Acesso em 4 nov 2023.

ATAQUES a infraestruturas críticas e a indústrias dobram em um ano. Ciso Advisor, 2023. Disponível em:<https://www.cisoadvisor.com.br/ataques-a-industrias-e-infraestruturas-dobraram-em-um-ano/>. Acesso em: 31 out 2023.

ATAQUES tornam defesas da Costa Rica mais fortes, diz presidente. Ciso Advisor, 2023. Disponível em: <https://www.cisoadvisor.com.br/ataques-tornam-defesas-da-costa-rica-mais-fortes-diz-presidente/ Acesso em: 15 out 2023.

BAEZNER, Marie; ROBIN Patrice. **Stuxnet.** Center for Security Studies (CSS), ETH Zürich, 2017. Disponível em: https://doi.org/10.3929/ethz-b-000200661. Acesso em: 8 nov 2023.

BARLETTA, William A. **Cyberwar or cyber-terrorism: the attack on Estonia.** International Seminar on Nuclear War and Planetary Emergencies, p. 481-486, 2018. Disponível em:<https://doi.org/10.1142/9789812834645_0051>. Acesso em 5 nov 2023.

BERG, B. van den; KUIPERS, S. L. **Vulnerabilities and cyberspace: a new kind of crisis**. Oxford Research Encyclopedia of Politics: 2022. Disponível em:<doi:10.1093/acrefore/9780190228637.013.1604>. Acesso em: 23 jun 2023.

BILEFSKY, Dan; TROIANOVSKI, Anton; FARQUHAR, Neil. **What is Victory Day in Russia, and why is it so significant?** The New York Times, 2023. Disponível em:<https://www.nytimes.com/2023/05/09/world/europe/russia-victory-day-may-9.html>. Acesso em: 4 nov 2023.

BRASIL. **Desarmamento e não-proliferação.** 2022. Disponível em:<https://www.gov.br/mre/pt-br/delbrasonu/paz-e-seguranca-internacional/desarmamento-e-nao-proliferacao#:~:text=O%20TNP%20tem%20como%20objetivo,foi%20prorrogado%20por%20tempo%20indeterminado>. Acesso em: 8 nov 2023.

BREWER, Ross. **Ransomware attacks: detection, prevention and cure.** Network Security, v. 2016, p. 5-9, 2016. Disponível em:<https://doi.org/10.1016/S1353-4858(16)30086-1>. Acesso em: 331 out 2023.

BUXTON, Oliver. **O que é Stuxnet?** Avast, 2022. Disponível em:<https://www.avast.com/pt-br/c-stuxnet#:~:text=Indiscutivelmente%20a%20primeira%20arma%20cibern%C3%A9tica,no%20programa%20nuclear%20do%20Ir%C3%A3>. Acesso em: 6 nov 2023.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional.** São Paulo: Editora Unesp, 2012.

CAETANO, Karizia Ribeiro Pereira. **O programa nuclear iraniano: ameaça internacional ou busca pela segurança do país**. 2014. 32 f. Monografia (Especialização em Relações Internacionais)—Universidade de Brasília, Brasília, 2014. Disponível em:<https://bdm.unb.br/handle/10483/8290>. Acesso em: 9 nov 2023.

CANO, Jeimy. **El ransomware: una estrategia de desestabilización geopolítica. El Caso de Costa Rica.** Global Strategy Report. 2022. Disponível em: <https://global-strategy.org/el-ransomware-una-estrategia-de-desestabilizacion-geopolitica-el-caso-de-costa-rica/ Acesso em: 15 out 2023.

CARNEIRO, Matheus A. C. **O programa nuclear iraniano frente às mudanças na balanla de poder regional do oriente médio pós-2001.** 89 p. TCC - Universidade Federal de Santa Catarina, Florianópolis, 2018. Disponível em:<https://repositorio.ufsc.br/bitstream/handle/123456789/188625/Monografia%20Matheus%20Carneiro.pdf?sequence=1&isAllowed=y>. Acesso em 8 nov 2023.

CHEN, Ping; DESMET Lieven; HUYGENS Christophe. *In:* DE Decker B.; ZÚQUETE A. **A Study on Advanced Persistent Threats.** Communications and Multimedia Security, p. 63-72, 2014. Disponível em:<https://doi.org/10.1007/978-3-662-44885-4_5>. Acesso em: 18 set 2023.

COLLINS, Sean; McCOMBIE, Stephen. **Stuxnet: the emergence of a new cyber weapon and its implications.** Journal of Policing, Intelligence and Counter Terrorism, v. 7, n. 1, p. 80-91, 2012. Disponível em:<https://doi.org/10.1080/18335330.2012.653198>. Acesso em: 11 nov. 2023..

COSTA RICA. Dados Mundiais, 2023. Disponível em:<https://www.dadosmundiais.com/america/costa-rica/index.php>. Acesso em: 3 out 2023.

COSTA Rica: perfil do país que extinguiu seu exército para investir em saúde e educação. BBC News Brasil. 2022.

Disponível em: <https://www.bbc.com/portuguese/internacional-63628015. Acesso em: 15 out 2023.

COUNCIL of Europe et al. **Guide to developing a National Cybersecurity Strategy**. 2ª edição, Strategic Engagement in Cybersecurity, 2021. Disponível em:<https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf>. Acesso em: 24 jun 2023.

CRAIGEN, Dan; DIAKUN-THIBAULT, Nadia; PURSE, Randy. **Defining Cybersecurity**. Technology Innovation Management Review: v. 4, p. 13-21, 2014. Disponível em: <https://www.timreview.ca/article/835>. Acesso em: 19 jun 2023.

CRITICAL Infrastructure Protection. Federal Register The Daily Journal of the United States Government, 1996. Disponível em:<https://www.federalregister.gov/documents/1996/07/17/96-18351/critical-infrastructure-protection>. Acesso em: 23 jun 2023.

CUNHA, Ana Paula Gonçalves. **A relação entre Estados Unidos e Irã: da Revolução Iraniana a 2009.** 88 p. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais), Universidade Federal do Pampa, Santana do Livramento, 2021. Disponível em:<https://repositorio.unipampa.edu.br/jspui/handle/riu/5687>. Acesso em: 7 nov 2023.

CYBER. In: Oxford Learner's Dictionaries, 2023. Disponível em: <https://www.oxfordlearnersdictionaries.com/definition/english/cyber#:~:text=%2Fsa%C9%AAb%C9%99(r)%2F,communication%20networks%2C%20especially%20the%20internet>. Acesso em: 19 jun 2023.

CYBER Kill Chain. Lockheed Martin, 2023. Disponível em:<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. Acesso em: 18 ou 2023.
CYBERNETICS. In: Cambridge Dictionary, 2023. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/cybernetics>. Acesso em: 22 jun 2023.

CYBERSECURITY. In: Collins Dictionary, 2023. Disponível em: <https://www.collinsdictionary.com/submission/16634/Cybersecurity#:~:text=From%20Oxford%20dictionary%3A%20The%20state,unauthorized%20use%20of%20electronic%20data>. Acesso em 21 jun 2023.

DATTA, Pratim Milton; ACTON, Thomas. **Ransomware and Costa Rica's national emergency: A defense framework and teaching case**. Journal of Information Technology Teaching Cases, p. 20438869221149042, 2022. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/20438869221149042?casa_token=SPGyhjVLf6 Acesso em: 14 out 2023.

DENIAL of Service (DoS) guidance. National Cyber Security Centre (NCSC), 2016. Disponível em:<https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection>. Acesso em: 23 jun 2023.

DICTIONARY of Military and Associated Terms. **Department of Defense**: Joint Publication 1-02, 2010.

DINNISS, H. **Guerra cibernética e as leis da guerra** . Cambridge, Reino Unido: Cambridge University Press. 2014

DODGE, Martin; KITCHIN, Rob. **Mapping Cyberspace**. Routledge, 2001.

DO ESPIRITO SANTO, M. M.; BALDASSO, T. O. **A Revolução Iraniana: Rupturas e Continuidades na Política Externa do Irã. Revista Perspectiva: reflexões sobre a temática internacional**, *[S. l.]*, v. 10, n. 18, 2018. Disponível em:< https://seer.ufrgs.br/index.php/RevistaPerspectiva/article/view/80167>. Acesso em: 8 nov. 2023.

EHALA, Martin. **The Bronze Soldier: Identity Threat and Maintenance in Estonia.** Journal of Baltic Studies, p. 139-158, 2009. Disponível em:<http://dx.doi.org/10.1080/01629770902722294>. Acesso em 3 nov 2023.

ENE, Carmen. **10.5 Trillion Reasons Why We Need a United Response to Cyber Risk**. Forbes, 2023. Disponível em:<https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=66333dde3b0c>. Acesso em: 18 set 2023.

ENTENDA o acordo nuclear com o Irã. G1, 2017. Disponível em:<https://g1.globo.com/mundo/noticia/entenda-o-acordo-nuclear-com-o-ira.ghtml>. Acesso em: 5 nov 2023.

ENTENDA o que é Phishing. TRE - SE: 2022. Disponível em:<https://www.tre-se.jus.br/comunicacao/noticias/2020/Marco/entenda-o-que-e-phishing>. Acesso em: 23 jun 2023.

ESTÔNIA. Dados Mundiais, 2023. Disponível em:<https://www.dadosmundiais.com/europa/estonia/index.php>. Acesso em 2 nov 2023.

ESTÔNIA registra pior incidente cibernético desde 2007. CisoAdvisor, 2022. Disponível em:<https://www.cisoadvisor.com.br/estonia-sofre-pior-ataque-cibernetico-desde-2007/>. Acesso em 3 nov 2023.

FACIO S., G. **EVOLUÇÃO DA POLÍTICA EXTERNA DA COSTA RICA**. Relações Internacionais , v. 88, não. 2 P. 19-38, 31 dez. 2015. Disponível em: <https://www.revistas.una.ac.cr/index.php/ri/article/view/7036>. Acesso em: 17 out 2023.

FANG, Binxing. **Cyberspace Sovereignty: reflections on building a community of common future in cyberspace.** Science Press: Beijing, Springer Nature: Singapore, 2018.

FELT, Adrienn; WAGNER, David. **Phishing on Mobile Devices.** 2012. Disponível em:<https://www.researchgate.net/publication/266465377_Phishing_on_Mobile_Devices>. Acesso em: 27 out 2023.

FERREIRA, Haroldo. **Cibersegurança**. São Paulo: Senac, 2021.

FISCHER, Eric. A. **Cybersecurity Issues and Challenges.** Library of Congress Washington DC, 2017.

GEERS, Kenneth. **Strategic Cyber Security**. NATO Cooperative Cyber Defence: 2011. Disponível em: <http://www.digar.ee/id/nlib-digar:103608>. Acesso em: 19 jun 2023.

GERHARDT, Tatiana; SILVEIRA, Denise. **Métodos de Pesquisa.** Porto Alegre: Editora UFRGS, 2009.

GHAFIR, Ibrahim; PRENOSIL, Vaclav. **Advanced Persistent Threat Attack Detection: An Overview.** International Journal of Advancements in Computer Networks and Its Security, v. 4, 2014. Disponível em:<https://www.researchgate.net/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview>. Acesso em: 18 set 2023.

GHERNAOUTI, Solange. **Cyber Power: crime, conflict and security in cyberspace**. EPFL Press, 2013.

GRAYSON, James. **Stuxnet and Iran's Nuclear Program.** Stanford University, 2011. Disponível em: http://large.stanford.edu/courses/2011/ph241/grayson2/. Acesso em: 10 nov. 2023.

GREATHOUSE, Craig B. Cyber war and Strategic Thought: Do the classic theorists still matter? *In:* **Cyberspace and International Relation: Theory, Prospects and Challenges**, p. 21-40, 2014. Disponível em:<https://www.researchgate.net/publication/281668945_Offense-Defense_Balance_in_Cyber_Warfare>. Acesso em: 3 nov 2023.

GREIG, Jonathan. Ransomware gang threatens to 'overthrow' new Costa Rica government, raises demand to $20 million. The Record. 2022. Disponível em: <https://therecord.media/ransomware-gang-threatens-to-overthrow-new-costa-rica-government-raises-demand-to-20-million. Acesso em: 14 out 2023.

HARKNETT, Richard J; STEVER, James A. **The New Policy World of Cybersecurity**. Public Administration Review: v. 71, p. 455-460, 2011. Disponível em: <https://doi.org/10.1111/j.1540-6210.2011.02366.x>. Acesso em: 19 jan 2023.

HEINEGG, Wolff H. **Territorial Sovereignty and Neutrality in Cyberspace**. International Law Studies: v. 89, p. 123-156, 2013. Disponível

em:<https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1027&context=ils>. Acesso em: 24 jun 2023.

HERMANN, Dominik; PRIDÖHL. Basic Concepts and Models of Cybersecurity. *In:* CHRISTEN, Markus et al. **The Ethics of Cybersecurity**. Springer Open: p. 11-44, 2020. Disponível em:<https://doi.org/10.1007/978-3-030-29053-5>, Acesso em 22 jun 2023.

HERZOG, Stephen. **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.** Journal of Strategic Security, v. 4, n. 2, p. 49-60, 2011. Disponível em:<http://dx.doi.org/10.5038/1944-0472.4.2.3>. Acesso em 4 nov 2023.

HOW to Recognize and Avoid Phishing Scams. Federal Trade Commission, 2022. Disponível em:<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>. Acesso em: 27 out 2023.

HUANGUO, Zhang et al. **Survey on cyberspace security**. Sci China Inf Sci, p. 1-43, 2015. Disponível em:<https://doi.org/10.1007/s11432-015-5433-4>. Acesso em: 22 jun 2023.

HUHN, SebastiaN. **A history of nonviolence? The social construction of Costa Rican peaceful identity**.Journal for the study of race, nation and culture, v. 15, p. 787-810, 2009. Disponível em: 10.1080/13504630903372504. Acesso em: 17 out 2023.

HUMAYUN, Mamoona et al. **Cyber Security Threats and Vulnerabilities: A Sistematic Mapping Study**. Arabian Journal for Science and Engineering: v. 45, p. 3171-3189, 2020. Disponível em:<https://doi.org/10.1007/s13369-019-04319-2>. Acesso em: 23 jun 2023.

INTERNATIONAL Law in Cyberspace. Entrevista concedida a Harold Hongju Koh. Harvard International Law Journal: v. 54, 2012. Disponível em:<http://hdl.handle.net/20.500.13051/4383>. Acesso em: 22 jun 2023.

IRÃ. Dados Mundiais, 2023. Disponível em:<https://www.dadosmundiais.com/asia/ira/index.php>. Acesso em 7 nov 2023.

IST ein Internetangriff der Ernstfall? Frant'furter Allgemeine, 2007. Disponível em:<https://www.faz.net/aktuell/politik/ausland/estland-im-visier-ist-ein-internetangriff-der-ernstfall-1436040/dos-overload-illustration-1448476.html>. Acesso em 3 nov 2023.

JACINTO, Mateus L. M. **Tecnologia a favor do poder: a relação Irã-Israel-EUA no caso Stuxnet.** 32 p. TCC - Universidade Federal de São Paulo, 2021. Disponível em:<https://repositorio.unifesp.br/bitstream/handle/11600/62891/TCC%20Mateus%20Modena%20-%20Vers%c3%a3o%20Final.pdf?sequence=1&isAllowed=y>. Acesso em: 8 nov 2023.

JOINT Comprehensive Plan of Action. 2015. Disponível em:<https://2009-2017.state.gov/documents/organization/245317.pdf>. Acesso em: 8 nov 2023.

JOINT Comprehensive Plan of Action. U.S Department of State, 2015. Disponível em:<https://2009-2017.state.gov/e/eb/tfs/spi/iran/jcpoa/>. Acesso em: 8 nov 2023.

JORGE, Bernardo W. G. A. **Estados Unidos, poder cibernético e a "guerra cibernética" do worm Stuxnet ao malware *Flame/Skywiper* - e além.** Boletim Meridiano, v. 13, n. 131, p. 43-48, 2012. Disponível em:<https://media.proquest.com/media/hms/OBJ/k4yjU?_s=fjtMziFsAqnwBnr0BJaSBmxVBeU%3D>. Acesso em: 8 nov 2023.

JOUBERT, Vincent. **Five years after Estonia's cyber attacks: lessons learned for NATO?** NATO Defense College, 2012. Disponível em:<https://www.files.ethz.ch/isn/143191/rp_76.pdf>. Acesso em: 2 nov 2023.

JUURVEE, Ivo; MATTIISEN, Mariita. **The Bronze Soldier Crisis of 2007: revisiting an early case of hybrid conflict.** International Centre for Defence and Security, 2020. Disponível em:<https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf>. Acesso em: 3 nov 2023.

KHONJI, Mahmoud; IRAQI Youssef; JONES, Andrew. **Phishing Detection: A literature Survey.** IEEE Communications Surveys & Tutorials, v. 15, n. 4, p. 2091-2121, 2013. Disponível em:<10.1109/SURV.2013.032213.00009>. Acesso em: 27 out 2023.

KU, Raymond S. R. **Cyberspace Law: Cases and Materials**. Wolters Kluwer Law & Business, 2020.

LEWIS, James A. **Cybersecurity and Critical Infrastructure Protection**. Center for Strategic and International Studies, 2006. Disponível em:<http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf>. Acesso em: 23 jun 2023.

LIMA, Martonio M. B.; FREITAS, Mateus Oliveira. **Programa Nuclear do Irã e Panorama Internacional.** Revista Jurídica, v. 03, n. 44, p. 355-380, 2016. Disponível em:<https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Juridica-UNICURITIBA_n.44.17.pdf>. Acesso em: 8 nov 2023.

LONGLEY, Kyle. **Peaceful Costa Rica, the First Battleground: The United States and the Costa Rican Revolution of 1948**. *The Americas*, vol. 50, no. 2, 1993, pp. 149–75. Disponível em: https://doi.org/10.2307/1007137. Acesso em: 17 out 2023.

LOWE, Christian. **Russian protesters "lay siege" to Estonian embassy.** Reuters, 2007. Disponível em:<https://www.reuters.com/article/uk-estonia-russia-scene-idUKL0354549820070503/>. Acesso em: 3 nov 2023.

MARTINS, Marco. **Ciberespaço: uma nova realidade para a segurança internacional.** Revista Nação e Defesa n. 133. Editora Instituto da Defesa Nacional: 2012. Disponível em: http://hdl.handle.net/10400.26/42448. Acesso em: 18 abr. 2023.

McGUINNESS, Damien. **How a cyber attack transformed Estonia.** BBC News, 2017. Disponível em:<https://www.bbc.com/news/39655415>. Acesso em 3 nov 2023.

MELCHIOR, Inge; VISSER, Oane. **Voicing past and present uncertainties: The relocation of Soviet World War II memorial and the politics of memory in Estonia.** Focaal, p. 33-50, 2011. Disponível em:<https://doi.org/10.3167/fcl.2011.590103>. Acesso em: 3 nov 2023.

MERCER, Christina. **How does a DDoS attack work?** Tech Advisor, 2017. Disponível em:<https://www.techadvisor.com/article/738798/how-does-a-ddos-attack-work.html>. Acesso em 4 nov 2023.

MESQUITA, Felipe Sousa. **Segurança Cibernética e a política internacional contemporânea: novos desafios e oportunidades.** Trabalho de Conclusão de Curso (Especialização em Relações Internacionais), Universidade de Brasília, 2019. Disponível em:<https://bdm.unb.br/bitstream/10483/25026/1/2019_FelipeSousaMesquita_tcc.pdf>. Acesso em: 23 jun 2023.

MOTEFF, John; COPELAND, Claudia; FISCHER, John. **Critical Infrastructures: What Makes an Infrastructure Critical?**. Library of Congress Washington DC Congressional Research Service: 2003. Disponível em:<https://apps.dtic.mil/sti/citations/ADA467306>. Acesso em: 23 jun 2023.

MURILO, Álvaro. Sete décadas do fim do Exército na Costa Rica: uma decisão rentável. San José - Costa Rica. 2018 Disponível em: <https://brasil.elpais.com/brasil/2018/12/03/internacional/1543808543_748985.html Acesso em: 13 out 2023.

MURRAY, Christine; SRIVASTAVA, Mehul. How Conti ransomware group crippled Costa Rica — then fell apart. Mexico City and London. 2022. Disponível em: <https://www.ft.com/content/9895f997-5941-445c-9572-9cef66d130f5. Acesso em: 14 out 2023.

NAKASHIMA, Ellen; WARRICK, Joby. **Stuxnet was work of U.S. and Israeli experts, officials say.** The Washington Post, 2012. Disponível em: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Acesso em: 10 nov. 2023.

NATIONAL Information Assurance Glossary. Committee on National Security Systems: n. 4009, 2010. Disponível em: <https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf>. Acesso em: 21 jun 2023.

NCSC advises organisations to act following Russia's attack on Ukraine. National Cyber Security Centre(NCSC), 2022. Disponível

em:<https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences>. Acesso em: 24 jun 2023.

FRAMEWORK for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018. Disponível em:<https://www.baltimorecityschools.org/sites/default/files/inline-files/NIST.CSWP_.04162018.pdf>. Acesso em: 23 jun 2023.

O'KANE, Philip; SEZER, Sakir; CARLIN, Domhnail. **Evolution of ransomware.** IET Network, v. 7, p. 321-327, 2018. Disponível em:<https://doi.org/10.1049/iet-net.2017.0207>. Acesso em: 31 out 2023.

OPPORTUNISTIC vs targeted cyberattacks. Seic, 2021. Disponível em:<https://www.seic.com/cyber-protection/sphere-blog/opportunistic-vs-targeted-cyberattacks>. Acesso em 3 nov 2023.

O que é urânio enriquecido e por que ele está no centro da tensão entre EUA e Irã. BBC News, 2019.

O que são ataques de DDoS? Kaspersky, 2023. Disponível em:<https://www.kaspersky.com.br/resource-center/threats/ddos-attacks>. Acesso em: 4 nov 2023.

OTTIS, Rain; LORENTS, Peter. **Knowledge based framework for cyber weapons and conflict**. Conference on cyber conflict. Tallinn, Estonia: p. 15–18, 2010. Disponível em: <https://www.proquest.com/conference-papers-proceedings/cyberspace-definition-implications/docview/869617247/se-2>. Acesso em: 22 jun 2023.

PAGANINI, Pierluigi. **CONTI RANSOMWARE CLAIMS RESPONSIBILITY FOR THE ATTACK ON COSTA RICA.** Security affairs. 2022. Disponível em: <https://securityaffairs.co/130505/cyber-crime/costa-rica-conti-ransomware.html. Acesso em: 13 out 2023.

PAMMENT, J et al. **Hybrid Threats: 2007 cyber attacks on Estonia.** Nato Strategic Communications Centre of Excellence, 2019. Disponível em:<https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>. Acesso em 4 nov 2023.

PATEL, Kathan; CHUDASAMA Dhaval. **National security threats in cyberspace**. National Journal of Cyber Security Law: v. 4, p. 12-20, 2021. Disponível em:<https://www.researchgate.net/profile/Dhaval-Chudasama/publication/352507748_National_Security_Threats_in_Cyberspace/links/60cc366ca6fdcc01d47df0d4/National-Security-Threats-in-Cyberspace.pdf>. Acesso em: 23 jun 2023.

PHISHING Activity Trends Report. APWG, 2023. Disponível em:<https://apwg.org/trendsreports/.>. Acesso em: 27 out 2023.

PRESIDENT Rodrigo Chaves says Costa Rica is at war with Conti hackers. BBC News, 2022. Disponível em:<https://www.bbc.com/news/technology-61323402>. Acesso em: 20 out 2023.

PROTECTION of War Graves Act. Diário Estadual, 2007. Disponível em:<https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/508042019007/consolide>. Acesso em: 2 nov 2023.

RANSOMWARE review: October 2023. Malwarebytes, 2023. Disponível em:<https://www.malwarebytes.com/blog/threat-intelligence/2023/10/ransomware-review-october-2023>. Acesso em: 31 out 2023.

RAUN, Toivo U. **Identity and Integration.** East European Politics and Societies, v. 23, n. 4, p. 526-534, 2009. Disponível em:<https://doi.org/10.1177/0888325409342113>. Acesso em: 3 nov 2023.

RICHARDSON, Ronny; NORTH, Max N. **Ransomware: Evolution, Mitigation and Prevention.** International Management Review, v. 13, p. 10-21, 2017. Disponível em:<https://digitalcommons.kennesaw.edu/facpubs/4276/>. Acesso em: 31 out 2023.

ROCHA, Gabriela Cristina. **Caso Stuxnet: Os Impactos do Ataque Cibernético ao Programa Nuclear do Irã com a Primeira Arma Cibernética à Segurança Internacional (2009-2010).** 2022. 57 p. TCC — Universidade Estadual Paulista "Júlio de Mesquita Filho", Marília, 2022. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/235226/rocha_gc_tcc_mar.pdf?sequence=6&isAllowed=y. Acesso em: 9 nov 2023.

ROSEVICS, Larissa. **Autonomia dos países bálticos: uma questão geopolítica.** Periódicos UNB, v. 13, n. 131, 2012. Disponível em:<https://periodicos.unb.br/index.php/MED/article/view/4515>. Acesso em 3 nov 2023.

SARMENTO, João Pedro T. P. M. **ABOLIÇÃO DAS FORÇAS ARMADAS: LIÇÕES DE COSTA RICA E PANAMÁ.** Pontifícia Universidade Católica do Rio de Janeiro, 2023. Disponível em:< http://www.iri.puc-rio.br/wp-content/uploads/2023/02/Eixo-Conflitos_Joao-Pedro-Sarmento.pdf> Acesso em: 15 out 2023.

SAYEGH, Emil. **CONTI Hacker Group: The Young "For-Profit" Super-Cybercriminal Threat.** Forbes. 2023. Disponível em: <https://www.forbes.com/sites/emilsayegh/2023/04/04/conti-hacker-group-the-young-for-profit-super-cybercriminal-threat/?sh=6af1e588763d. Acesso em: 13 out 2023.

SCHATZ, Daniel; BASHROUSH, Rabih; WALL, Julie. **Towards a More Representative Definition of Cyber Security.** Journal of Digital Forensics, Security and Law: v. 12, 2017. Disponível em:< https://doi.org/10.15394/jdfsl.2017.1476>. Acesso em: 21 jun 2023.

SCHMIDT, Andreas. The Estonian Cyberattacks. *In:* HEALEY, Jason et al. **The fierce domain - conflicts in cyberspace 1986-2012.** Atlantic Council, 2013. Disponível em:<https://www.atlanticcouncil.org/in-depth-research-reports/books/a-fierce-domain-conflict-in-cyberspace-1986-to-2012/>. Acesso em: 2 nov 2023.

SHAHEEN, Salma. Offense-Defense Balance in Cyber Warfare.*In:* **Cyberspace and International Relation: Theory, Prospects and Challenges**, p. 77-93, 2014. Disponível em:<https://www.researchgate.net/publication/281668945_Offense-Defense_Balance_in_Cyber_Warfare>. Acesso em: 3 nov 2023.

SHARMA et al. **Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures.** Journal of Ambient Intelligence and Humanized Computing, 2023. Disponível em:<https://link.springer.com/article/10.1007/s12652-023-04603-y>. Acesso em: 19 set 2023.

SINGER, P. W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What everyone needs to know.** New York: Oxford University Press, 2014.

STARKS, Tim. **The Biden national cyber strategy is unlike any before it**. Washington Post: 2023. Disponível em:<https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it/>. Acesso em: 24 jun 2023.

STEFFENS, Timo. **Attribution of Advanced Persistent Threats**. Springer Vieweg Berlin, 2020. Disponível em:<https://link.springer.com/book/10.1007/978-3-662-61313-9>. Acesso em: 20 out 2023.

STOUFFER, Clare. **What is a zero-day exploit? Definition and prevention tips.** Norton, 2023. Disponível em:<https://us.norton.com/blog/emerging-threats/zero-day-exploit>. Acesso em: 8 nov 2023.

TAHIR, Rabia. **A Study on Malware and Malware Detection Technique**. International Journal of Education and Management Engineering (IJME), v. 8, n. 2 p. 20-30, 2018. Disponível em:<10.5815/ije me.2018.02.03>. Acesso em: 19 out 2023.

TIDY, Joe. **Meet the hacker armies on Ukraine's cyber front line**. BBC News: 2023. Disponível em:<https://www.bbc.com/news/technology-65250356>. Acesso em: 24 jun 2023

TRUMP anuncia retirada dos EUA de acordo nuclear com o Irã. G1, 2018. Disponível em:<https://g1.globo.com/mundo/noticia/trump-anuncia-retirada-dos-eua-de-acordo-nuclear-com-o-ira.ghtml>. Acesso em: 6 nov 2023.

UNITED States Announces $25 Million to Strengthen Costa Rica's Cybersecurity. cr.usembassy.gov. 2023. Disponível em: <https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/. Acesso em: 13 out 2023.

U.S. Relations With Costa Rica. state.gov 2023. Disponível em: <https://www.state.gov/u-s-relations-with-costa-rica. Acesso em: 13 out 2023.

VEALE, Michael; BROWN, Ian. **Cybersecurity**. Internet Policy Review: v. 9, p. 1-22, Berlim, 2020. Disponível em: <http://hdl.handle.net/10419/233106>. Acesso em: 19 jan 2023.

VICKERS, Jack Meegan. **The rise and the fall of the Conti ransomware group.** Global Initiative, 2023. Disponível em: <https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime/>. Acesso em: 17 out 2023.

VIGANÒ, Eleonora; LOI, Michele; YAGHMAEI, Emad. Cybersecurity of Critical Infraestructure. *In:* CHRISTEN, Markus et al. **The Ethics of Cybersecurity**. Springer Open: p. 11-44, 2020. Disponível em:<https://doi.org/10.1007/978-3-030-29053-5>, Acesso em 22 jun 2023.

WALTZ, Kenneth. **Theory of International Politics.** New York: McGraham Hill, 1979.

WARREN, Matthew. **Case Studies in Information Warfare and Security.** 2013. Disponível em:<https://books.google.com.br/books?hl=pt-BR&lr=&id=vub26dKsmpIC&oi=fnd&pg=PA72&dq=estonia+after+cyber+attacks+2007&ots=BXiOfw7lMY&sig=IF0SInimADRF5Wyl6H82iLIi_tQ#v=onepage&q=estonia%20after%20cyber%20attacks%202007&f=false>. Acesso em: 3 nov 2023.

WEISSBRODT, David. **Cyber-conflict, Cyber-crime, and Cyber-espionage**. Minnesota Journal of International Law: v. 22, p. 347, 2013. Disponível em:<https://scholarship.law.umn.edu/faculty_articles/223>. Acesso em: 24 jun 2023.

WHAT is a DDoS Attack? IndusFace, 2023. Disponível em:<https://www.indusface.com/learning/what-is-a-ddos-attack/>. Acesso em 3 nov 2023.

XU, Shouhuai. **Cybersecurity dynamics**. Symposium and Bootcampo on the Science of Security: n. 14, p. 1-2, 2014. Disponível em: <https://doi.org/10.1145/2600176.2600190>. Acesso em 21 jun 2023.

YE, Yanfang et al. **A Survey on Malware Detection Using Data Mining Techniques.** ACM Computing Surveys, v. 50, p. 1-40, 2017. Disponível em:<https://dl.acm.org/doi/10.1145/3073559>. Acesso em: 18 out 2023.

ZAMORA, Carlos Murillo. **Algunas consideraciones sobre política exterior y de defensa. El caso de Costa Rica.** Rev. Cient. Gen. José María Córdova, Bogotá , v. 10, n. 10, p. 27-48, Jan. 2012 . Disponível em: <http://ref.scielo.org/9g8cmk>.Acesso em: 17 out 2023.