UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA

RELAÇÕES INTERNACIONAIS PARA DOCENTES DA EDUCAÇÃO BÁSICA

CIBERNÉTICA E RELAÇÕES INTERNACIONAIS: O USO DA GUERRA CIBERNÉTICA COMO FERRAMENTA DE POLÍTICA EXTERNA E SUAS IMPLICAÇÕES PARA A SEGURANÇA GLOBAL

ARIANA ALMEIDA DO NASCIMENTO

Foz do Iguaçu
2024

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA

RELAÇÕES INTERNACIONAIS PARA DOCENTES DA EDUCAÇÃO BÁSICA

CIBERNÉTICA E RELAÇÕES INTERNACIONAIS: O USO DA GUERRA CIBERNÉTICA COMO FERRAMENTA DE POLÍTICA EXTERNA E SUAS IMPLICAÇÕES PARA A SEGURANÇA GLOBAL

ARIANA ALMEIDA DO NASCIMENTO

Artigo Científico apresentado a Universidade Federal da Integração Latino-Americana, como requisito parcial à obtenção do título de pós-graduação em Relações Internacionais para docentes da educação básica

Orientador: Prof. **Lucas Ribeiro Mesquita**

Foz do Iguaçu
2024

ARIANA ALMEIDA DO NASCIMENTO

CIBERNÉTICA E RELAÇÕES INTERNACIONAIS: O USO DA GUERRA CIBERNÉTICA COMO FERRAMENTA DE POLÍTICA EXTERNA E SUAS IMPLICAÇÕES PARA A SEGURANÇA GLOBAL

Artigo Científico apresentado a Universidade Federal da Integração Latino-Americana, como requisito parcial à obtenção do título de pós-graduação em Relações Internacionais para docentes da educação básica

BANCA EXAMINADORA

_____
Orientador: Prof. (Titulação) (Nome do orientador)
UNILA

_____
Prof. (Titulação) (Nome do Professor)
(Sigla da Instituição)

_____
Prof. (Titulação) (Nome do Professor)
(Sigla da Instituição)

Foz do Iguaçu, _____ de _____ de _____.

CIBERNÉTICA E RELAÇÕES INTERNACIONAIS: O USO DA GUERRA CIBERNÉTICA COMO FERRAMENTA DE POLÍTICA EXTERNA E SUAS IMPLICAÇÕES PARA A SEGURANÇA GLOBAL

RESUMO

O presente artigo tem como objetivo apresentar as ameaças presentes no ciberespaço, bem como suas repercussões para a segurança global, consequências no âmbito político e nas relações diplomáticas. A guerra cibernética e a proteção internacional são assuntos interligados que se tornaram cada vez mais importantes conforme a tecnologia da informação assume uma função crucial nas interações e na segurança global, uma vez que, o progresso tecnológico traz consigo uma série de riscos e desafios. A segurança cibernética refere-se à salvaguarda de sistemas ligados à Internet, englobando equipamentos, programas e informações, contra invasões virtuais. No contexto das Relações Internacionais, essa questão é de grande relevância, uma vez que diversas Organizações Internacionais e nações dependem da tecnologia para suas operações. O procedimento metodológico adotado consistiu em uma análise das publicações sobre Relações Internacionais e Segurança Global, complementada por consultas em artigos, dissertações, revistas e textos de engenharia de *software*, visando tornar o estudo mais abrangente e consistente. Nesse cenário, as estratégias de segurança são essenciais, pois estabelecem o referencial normativo que orienta a implementação e a supervisão das medidas de proteção cibernética, além de atribuir funções e responsabilidades.

Palavras-chave: Relações Internacionais; Guerra Cibernética; Segurança Global; Política Externa; Armas Cibernéticas.

ABSTRACT

This article aims to present the threats present in cyberspace, as well as their repercussions for global security, consequences in the political sphere and diplomatic relations. Cyber warfare and international protection are interconnected issues that have become increasingly important as information technology assumes a crucial role in global interactions and security, since technological progress brings with it a series of risks and challenges. Cyber security refers to the safeguarding of systems connected to the Internet, encompassing equipment, programs and information, against virtual invasions. In the context of International Relations, this issue is of great relevance, since various International Organizations and nations depend on technology for their operations. The methodological procedure adopted consisted of

an analysis of publications on International Relations and Global Security, complemented by consultations of articles, dissertations, magazines and *software* engineering texts, in order to make the study more comprehensive and consistent. In this scenario, security strategies are essential, as they establish the normative framework that guides the implementation and supervision of cyber protection measures, as well as assigning roles and responsibilities.

Keywords: International Relations; Cyber Warfare; Global Security; Foreign Policy; Cyber Weapons.

1 INTRODUÇÃO

A Internet está diariamente mudando carreiras, procedimentos e serviços na sociedade atual. Com a interconexão global, surgem novas maneiras de se comunicar que conseguem alterar os métodos clássicos de interação nas esferas política, econômica e social. Ao superar as barreiras geográficas dos países por meio de uma infraestrutura de informação conectada, forma-se um ambiente em nível global conhecido como ciberespaço.

O ciberespaço impulsiona o progresso do país ao estimular a melhoria das infraestruturas de telecomunicações, atualizar os serviços disponíveis para a população, fomentar o crescimento industrial e econômico, e intensificar a competitividade, resultando em produtos e serviços de maior qualidade a preços mais acessíveis. No entanto, a dependência total ou parcial desse espaço digital para serviços e operações pode expor fragilidades e aumentar o risco de ataques. Assim, a segurança cibernética se torna a estratégia padrão para reduzir as vulnerabilidades em ambientes conectados. Ademais, há diversos tipos de ameaças, especialmente aquelas geradas por pessoas com a intenção de comprometer outros sistemas, dando origem ao conceito de Guerra Cibernética.

A Guerra Cibernética é um conceito abrangente, cujo significado inclui a utilização de poder tecnológico no ambiente digital. Esse tipo de confronto não requer grandes proporções, prolongamento ou violência, características frequentemente ligadas ao conceito tradicional de guerra. Quando uma nação realiza um ataque a outra visando danificar sistemas essenciais, como os computadores militares ou outras tecnologias, e a nação alvo responde, isso pode ser classificado como uma Guerra Cibernética. Além disso, há discussões sobre a adequação das normas

estabelecidas para conflitos convencionais à realidade das guerras cibernéticas.

Apesar da segurança cibernética ser um campo estabelecido, sua evolução conceitual está em expansão. Muito do que precisa ser realizado daqui em diante exige uma reflexão mais profunda sobre métodos, provas e enfoques críticos que questionem a natureza das estruturas institucionais relacionadas às questões cibernéticas. O campo pode obter valiosas lições a partir das abordagens da teoria e da ética nas Relações Internacionais.

Dada a relevância do espaço cibernético para estudos, aprendizado, comércio e interações sociais, as atividades nesse ambiente acarretam significativos riscos, mas também oferecem amplas oportunidades. O futuro pode não ser dominado por conflitos e violência, mas a fronteira entre a estabilidade e o descontrole está constantemente sujeita a exploração no ciberespaço. A colaboração surge como a solução mais eficaz para garantir um futuro seguro.

Diante do exposto, o objetivo do presente estudo é abordar a relevância dessa temática no contexto das Relações Internacionais, apresentando diferentes perspectivas de autores, a fim de, proporcionar uma compreensão mais aprofundada sobre a questão, buscando assim, enriquecer a discussão de ações nessa área.

O presente estudo aborda acerca da guerra cibernética e a segurança global. O objetivo é investigar como a globalização e a expansão da internet influenciam a segurança e a autonomia dos países. Além de examinar potenciais ferramentas e soluções para garantir a segurança global de forma mais eficaz; o estudo busca compilar diversas opiniões de especialistas na área, apresentando-as sob a perspectiva das Relações Internacionais e tornando-as compreensíveis para diferentes públicos que possam ser impactados pelos riscos, desafios, legislações e acordos mencionados ao longo do texto.

Para a elaboração deste estudo, foram consultadas fontes bibliográficas sobre política externa e segurança internacional, programação de computadores e segurança *online*.

2 O CIBERESPAÇO

Toda guerra necessita de um local para ocorrer, um cenário onde as ações são desempenhadas e onde se pode observar o progresso e a intensidade dos ataques. Não existem apenas os espaços tradicionais, como terrestre, marítimo e aéreo;

atualmente, o ciberespaço representa uma dimensão igualmente crucial, embora seja talvez o espaço mais complexo de se delimitar, pois é interconectado globalmente, está em constante transformação e não permite a definição de fronteiras eficazes, como ocorre com as áreas geográficas convencionais (FERREIRA, 2018).

O ciberespaço teve seu início com a ARPANET, uma rede de longa distância desenvolvida em colaboração com universidades renomadas dos Estados Unidos da América (EUA) e a *Advanced Research Projects Agency* (ARPA). A proposta era explorar a eficácia da transmissão de dados em alta velocidade para fins militares. Em 1969, essa iniciativa marcou o início de todas as redes de computadores e da internet como a conhecemos atualmente, sendo essa a primeira aplicação do protocolo TCP, que ainda é amplamente utilizado para comunicação em redes. À medida que a tecnologia avançou, diversas outras redes foram integradas e novos protocolos de troca de informações foram criados, tornando a Internet cada vez mais intricada e ampliando o ciberespaço. Além disso, não só as dimensões desse ambiente cresceram, mas seu valor em termos de poder e influência também aumentou. Controlar a internet significa controlar as informações (KAISER, 2015).

Devido seu imenso potencial, o ciberespaço rapidamente se converteu em um alvo para as primeiras invasões de privacidade. No final da década de 1980, o espião alemão Marcus Hess comprometeu um terminal de acesso em Berkeley. Com esse ponto de entrada, ele conseguiu acessar a ARPANET e invadir 400 computadores militares, incluindo mainframes do Pentágono, com a intenção de vender informações sigilosas para a KGB. A partir desse momento, os vírus de computador deixaram de ser uma simples diversão acadêmica e se tornaram um desafio significativo para a segurança da informação (KAISER, 2015).

> O ciberespaço consiste na junção de diversas redes de comunicação, repositórios de dados e fontes informativas, formando uma extensa e variada teia de intercâmbio eletrônico. Isso resulta em um ecossistema de rede, um espaço que se diferencia do mundo físico tradicional. É um ambiente virtual e imaterial, verdadeiramente universal, presente onde existem cabos telefônicos, cabos coaxiais, fibras óticas ou ondas eletromagnéticas. O ciberespaço é mais do que uma dimensão virtual; ele se fundamenta na realidade física composta por servidores, cabos, computadores, satélites e outras tecnologias. Frequentemente, utilizamos os termos ciberespaço e Internet como se fossem sinônimos, embora a Internet seja apenas uma fração do ciberespaço, reconhecendo-se, no entanto, como a parte mais relevante atualmente (GALOYAN, 2019, p. 8).

A segmentação dos nomes no ciberespaço resulta em uma segunda questão que frequentemente causa confusões entre os usuários comuns. Embora o

ciberespaço esteja conectado em uma escala global, não se trata de um ambiente sem limites ou de um "bem universal". Assim como no mundo físico, onde estabelecemos fronteiras imaginárias, latitudes, longitudes e meridianos, no ciberespaço não é diferente. Esse espaço depende da infraestrutura física e das pessoas que estão relacionadas à geografia, o que implica que está sujeito às nossas percepções humanas sobre espaço, soberania, nacionalidade e propriedade (SINGER, 2014).

2.1 A guerra cibernética

Uma guerra cibernética pode ser considerada uma manifestação na web contra a apropriação indevida de informações na Internet, a interrupção de pesquisas nucleares por meio de ações cibernéticas e até mesmo atos de hostilidade em situações bélicas com o emprego de tecnologia avançada. Nesse contexto, as Forças Armadas dos Estados Unidos enfrentam numerosos ciberataques diariamente. Diferentemente de um ataque tradicional, um ataque cibernético utiliza ferramentas digitais e estratégias distintas baseadas em sistemas computacionais (SINGER, 2014).

O ataque cibernético não respeita fronteiras territoriais nem restrições nacionais; ocorre de maneira mais veloz e pode ter diversos alvos, sempre afetando um dispositivo e as informações que ele abriga. Os objetivos de tal ataque podem incluir, por exemplo, causar danos a algo físico, mas essa destruição sempre se inicia, primordialmente, por um evento no domínio digital. Ademais, é complicado identificar quem deu início ao ataque e como isso foi feito. Em certas situações, os *hackers* inserem seus nomes no *malware* que desenvolveram para serem reconhecidos, pois isso representa prestígio para eles.

Há várias categorias de ataques, são eles:

- **Ataques de disponibilidade -** Buscam obstruir o acesso a uma rede. Esses ataques frequentemente a inundam com muitos acessos, o que pode resultar em uma negação de serviço ou até mesmo em sua desativação, interrompendo assim os processos que dependem dessa rede, sejam eles físicos ou virtuais.

- **Ataques de confidencialidade -** São tentativas de acessar redes de computadores com o objetivo de observar as ações e obter informações sobre os

sistemas e os dados dos usuários. O tempo e os recursos necessários para essa atividade variam conforme o volume de dados que se busca acessar.

- **Ataques de integridade -** Consistem na intrusão em um sistema com o objetivo de alterar, ao invés de obter informações. Eles interferem nos dados do ambiente virtual, assim como nos sistemas e nas pessoas que dependem dessas informações. Essa modalidade de ataque pode ocorrer como um ato de vandalismo ou com a intenção de provocar danos substanciais ao sistema.

Certamente, toda modalidade de ataque requer um planejamento cuidadoso e uma execução quase impecável para que os objetivos sejam alcançados sem interrupções. Muitas vezes, é desafiador diferenciar os diversos tipos de ataques, uma vez que, por exemplo, tanto um ataque à confidencialidade quanto um ataque à integridade aproveitam vulnerabilidades para conseguir acesso a um sistema (NETO, 2017).

Existem diversas categorias de *Malware* que geram aplicações em máquinas contaminadas, permitindo o controle total das funções essenciais do sistema e, consequentemente, impactando o usuário. Os três aspectos mais significativos, que podem acessar e explorar outros dispositivos, são os seguintes:

a) Não há fronteiras territoriais, por exemplo, uma pessoa no Brasil pode invadir os sistemas da África do Sul para realizar ataques a infraestruturas na China, com o controle feito por máquinas situadas nos Estados Unidos, o que torna a identificação dessa ação bastante desafiadora;

b) O usuário pode nem perceber que seu computador está sendo manipulado por outra pessoa;

c) Quando ocorre uma ação maliciosa, uma análise avançada pode, na melhor das hipóteses, rastrear o computador utilizado para dar início ao ataque e, assim, identificar a pessoa responsável por trás disso.

Contudo, a guerra cibernética refere-se à manipulação ou ao ataque de sistemas de controle *online* e redes dentro de um contexto de combate ou confronto virtual. Engloba tanto ações ofensivas quanto defensivas em relação a riscos de ciberataques, vigilância e sabotagem. Existe um debate sobre a validade de classificar essas ações como guerra, em função das legislações internacionais que definem o que isso significa. Na prática, as nações têm aprimorado suas competências cibernéticas e se envolvido em conflitos digitais, tanto de modo agressivo quanto

defensivo.

A característica descentralizada dos ataques que ocorrem pela Internet dificulta a identificação da motivação e dos responsáveis, tornando incerta a avaliação de quando uma ação específica pode ser classificada como um ato de guerra. Assim, não está claro quando se deve iniciar a defesa ou até mesmo responder a um ataque. O crescimento do ciberespaço como um campo de combate gerou iniciativas para descobrir maneiras de utilizá-lo para fomentar a paz, como a limitação do uso de armas cibernéticas e atividades de espionagem, tornando a Segurança Cibernética um tema de grande relevância (PLAZA, 2022).

2.2 Armas cibernéticas

Ataques cibernéticos ocorrem por meio de programas projetados especificamente para explorar falhas em um sistema alvo. Esses programas prejudiciais são conhecidos como *malwares*. Frequentemente referidos como vírus, os *malwares* são introduzidos de forma discreta em um sistema, permitindo que um agente externo acesse as informações da vítima, capture dados ou até comprometa aplicações e o próprio sistema operacional (DE MELO et al., 2012).

As armas cibernéticas consistem em *softwares* projetados especificamente para segurança e defesa, visando atacar ou proteger sistemas determinados. Essa especificidade eleva significativamente os custos de desenvolvimento dessas armas, que incluem despesas com pessoal, inteligência incorporada, tempo de desenvolvimento e investimentos financeiros. Quanto mais direcionada for a arma, maiores serão os custos, assim como menores as possibilidades de ela ser reutilizada em um novo ataque a um sistema diferente (CRUZ JUNIOR, 2013).

Os vírus geralmente são criados para infectar a maior quantidade possível de sistemas, propagando-se de forma indiscriminada. Eles quase não contam com técnicas de disfarce, o que os torna mais fáceis e econômicos de produzir. Muitas vezes conseguem alcançar suas metas devido à inexperiência e à falta de segurança de certos usuários. No entanto, ferramentas de ataque cibernético direcionadas a alvos amplos frequentemente falham em penetrar e controlar sistemas essenciais. Frequentemente, o que é reportado como uma violação aos sistemas de organizações significativas no contexto global são, na maioria das vezes, ataques específicos (CRUZ JUNIOR, 2013, p. 7).

Entretanto, há armamentos que são criados com o propósito específico de invadir um sistema particular. Esses armamentos envolvem significativos investimentos com o intuito de maximizar as probabilidades de êxito do ataque, enquanto se busca manter sua operação o mais discreta possível, disfarçada dentro da estrutura do sistema visado.

> Um exemplo clássico de arma cibernética é o STUXNET. Este código malicioso foi desenvolvido com a finalidade específica de invadir o sistema SCADA5, utilizado para controlar as centrífugas de enriquecimento de urânio no Irã. As diferenças entre vírus como o ILOVEYOU e o STUXNET são significativas. Enquanto o primeiro era generalista, o STUXNET tinha um alvo claramente definido, empregando uma estratégia de ataque única e mecanismos de intervenção em sistemas físicos, além de contar com recursos de autoproteção e ocultação para não ser detectado até cumprir sua missão. No entanto, ele não possuía nenhuma capacidade de aprendizado, inteligência autônoma ou auto mutação, características que se esperam nas gerações futuras de vírus. Essa complexidade resulta em diferenças marcantes nos recursos necessários e nos custos de desenvolvimento entre essas duas categorias de malware (CRUZ JUNIOR, 2013, p. 7).

Entretanto, uma arma cibernética ofensiva não afeta apenas os recursos físicos, mas também gera repercussões nos âmbitos políticos e sociais. Um bom exemplo para ilustrar essa situação é o caso do Irã após o STUXNET. A principal consequência a nível nacional foi a diminuição da confiança dos cidadãos na habilidade do governo de salvaguardar uma área tão crucial como a nuclear. Apesar das negativas do governo iraniano, isso se tornou evidente (DE ARAÚJO, 2012).

Uma outra repercussão foi a dificuldade do Irã em se vingar, visto que a origem do ataque não era evidente ou estava suficientemente ambígua, o que fez com que o país parecesse vulnerável e um alvo acessível para ações similares. O STUXNET, mesmo não tendo impactado diretamente os cidadãos iranianos e sem gerar consequências imediatas, gerou um clima de apreensão entre a população, que se sentia decepcionada com seu governo pela ineficácia em garantir a segurança cibernética (BAEZNER et al., 2017).

3 SEGURANÇA CIBERNÉTICA NO MUNDO

Moresi (2012) destaca que a segurança cibernética representa um dos principais desafios que os governos em várias nações devem enfrentar, especialmente no que diz respeito à proteção das infraestruturas essenciais, como energia, defesa, transporte, telecomunicações e finanças. Embora os termos defesa

cibernética, segurança cibernética e guerra cibernética sejam semelhantes, eles possuem significados distintos, o que torna fundamental a compreensão das diferenças entre cada um deles.

A guerra cibernética pode ser entendida como um mecanismo de ação política ou militar. O especialista em crimes digitais, Milagre (2012), apresenta três perspectivas distintas para definir a guerra cibernética: com base na evolução do conflito, no tipo de armamento utilizado e nas forças que estão envolvidas na disputa:

> *Cyberwar* pode ser analisado a partir do contexto do conflito: em uma perspectiva de guerra fria (envolvendo disputas indiretas, espionagem, subversão ou inovações tecnológicas) ou como uma guerra de guerrilha ou subversiva (uma forma não convencional de combate que visa desestabilizar a ordem vigente). Também se encaixa dentro do conceito de guerra psicológica; [...] também é possível classificar o *Cyberwar* segundo a natureza das armas utilizadas: como uma guerra tecnológica; e pela natureza das forças envolvidas: trata-se de uma guerra irregular, onde ocorre um confronto entre um exército e um grupo guerrilheiro, com um campo de batalha que não possui limites definidos. Há uma dificuldade em distinguir entre civis e militares, mas também pode ser uma guerra regular, envolvendo exércitos virtuais (MILAGRE, 2012, p.10).

Conforme afirmam Mandarino Júnior e Canongia (2010), a segurança cibernética envolve tanto medidas preventivas quanto repressivas, enquanto a defesa cibernética se concentra em ações ofensivas. Segundo a Portaria n˚ 45 (Brasil, 2009), a esfera pública utiliza duas expressões relacionadas ao conceito de segurança cibernética: (i) infraestrutura crítica da informação; e (ii) ativos de informação. Neste documento, a infraestrutura crítica da informação é definida como um subconjunto de ativos de informação que impactam diretamente o cumprimento e a continuidade das funções do Estado, além da segurança da sociedade. A definição de ativos de informação, por outro lado, abrange os meios utilizados para o armazenamento, a transmissão e o processamento de dados, os sistemas de informação e os locais onde esses recursos estão situados, incluindo as pessoas que têm acesso a eles.

Os responsáveis por ataques cibernéticos são comumente chamados de *hackers* ou criminosos digitais. Conforme explicado pela Mcafee (2019), uma das principais empresas de soluções de segurança, o termo *hacker* pode ser dividido em 9 categorias, como demonstrado na tabela 1 a seguir.

Tabela 1 – A Definição de Hackers

Hackers	Descrição
Hackers White Hat	Apelidados de hackers bonzinhos, esses profissionais são experientes em segurança de sistemas e se dedicam a realizar testes de penetração e diversas outras técnicas para assegurar que as informações de uma empresa permaneçam protegidas.
Hackers Black Hat	Os hackers, frequentemente referidos simplesmente como tal, são frequentemente vistos como vilões. Esse termo é normalmente associado a indivíduos que invadem sistemas ou computadores, além de desenvolverem malwares. Esses hackers, em comparação com os *Hackers White Hat*, operam de maneira mais ágil, pois tendem a explorar as vulnerabilidades resultantes de falhas humanas ou descuidos, ou ainda a inventar novas modalidades de ataque.
Hackers Gray Hat	Estes Hackers empregam suas habilidades não somente para benefício próprio, mas também atuam de formas que não são totalmente legais. Por exemplo, um hacker que se infiltra em um sistema empresarial para detectar uma vulnerabilidade e divulga essa descoberta na internet, mesmo ajudando a organização de maneira construtiva, comete um crime ao acessar um sistema sem permissão.
Script Kiddies	Termo negativo utilizado para se referir a *hackers Black Hat* que utilizam *softwares* obtidos na internet para invadir redes e modificar sites com o intuito de ganhar notoriedade. Alguns deles pertencem à categoria de *hackers Green Hat*: são entusiastas iniciantes que almejam adquirir conhecimento na área e, futuramente, se tornar *hackers Black Hat* reconhecidos.
Hacktivists	*Hackers* que buscam contribuir para transformações sociais.
Hackers Patrocinados por Governos	Autoridades de diversos países reconhecem a importância de estarem estrategicamente posicionadas no ambiente digital, onde a gestão do ciberespaço se torna crucial para suas metas militares. Esses hackers operam sem restrições de tempo e dispõem de recursos financeiros para direcionar suas ações contra civis, organizações e até mesmo outras nações.
Hackers espiões	Companhias contratam especialistas em *hacking* para penetrar em organizações rivais e furtar informações confidenciais. Esses profissionais podem realizar invasões à distância ou conseguir posições de trabalho

	para operar como espiões internos.
Whistleblowers	Denominados como "infiltrados com más intenções", essas pessoas estão integradas a uma organização e utilizam seu acesso aos sistemas para divulgar informações que podem gerar alarmes. Esses hackers têm a capacidade de coletar dados para explorar segredos de negócios ou para buscar oportunidades de trabalho em outras companhias.
Ciberterroristas	Frequentemente guiados por convicções religiosas ou políticas, esses hackers buscam gerar e difundir medo, desordem e agressão ao paralisar a operação de serviços essenciais de infraestrutura. Os ciberterroristas são, sem dúvida, os mais ameaçadores e possuem uma grande diversidade de competências e metas.

Fonte – Mcafee, 2019.

Segundo (Morelli, 2015), um especialista espanhol em segurança online, existe uma distinção significativa entre os dois conceitos. Ele afirma que os *hackers* têm como objetivo melhorar a segurança de todos os usuários da internet, ao localizar falhas e vulnerabilidades nos sistemas para que possam ser resolvidas. Em contraste, os cibercriminosos, que são os reais delinquentes nesse ambiente digital, invadem sistemas, roubam senhas e furtam informações.

Tabela 2 – Principais Problemas de Segurança na Internet

Ameaça	Descrição
Phishing	Método de Engenharia Social que se apresenta como um site popular, como o de uma instituição financeira, com o objetivo de coletar dados pessoais de um usuário, tais como o número da conta e a senha de acesso.
Misrepresentation	A falsificação se refere à prática de fazer declarações incorretas ou exageradas a respeito de bens ou serviços, ou ainda fornecer produtos que são falsos ou de qualidade inferior.
Scams	As fraudes se apresentam de diversas maneiras, visando iludir pessoas desavisadas para que elas coloquem seu dinheiro em risco ou realizem atos ilegais.
Denial of Service (DoS)	A Negação de Serviço é uma prática que visa interromper o acesso a um site específico na internet, dificultando ou prejudicando operações comerciais e transações.
Perda do Controle	Um invasor obtém acesso ao dispositivo de um usuário e utiliza esse computador para realizar

	um ato ilícito.
Perda de Dados	Extravio de propriedade intelectual ou de informações confidenciais da organização.

Fonte – Comer, 2016.

A tabela 2 destacou-se os principais desafios relacionados à segurança na rede. Entre as ameaças à segurança, incluem-se malwares, vírus, *worms, adwares, ransomwares, trojans, bot/botnet, spyware, backdoor e rootkit,* cujas definições estão disponíveis na tabela 3.

Tabela 3 – Software mal intensionados

Técnica	Descrição
Malware	A sigla "malware", que se refere a programas maliciosos como vírus, worms e trojans, é um termo genérico que designa qualquer tipo de software criado com a intenção de prejudicar um computador, servidor ou rede. Esse tipo de software pode se manifestar de diversas maneiras e tem o potencial de causar danos significativos a um sistema ou a uma rede empresarial.
Vírus	Trata-se de um software que, ao ser ativado, tem a capacidade de comprometer todos os dispositivos que estão na mesma rede, furtando informações, danificando arquivos e disparando mensagens indesejadas para contatos de e-mail (expandindo o ataque), ou até assumindo o controle total do computador.
Worms	Diferentemente dos vírus, os worms não dependem de qualquer atividade do usuário para se espalhar. Eles se apresentam como anexos de e-mails ou em dispositivos contaminados e se multiplicam pela rede, resultando em lentidão na mesma.
Ransomware	Trata-se de um criminoso cibernético que acessa sistemas, apropria-se de informações e solicita um pagamento, frequentemente em moeda digital, para liberar os dados.
Adwares	Originário de publicidades em páginas da web, o malware se camufla como um anúncio para atrair sua interação.
	Os cavalos de Troia, também conhecidos como trojan-horse, são softwares que podem ser baixados de sites na internet, disfarçados como cartões virtuais animados, álbuns de fotos, jogos ou protetores de tela. Esses programas

Trojans	estão entre os tipos mais ameaçadores de malware, pois estão envolvidos em diversos tipos de ataques cibernéticos. Eles têm a capacidade de instalar outros malwares, permitir que um invasor acesse o computador remotamente, implementar ferramentas de negação de serviço, modificar ou deletar arquivos e pastas, formatar o disco rígido, monitorar e capturar dados sensíveis, além de configurar um servidor proxy que pode levar um computador a enviar spam pela rede.
bot/botnet	Um computador que foi contaminado por um bot é frequentemente denominado de zumbi, uma vez que pode ser gerenciado à distância, sem que o proprietário tenha ciência disso. Por outro lado, uma Botnet é uma rede composta por centenas ou até milhares de computadores zumbis, possibilitando aumentar a eficácia das atividades prejudiciais realizadas pelos bots.
Spyware	Trata-se de um software desenvolvido para acompanhar as ações de um sistema e transmitir os dados obtidos para outras partes. Pode ser utilizado de maneira correta ou de forma prejudicial.
Backdoor	Trata-se de um software que possibilita a um invasor reestabelecer acesso a um sistema que foi comprometido, utilizando serviços criados ou alterados especificamente para essa finalidade.
Rootkit	Trata-se de uma série de ferramentas e métodos que possibilitam ocultar e proteger a presença de um intruso ou de outro software prejudicial em um computador afetado.

Fonte – Shcultz, 2020a.

As táticas mais comuns empregadas por criminosos virtuais podem ser conhecidas por diversas pessoas. No entanto, à medida que a tecnologia e os métodos de proteção evoluem, esses indivíduos procuram atualizar suas estratégias e abordagens para conseguir acessar sistemas ilegalmente.

3.1 Estratégia Nacional de Defesa (END)

A Estratégia Nacional de Defesa (END), sancionada no final de 2008 e atualizada em 2012, definiu orientações sobre a organização e utilização das Forças Armadas para a proteção do país, ressaltando especialmente três áreas de relevância estratégica: o espaço, o ciberespaço e o campo nuclear (Brasil, 2012a).

> A Estratégia Nacional de Defesa estabelece a conexão entre a noção de autonomia nacional e a política que a sustenta, ao mesmo tempo em que se relaciona com as Forças Armadas, encarregadas de proteger essa autonomia. Esse documento trata de aspectos políticos e institucionais fundamentais para a segurança do país, incluindo os objetivos de sua “grande estratégia” e os métodos para envolver a população na defesa. Também aborda questões militares que surgem da influência dessa ‘grande estratégia’ sobre a direção e as práticas operacionais das três Forças Armadas. A Estratégia Nacional de Defesa será complementada por planos tanto para situações de paz quanto para conflitos, visando responder a diferentes cenários de atuação (Brasil, 2012a, p. 5, **grifo nosso**).

A END engloba o conceito de segurança cibernética, cuja proteção é responsabilidade do governo. No entanto, segundo Acácio (2012, p. 7), ao aprofundar-se na END, "o setor cibernético é caracterizado por um elevado nível de incertezas e escassez de informações". Nesse contexto, é importante ressaltar a dependência tecnológica que o Brasil tem em relação a produtos estrangeiros e a prestadoras de telecomunicações não nativas. Essa vinculação com nações mais avançadas em tecnologia da informação e comunicação é um desafio que provavelmente não poderá ser superado em um curto período, reforçando a necessidade de elaborar uma estratégia abrangente.

Conforme mencionado por Alves Júnior (2011), os Estados Unidos têm uma história consolidada na criação de estratégias voltadas para a segurança digital. As gestões de Bill Clinton, em 2000, e de George W. Bush, nos anos de 2002 e 2008, desenvolveram iniciativas com esse foco.

3.2 Política Cibernética de Defesa (PCD)

Conforme Hunker (2010), uma estratégia de segurança cibernética diz respeito às ações implementadas para assegurar a proteção no ambiente digital. Não só os órgãos governamentais devem instituir tais estratégias, mas também as empresas privadas, provedores de internet e organizações não governamentais, que precisam incorporar políticas de segurança cibernética. O autor salienta que, a primeira ideia associada a essa política é a defesa contra a criminalidade virtual. Contudo, essas diretrizes também se fundamentam em infraestruturas relacionadas ao ciberespaço e ao armazenamento de informações, entre outros aspectos, levando em consideração a cultura e as particularidades de cada nação.

A PCD abrange todos os elementos da manifestação militar do poder nacional, assim como as organizações que possam estar envolvidas em operações de defesa

ou em guerras cibernéticas. Seus propósitos são:

Os objetivos da Política de Defesa Cibernética incluem:

> a) garantir, de maneira colaborativa, a utilização eficaz do espaço cibernético (preparação e aplicação operacional) pelas Forças Armadas (FA) e prevenir ou dificultar seu uso em detrimento dos interesses da Defesa Nacional;
> b) desenvolver e gerenciar as competências humanas essenciais para a realização das atividades do Setor Cibernético (St Ciber) dentro do Ministério da Defesa (MD);
> c) colaborar na geração de conhecimento de Inteligência proveniente de fontes cibernéticas que sejam relevantes para o Sistema de Inteligência de Defesa (Sinde) e para as instituições governamentais conectadas à Segurança da Informação e Cibernética (SIC), especialmente o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
> d) formular e manter a doutrina atualizada sobre o emprego do St Ciber;
> e) adotar ações voltadas à gestão da SIC no âmbito do MD;
> f) ajustar as estruturas de Ciência, Tecnologia e Inovação das três Forças e promover pesquisas e desenvolvimentos que atendam às demandas do St Ciber;
> g) estabelecer os princípios fundamentais que orientem a elaboração de legislação e normas específicas para o uso do St Ciber;
> h) apoiar os esforços de mobilização nacional e militar para garantir a capacidade operacional e, consequentemente, a capacidade dissuasória do St Ciber;
> i) colaborar para a proteção dos ativos de informação da Administração Pública Federal (APF) em relação à Segurança Cibernética, especialmente aqueles fora da jurisdição do MD (Brasil, 2012a, p. 2).

A estratégia está intimamente ligada à política. De acordo com Ribeiro (2011, p. 161), o foco de um direcionamento estratégico inclui a formação de um centro de referência especializado, a elaboração de metodologias e sistemas, a estipulação de métricas e indicadores, além da colaboração entre os setores público e privado, bem como com a comunidade internacional. Todos esses aspectos devem ser fundamentados em uma estrutura legal e em um marco regulatório que assegurem esses objetivos.

No conjunto de políticas de segurança abordadas nesta análise, vários aspectos se repetem, entre os quais os mais notáveis são: (i) a formação de um centro de gestão de segurança digital; (ii) a constituição de equipes dedicadas à resposta a incidentes; (iii) a ênfase na formação, no avanço e na pesquisa; (iv) a fomento e intensificação da colaboração local; e (v) a obtenção de soluções de criptografia, sejam elas desenvolvidas internamente ou compradas.

Com base na avaliação das políticas e estratégias, conclui-se que um modelo de segurança digital deve incluir a criação, implementação, monitoramento e atualização de políticas, diretrizes, normas, procedimentos, ferramentas e tecnologias que direcionem a gestão desse modelo. Além disso, para garantir a eficácia do

modelo, é fundamental que a política de segurança digital aborde todas as vulnerabilidades existentes e, principalmente, envolva os participantes essenciais em seu planejamento, execução, avaliação e intervenção. A segurança cibernética, naturalmente, atua na prevenção de ameaças e ataques virtuais. Porém, quais são os ataques e riscos mais relevantes no ambiente digital? A tabela 2 a seguir ilustra os principais desafios que os usuários encontram ao navegar na Internet.

3.3 Modelos de Segurança Cibernética

Conforme mencionado, a PCD define os patamares de execução e as orientações referentes à segurança digital. Na PCD, as orientações detalham as ações que devem ser realizadas pelo Ministério da Defesa, incorporando princípios doutrinários fundamentais e abrangentes (Brasil, 2012b). É importante destacar as orientações que visam atingir o objetivo de evolução do setor cibernético (St Ciber) da PCD:

> Diretrizes atinentes ao Objetivo Nº IV - desenvolver e manter atualizada a doutrina de emprego do St Ciber: a) criar a doutrina de Defesa Cibernética mediante proposta do órgão central do S(MD)C; [...] f) designar o órgão central do SMDC como responsável por propor as inovações e atualizações de doutrina para o setor cibernético no âmbito da Defesa (Brasil, 2012a, p.3).

Considerando essas orientações, percebe-se que um dos principais obstáculos será a criação de um documento que abranja os requisitos e aspectos de governança, incluindo temas ligados ao planejamento, à estratégia e à tomada de decisões de forma integrada. Nesse contexto, o documento é designado como Modelo de Segurança Cibernética.

Mandarino Júnior e Canongia (2010) indicam que ainda não há um modelo estabelecido e avaliado para a criação de ações estruturadas voltadas à prevenção e ao enfrentamento de ataques e delitos cibernéticos. Contudo, é importante destacar que o Governo Federal instituiu o Grupo Técnico de Segurança Cibernética através da Portaria n˚ 45 (Brasil, 2009), que inclui membros dos Ministérios da Justiça, Defesa, Relações Exteriores e dos Comandantes das Forças Armadas, com a finalidade de desenvolver diretrizes e estratégias para a segurança na administração pública federal. Assim, é possível notar o esforço do governo na elaboração de um modelo de segurança cibernética.

No cenário global, é perceptível a realização de múltiplas iniciativas voltadas para a elaboração de estruturas de segurança cibernética. Um exemplo notável é o

do Departamento de Energia dos Estados Unidos, que criou o Modelo Federal de Segurança Cibernética. Conforme mencionado em Network Security (2009, p. 2), esse sistema “funciona como um *software* virtual. Quando uma entidade é alvo de um ataque em sua estrutura, a comunicação segura e oportuna com os demais órgãos da Federação ajuda a resguardá-la da agressão, podendo até envolver uma resposta ativa.”

Atualmente, o sistema fornece dados sobre endereços IP e domínios que levantam suspeitas, mas em breve terá a capacidade de trocar endereços de *e-mail* duvidosos e links da web entre os sistemas da Federação. A criação do sistema foi agraciada com o Prêmio de Inovação em Segurança Cibernética de 2009. A equipe está convencida de que, além de salvaguardar os bens públicos, a tecnologia pode ser aplicada também no setor privado.

O *National Institute of Standards and Technology (Nist)*, entidade dos Estados Unidos que visa incentivar a inovação e a competitividade no setor industrial por meio da criação de normas que asseguram maior segurança econômica e qualidade de vida, elaborou e mantém um modelo resultante da cooperação entre o governo e a iniciativa privada. Esse *framework* consiste em um conjunto de diretrizes e melhores práticas do setor que auxiliam as empresas na administração dos riscos de segurança cibernética. Ele orienta as ações de segurança digital, levando em conta os riscos associados a essa esfera como parte dos riscos de gerenciamento dos processos empresariais, adotando uma linguagem unificada para a gestão desses desafios (National Institute of Standards and Technology, 2014).

Os modelos desempenham um papel crucial na evolução e na compreensão da teoria relacionada à segurança cibernética, pois contribuem para a minimização dos perigos associados à cibersegurança. No entanto, sua implementação ainda está sendo estruturada pelos diferentes países.

4 A FORÇA DE DEFESA CIBERNÉTICA

Esse tema tem ganhado destaque na defesa mundial. Nações como China, Alemanha e Síria já vem se mobilizando para formar uma quarta força militar, com o objetivo de salvaguardar e regular seu ciberespaço. Embora seja um conceito recente, a guerra cibernética já se consolidou como uma realidade. Em 2017, nas primeiras semanas do ano, a Alemanha enfrentou mais de 280 ataques cibernéticos sofisticados

e profissionais, com o objetivo de obter informações militares. O STUXNET, reconhecido como uma das mais poderosas ferramentas cibernéticas já desenvolvidas, juntamente com a repercussão gerada pelo caso Snowden, que revelou a extensão das operações da NSA em coleta e análise de dados, evidenciam que a guerra cibernética não é um fenômeno isolado nem uma preocupação futura; ela já ocorre e há bastante tempo. Desde a criação da ARPANET, os computadores em rede têm armazenado informações valiosas, o que os torna alvos interessantes para aqueles que buscam reunir esses dados (GALOYAN, 2019).

Esse tipo de ocorrência serve como um catalisador para o desenvolvimento e o aumento do investimento em segurança digital. Os ataques estão se tornando mais sofisticados e organizados, sugerindo a participação de estados na concepção dessas ferramentas cibernéticas. Isso acontece porque, para desenvolver uma arma cibernética poderosa e eficaz, são requeridos significativos investimentos financeiros, além de um tempo considerável e profissionais altamente qualificados (GALOYAN, 2019).

Em 2009, o Google foi alvo de um significativo ataque cibernético, que na verdade fazia parte de uma ofensiva ainda maior que atingiu várias outras empresas, todas conectadas à administração dos Estados Unidos, além de fornecedores do Pentágono e alguns integrantes do Congresso americano. Após uma investigação pelo governo dos EUA e um subsequente relatório do FBI, constatou-se que o malware tinha sido criado por um hacker sem vínculos governamentais, mas que contava com o que foi denominado como "acesso especial" de oficiais de Pequim. O documento do FBI também confirmou a existência de um Exército Cibernético da China e revelou a identidade de 30.000 espiões cibernéticos chineses, além de mais 150.000 espiões atuando no setor privado (HJORTDAL, 2011).

5 CONSIDERAÇÕES FINAIS

Considerando os cenários analisados, foi possível examinar as potenciais ameaças no ciberespaço e seus impactos na segurança global, bem como nas esferas política e diplomática. Esses efeitos podem seguir duas direções: A cooperação internacional e a anarquia. A primeira busca resguardar a população mundial e outros agentes afetados pelas repercussões adversas de falhas na cibersegurança, por meio de iniciativas legais, investimentos em proteção de dados e ações colaborativas entre

Estados, organizações internacionais, ONGs e empresas privadas. Em contraste, a segunda opção fomenta a insegurança e acentua desigualdades entre os agentes, especialmente ao utilizar o ciberespaço como um meio bélico.

O futuro da guerra cibernética indica tendências encorajadoras que podem levar a situações mais benéficas. Contudo, se as iniciativas de combate aos crimes no ambiente digital não forem eficazes, as realidades descritas nos cenários negativos e apocalípticos se tornarão mais plausíveis. Esses cenários, como mencionado, têm a capacidade de provocar transformações permanentes no Sistema Internacional, incluindo a desintegração de parcerias e um aumento nas tensões políticas e diplomáticas entre países.

Dessa forma, até o ano de 2050, a segurança global no ciberespaço pode se consolidar como um importante instrumento de colaboração entre nações. Contudo, igualmente, existe a possibilidade de que se torne um fator que instigue novos conflitos cibernéticos, os quais poderiam escalar para níveis maiores de devastação. Assim, é essencial que os envolvidos avaliem as tendências e variáveis mencionadas e desenvolvam estratégias que os levem a cenários mais favoráveis para suas metas.

REFERÊNCIAS BIBLIOGRÁFICAS

Acácio, Igor D. P. **Segurança cibernética na política de defesa brasileira**: um caso de securitização? In: Encontro Sul-americano de Defesa e Encontro da Associação Brasileira de Estudos da Defesa, 1./4., 2012, São Paulo. Anais … São Paulo: 2012. p. 1-17.

Alves Júnior, Sérgio A. G. **Políticas nacionais de segurança cibernética**: o regulador das telecomunicações – Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT). Brasília: UnB, 2011. Dissertação (Mestrado) – Programa de Pós-Graduação em Regulação e Gestão de Negócios (Regen) da Faculdade de Economia, Administração e Contabilidade (Face) da Universidade de Brasília (UnB), Brasília.

BAEZNER, Marie; ROBIN, Patrice. **Stuxnet**. ETH Zurich, 2017

BRASIL. **Gabinete de Segurança Institucional. Portaria n˚ 45**, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (Creden), o Grupo Técnico de Segurança Cibernética e dá outras providências. Diário Oficial da União (DOU), Brasília, n. 172, 9 set. 2009. Seção 1, p. 2-3.

BRASIL. **Decreto nº 576, de 17 de julho de 2012**. Aprova a revisão da Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial da União (DOU), Brasília, n. 247, 17 jul. 2012a. Seção 1, p. 1-3. Disponível em: < http://www2.camara.leg. br/legin/fed/decleg/2013/decretolegislativo-373-25-setembro-2013-777085- publicacaooriginal-141221-pl.html>. Acesso em: 09 Out. 2024.

COMER, D. E**. Redes de Computadores e Internet**-6. [S.l.]: Bookman Editora, 2016.

CRUZ JÚNIOR, Samuel César da. **Tecnologias e riscos**: armas cibernéticas. 2013.

DE ARAÚJO, JORGE, Bernardo Wahl G. **Estados Unidos, poder cibernético e a "guerra cibernética"**: Do Worm Stuxnet ao Malware Flame/Skywiper–e além. BOLETIM MERIDIANO47, p. 43, 2012.

DE MELO, Laerte Peotta et al. **Análise de malware:** Investigação de códigos maliciosos através de uma abordagem prática. SBSeg, v. 11, p. 9-52, 2011. Disponível em: https://www.researchgate.net/profile/Rafael_De_Sousa_Junior/publication/268265685_Analis e_de_Malware_Investigacao_de_Codigos_Ma_liciosos_Atraves_de_uma_Abordagem_Pratic a/links/54bea3aa0cf28ad7e71880f7.pdf. Acesso em: 4 out. 2024.

FERREIRA, Walfredo Bento Neto. T**erritorializando o "novo" e (re) territorializando os tradicionais:** a cibernética como espaço e recurso de poder. Revista Brasileira de Estudos Estratégicos, n. 4, 2018.

GALOYAN, Albert. **Segurança cibernética no âmbito das relações internacionais**. 2019. 50 f. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais)— Universidade de Brasília, Brasília, 2019.

HJORTDAL, Magnus**. China's use of cyber warfare**: Espionage meets strategic deterrence. Journal of Strategic Security, v. 4, n. 2, p. 1-24, 2011.

HUNKER, Jeffrey. **US international policy for cybersecurity**: five issues that won't go away. Journal of National Security Law & Policy, v. 4, n. 1, p. 197-216, 2010

KAISER, Robert. **The birth of cyberwa**r. Political Geography, v. 46, p. 11-20, 2015.

MANDARINO Júnior, Raphael; Canongia, Claudia (Orgs.). Livro verde: **segurança cibernética no Brasil**. Brasília: Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações (GSIPR/SE/DSIC), 2010.

MCAFEE. **9 Tipos de hackers e suas motivações**. 2019. [Online] Disponível em: https://www.mcafee.com/blogs/languages/portugues/9-tipos-de-hackers-e-suas-motivacoes/. Acesso em: 17/10/2024.

MILAGRE, José A. **Guerra e defesa cibernética**. Blog online. Disponível em: https://www.google.com/search?q=%3Chttp%3A%2F%2F+josemilagre.com.br%2Fblog%2Fsala-de-estudos%2Fcyberwar%2Fpesquisas-2%2Fguerra-e-defesacibernetica&sourceid=chrome&ie=UTF-8. Acesso em: 23 Out. 2024.

MORELLI, M. **"É preciso diferenciar hacker de cibercriminoso**". 2015. [Online] disponível em: https://veja.abril.com.br/tecnologia/e-preciso-diferenciar-hacker-de-cibercriminoso/. Acesso em: 17/10/2024.

MORESI, Eduardo A. D. et al. **Defesa cibernética: um estudo sobre a proteção da infraestrutura e o software seguro.** In: Conferencia Iberoamericana de Complejidad, Informática y Cibernética, 2., 2012, Orlando-FL. Anais... Orlando: 2012.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Nist). **Framework for improving critical infrastructure cybersecurity.** Versão 1.0. 2014. Disponível em: . Acesso em: 10 Out. 2024.

NETO, Ricardo Borges Gama. **Guerra cibernética / guerra eletrônica** – conceitos, desafios e espaços de interação. Política Hoje, v. 26, n. 1, 2017.

NETWORK Security. **US lab develops federated model for defence against cyber attack.** Network Security – News, v. 2009, n. 9, p. 2, 2009.

PLAZA, William R. **Qual foi o primeiro vírus de computador?.** Hardware.com.br, [S. L], 24 maio. 2022. Disponível em: https://www.hardware.com.br/artigos/qual-primeiro-virus-decomputador/. Acesso em: 22 out. 2024.

RIBEIRO, Sérgio L. **Estratégia de proteção da infraestrutura crítica de informação e defesa cibernética nacional**. In: Barros, Otávio S. R.; Gomes, Ulisses M.; Freitas, Whitney L. (Orgs.). Desafios estratégicos para a segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 145-163.

SCHULTZ, F. **Segurança Cibernética**: o que é e como ser um especialista no assunto. 2020. [Online] Disponível em: https://milvus.com.br/seguranca-cibernetica-o-que-e/. Acesso em: 17/10/2024.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity:** What everyone needs to know. oup usa, 2014.