26° EDIÇÃO

MINIONU

GUIA DE ESTUDOS

CSNU (2025)

REGULAMENTO DE SEGURANÇA INTERNACIONAL FRENTE AO CIBERTERRORISMO

DIRETOR
FELIPE CAMILO

DIRETORES ASSISTENTES
FERNANDA COSTA
LUCCA ROCHA

11 A 14 DE OUTUBRO DE 2025

Sumário

1. APRESENTAÇÃO DA EQUIPE

1.1 Felipe Camilo Costa – Diretor

Caros delegados, é um imenso prazer poder recebê-los em nosso comitê. Eu sou Felipe, tenho 20 anos, estou no sexto período do curso de Relações Internacionais, e serei seu diretor nesta edição do Conselho de Segurança das Nações Unidas. Desde quase sempre, a tecnologia foi um interesse particular meu, principalmente devido ao fato de que, assim como vocês, vivi minha vida inteira em um contato muito próximo com ela. Ao ter a ideia para esse comitê, fui muito motivado por todas as situações inusitadas que pude ver ao longo dos anos do uso de ferramentas tão maravilhosas, como a internet, para cometer atos perigosos, e foi com isso em mente que decidi abordar a questão "se as redes fossem utilizadas como um dos principais instrumentos para grupos maliciosos cometerem atos ilícitos, quais seriam as melhores maneiras de resolver isso?". Com isso em mente, fico animado para ver suas discussões e perspectivas para solucionar essa questão tão atual.

Para além disso, falando um pouco mais de mim mesmo, além desse interesse pela tecnologia, me interesso também por jogos, livros, quadrinhos, filmes e desenhos. Inclusive, creio que seja difícil não pensar em filmes de ficção científica ao tocar nesse tema, sendo essa uma ótima forma de se imergir nele antes das simulações. Em particular, recomendo um filme muito querido meu chamado *Digimon Adventure: Bokura no War Game (Nosso jogo de guerra)*. Apesar de ser muito fantasioso, o filme acaba por passar por temas adjacentes ao de discussão do comitê, e pode ser interessante para vocês. No mais, fico muito feliz de contar com sua presença nessa simulação, que tenho plena certeza que será ótima. Vejo vocês lá!

1.2 Fernanda Costa – Diretora Assistente

Meu nome é Fernanda Costa e estou muito honrada em retornar a este evento que tanto admiro, agora como Diretora Assistente. Me apresentando um pouco, além de estudante de Relações Internacionais na PUC Minas, sou bailarina e professora de dança e por meio do meu trabalho, tenho contato com pessoas de diferentes partes do mundo, o que despertou em mim um grande interesse por temas globais. Me levando ao desejo em iniciar o curso de Relações Internacionais em 2024. Este é meu segundo MINIONU e estou muito feliz em retornar para esse ambiente inspirador. No ano passado, tive a incrível experiência de fazer parte como voluntária no comitê da ASEAN que discutiu o tráfico internacional de drogas na região do Triângulo Dourado.

Voltar este ano como diretora assistente me faz sentir ainda mais inspirada e preparada para contribuir para o sucesso do CSNU. Fico especialmente animada, pois sempre tive muito interesse por tecnologia e, com o nosso tema tão urgente e desafiador como o ciberterrorismo, acredito que ao longo dos dias de debates conseguiremos trabalhar

em conjunto para buscar uma solução para as problemáticas desse tema. Estou ansiosa para conhecer vocês e animada em colaborar para este comitê. Que possamos, juntos, fazer desta edição do MINIONU um momento único. Nos vemos em outubro, e sejam todos muito bem-vindos!

1.3 Lucca Mares – Diretor Assistente

Olá caros delegados, é um prazer enorme tê-los em nosso comitê. Em primeiro lugar, me chamo Lucca Mares Rocha, tenho 20 anos, estou no quarto período do curso de Relações Internacionais na PUC Minas e esta é minha segunda participação no MINIONU.

Participei na edição passada como voluntário no comitê da Cúpula De Chagos, que tratou da questão da tutela em Chagos e a autodeterminação de povos não representados, e estou extremamente animado para voltar novamente este ano, agora como diretor assistente. Escolhi o curso de Relações Internacionais pois sempre tive afinidade com as matérias da parte de humanas e linguagens, principalmente as de história e geografia, que me fizeram abrir os olhos para o internacional. Além disso, desde pequeno tinha a vontade de atuar profissionalmente em alguma organização internacional, como por exemplo a Médicos sem Fronteiras, ou até o próprio CSNU.

Volto ao MINIONU neste ano como diretor assistente do Conselho de Segurança das Nações Unidas, com muito ânimo e grande satisfação por fazer parte de um excelente comitê, que abordará um tema de extrema relevância no cenário mundial atual. Escolhi participar deste comitê por sempre ter tido curiosidade e interesse pelos temas relacionados à tecnologia e segurança. Tenho plena convicção de que os debates serão fundamentais para a compreensão e enfrentamento das problemáticas do ciberterrorismo na atualidade. Estou muito feliz com a participação de todos na simulação e nos vemos em outubro. Até lá!

2. APRESENTAÇÃO DO TEMA

O CSNU este ano lidará com a questão do ciberterrorismo e suas implicações nas questões de segurança internacionais. Para isso é necessário entender o que de fato é o terrorismo e como sua dinâmica se altera dentro da ideia de segurança digital.

2.1 O que é terrorismo?

Definir o que é o terrorismo é uma tarefa bastante complexa. Na percepção popular, diversos tipos de atos violentos acabam por serem agrupados pela mídia dentro da ideia guarda-chuva de terrorismo, mesmo que o contexto ao redor destes tenham pouco ou nada haver entre si. Tentar encontrar a resposta para essa questão em dicionários também não gera as respostas mais satisfatórias, já que em muitos deles a definição de terrorismo é antiquada ou então incompleta. Mas por que há tanta dificuldade em responder o que é o terrorismo?

Bruce Hoffman em seu livro *"Inside Terrorism"* comenta que tal dificuldade se encontra em dois pontos acerca do termo terrorismo: A mudança no significado e uso deste ao longo dos anos e a assimetria entre as situações em que o termo foi utilizado para descrever determinadas ações e grupos em contextos distintos. Devido a essa falta de uniformidade no uso do termo, torna-se complicado apontar com precisão o que é o terrorismo e como ele se diferencia de outras formas de violência, todavia Hoffman neste mesmo livro apresenta uma definição para o termo que nos ajuda a compreendê-lo melhor.

Hoffman afirma que o terrorismo é inerentemente político - ou seja, por trás de um ato terrorista há uma razão política – violento, seja de forma prática ou por ameaças, de forma que cause impacto psicológico em seus alvos, conduzido por um grupo – seja esse mais formalizado em uma hierarquia ou organizado em células autônomas – ou indivíduos inspirados pelas ideologias de outros grupos terroristas e de caráter subnacional, ou seja, conduzido por organizações não estatais (HOFFMAN, 2006).

Com essa definição em mente, torna-se evidente o quão amplo é o conceito de terrorismo, e como ele acaba por, inevitavelmente, ser dotado de uma série de nuances complexas. De fato, as ações de um grupo terrorista são dotadas de violência com o propósito de gerar ou reforçar o medo de um determinado alvo (sendo este grupos, governos, indivíduos, sociedades, etc.). Todavia, tais ações existem com o propósito de gerar a mudança no sistema político, viabilizando a conquista ou aumento de poder político de um determinado grupo. Isso entra em uma ideia de que se um grupo pode ser visto como terrorista de um determinado ponto de vista, de outro ele pode ser entendido como um grupo revolucionário que luta por uma determinada causa.

Porém, por volta da década de 1990, com o fortalecimento da globalização, um novo tipo de terrorismo, de caráter transnacional[1] (SEIXAS, 2008), surge e rapidamente ganha relevância a nível internacional, em especial com o atentado de 11 de setembro. Como Seixas (2008) apresenta, esse novo tipo de terrorismo transformou radicalmente a maneira como as pessoas entendem e percebem o fenômeno do terrorismo, que passa a ser fortemente associado ao fundamentalismo religioso.

Todavia, como Seixas pontua no mesmo artigo, o fundamentalismo religioso não é um componente intrínseco do que ele categoriza como Terrorismo Transnacional. Esse terrorismo pode provir de qualquer grupo ideológico, religioso ou nenhum desses. Mas, ainda que a motivação basal seja distinta entre eles, todos possuem objetivos similares na sua resposta ao atual sistema capitalista neoliberal de caráter globalista, e as rupturas e desigualdades que acaba por promover. Dessa forma, o terrorismo "contemporâneo" se distingue da sua concepção clássica na ideia de que ao invés de opor-se unicamente a um Estado de terror específico, sendo um movimento de caráter muitas vezes interno, ele se opõe a um sistema organizacional internacional e a forma como este é imposto e mantido por vezes através do terror e da violência, unindo pessoas de diferentes países sob uma mesma bandeira ideológica (SEIXAS, 2008).

Assim, de certa forma, o terrorismo transnacional não apenas é um movimento de cunho intrinsecamente internacional, mas também possui formas particularmente distintas de se organizar, operar e expandir atualmente (SEIXAS, 2008), em especial com a propagação e evolução da internet e do ciberespaço como um todo, permitindo o surgimento do chamado "ciberterrorismo".

Imagem 1 – Membros do IRA em comemoração em Londonderry

Fonte: (CARSON, Niall, 2010)

[1] Transnacional, aqui, faz referência ao fato de que tais grupos terroristas atuam em diversos países simultaneamente, ao invés de atuarem em um único país. Taís países de atuação do grupo terrorista podem ou não serem partes de uma mesma região.

2.2 A criação e desenvolvimento do ciberespaço

Antes de aprofundar a questão de “o que é o ciberterrorismo?” é necessário entender com maior profundidade o meio pelo qual esse tipo de atividade ocorre. Apesar da internet como conhecemos ser um fenômeno bem recente, surgindo por volta da segunda metade da década de noventa e início dos anos 2000, a ideia de uma rede difundida de computadores conectados e capazes de trocarem informações entre si foi conceituada pela primeira vez em 1962 por J.C.R Licklider, pesquisador do Instituto de Tecnologia de Massachusetts (MIT) (Leiner et al., 1997).

Após sua primeira concepção, em 1965, um computador na Califórnia foi ligado a outro em Massachusetts através de uma linha telefônica, ainda que suas capacidades fossem particularmente limitadas quando comparado a redes modernas. Durante esse período, o desenvolvimento deste tipo de tecnologia era ainda muito coligado ao contexto da Guerra Fria, com a aplicação de uma rede de computadores sendo primariamente voltada para questões de segurança, levando à criação da ARPANET (U.S Advanced Research Projects Agency Network). Logo, esse tipo de tecnologia ainda era exclusivo a grupos de pesquisa e militares. Foi somente em 1970 que a primeira rede de computadores com acesso público foi lançada (ABREU, 2009).

Na década 1970, o conceito de “arquitetura de rede aberta” foi cunhado. Antes dessa tecnologia, redes de dados só eram capazes de comunicar-se com computadores que possuíssem a mesma arquitetura de hardware. Nessa nova abordagem, As redes são construídas de forma com que possam se comunicar com qualquer computador independente da arquitetura específica dele, permitindo que provedores de rede escolham livremente qual tecnologia desejam usar sem perder conectividade com outros computadores que usem arquiteturas distintas. (Leiner et al., 1997).

Sob este preceito, Robert Kahn, responsável por introduzir a ideia de arquitetura aberta, estabelece quatro regras centrais para este tipo de arquitetura:

a) Cada rede deve ser autossuficiente;
b) A comunicação deve ser feita pela lógica do menor esforço, ou seja, dados que se encontram numa linha desfuncional devem ser retransmitidos para uma outra[2];

[2] Ao utilizar um computador conectado à rede, quando as informações enviadas por este se encontram em uma linha de rede congestionada, defeituosa, lenta ou que apresente qualquer outro problema para a transmissão de dados, essas informações são redirecionadas para linhas funcionais, em ordem de preservar a velocidade de transmissão.

c) As redes seriam conectadas através de roteadores[3] e gateaways,[4] sem reter as informações neles, reduzindo complicações;
d) Não haveria controle global a nível operacional.
(Leiner et al., p.2, 1997).

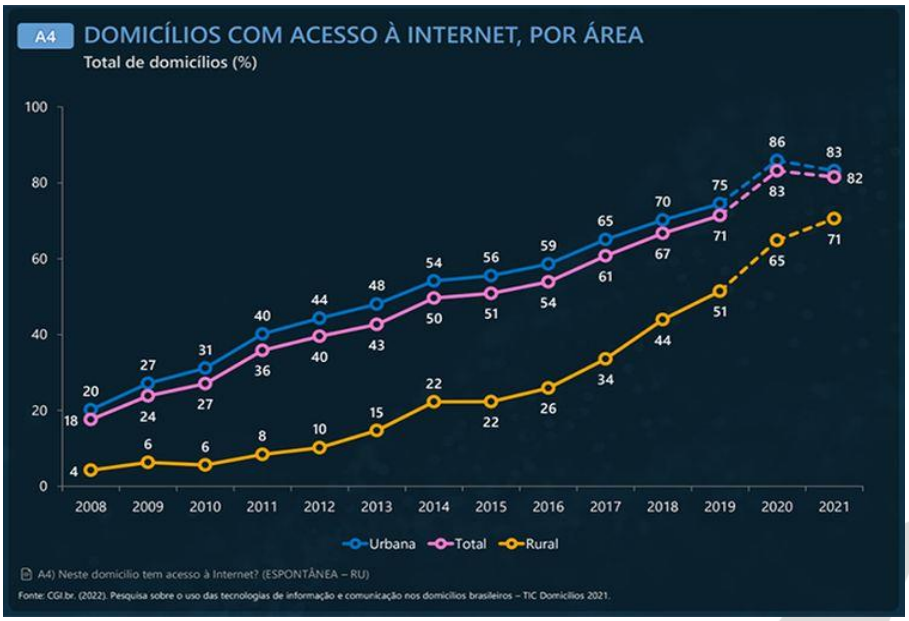
Com o advento dos anos 1980, as fundações do que viria a ser a internet foram lançadas - com o surgimento da correspondência eletrônica, o lançamento dos primeiros computadores pessoais, etc.- e foi também o início de uma separação mais expressiva entre a rede de militar e a rede civil - já que se num primeiro momento a maior parte dos usos das redes era dedicada a fins militares, nesta época novas funcionalidades e conexões de rede surgem que se afastam deste propósito primário, abrindo ainda mais as redes ao uso do público comum. Isso levou a um grande interesse por parte de empresas privadas para o uso deste novo espaço, já que representava uma nova fonte de lucro em potencial. Isso levou ao começo da provisão de serviços digitais, inicialmente serviços de comércio online (ABREU, 2009).

Nesta época, o pesquisador chamado Tim Berners-Lee criou em 1989 o conceito de "World-Wide Web", Rede Mundial, em que qualquer computador no mundo poderia se comunicar entre si desde que tivessem acesso à internet. O resultado deste fenômeno foi o começo da popularização do uso das redes por outras comunidades para além de desenvolvedores e órgãos de defesa. Com o desenvolvimento de redes locais (LANs) e computadores pessoais (PCs), começou a surgir o que hoje denominamos como internet (ABREU, 2009).

Por volta da década de 1990, redes de conexão pertencentes a entes privados começaram a tornar-se mais comuns, e por consequência houve uma expansão gradual da internet para outras regiões do mundo, incluindo o Brasil. Essa expansão tornou-se ainda mais consolidada ao longo do século XXI, como indica o seguinte gráfico da expansão da internet no cenário brasileiro, concebido pela Agência Brasil:

[3] Roteadores são dispositivos que funcionam como centros de transmissão de dados. Eles recebem os dados enviados por computadores, leem estes dados, e então os direcionam para as redes apropriadas.
[4] Gateways funcionam como tradutores entre redes. Isso significa que, graças aos gateways, linhas e redes que operam com tecnologias ou protocolos distintos conseguem comunicar-se entre si, permitindo uma maior conectividade entre computadores e máquinas ligadas à rede no geral.

Imagem 2 – Gráfico de domicílios com acesso a internet no Brasil.



Fonte: (AGÊNCIA BRASIL, 2021)

A partir de então, o mundo tornou-se gradativamente mais conectado, e com a evolução tecnológica a conexão de rede tornou-se mais rápida, ampla e potente. Atualmente qualquer pessoa com acesso à internet possui não apenas a capacidade de se comunicar com qualquer pessoa do mundo inteiro em segundos, mas também um acesso muito facilitado a uma gama diversificada de conteúdo e informação. (ABREU, 2009).

Entretanto, apesar dos benefícios proporcionados pelo mundo online, ele também trouxe uma nova perspectiva quanto a questões de segurança. Se antes agentes maliciosos eram limitados a meios físicos e ao espaço físico para realizar suas práticas, atualmente tais restrições já possuem bem menos relevância. Isso pois, graças à conectividade e à facilidade de atuação que as redes promovem, um agente mal-intencionado é capaz de cometer práticas maliciosas de qualquer lugar contra qualquer pessoa que esteja no ambiente digital.

Não suficiente, devido à forma como as redes foram construídas, a capacidade de identificar e localizar tais atores não é tão fácil quanto parece, já que qualquer usuário é capaz de ocultar ou falsificar seus dados com facilidade, assim como mascarar sua localização através de tecnologias como VPNs (Virtual Private Network), tecnologia que permite a um computador ligar-se diretamente a um servidor remoto privado, criando um “túnel” que encripta certas informações como a localização de um computador. É frente a essa questão que grupos ciberterroristas conseguem se proliferar e agir com extrema facilidade (THE EDITORS OF ENCYCLOPEDIA BRITANNICA, 2025) .

Em sua forma mais extrema, grupos e agentes maliciosos são capazes de atuar em quase completa anonimidade ao utilizar uma parte oculta da internet conhecida popularmente como Dark Web. Essa parte profunda da rede, que só pode ser acessada por programas como o Tor, permite uma anonimidade quase que total para seus usuários e, devido a uma baixa regulamentação quando comparado as camadas mais superficiais da internet, possibilita que estes pratiquem uma variedade de ações criminosas que não seriam possíveis em ambientes comuns (SAYYED; PAUL, 2025).

Essa anonimidade é inclusive utilizada por grupos extremistas para organizarem-se, recrutarem novos membros e elaborar suas ações devido a possibilidade de criação de canais de conversa criptografados, e as vezes até temporários, que dificultam o monitoramento por parte das autoridades legais. Além deste trabalho tático e humano, a Dark Web também é utilizada por estes grupos para, através de operações envolvendo criptomoedas, arrecadar financiamento para suas ações (SAYYED; PAUL, 2025, p. 2). Assim, é possível perceber como a realidade digital altera significativamente a dinâmica de segurança antes observada, e nos leva a perguntar, como nos adaptamos a esse novo status-quo?

2.3 Questões de segurança digital

Apesar dos diversos benefícios que a internet tem proporcionado à humanidade desde sua concepção por volta da década de 1969 - como a facilitação para a troca de informações, o armazenamento de dados em escalas muito superiores ao visto antes, a conectividade ampliada entre pessoas e instituições, etc - Essa nova tecnologia também trouxe uma série de novas preocupações, por exemplo: Como tornar o meio digital mais seguro contra ações ciberterroristas?

A resposta para essa pergunta é de cunho complicado, visto que a própria maneira como a cibersegurança era entendida transformou-se ao longo do tempo. Segundo o artigo *“Regulating security on the Internet: control versus trust* “ (Regulando Segurança na Internet: Controle versus Confiança), escrito por Bibi Van Den Berg e Esther Keymolen, ao longo da concepção e anos iniciais de desenvolvimento da internet, questões de cibersegurança eram vistas como de cunho apenas técnico, levando a diversas pesquisas acerca de tópicos dentro da área denominada “segurança de informação”, focada primariamente em três pontos: proteção de confidencialidade de dados, manter a integridade de data segura e garantia da disponibilidade de redes, sistemas e dados. (BERG e KEYMOLEN, 2017)

Contudo, com o passar do tempo, essas questões deixaram de ser vistas como meramente técnicas, e o conceito de cibersegurança passou a considerar o papel da atividade humana nas redes como um aspecto importante para garantir a segurança no ciberespaço. Com isso em mente, governos do mundo todo elaboraram leis e normas que regulam a capacidade de atuação dos usuários das redes. Dessa maneira, a segurança das redes não

apenas passou a ser uma responsabilidade coletiva das empresas responsáveis pelos domínios e servidores, instituições e organizações de segurança, governos e até usuários, como também passou a ser encarada como uma questão de segurança nacional. (BERG e KEYMOLEN, 2017)

Dessa maneira, a maioria dos governos adotou um posicionamento de que “para se aumentar a segurança na internet, é necessário aumentar o controle sobre ela.” (BERG e KEYMOLEN, 2017). A lógica por trás desse posicionamento se encontra no preceito de que ao aumentar o controle sobre as atividades que ocorrem na internet, e por extensão sobre seus usuários, se eliminaria qualquer possibilidade de atos perigosos feitos através da rede. Mas como seria possível aumentar esse controle?

Considerando a dificuldade de se aplicar tais regulamentos de forma direta, surge uma ideia denominada de “Tecno-regulação” ou “código como lei”. Tecno-regulação é o conceito de que, com o propósito de aplicar de maneira mais efetiva as normas de cibersegurança, a melhor solução seria introduzi-las diretamente nos sistemas de rede, de forma a orientar as ações dos usuários – tanto ao estimular que tomem certas ações positivas quanto reprimir e até impossibilitar que ações maliciosas sejam realizadas pelos usuários. Além de desestimular ações criminosas nas redes, a Tecno-regulação também confere uma série de incentivos positivos para que seus usuários mantenham um comportamento normativo em meio às redes. (BERG e KEYMOLEN, 2017)

Assim, ao aplicar a Tecno-regulação a sistemas de redes, não apenas seria possível ampliar o controle e a suposta segurança do ambiente de forma independente dos usuários, como também se apresenta como uma forma que possui pouco ou nenhum custo prático para que governos a executem, por ser uma responsabilidade conferida aos desenvolvedores destes sistemas, e este por sua vez seria mais barato do que o monitoramento constante das atividades deste sistema. Neste cenário, o papel do Estado é de estabelecer normas e regulamentos e garantir que as empresas desenvolvedoras os cumpram. (BERG e KEYMOLEN, 2017)

Apesar dos benefícios que estas medidas podem trazer para a cibersegurança como um todo, conforme a passagem do tempo ficou claro que não é possível dizer que há uma relação direta entre o aumento do controle das redes com o aumento da sua segurança. Isso pois apesar de estas medidas conseguirem comprometer as atividades de hackers, elas logo perdem efetividade já que motivam a busca por novas formas de hacking que são capazes de burlar esses sistemas. O efeito disso acaba por ser uma espécie de “corrida armamentista” digital entre os sistemas de defesa digitais e os indivíduos que almejam superá-lo. A essa forma, para que tal método provasse-se funcional, seria necessário pensar em maneiras de

sistemas criados sob a ótica da Tecno-regulação serem protegidos contra ataques e ransomwares.

Além disso, outro problema encontrado com esta abordagem é que ao aplicar a Tecno-regulação, normalmente os usuários não são informados de que estão submetidos a tais regulamentos, gerando uma questão de falta de transparência (BERG e KEYMOLEN,2017). Outra questão se encontra na conjuntura de que as empresas donas de domínios (sites) e servidores que compõem a internet global contestam a regulamentação imposta por governos, defendendo que isso fere sua autonomia e a de seus usuários.

Um exemplo recente claro deste fenômeno é a série de conflitos com entes governamentais de vários países que Elon Musk, empresário dono da rede social X, antigo Twitter, se envolveu nos últimos anos. A problemática maior envolvida com este tipo de ocorrência é de que ao desconsiderar certas normas e regulamentos de comportamento nas redes, acaba-se por potencialmente gerar um ambiente inseguro[5]. Com isso em mente, é preciso se perguntar, quais outros meios seriam possíveis para gerar cibersegurança capaz de, efetivamente, lidar com estes problemas?

Algumas outras linhas de ação são possíveis para se lidar com atividades ilícitas nas redes, como por exemplo a ideia da *Bright Internet*, apresentada no artigo *"Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach",* (Jae Kyu Lee, Younghoon Chung, Hun Yeong Kwon, Beopyeon Kim; Information Systems Frontiers; 2020). O conceito de *Bright Internet* consiste numa forma de atuação em que a privacidade de usuários comuns da rede seja preservada enquanto permite que esta seja quebrada no caso de usuários maliciosos.

A maneira como isso seria executado se dá, essencialmente, na ação deliberada do usuário de denunciar ações ilícitas observadas ou da qual foram vítimas, de maneira que preserve a sua anonimidade (LEE et al., 2020). Ao se agruparem tais denúncias em um banco de dados maior, seria possível triangular estas informações para conseguir localizar o ponto de origem de tais atividades, e assim atuar com o aparato legal sob tais agentes, rompendo seu anonimato e agindo de forma mais eficiente para a neutralização da atividade criminosa (LEE et al., 2020). Da mesma forma, usuários também poderiam deliberadamente quebrar seu anonimato visando conferir maior confiabilidade a si próprios, preservando assim o direito de escolha dos usuários. (LEE et al., 2020).

Pensando em um contexto específico do ciberterrorismo internacional, ações desse tipo poderiam ser aplicadas tanto a nível micro - nacionalmente em cada país - quanto em nível macro - em que os atores internacionais comunicariam e agiriam de forma a denunciar

[5] Moraes determina bloqueio do X no Brasil após Elon Musk descumprir decisão judicial*, BBC, 30 de agosto de 2024.* Disponível em: https://www.bbc.com/portuguese/articles/c4gz28359d4o

atividades ciberterroristas, triangular a origem destas ações e assim atuar com os devidos meios legais, ou bélicos, dependendo do caso, para neutralizar os pontos focais de grupos ciberterroristas. (LEE et al., 2020).

Entretanto, essa linha de ação possui também levanta questionamentos como: depender da ação voluntária dos atores seria eficiente? E como lidar com pistas falsas que corrompam as informações disponíveis no banco de dados? Além disso, seria necessário discutir se a construção e investigação deste banco de dados seria feito de forma coletiva entre os países e empresas como um todo ou conduzida por um órgão internacional separado formado por atores específicos.

Ambas as abordagens supracitadas são, em grande parte, construídas com base na realidade e funcionamento das redes no cenário ocidental, em que boa parte do ambiente digital é construído por empresas privadas, tanto no aspecto software quanto no hardware físico que sustenta o ciberespaço. Entretanto, observando outros exemplos que fogem a essa lógica, temos realidades em que Estados controlam as atividades do ambiente digital através de políticas e do domínio da infraestrutura de telecomunicações.

Um exemplo disso se dá na China, em que a maior parte das linhas de rede são propriedade do Estado, por meio da China TELECOM, e muitos dos domínios são criados também por este, enquanto apenas algumas das linhas são alugadas por entes privados. Neste tipo de cenário, o Estado possui uma capacidade ainda maior de controle acerca das atividades e dos usos da rede, já que pode monitorar o espaço online de maneira direta, assim como ditar a maneira como os sistemas são construídos e apresentados aos seus usuários. (China Telecom, [s.d.]) Um exemplo ainda dentro da lógica chinesa é o “Grande Firewall” que é um sistema regulatório da internet aplicado pelo governo que separa o ciberespaço chinês do resto do mundo. (GISONNA; NICHOLAS, 2025)

Esse tipo de prática de fato gera um debate intenso quanto a autonomia e privacidade dos usuários, todavia poderia tornar o ambiente digital mais seguro para instituições e grupos associados aos governos, já que os agentes legais e administrativos seriam menos dependentes de entes privados ou da colaboração voluntária dos usuários para identificar, localizar e punir atividades ilícitas. Outra possível vantagem de uma rede “nacionalizada” é a possibilidade de, ao não depender de provedores de serviços internacionais, poderem criar um ciberespaço desconectado do resto do mundo, indo de encontro ao movimento globalizante que ocorre desde os primórdios da internet como conhecemos.

Atualmente, esta ainda não é a realidade da maior parte dos países do mundo, mesmo daqueles que de fato possuem uma rede altamente nacionalizada. Contudo, frente a um cenário em que movimentos anti-globalistas vêm ganhando força em diversas partes do mundo. Entretanto, esta solução pode levar a uma perda geral da privacidade e liberdade dos

usuários destas redes nacionalizadas, o que pode resultar em um ambiente digital autoritário com repercussões que vão além do ambiente cibernético.

2.4 O que é ciberterrorismo?

Quando se pensa em terrorismo e atentados terroristas, a imagem que é invocada no imaginário popular é de ações marcadas pela violência armada. Por mais que esta ainda seja a maneira mais "convencional" pela qual grupos terroristas podem infligir o terror, ela definitivamente não é a única, principalmente devido à "digitalização" do mundo.

Com o surgimento, propagação e evolução da internet e de outras tecnologias digitais como smartphones, sistemas operacionais, computadores, etc. Muitos dos processos usuais do dia a dia deixaram de ser praticados de forma analógica (com registros em papel, sistemas físicos etc.) para darem lugar a opções virtuais, com isso ocorrendo nos mais diversos setores, desde transações bancárias até comunicação.

Este último por sua vez é de extrema relevância, como é apontado no artigo "O uso do ciberespaço para infringir o terror" de Claudio Augusto Payá Santos e Juan José Delgado Moran. Para os autores, o uso da internet permite um novo patamar de transnacionalidade de grupos terroristas jamais antes visto, pois se antigamente havia diversas restrições para o transitar internacional de informação, com as redes essas se tornam praticamente inexistentes, permitindo a propagação e comunicação em escala global de quaisquer grupos terroristas, reforçado pela possibilidade de anonimato e ocultação destes nos meios digitais.

Para além disto, neste mesmo artigo os autores apresentam a visão de Gabriel Weiman (2004) que identifica os seguintes usos possíveis do ciberespaço de cunho terrorista:

a) Guerra psicológica; ao espalhar imagens que gerem terror a população, como cenas de tortura, execuções, etc.
b) Propaganda e radicalização; já que devido à alta conectividade das redes e a capacidade de manipulação da informação, grupos ciberterroristas são capazes de não apenas espalhar sua ideologia, mas também expor suas glórias e feitos enquanto ocultam suas falhas.
c) Instrumento de financiamento; desde antes da internet grupos terroristas eram financiados por capital privado de pessoas e organizações interessadas, ou cooptadas, por sua causa. Com o advento da internet, essa prática torna-se ainda mais facilitada, pela conveniência e maior possibilidade de anonimidade, trazido pelas transações monetárias feita no meio digital. Outro possível facilitador desse tipo de prática são as criptomoedas, como o Bitcoin, um tipo de token monetário que não é administrado por entes governamentais, tornando possível transações de grandes quantias que sejam mais difíceis de serem rastreadas.
d) Instrumento de recrutamento e mobilização; como dito anteriormente, a presença online de grupos ciberterroristas facilita em muito a propagação de ideias radicais. Ao radicalizar usuários das redes, estes grupos conseguem com maior facilidade recrutar novos membros a sua causa, e ainda mobilizá-los em escala internacional para a condução de suas atividades de nível macro. Nessa lógica, membros recrutados não precisam necessariamente apoiar a causa tomando ação direta nas

atividades ilícitas do grupo, mas podem também ajudar de formas menos diretas, como fonte de inteligência – angariando e distribuindo informações, aproveitando-se da discrição para espionar alvos, colaborando no acesso a dados sensíveis, etc. - por exemplo.

e) Instrumento de rede e ocultação de estruturas; antes da internet a composição hierárquica de grupos terroristas era fortemente verticalizada, ou seja, construída em volta de um grupo específico e indo de cima para baixo, sendo necessária sua extrema ocultação para que a lógica operacional destes grupos não fosse comprometida. Contudo, no mundo conectado de hoje, pode se observar uma horizontalização da hierarquia, com ela agora sendo difundida entre diversos grupos e indivíduos, de maneira que mesmo que uma célula seja comprometida, as demais conseguem seguir suas operações e manterem-se no anonimato, este que por sua vez é reforçado pelas diversas características inatas do meio digital.
f) Pano de fundo documental; através de meios como a deep web, grupos ciberterroristas possuem acesso a uma multitude de fontes de informação que os permitam melhorar e ampliar suas capacidades de atuação. Confecção de explosivos, táticas de guerrilha, conhecimento de armas, estratégias particulares do grupo, entre outros conhecimentos são facilmente repassados através das redes.

(SANTOS e MORAN, 2016).

Mas, para além destes usos supracitados, uma outra capacidade do chamado ciberterrorismo é a do roubo de informações e adulteração de sistemas cruciais por meio da prática conhecida como *hacking* e o uso dos chamados *ransomwares,* aplicações maliciosas capazes de bloquear um dispositivo ou criptografar as informações contidas nele. Ambas as práticas podem ser altamente nocivas tanto para os membros de um governo quanto para o funcionamento do próprio governo, servindo como forma de atentar contra ele sem necessariamente apelar para ação armada. Tal caso é de tamanha seriedade que foi discutido recentemente o Conselho de Segurança das Nações Unidas, onde debateram-se especificamente as ameaças representadas por ataques cibernéticos a hospitais e outras instalações e serviços de saúde (SANTOS, 2024).

Atualmente, o ciberterrorismo – apesar de ser um fenômeno recente – já se encontra presente em discursos e discussões entre os países quando se pensa em suas relações internacionais. Um exemplo disso é como em tempos recentes infrações de sistemas de dados dos Estados Unidos são frequentemente associados a grupos ciberterroristas chineses, ainda que não necessariamente haja evidências concretas quanto a isso. Isso traz também uma pergunta: Caso uma determinada região possua uma concentração maior de grupos ciberterroristas, como medidas de segurança devem ser tomadas sem que haja uma estigmatização e possível quebra da soberania dos países desta região em prol da segurança internacional?

Com tais fatores em mente, questões de segurança quanto a problemática do ciberterrorismo encontram duas questões principais: Devido ao fato de o ambiente digital ser formado majoritariamente por espaços pertencentes à grandes empresas de tecnologia, qual

seria o papel delas nas atividades necessárias para limitar e impedir as ações de grupos ciberterroristas nestes espaços? E, considerando que grupos ciberterroristas não necessariamente são compostos por pessoas que habitem um mesmo Estado, qual órgão legal seria responsável por julgar e penalizar os indivíduos envolvidos nestas atividades – ou seja, essa responsabilidade pertence a corte de justiça do Estado de origem do indivíduo ou de tribunais internacionais?

3. APRESENTAÇÃO DO COMITÊ

O Conselho de Segurança das Nações Unidas (CSNU) é o órgão da Organização das Nações Unidas (ONU) responsável por lidar com questões diversas relacionadas à segurança internacional. Fundado em 1945, conjuntamente com a própria ONU, o CSNU possui quinze membros, com cinco deles (Estados Unidos da América, Rússia, China, Reino Unido e França) possuindo assento permanente no comitê e poder de vetar as resoluções do CSNU, enquanto os demais são eleitos para desempenhar mandatos de dois anos. Diferentemente da maioria dos órgãos que compõem a ONU, o CSNU possui caráter mandatório, ou seja, ele possui a capacidade de impor suas resoluções para os demais países que assinaram a carta da ONU, podendo impor sanções e até mesmo ações militares para a resolução de problemas.

Apesar do caráter mandatório, o ambiente de debate do CSNU ainda prioriza a colaboração entre seus membros visando a resolução de problemas que, individualmente, seus membros não seriam capazes de resolver de forma eficiente, justa e evitando o conflito dentro do possível. Assim sendo, o comitê possui moderação tradicional e conta com a presença de 22 delegações, 15 votantes – sendo 5 delas permanentes e com poder de veto- e 7 membros observadores, operadas em duplas de delegados, totalizando 44 delegados.

4. PRINCIPAIS POSICIONAMENTOS

4.1 Países pró-Bright Internet

Estes são os países que, confrontados com a problemática de uma ameaça “invisível” e difícil de ser localizada, entendem que a melhor forma de lidar com a ameaça do ciberterrorismo é estabelecendo uma rede colaborativa entre entidades Estatais e não estatais a nível global com o objetivo de formar um banco de dados dessas atividades visando triangular as atuações e origens de grupos terroristas. O propósito desta medida seria de construir um banco de dados de atividades digitais ilegais para, com base nas informações providas, triangular a localização e entidade dos usuários que praticaram tais atividades.

Dentro da lógica da *Bright Internet*, duas aplicações são possíveis: a nível micro, no âmbito interno de cada país, e a nível macro, realizado por atores internacionais. Ainda dentro

desta linha de ação, há duas abordagens distintas: uma centralizada, com o monitoramento do banco de dados e as ações feitas em cima destes conduzidas por um grupo seleto de atores, em específico aqueles que possuíam maior conhecimento técnico e capacidade bélica para realizar operações de neutralização. Outra vertente é uma mais universalizada, em que cada ator Estatal aplicaria a lógica da *Bright Internet* a nível nacional, conduzindo suas operações com base no seu próprio aparato legal e de acordo com suas legislações e capacidades, com a cooperação internacional sendo focada na identificação de pontos de origem do ciberterrorismo.

4.2 Países pró Tecno-regulação

Estes são os países que entendem que para de se ampliar a cibersegurança atual das redes e possuir uma forma de lidar eficientemente com o ciberterrorismo, seria ampliando o controle governamental sobre as redes através de medidas regulatórias que estabeleçam limites rígidos para a capacidade de atuação de usuários, construindo o ciberespaço de forma a condicionar o comportamento destes através de uma série de incentivos e reprimendas.

Nesta linha, o foco seria na criação de uma série de diretrizes universais que seriam aplicadas sobre os responsáveis pela criação e moderação do espaço digital, para enfatizar a aplicação de regulações construídas dentro do sistema bruto das redes, que padronizaram a conduta de governos para com a cibersegurança. Da mesma forma, haveria um foco no desenvolvimento dos meios de segurança interna dos sistemas digitais, visando limitar e impedir que agentes maliciosos consigam burlar suas regras para realizar atividades ciberterroristas. Assim sendo, essa abordagem se constroi em cima da ideia de prevenir a ação ciberterrorista ao invés da identificação e neutralização direta de grupos maliciosos.

4.3 Países pró-isolamento

Este posicionamento é referente aos países que, com o propósito garantir sua segurança nacional, entendem que a melhor abordagem seria a de se remover da rede global, optando por um ecossistema de redes nacionalizado. Ao optar por uma plataforma regional de internet, o governo local possui uma capacidade ampliada de monitoramento de suas atividades e de, consequentemente, lidar com qualquer tipo de atividade suspeita online.

A desvantagem deste tipo de abordagem se encontra em três questões principais: o isolamento do resto da comunidade global, a perda de acesso a serviços e dados contidos na rede global, e a possível perda de liberdade e autonomia por parte dos usuários desta plataforma nacionalizada. Uma outra questão a ser considerada também é a vulnerabilidade a este sistema que tecnologias como VPNs geram, não sendo uma resolução definitiva.

5. PRINCIPAIS QUESTÕES PARA A DISCUSSÃO

A temática do ciberterrorismo já foi discutida por outras instituições do sistema ONU, como o Escritório das Nações Unidas sobre Drogas e Crime (UNODC), e já foi citada ocasionalmente em reuniões do CSNU, como apontado previamente. Todavia, dada a novidade do tópico e recência de suas implicações para o desenvolvimento da internet, a discussão acerca do ciberterrorismo e suas implicações para a segurança internacional ainda é relativamente recente dentro do comitê. Sendo assim, cabe às delegações presentes discutirem a temática a partir das seguintes linhas de reflexão:

- Considerando o caráter descentralizado e anônimo do ciberterrorismo, como aplicar medidas de segurança efetivas para o problema?
- Como abordar as implicações da globalização para a viabilização e agravamento do ciberterrorismo?
- Quais medidas podem ser tomadas para ampliar a segurança das redes públicas e privadas contra os ciberterroristas?
- Considerando a possibilidade de criação de um sistema de segurança cibernética internacional, sobre quais propósitos e ações coletivas ele deve ser construído?
- Qual direcionamento é o mais eficiente para a regulação de atividades terroristas por meios digitais? O enfoque no controle em detrimento da privacidade e liberdade dos usuários das redes ou o foco na construção de um sistema autorregulado que preserve a autonomia dos atores, mas que seja possivelmente menos eficiente?
- Qual o papel e a responsabilidade das principais empresas responsáveis pela construção, manutenção e moderação dos espaços digitais no problema do ciberterrorismo?
- Considerando a possibilidade de a maior parte dos atos ilícitos online se originarem em de determinada(s) região(es), como lidar com o problema sem ferir a integridade e soberania dos atores que compõem esta região?
- Quais medidas legais devem ser aplicadas aos responsáveis pelas ações ciberterroristas? Seu julgamento deve ser realizado por meios legais internacionais ou nacionais? No caso do último, será realizado pela corte do país de origem da atividade ou pelo país vitimado?

6. Lista de delegações

Nome das Delegações	Tipo de Delegação[6]
Agência de Segurança Cibernética e Infraestrutura (CISA)	Membro Observador
República Argelina Democrática e Popular	Membro Oficial
República Federativa do Brasil	Membro Observador
República Popular da China	Membro Oficial (Permanente)
Reino da Dinamarca	Membro Oficial
Escritório das Nações Unidas Contra o Terrorismo (UNOCT)	Membro Observador
República da Eslovênia	Membro Oficial
Estados Unidos da América	Membro Oficial (Permanente)
República Francesa	Membro Oficial (Permanente)
Google	Membro Observador
República Cooperativista da Guiana	Membro Observador
República Helênica	Membro Oficial
Interpol	Membro Observador
Organização Internacional de Normalização (ISO)	Membro Observador
Microsoft	Membro Observador
Massachussets Institute of Technology (MIT)	Membro Observador
República do Panamá	Membro Oficial
República Islâmica do Paquistão	Membro Oficial
Reino Unido da Grã-Bretanha e Irlanda do Norte	Membro Oficial (Permanente)
República da Coréia	Membro Oficial
Federação Russa	Membro Oficial (Permanente)
República da Serra Leoa	Membro Oficial
República Federal da Somália	Membro Oficial

[6] **Membros Observadores** não possuem capacidade de voto em questões substanciais, apenas procedimentais. **Membros Oficiais** votam em ambos os tipos de questões. **Membros Oficiais Permanentes** podem além de votar em ambos os tipos de questões vetar resoluções do comitê

REFERÊNCIAS:

ABREU, Karen Cristina Kraemer**. História e usos da Internet**. Disponível em: https://arquivo.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf. Acesso em: 7 fev. 2025.

CHINA TELECOM**. 中国电信集团有限公司**. Disponível em: http://www.chinatelecom.com.cn/corp/01/index.html. Acesso em: 29 jun. 2025.

GISONNA, Nicholas**. Great Firewall**. 2 abr. 2025. (Nota técnica).

HOFFMAN, B**. *Inside Terrorism***. 2. ed. Nova Iorque, NY, USA: Columbia University Press, 2006.

LEE, J. K**.** et al. Reconciliation of privacy with preventive cybersecurity: The Bright Internet approach. ***Information Systems Frontiers: a journal of research and innovation***, v. 22, n. 1, p. 45–57, 2020.

LEINER, B. M**.** et al. The past and future history of the Internet. ***Communications of the ACM***, v. 40, n. 2, p. 102–108, 1997.

PAYÁ SANTOS, C. A.; DELGADO MORÁN, J. J. El uso del ciberespacio para infringir el terror. ***Estudios en Seguridad y Defensa***, v. 11, n. 22, p. 91–108, 2017.

SANTOS, U. **Conselho de Segurança debate riscos de ataques cibernéticos com ransomware**. Disponível em: https://news.un.org/pt/story/2024/11/1840406. Acesso em: 20 nov. 2025.

SAYYED, Hifajatali; PAUL, Sanu Rani**.** Exploring the role of encryption and the dark web in cyber terrorism: legal challenges and countermeasures in India**. *Cogent Social Sciences***, [S. l.], v. 11, n. 1, p. 1–10, 2025. Disponível em: https://doi.org/10.1080/23311886.2025.2479654. Acesso em: 29 jun. 2025.

SEIXAS, E. C**.** “Terrorismos”: uma exploração conceitual. ***Revista de Sociologia e Política***, v. 16, n. suppl, p. 9–26, 2008.

VAN DEN BERG, B.; KEYMOLEN, E. Regulating security on the Internet: control versus trust. ***International Review of Law, Computers & Technology***, v. 31, n. 2, p. 188–205, 2017.

Em 2021, 82% dos domicílios brasileiros tinham acesso à internet. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2022-06/em-2021-82-dos-domicilios-brasileiros-tinham-acesso-internet. Acesso em: 7 fev. 2025.