DESAFIOS DO CIBERTERRORISMO: IMPACTOS NA SEGURANÇA INTERNACIONAL E NO ESTADO MODERNO

CHALLENGES OF CYBERTERRORISM: IMPACTS ON INTERNATIONAL SECURITY AND THE MODERN STATE

AMANDA QUEIROGA DE SOUSA
CAROLLYNE GOMES DOS SANTOS[1]

RESUMO

Em um mundo onde as fronteiras físicas cedem espaço às fronteiras digitais, a Segurança Internacional enfrenta uma ameaça iminente: o ciberterrorismo. Este artigo propõe uma análise aprofundada da evolução dessa ameaça virtual e sua influência impactante no cenário internacional. No complexo teatro da Segurança Internacional, onde as ameaças transcendem as fronteiras geográficas, o ciberterrorismo emerge como uma força disruptiva, desafiando noções convencionais de segurança estatal. Ao explorar as conexões intrínsecas entre segurança internacional e a esfera digital, buscamos desvendar as complexidades que tornam o ciberterrorismo tão significativo para o tecido do Estado moderno.

Esta pesquisa não apenas delineia a ascensão do ciberterrorismo ao longo do tempo, mas também destaca a interseção crítica entre a segurança nacional e a era digital. Em um cenário onde bits e bytes se tornam armas, compreender não apenas a natureza evolutiva dessa ameaça, mas também seu potencial de desestabilização em níveis nacionais e internacionais, é imperativo. Propomos uma imersão crítica no universo digital, visando não apenas compreender as nuances do ciberterrorismo, mas também destacar estratégias eficazes para preservar a segurança do Estado no

[1] Amanda Queiroga de Sousa e Carollyne Gomes dos Santos são estudantes do curso de Relações Internacionais da Universidade São Judas Tadeu, sendo este artigo apresentado como exigência parcial para a conclusão de curso em dezembro de 2023, sob orientação do Prof. Dr. Mauricio Homma.

século XXI. Ao mapear a trajetória dessa evolução, este estudo oferecerá insights valiosos e medidas necessárias para fortalecer a resiliência dos Estados contra essa ameaça iminente.

Palavras-chave: Ciberterrorismo. Segurança Internacional. Ameaças Digitais. Governança no Ciberespaço.

ABSTRACT

In a world where physical boundaries yield to digital frontiers, International Security faces an imminent threat: cyberterrorism. This article proposes an in-depth analysis of the evolution of this virtual threat and its impactful influence on the international landscape. In the complex theater of International Security, where threats transcend geographical borders, cyberterrorism emerges as a disruptive force, challenging conventional notions of state security. By exploring the intrinsic connections between international security and the digital sphere, we aim to unravel the complexities that make cyberterrorism so significant for the fabric of the modern state.

This research not only outlines the rise of cyberterrorism over time but also highlights the critical intersection between national security and the digital era. In a scenario where bits and bytes become weapons, understanding not only the evolutionary nature of this threat but also its potential for destabilization at national and international levels is imperative. We propose a critical immersion into the digital universe, aiming not only to comprehend the nuances of cyberterrorism but also to highlight effective strategies for preserving state security in the 21st century. By mapping the trajectory of this evolution, this study will offer valuable insights and necessary measures to strengthen the resilience of states against this imminent threat.

Keywords: Cyberterrorism. International Security. Digital Threats. Cyberspace Governance.

Introdução

Num mundo onde as fronteiras físicas cedem espaço às fronteiras digitais, a Segurança Internacional se vê confrontada por uma ameaça premente: o ciberterrorismo. Este artigo de TCC propõe uma análise aprofundada sobre a evolução dessa ameaça virtual e sua impactante influência no panorama internacional. No complexo teatro da Segurança Internacional, onde ameaças transcendem fronteiras geográficas, o ciberterrorismo emerge como uma força disruptiva, desafiando concepções convencionais de segurança estatal.

Ao explorar as intrínsecas relações entre segurança internacional e a esfera digital, buscamos desvendar as complexidades que tornam o ciberterrorismo tão significativo para o tecido do Estado moderno. Esta pesquisa não apenas delineou a ascensão do ciberterrorismo ao longo do tempo, mas também destaca a interseção crítica entre segurança nacional e a era digital. Em um cenário onde bits e bytes tornam-se armas, é imperativo compreender não apenas a natureza evolutiva dessa ameaça, mas também seu potencial de desestabilização em níveis nacionais e internacionais.

De acordo com o estudo Digital 2023: Global Overview Report, aproximadamente 64,4% da população mundial usa a internet, com 59,4% também acessando redes sociais. O crescimento do uso de tecnologias avançadas estende-se aos Estados e outros atores que as empregam deliberadamente para criar, armazenar, modificar e trocar informações através das redes.

O manuseio de tecnologias da informação e comunicação, como conhecemos hoje, só foi possível através da exploração comercial da Arpanet, inicialmente criada para transmitir dados militares sigilosos e conectar departamentos de pesquisa nos Estados Unidos. A internet, com suas três camadas técnicas distintas e a quarta camada que trata das interações sociais transnacionais, impõem adversidades quanto à sua governança.

O ciberespaço começou a ser explorado com mais afinco na agenda de pesquisa de segurança após os atentados de 11/09/2001, evidenciando o uso da internet e outras tecnologias da informação e comunicação. Outros casos internacionais, como o worm Stuxnet utilizado para atacar instalações nucleares iranianas, também destacam a necessidade de soluções para a falta de governança no ciberespaço, apresentando-se como novas formas de terrorismo. Essas informações ressaltam a importância crítica de abordar o tema do ciberterrorismo na interseção entre segurança internacional e o cenário digital.

Conectando os Pontos: Terrorismo Tradicional vs Ciberterrorismo

Com o propósito de definir um conceito para o que é o terrorismo, diversos atores e pesquisadores da área buscaram uma acepção neutra sobre os métodos para que não se confunda com outras formas de violência política.

Em seu livro Explaining Terrorism: Causes, processes and consequences (1981), Martha Crenshaw estabelece a compreensão do terrorismo como “uma forma de violência com a intenção de influenciar uma audiência, executado com base na surpresa, conspiração e decepção”.

Cuidadosamente planejados e executados, esses atos são a maneira que aqueles que estão fora do poder e se julgam como incapazes de alcançar seus objetivos de outra forma encontram para receber suporte público e criar mudanças políticas ou sociais, através da escolha de hora, lugares e vítimas que choquem, amedrontem e revoltem.

Mesmo em sua forma mais tradicional, tais atos extremistas se tornam atrativos e significantes em virtude da combinação de feitos de baixo custo, facilidade e grande potencial político e psicológico. Durante a história da humanidade se sucederam ataques em diversas regiões do globo, desde grupos paramilitares na América Latina nas décadas de 70 e 80 (como as Operações Condor), ataques da Frente de Libertação Nacional (FLN) na Argélia durante a luta pela independência até o fatídico 11 de Setembro de 2001 realizados pela Al-Qaeda nos Estados Unidos.

A fim de definir o que é o ciberterrorismo, se faz necessário entender o ambiente em que ocorre e os atores presentes. De acordo com Kuehl (2009, p. 4), o ciberespaço é definido como

> Um domínio global dentro do ambiente da informação cujo caráter distintivo e único é moldado pelo uso de eletrônicos e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas utilizando tecnologias de informação e comunicação. (Kuehl, 2009, tradução nossa)

Como descrito por Joseph Nye (2010), nessa arena os atores são diversos e o cenário se torna novo no ciberespaço pois atores não estatais e de baixo poder podem ter hard e soft power que não teriam se não fosse por toda tecnologia e Internet, com "armas" de baixo preço, animosidade e novas assimetrias de vulnerabilidades.

Apesar de “nem todos os cachorros serem iguais” (Nye, 2010, p.9) o domínio do ciberespaço possui agentes de diferentes níveis, com suas respectivas forças e fraquezas. Estão entre eles, os Governos, Organizações e networks de grande estruturas, Indivíduos e networks de estruturas menores.

O poder nesse novo palco se faz através da habilidade de criar vantagens e influenciar eventos. Nye (2010) mais uma vez pontua quais são as faces de poder no cyber domínio, entre elas estão a habilidade de desviar a pretensão de um ator, a consolidação de agenda por exclusão de estratégias (que pode acontecer por meio do hard ou soft power) e a formação de preferências de outros.

Sendo um campo onde os humanos e suas organizações utilizam as tecnologias para agir e criar efeitos (Kuehl, 2009), o ciberespaço traz consigo problemas de espionagem econômica, crimes, guerra cibernética e ciberterrorismo. Tais adversidades criam uma nova demanda por proteção contra crimes em que a atribuição da responsabilidade a algum ator é inacessível.

Nesse sentido, o ciberterrorismo pode se apresentar de diversas formas, como ataque cibernético direcionado a infraestruturas críticas (Stuxnet em 2010), ataques cibernéticos a sistemas de energia, sistemas de água, transportes e saúde e uso de

plataformas sociais utilizadas para a propagação de desinformação, a fim de semear o caos ou criar tensões sociais.

De ARPANET a Web Global, o caminho evolutivo da internet

É fato que a tecnologia é para a era atual o que a eletricidade foi para a revolução industrial (Castells, 1999), é capaz de promover novos empregos e níveis educacionais e econômicos em grande parte do globo.

A princípio a internet surgiu como um projeto piloto da década de 1960 desenvolvido pela Agência de Projetos de Pesquisa Avançada (ARPA) como uma rede de comunicação robusta com a missão de transmitir dados militares e interligar departamentos de pesquisa dos Estados Unidos que sobreviveria a falhas de hardware e ataques.

Após diversos testes realizados através da conexão das universidades e instituições de pesquisa, em 1980 a ARPANET se tornou conhecida como a "internet" e se iniciou o uso comercial, trazendo inovações como o primeiro navegador web (WorldWideWeb, mais tarde renomeado de Nexus) e possibilitou o uso do público geral.

No panorama atual, a pesquisa do Digital 2023: Global Overview Report divulga que o volume de usuários da Internet é de 5,16 bilhões, número que representa 64,4% dos 8.01 bilhões da população mundial. Desses, 4,76 bilhões têm acesso a redes sociais - ou seja, 59,4% das pessoas no mundo.

A história da internet continua a se desenrolar conforme as inovações e desenvolvimentos tecnológicos, mas essa ferramenta desempenhou um papel fundamental em diversas áreas ao longo das últimas décadas. Transformou a maneira como os humanos se comunicam, coletam informações, realizam negócios e acessam entretenimento.

O ciberespaço pode ser utilizado de diversas maneiras pelos seus variados atores, que podem ser anônimos e distantes fisicamente. É observado a presença de civis

comuns, hacktivistas, grupos criminais e governos na internet, cada um com o seu respectivo objetivo de uso.

Quando se trata de atores estatais, verificamos o uso dos meios tecnológicos para diplomacia pública, comunicação com os cidadãos, serviços públicos, monitoramento de ameaças à segurança nacional, uso militar e coerção física e legal de indivíduos.

Em um constante ciclo de progresso condicionado pela dinâmica da sociedade, o desenvolvimento cultural e educacional promove desenvolvimento tecnológico, que promove desenvolvimento econômico e social, retornando a estimular o cultural e educacional.

Apesar de tamanha modernização, há outro lado dessa era, da iniquidade, pobreza, miséria e exclusão social (Castells, 1999). Houve redução de pobreza em alguns países com as oportunidades oferecidas pelas tecnologias, mas ainda não é possível alcançar a todos, visto que, existem limitações geográficas do ciberespaço e limites socioeconômicos e políticos como restrição de uso, diferentes custos para acesso e legislações diferentes dos Estados (Cepik, Canabarro e Borne, 2014).

Ciberterrorismo praticado por Estados e atores independentes

O crescente entrelaçamento entre o mundo físico e o ciberespaço destaca a importância crucial dessa interconexão na era globalizada. À medida que a Internet e o ciberespaço se tornam serviços públicos globais, a dependência crescente dessas tecnologias gera desafios significativos para a segurança nacional e internacional. A securitização da Internet, impulsionada pelo contexto político-estratégico, ganhou destaque após os eventos de 11 de setembro de 2001.

Essa dinâmica interconexão é evidenciada pela imbricação entre instrumentos físicos, como roteadores e servidores, e suas localizações geográficas. Esses elementos fundamentais do ciberespaço não existem em um vácuo digital; eles ocupam espaços físicos específicos, sujeitos às leis dos governos locais. Nesse sentido, a coerção física por parte dos governos emerge como uma ferramenta

potente, exercendo influência direta sobre empresas e indivíduos que operam nesse ambiente virtual.

A Internet, inicialmente concebida como um projeto piloto sob o comando do Departamento de Defesa dos Estados Unidos, expandiu-se globalmente, tornando-se acessível em todo o mundo. No entanto, a avaliação otimista inicial de uma desvinculação entre usuários e espaços físicos soberanos foi revisada. A estrutura em camadas da Internet, incluindo aspectos físicos, técnicos e lógicos, além das interações sociais transnacionais, desafia os processos tradicionais de governança política.

A geografia do ciberespaço é delineada por constrangimentos técnicos, limites socioeconômicos e políticos. Questões como exclusão digital, custos de conexão e legislação estatal impactam diretamente a capacidade de uso e organização dos usuários, transcendendo as fronteiras do mero domínio técnico para influenciar áreas diversas da sociedade e pautar a agenda global na era digital.

A complexidade da governança da Internet, com desafios como segurança cibernética e securitização do ciberespaço, amplia ainda mais o escopo da discussão. Essas questões transformam a governança da Internet em uma matéria que vai além dos círculos especializados em computação, exercendo impacto em diversas áreas da vida social e na agenda política global.

O atual crescimento da Internet é caracterizado por duas tendências marcantes: ubiquidade e convergência digital. A ubiquidade refere-se à onipresença da rede, com diversos dispositivos sendo desenvolvidos para conexão por meio dos protocolos de comunicação da Internet. A convergência digital, por sua vez, integra diferentes mídias em um único canal de transmissão, revolucionando instituições e modos de produção midiática.

Entretanto, esse crescimento não ocorre sem implicações políticas significativas. A transmissão em tempo real de eventos e a interação bidirecional facilitada pela Internet têm impactos profundos na opinião pública e nas relações internacionais. Nesse contexto, a segurança nacional e internacional é afetada por ações

cibernéticas deliberadas, evidenciando a securitização do ciberespaço como um tema central no debate contemporâneo.

A militarização do ciberespaço por países como os Estados Unidos, China e Rússia resultou na criação de comandos cibernéticos e centros de defesa cibernética. A interação entre terrorismo e ciberespaço, destacada após os eventos de 11 de setembro, levanta questões teóricas e práticas sobre a distinção entre diferentes tipos de incidentes cibernéticos e as respostas precisas dos países a essas ameaças.

A complexidade dessa interação é evidente na falta de uma definição consensual de terrorismo, um conceito inerentemente político. A imbricação entre ciberespaço e terrorismo, embora complexa, destaca desafios específicos, como a definição de ciberterrorismo e a associação entre organizações criminosas, anonimato e Estados. A análise revela que, embora o ciberespaço tenha um potencial impacto significativo, a capacidade real dos grupos terroristas causarem danos substanciais à infraestrutura global da Internet é limitada.

O entrelaçamento entre o mundo físico e o ciberespaço destaca, portanto, uma realidade complexa e interdependente, onde instrumentos físicos têm localizações geográficas específicas e estão sujeitos às leis dos governos. A coerção física por parte dos governos exerce influência direta sobre empresas e indivíduos no ciberespaço, evidenciando a necessidade de uma abordagem integrada que considere tanto os aspectos técnicos quanto às questões políticas relacionadas às tecnologias da informação e comunicação.

O fenômeno do ciberterrorismo praticado por Estados emerge como uma ameaça significativa nas relações internacionais, redesenhando as fronteiras do conflito e apresentando desafios singulares à segurança nacional. Ao analisarmos as obras "Cyber War: The Next Threat to National Security and What to Do About It" de Carr (2010) e "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," editado por Dudziak (2014), obtemos uma compreensão abrangente desse cenário complexo.

De acordo com Carr, o ciberespaço tornou-se uma arena onde Estados conduzem operações ofensivas, escapando das táticas tradicionais de guerra. Essa mudança paradigmática levanta questões críticas sobre a definição de um ato de guerra e as estratégias adequadas para responder a ataques cibernéticos. A identificação clara do agressor torna-se um desafio, desafiando as estruturas de dissuasão convencionais.
A análise de Carr sobre o ciberespaço como uma arena para operações ofensivas estatais destaca uma mudança paradigmática nas estratégias militares. A capacidade de conduzir ataques cibernéticos permite que os Estados contornem as abordagens tradicionais de guerra, apresentando um desafio para a definição clara de um ato de guerra. A complexidade reside na dificuldade de identificar claramente o agressor, desafiando as estruturas de dissuasão convencionais que dependem da atribuição de responsabilidades.

Dudziak, por sua vez, destaca o papel influente do ciberespaço na política externa, onde ativismo online, hacktivismo e ciberterrorismo ultrapassam fronteiras nacionais para moldar agendas políticas globais. Isso amplia a visão da ameaça cibernética, indicando que os Estados enfrentam não apenas desafios de outros Estados, mas também de atores não estatais que buscam influenciar o cenário internacional de maneiras diversas.

A interconexão dessas perspectivas sublinha a complexidade contemporânea das relações internacionais. A necessidade de estratégias robustas de segurança cibernética torna-se crucial, não apenas para enfrentar ameaças convencionais, mas também para abordar os desafios únicos apresentados pelo ciberterrorismo estatal e por atores não estatais. A falta de consenso internacional sobre normas cibernéticas intensifica essa complexidade, visto que a identificação de culpados e a atribuição de responsabilidades são desafios cruciais em um ambiente onde as ações no ciberespaço ultrapassam barreiras físicas e jurídicas.

A proposta holística de Carr destaca a importância de fortalecer as capacidades de defesa cibernética, estabelecer normas internacionais claras e buscar soluções

diplomáticas para disputas cibernéticas. A cooperação entre Estados torna-se indispensável para garantir a segurança nacional e a estabilidade global no ciberespaço. No entanto, o equilíbrio delicado entre interesses nacionais, segurança cibernética e preservação das liberdades individuais demanda o desenvolvimento de políticas e regulamentações eficazes. Essa abordagem se torna essencial para enfrentar os desafios multifacetados apresentados pelo cenário emergente do ciberterrorismo em nível internacional.

Em síntese, o ciberterrorismo praticado por Estados redefine as dinâmicas tradicionais das relações internacionais, exigindo uma reavaliação constante das estratégias de segurança em um ambiente onde as fronteiras entre guerra e paz são cada vez mais tênues.

Os ataques cibernéticos em cenários de conflitos geopolíticos emergem como uma arma poderosa e estratégica no arsenal dos Estados e atores não estatais. Estes incidentes transcendem fronteiras físicas, desencadeando impactos significativos em governos, organizações e populações.

Em meio à complexidade da ciberguerra, a Ucrânia se destaca como um palco onde as hostilidades estendem-se para o ciberespaço. Grupos hackers, muitas vezes vinculados à Rússia, têm direcionado ataques contra infraestrutura crítica, instituições financeiras e o governo ucraniano. Métodos sofisticados, como malware personalizado e técnicas de phishing, são empregados para minar a estabilidade e a segurança nacional.

As tensões entre os Estados Unidos e o Irã também se desdobram digitalmente. Ataques cibernéticos, atribuídos a grupos iranianos, visam sites do governo dos EUA e aliados, assim como empresas privadas. Essa forma de agressão virtual torna-se uma extensão natural das disputas geopolíticas, explorando vulnerabilidades digitais para obter vantagem estratégica.

Enquanto isso, na Península Coreana, o ciberespaço é um campo de batalha adicional. A Coreia do Norte, frequentemente acusada de conduzir atividades cibernéticas agressivas, tornou-se alvo de ataques também. A atribuição desses eventos muitas vezes permanece nebulosa, mas a presença da NSA nos bastidores sugere uma complexa dança de operações cibernéticas entre Estados.

Na guerra na Síria, as hostilidades extrapolam os campos de batalha tradicionais para o mundo digital. Grupos diversos, com motivações variadas, empregam táticas de espionagem, propaganda online e ataques direcionados a sistemas governamentais e organizações humanitárias. A ciberguerra torna-se assim uma ferramenta multifacetada, moldando narrativas e influenciando dinâmicas em conflitos reais.

Os ataques cibernéticos perpetrados por atores não estatais emergem como uma força transformadora no panorama global, desafiando governos, instituições e empresas. Esses grupos, muitas vezes agindo à margem da legalidade, utilizam o ciberespaço como um campo de batalha para expressar suas agendas, disseminar mensagens e, em alguns casos, buscar vantagens estratégicas.

O grupo ativista online Anonymous é um exemplo proeminente. Conhecido por sua habilidade em mobilizar ações coletivas, o Anonymous protagonizou a "Operação Payback" em 2010. Nesse episódio, o grupo direcionou seus esforços contra empresas que retiraram seu apoio ao WikiLeaks. Através de ataques de negação de serviço (DDoS), eles temporariamente interromperam os serviços online de gigantes corporativos como PayPal, Visa e MasterCard, ilustrando o poder descentralizado que atores não estatais podem exercer no ciberespaço.

Além disso, a natureza transnacional do ciberespaço permite que grupos como o Anonymous atuem globalmente, desafiando fronteiras físicas e jurídicas. Suas ações muitas vezes se entrelaçam com causas sociais e políticas, exemplificando como o ativismo digital pode moldar debates públicos e influenciar a narrativa global.

No reino do ciberterrorismo, o papel dos atores não estatais também se destaca. O ransomware WannaCry, por exemplo, foi disseminado por indivíduos ou grupos visando obter ganhos financeiros. Ao criptografar dados em computadores e exigir pagamento em bitcoin para a sua liberação, esses atores demonstram como a motivação financeira pode ser um poderoso catalisador para ataques cibernéticos em larga escala.

Enquanto governos se esforçam para lidar com ameaças cibernéticas originadas por atores não estatais, a agilidade, a falta de uma estrutura hierárquica rígida e a capacidade de adaptação desses grupos apresentam desafios únicos. O cenário atual sugere que o ciberespaço continuará a ser um terreno fértil para a expressão de poder e influência por parte de atores não estatais, redefinindo as dinâmicas do jogo geopolítico de maneiras imprevisíveis.

Abordagens estratégicas para a Segurança Internacional: Propostas e Soluções

Na contemporaneidade, serviços variados prestados à sociedade pelos Estados se dão através do ciberespaço (sistemas de comunicação, financeiros, energia, água e outros) que caso venham a ficar indisponíveis poderia levar ao colapso até mesmo a segurança nacional.

Como citado anteriormente, a securitização do ciberespaço já se tornou pauta da agenda dos governos para que a utilização de todos os atores seja confiável e segura. A União Internacional de Telecomunicações (UIT) define que a cibersegurança se trata de um conjunto de políticas e ações que podem ser aplicadas a fim de proteger o ambiente cibernético.

Com o propósito de avaliar o empenhamento das nações para promover melhorias, a UIT e a Organização das Nações Unidas (ONU) realizam desde 2015 o Global Cybersecurity Index (GCI) ponderando diversos fatores que determinam o nível de preparação e resiliência dos países. São avaliados aspectos como a capacidade de

cibersegurança, legislação e estratégias, cooperação internacional e investimentos em segurança cibernética.

Exemplificando os gaps entre os países desenvolvidos e em desenvolvimento nesse quesito, a classificação no ranking geral do CGI de 2020 é liderado por Estados Unidos, Reino Unido e Arábia Saudita. Esse relatório salienta possíveis evoluções para os Estados, como monitoramento e atualização de estratégias, criação de métricas significativas, participação de convenções e envolvimento dos diversos atores.

Se referindo a normas internacionais estabelecidas ao redor do globo, alguns atores consideram os delitos cyber-capacitados e cyber-dependentes (cometidos por meio da tecnologia e que a tem como alvo e cometidos sem tecnologia mas que quando utiliza promove mudança significativa e em alta escala, respectivamente) como aqueles que necessitam de criminalização pelo seu cometimento.

Visando descrever condutas penalmente relevantes na época como acesso ilegal, violação de dados e direitos autorais, falsificação, fraude e pornografia infantil, em 2001 a Convenção de Budapeste foi o palco da Convenção sobre Crimes Cibernéticos do Conselho da Europa e buscou fornecer uma estrutura legal para o enfretamento de ameaças à cibersegurança.

Foram estabelecidas diretrizes para a definição de crimes cibernéticos, os procedimentos de investigação e cooperação internacional, proteção de dados e prevenção. Países dentro e fora da Europa aderiram a essa convenção e incluíram em suas legislações as normas acordadas no evento.

No Capítulo III da Convenção de Budapeste, se estabeleceu procedimentos para a cooperação entre países signatários em relação às ameaças transfronteiriças tais quais os canais de cooperação, os procedimentos para solicitação de cooperação, encorajamento de agilidade e eficiência na cooperação e proteção legal.

Ainda que o auxílio mútuo tenha que seguir as condições do direito interno dos Estados signatários, a cooperação através de canais de comunicação se dá diretamente através de autoridades como a Organização Internacional da Polícia Criminal (Interpol) e a Rede 24/7, com a troca de evidências armazenadas por meio

de sistemas informáticos, que só serão repassadas caso estejam de acordo com o pedido da Parte requerente e respeitando o interesse essencial da Parte requerida.

Entre os diversos artigos acertados no evento, também foram definidos os processos formais para a solicitação de assistência, que deve incluir a infração investigada e qual a relação do conteúdo pedido com a transgressão. Os prazos para os casos urgentes podem ser atendidos mais rapidamente pela Parte requerida se os dados relevantes estiverem vulneráveis à perda ou modificação.

Em constante evolução, a área de segurança cibernética é mutável e busca constante evolução para acompanhar desafios emergentes. Além de relatórios e normas estabelecidas em fóruns, existem práticas que auxiliam no combate de cibercrimes como criptografia, padrões de segurança (ISO 27001, NIST), firewalls, antivírus, gestão de acessos e assim por diante.

Conclusão

Neste estudo, mergulhamos nas complexidades da interseção entre Segurança Internacional e Ciberterrorismo, explorando uma evolução histórica e contemporânea que redefine o panorama global. O ciberterrorismo, emergindo como um desafio formidável, desafia as bases convencionais de segurança estatal em um mundo onde as fronteiras físicas cedem terreno às digitais.

A compreensão da interconexão entre segurança nacional e o ambiente digital é crucial, especialmente quando bits e bytes se transformam em ferramentas de potencial desestabilizador. A ausência de uma definição consensual para o ciberterrorismo cria lacunas teóricas e práticas, enquanto a militarização do ciberespaço por Estados destaca a urgência de uma abordagem integrada, reconhecendo a complexidade dessa nova arena de conflito.

A securitização do ciberespaço, catalisada por eventos como o 11 de setembro, tornou-se central na agenda governamental. A governança da Internet, permeada por desafios de segurança cibernética, transcende os domínios técnicos,

influenciando diversas esferas sociais e a política global. Nesse contexto, propostas e soluções estratégicas, como o Global Cybersecurity Index, refletem o reconhecimento da importância da cooperação internacional e investimentos para fortalecer a resiliência dos países.

Normas internacionais, como a Convenção de Budapeste, estabeleceram diretrizes para enfrentar ameaças à cibersegurança, promovendo a cooperação entre países. No entanto, desafios persistem, e a busca por soluções eficazes demanda uma abordagem multifacetada. Em um mundo onde as fronteiras digitais desafiam as físicas, a segurança internacional entra em uma nova era, exigindo uma visão holística que considere não apenas as dimensões técnicas, mas também os aspectos políticos, econômicos e sociais.

A crítica reside na necessidade de adaptação contínua e inovação diante das rápidas mudanças no cenário digital. A resiliência dos Estados frente ao ciberterrorismo não será alcançada apenas por meio de estratégias técnicas, mas também pela compreensão profunda das implicações políticas e sociais dessa realidade emergente. O futuro da Segurança Internacional dependerá da capacidade de navegar por esse novo terreno com sabedoria e flexibilidade, construindo respostas eficazes para proteger sociedades cada vez mais interligadas e dependentes da tecnologia.

Referências

CASTELLS, Manuel. **Information Technology, Globalization and Social Development**. Geneva: United Nations Research Institute For Social Development, 1999. Disponível em: https://cdn.unrisd.org/assets/library/papers/pdf-files/dp114.pdf. Acesso em: 10 out. 2023.

CASTELLS, Manuel. **A sociedade em rede**. [S. I.]: Paz e Terra, 2002. Disponível em: https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 17 out. 2023.

CEPIK, Marco *et al*. **Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI**: a securitização do ciberespaço e o terrorismo: uma abordagem crítica. Brasília: Ipea, 2014. Disponível em:

https://repositorio.ipea.gov.br/bitstream/11058/3007/1/Livro-Do_11_de_setembro_de_2001_%C3%A0_guerra_ao%20terror-reflex%C3%B5es_sobre_o_terrorismo_no_s%C3%A9culo_XXI. Acesso em: 20 out. 2023.

CRENSHAW, Martha. **The Causes of Terrorism**. New York: Comparative Politics, 1981. Disponível em: https://www.jstor.org/stable/pdf/421717.pdf?refreqid=fastly-default%3Acca827202e51f4c843c327d7b2b68b9a&ab_segments=&origin=&initiator=&acceptTC=1. Acesso em: 05 nov. 2023.

EUROPE, Council Of. **Convenção sobre o cibercime**. 2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 23 nov. 2023.

FONSECA, Leila Oliveira da. **A cibersegurança sob o prisma das Relações Internacionais**. Disponível em: https://relacoesexteriores.com.br/ciberseguranca-relacoes-internacionais/. Acesso em: 22 nov. 2023.

KUEHL, Daniel T.. **From Cyberspace to Cyberpower: Defining the Problem**. [S. L.]: National Defense University Press, 2009. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210. Acesso em: 10 nov. 2023.

Lumi Kamimura Murata, D. A. M., & Ritzmann Torres, M. P. (2023). **A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?**. Boletim IBCCRIM, 31(368). Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 22 nov. 2023

NYE, Joseph. **Cyber Power**. Cambridge: Harvard Kennedy School, 2010. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. Acesso em: 28 out. 2023.

NYE, Joseph S. **Cyber War and Peace**. 2012. Disponível em: https://www.belfercenter.org/publication/cyber-war-and-peace. Acesso em: 28 out. 2023.

REPORTAL, Data. **DIGITAL 2023: GLOBAL OVERVIEW REPORT**. 2023. Disponível em: https://datareportal.com/reports/digital-2023-global-overview-report. Acesso em: 23 nov. 2023.