Pontifícia Universidade Católica do Rio de Janeiro

Instituto de Relações Internacionais

Yuri Ramos Braga Ferreira

Cibercrimes, Cibersegurança e Abismo Tecnológico nas Relações Internacionais: Uma pesquisa exploratória sobre a nova dimensão da existência humana.

Orientador: Márcio Antonio Scalercio

Rio de Janeiro
2023.1

Pontifícia Universidade Católica do Rio de Janeiro

Instituto de Relações Internacionais

Yuri Ramos Braga Ferreira

Cibercrimes, Cibersegurança e Abismo Tecnológico nas Relações Internacionais: Uma pesquisa exploratória sobre a nova dimensão da existência humana.

Orientador: Márcio Antonio Scalercio

Monografia apresentada ao Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (PUC Rio) como requisito parcial para a obtenção do título de Bacharel em Relações Internacionais.

Rio de Janeiro
2023.1

Aos meus avós: Ataide Lomeu Braga, Helenice Ramos Braga, Nalzira Nunes Ferreira e Geraldo de Souza Ferreira

Agradecimentos

Gostaria de agradecer ao meu orientador, Prof. Márcio Antonio Scalercio por ter me aceitado como seu orientando no período de 2022.2 e 2023.1, por acreditar no meu projeto de pesquisa, e sobretudo por ter tido paciência comigo. O professor Scalercio foi extremamente compreensivo em um período muito difícil da minha vida, em que me encontrei impossibilitado de realizar parte da monografia no período de tempo recomendado pelo IRI devido a questões de saúde, mas ainda assim ele não desistiu de mim e do projeto, e foi essencial para que eu pudesse encontrar o ângulo correto para abordar este trabalho, apesar de 2023 também ter sido um período complicado em sua vida. Suas aulas na PUC também moldaram grande parte do que eu sou hoje, e meu entendimento das questões da criminologia e da guerra. Para ele eu fui apenas mais um orientando em um universo enorme, mas para mim ele foi um amigo e mentor.

Gostaria de agradecer também dois professores importantes do departamento de relações internacionais da PUC Rio, Prof. Wrobel e Prof.(a) Renata Summa, que acreditaram em mim o suficiente para assinar minha carta de intercâmbio, e me deram a chance de realizar um sonho de vida: um intercâmbio acadêmico pela PUC Rio. Com a ajuda deles fui capaz de ir a Inglaterra e estudar na Queen Mary University of London, onde desenvolvi mais conhecimentos a respeito dos temas de tecnologia, crimes, saúde e guerra, que foram utilizados nesta monografia. Outra professora que também merece destaque é a Prof.(a) Luciana Badin, que foi responsável por ministrar diferentes aulas sobre tecnolgia da informação e capitalismo de vigilância. O conhecimento que ela me transmitiu foi de extrema importância, tanto no meu intercâmbio, quanto para a realização deste trabalho.

Gostaria de reservar um local especial para agradecer ao nosso Coordenador, Prof. Ricardo Oliveira, por ter sido uma das pessoas mais importantes para que este trabalho pudesse ser realizado. O Prof. Ricardo é possivelmente uma das melhores pessoas que já conheci, e esteve presente durante minha banca avaliadora de intercâmbio, onde tenho certeza de que ele zelou por mim. Além disso ele me ajudou muito durante minha recuperação da cirurgia a que foi submetido no ano de 2022, inclusive doando seu tempo e esforço para que fosse capaz de me ajudar, ou indicar outras pessoas que pudessem fazê-lo, e por me dar perspectiva quando tudo parecia incerto.

Tenho também que agradecer algumas mulheres incríveis que me acompanharam na minha trajetória, nos períodos bons e ruins. Primeiramente às minhas queridas amigas

Ada Victória Martins de Sousa (Terra), Cássia Emily Guimarães (Urano), Larissa Costa (Vênus), Lana Juno (Júpiter), Vulpes Simões (Sol) e Isho Meireles Futuro (Sírius), que sempre estiveram dispostas a ouvir minhas loucuras e serem as melhores companheiras à distância que qualquer pessoa poderia querer durante o terrível período da Pandemia de COVID-19. Também gostaria de agradecer especialmente duas pessoas: minha querida amiga Alessandra Torres, que além de ser uma das melhores pessoas mais brilhantes, honrosas e guerreiras que eu já tive o privilégio de conhecer, foi um grande apoio emocional no período de realização deste trabalho, e inclusive contribuiu com ideias e discussões que me ajudaram a completá-lo nos meses finais de escrita. Por fim a minha querida irmã de outra mãe Brenda Leite (Saturno) que sempre esteve presente na minha vida durante o período da minha faculdade, até a conturbada pandemia, as tentativas frustradas de intercâmbio e até hoje. Espero um dia poder retribuir tudo que elas fizeram por mim.

Por fim eu deixo um espaço para agradecer às duas pessoas mais importantes da minha vida, meus pais: Cássia Rosane Ramos Braga e Gilmar Nunes Ferreira. Meu pai sempre se dedicou muito para que eu tivesse um espaço seguro para estudar e compartilhar minhas ideias, por mais absurdas que fossem, com ele, e até hoje ainda está entretendo meus hobbies estranhos e fascinações supérfluas, foi meu pai que despertou meu amor por história e pelos estudos acadêmicos, e sempre me fez questionar a realidade a minha volta. Já minha mãe é a melhor pessoa que existe na minha vida. Ela sempre foi responsável pela minha educação, por toda a ajuda financeira e emocional, por ter sido a pessoa que me incentivou a nunca me dar por vencido e sempre procurar me superar constantemente, por ter me dado livros, me levado à museus, viagens internacionais e todo tipo de atividade enriquecedora, e esteve presente comigo durante todo meu processo de formação como ser humano. Sem ela, nada disso seria possível.

Resumo

A presente pesquisa propõe apresentar os conceitos de cibercrimes e cibersegurança, e relacioná-los com a questão da administração estatal e do regionalismo, tendo em vista as dificuldades impostas pelo fenômeno do Abismo Tecnológico, partindo das teorias desenvolvidas sobre a criminologia moderna, e os direitos inalienáveis dos seres humanos. O trabalho parte de uma leitura sobre o que é entendido como cibercrime e como suas características se comparam com sua contraparte física, o que define cibersegurança e quais devem ser as medidas tomadas para conseguir promovê-la e, por fim, como o Abismo Tecnológico interfere nas abordagens a esses dois fatores, considerando um passado de exploração colonial e imperialista a que certos países foram submetidos. Portanto, foi desenvolvida neste trabalho uma abordagem que analisa estes fenômenos como estudos de caso dentro de um framework Norte/Sul, para apresentar os aspectos positivos das políticas utilizadas por países que foram bem-sucedidos nos esforços de combate ao cibercrime, mesmo com suas limitações e peculiaridades, com o intuito de discorrer sobre estas questões importantes e apresentá-las de forma concisa para que mais discussões e pesquisas possam ser realizadas à respeito desta temática recente.

Palavras-Chave: Tecnologia, Cibercrime, Cibersegurança, Abismo Tecnológico, Criminologia, Desenvolvimento.

Abstract

This Research aims to present the concepts of cybercrime and cybersecurity, and how they relate to State administration and regionalism, considering the difficulties imposed by the phenomenon of the Technological Abyss (also known as Digital Abyss), utilizing, as a basis, modern criminology theories and the inalienable rights of all human beings. This body of work is built upon an interpretation about what is understood as cybercrime and how its characteristics could be compared to its physical counterpart, what is defined as cybersecurity and what actions should be taken to promote it, and lastly how the Technological Abyss interferes in the approaches to these two factors considering the colonialist and imperialist past that certain countries were subjected to. Therefore, the focus of this research was to analyze these phenomena as case studies inside of a North/South framework, to present positive of the policies used by countries that were successful in their efforts to combat cybercrime, even with their limitation and particularities, with the intention of writing about these important issues and present them in a concise manner, so that more debates and researches could be conducted about this recent topic.

Key Words: Technology, Cybercrime, Cybersecurity, Technological Abyss, Criminology, Development.

SUMÁRIO

INTRODUÇÃO

Nos últimos anos, temos assistido à aceleração dos avanços tecnológicos em matéria digital. Diversas tarefas de rotina são realizadas de forma virtual, tais como comprar comida, adquirir objetos de lazer e realizar seu trabalho. Isto trouxe uma melhora na qualidade de vida das pessoas, já que se pode poupar tempo e esforço utilizando as redes de informação. Entretanto, isso também fez as pessoas ficarem extremamente dependentes dessas redes, por fatores como a facilidade ao acesso a aparelhos celulares para camadas menos abastadas da população e a evolução da tecnologia de conexão à internet da discada para o Wi-Fi.

Nesta nova realidade, devemos nos atentar para os riscos envolvidos em uma alta dependência de instrumentos da tecnologia de informação. Apesar de constituírem um tipo de aparato hoje considerado indispensável para nosso cotidiano, novas dinâmicas surgem quando estamos inseridos dentro de um mundo conectado – sobretudo com relação à exposição de informações e à privacidade. Enquanto algumas pessoas utilizam da rede para marcar encontros, trocar informações rotineiras e realizar pesquisas, a Internet possui capacidade para se tornar uma plataforma de conflitos. Nesse contexto, as figuras do militante virtual e do *Hacker*[1] têm aparecido com mais frequência, ainda mais durante o cenário da Pandemia de COVID 19 (ROLFINI, 2020).

Também temos visto a crescente utilização da rede por grupos criminosos para realizar ou agir como um suporte para ataques, assim como por Estados Nações como os Cyber ataques à Ucrânia efetuados pela Rússia em 2015 e 2016 (BROADHURST et al, 2017). Esses eventos podem consistir em um real ataque cibernético para causar dano agravado em sistemas de informações e infraestrutura digital, realizar *data mining*[2] para financiar armas e munições, ou para recrutar novos membros. Em 2018, o Hamas utilizou a instalação de um Spyware em telefones celulares de soldados israelenses para espioná-los e, assim, organizar ataques. A mesma estratégia já havia sido utilizada em 2017 com o Spyware Viperal. (ITCHANNEL, 2018)

Vale ressaltar que o Ciberterrorismo, um tipo particular de cibercrime, hoje possui um nível de complexidade que acompanhou o desenvolvimento tecnológico mundial desde o início do século XXI. Anna-Maria Taliharm apresenta um caso considerado como uma das primeiras

[1] O termo originalmente foi criado para se referir a programadores inteligentes, mas passou a ser associado com indivíduos capazes de invadir sistemas de segurança, normalmente sistemas de computadores e redes de informação.
[2] A "Mineração de Dados" consiste em um conjunto de ferramentas para analisar grandes conjuntos de dados a procura de padrões consistentes, detectando assim novos subconjuntos de dados.

manifestações do Ciberterrorismo: em 1997, as Guerrilhas étnicas de Tamil utilizaram uma estratégia de *Flood*[3] para atrapalhar as comunicações da Embaixada do Sri Lanka. Desde esse momento, o Ciberterrorismo assumiu diversas formas e foi capaz de evoluir e prosperar no ambiente virtual, tornando-se menos óbvio e mais furtivo e só veio a aumentar, tanto em incidência como em força. Estados como o Sri Lanka conseguiram se adaptar, mas persistem entre os mais vulneráveis a esse tipo de ataque. Só no ano 2000, somente 5% da população mundial usava internet, sendo que mais da metade estava localizada na América do Norte. (FARAH, 2000.)

Enquanto esses tipos de ataques ocorrem dentro do ambiente virtual, não há indícios de que o desenvolvimento de novas tecnologias para aumentar as redes e tornar conexões mais rápidas será desacelerado, como se pode observar na disputa entre EUA e China em torno do novo 5G (QUEIROZ, 2020). Além disso, a nova pandemia do COVID-19 impulsionou um movimento por ainda mais dependência dos meios digitais – que permanecerá por certo tempo. Para Tedros Adhanon, Diretor-Geral da Organização Mundial da Saúde (OMS), "Não haverá retorno ao antigo normal em um futuro próximo." (G1, 2020)

Isto indica que o trabalho remoto, realizado em casa, continuará sendo parte da normalidade, mesmo após a Pandemia. As pessoas precisarão trabalhar e realizar outras funções essenciais pela rede, o que resultará em mais brechas na segurança digital e potencialmente mais ocorrências de cibercrimes. Já se observam os sintomas iniciais. A plataforma ZOOM, por exemplo, está tendo sua capacidade de proteger as informações de seus usuários questionada. A segurança digital será, em pouco tempo, tão importante quanto a segurança física. O Departamento de Educação da Cidade de Nova Iorque pediu em abril de 2020, por meio de nota oficial, para que os professores e alunos deixassem de utilizar a plataforma, no auge da pandemia de Corona Virus. (CARVALHO, 2020)

Considerando que a nova rotina de trabalho e vida das pessoas já apresenta problemas básicos como esse, tendo em vista que os Cibercrimes são muito mais insidiosos quando comparados com crimes tradicionais, os problemas de Cibersegurança podem aumentar em escala considerável. A maioria dos atos criminosos no ambiente digital ocorre em atividades relacionadas a financiamento, incluindo lavagem de dinheiro e transações digitais. De acordo com o documento *Security Outcomes Report Volume 3* (CISCO SECURE, 2022), países como o Canadá são capazes de lidar eficientemente com estes problemas através da criação da Cyber

[3] Trata-se de uma ação geralmente empreendida por vírus ou hackers, na qual um destinatário é "inundado" com um número gigantesco de mensagens para um destinatário de modo a dificultar sua capacidade de resposta ou mesmo leitura de qualquer outra mensagem.

Resiliência, ou seja, a capacidade de antecipar, resistir, se recuperar e se adaptar a condições adversas, estresses, ataques, ou danos que são causados ou são facilitados por recursos cibernéticos. Contudo, não são todos os países que dispõem das vantagens de infraestrutura tecnológica para combater estas formas de ofensas digitais.

Este fenômeno ficou conhecido como "Abismo Tecnológico" ou a diferença grande entre a utilização das redes digitais entre o Hemisfério Norte e o Sul. Ao longo das duas décadas do novo milênio, esforços foram feitos para democratizar o acesso às redes e, com isso, a vulnerabilidade antes apresentada como particular ao Hemisfério Norte está vindo para o Sul, e isso poderá se traduzir em novos desafios de Cibersegurança. Segundo a Covenção de Budapeste do Conselho Europeu, o cibercrime deve ser entendido como:

> *"Offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices.*
>
> *Offences committed by means of computer systems. This list is limited to those "old" forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale."* (SEGER, 2011)

A referida Convenção foi ratificada por 47 membros da União Europeia, bem como EUA, Japão, Canadá e África do Sul – signatários que compartilhavam o objetivo de criar as bases técnicas para que o cibercrime fosse corretamente detectado e julgado. O trecho acima também desconstrói a ideia de que um país com menor acesso a tecnologias digitais estaria mais seguro de ataques. Isso porque, na categoria de cibercrime, antigas formas de crimes passam a ser facilitadas através do uso de sistemas de computadores. Ainda, países que possuem um sistema de informação desatualizado também sofreriam com crimes que poderiam ser prevenidos possuindo um sistema mais refinado e protegido. Sendo assim, países com déficit tecnológico ainda estariam sujeitos a outras formas de ações criminosas, porém de modo diferente em comparação a nações com conexões robustas.

Entretanto, as tecnologias de informática, apesar de terem se tornado mais acessíveis ainda apresentam inúmeras dificuldades para determinados países ou pessoas. Nações mais desenvolvidas podem requerer que parte de sua população possua "senso comum" para se prevenir de possíveis ataques, o que em certos países como os EUA funciona como uma medida preventiva ao cibercrime, mas isto se traduz de forma diferente em nações menos conectadas, onde a tecnologia de informática ainda não é totalmente entendida e assimilada pelos

indivíduos, apesar disso os sistemas de computadores ainda existem nesses países em alguma medida, o que torna possível a realização de atos criminosos.

Isto é um dos efeitos colaterais do abismo tecnológico e da democratização das conexões digitais. À medida que mais países adotam novas tecnologias, novas formas de cibercrime começam a ocorrer em seu território, da mesma forma que países que ainda mantêm suas antigas tecnologias, podem sofrer com outras formas de cibercrime, além do desconhecimento de sua população sobre como as novas tecnologias podem dificultar estratégias de prevenção. Diante desse quadro, a questão que me proponho a discutir na pesquisa é: como o abismo tecnológico que o mundo vivencia afeta os esforços para o combate aos cibercrimes, e a promoção da cibersegurança?

METODOLOGIA

A metodologia usada nesta pesquisa foi a de estudos de caso sobre o assunto específico do cibercrime. É um método que permite uma ampla pesquisa sobre o tema, além de fornecer subsídios para que novas discussões a respeito dos crimes virtuais possam ser iniciadas. Foi realizado um estudo abrangente, assim como uma coleta de informações e dados de sites oficiais de governos, organizações internacionais, sites de organizações não governamentais, e textos escritos por organizações de segurança e também autores que exploram as teorias do cibercrime e da cibersegurança para oferecer uma visão ao mesmo tempo prática e teórica sobre os casos aqui estudados, se concentrando primariamente nas questões da cibersegurança e do abismo tecnológico e sua relação íntima com os cibercrimes. O intuito desta pesquisa não é contradizer ou acrescentar discussões já iniciadas no campo teórico da cibercriminologia, mas sim servir como ponto de referência para que novos trabalhos possam ser realizados. Tendo isto como foco, os estudos de caso foram a forma mais prática de organizar os dados apresentados nestas páginas.

Esta pesquisa terá como seu foco principal a partir da próxima sessão, dissertar sobre informações teóricas que podem ajudar a compreender melhor o que são as medidas preventivas para conter cibercrimes, e como estas medidas se relacionam com a cibersegurança. Nos próximos capítulos deste trabalho, estes dois conceitos serão devidamente explorados, o que é crucial para a análise, já que o cibersegurança será entendida aqui como a principal ferramenta pela qual Estados, organizações, empresas e indivíduos possuem para se defender das ações de

cibercriminosos. Portanto, a cibersegurança está intimamente ligada às dimensões destes atos de agressão.

Além da compreensão entre as duas definições, também é preciso entender a fronteira entre crimes e cibercrimes. Como será visto mais adiante, no mundo material, ou mundo físico, "crime" pode ser definido de várias formas, cada uma com seus motivos, ações e agravantes. Sua contraparte no mundo virtual também possuí características únicas para cada ação criminosa. Um Hacker, um ativista digital, um ladrão de informações, um distribuidor de conteúdo pirateado, ou um ciberbully[4], apesar de poderem cometer ações de cibercrime, não são por si enquadrados na mesma definição de cibercriminoso, da mesma forma que um ladrão e um assassino não podem ser considerados iguais em relação à gravidade de seus crimes. Ou seja, cuidados devem ser tomados para não utilizar esta definição como um rótulo para qualquer tipo de ação criminosa facilitada pelos sistemas de computador.

Após isso serão apresentadas políticas de prevenção ao cibercrime que foram utilizadas por nações detentoras de tecnologia de informação de ponta, e que foram consideradas eficientes na contenção e prevenção de ataques ou de ações voltadas para atos terroristas que ocorressem dentro do ambiente virtual ou, que foram facilitadas através de algum componente digital. Países previamente citados por exemplo, Inglaterra e EUA possuem vasto repertório neste campo, assim como os Estados membros da União Européia, que também tem apresentado evolução nessas políticas. É importante ressaltar que o que está sendo analisado não são estas nações em específico, mas sim políticas eficientes que foram utilizadas por esses países e se mostraram funcionais para prevenir este tipo de ação criminosa.

Em seguida o Abismo Tecnológico será analisado para entender seu impacto nas políticas de cibersegurança dos países do Sul Global. Antes de identificar os problemas causados pelo Abismo, é necessário entender o que é este fenômeno, como ele surgiu, quais fatores proporcionaram seu aparecimento e como ele está sendo combatido pelas potências mundiais. Primeiramente a ascensão das grandes potências ao seu patamar atual de desenvolvimento deve ser entendida, para isso o estudo do Dr. Ha-Joon Chang chamado "*Kicking Away the Ladder*" será abordado. Apesar de sair um pouco da temática apresentada neste trabalho, a teoria do Dr. Chang se mostra necessária para compreender a posição, tanto do Norte quanto do Sul Global em matéria de desenvolvimento e como um influenciou o outro.

[4] Uma pessoa que utiliza das redes de informação para fazer bullying com outros indivíduos. Isto é um grande problema desde o aparecimento das redes sociais.

A última etapa da pesquisa se concentrará em mostrar a situação do Sul Global quanto aos esforços para a criação de sua própria cyber resiliência, tendo em vista suas características enquanto nações, e o quais medidas devem ser tomadas para que esses países não sejam vítimas de ações criminosas que não podem ser compreendidas e impedidas devido ao abismo tecnológico, e como o Norte Global pode ajudar estas nações mais vulneráveis. Também serão apresentados casos de países que conseguiram se prevenir ou conter ações criminosas dentro do ambiente virtual como Brasil e Chile e Argentina, e como essas medidas de prevenção já existentes podem ser adaptadas e exportadas para outros países, de modo a facilitar o combate ao cibercrime. A abordagem regionalista desta pesquisa não tem a pretensão de dividir ou traçar fronteiras digitais no ciberespaço, mas sim servir como uma ferramenta ilustrativa para apresentar os diferentes casos em que podem ser observadas tentativas de Estados Nações de interferir direta no meio digital, que deve ser tratado como uma nova dimensão da existência humana,

Capítulo 1. CRIMES E CIBERCRIMES

1.1 Crimes e a Estrutura Social

A criminologia costuma utilizar o chamado "Modelo de Consenso" para definir o que pode ser considerado "comportamento criminoso", ou não na maioria das sociedades (BROWN et al. 2010). Este modelo se baseia na ideia de que existe um consenso por parte da opinião pública sobre o quais atitudes são passíveis de punição, e se isso é corretamente refletido nas leis que regem o ordenamento jurídico desta sociedade. Sendo assim o entendimento de "crime" é intimamente conectado com o que cada sociedade percebe como uma ação antissocial, aqui entendida como algo que vai contra os valores esposados pelos indivíduos que fazem parte ativamente deste meio social. Crime poderia ser definido então como "um ponto de conflito entre o indivíduo e a sociedade" (IVINS, 1911). Um exemplo prático disto seria a questão das drogas recreativas. Para certos países drogas como a maconha devem ser legalizadas seguindo os princípios de sua teia social de que isto pode ser benéfico para controlar o tráfico, reduzir casos de ansiedade ou depressão, e ajudar no tratamento médico para certas doenças como o câncer. Já outros países consideram o uso das drogas como algo que causa um impacto negativo em sua sociedade, e, portanto, são necessárias ações diretas para que este impacto seja remediado.

Isto também significa que a segurança é um reflexo do que a opinião pública considera como sendo ameaçador. Para se sentir seguro é necessário que o indivíduo tenha ciência daquilo que o ameaça, e partir disto entender as medidas que precisam ser tomadas, tanto por ele, quanto pelo Estado para garantir sua proteção. Grande parte da segurança é realizada através do "senso comum" sobre as ameaças, como não andar à noite, ou em certas áreas de sua cidade, trancar sua porta quando sair de casa. Certos países como os EUA, tem como prerrogativa o armamento da população civil como um fator positivo para o aumento da segurança, ou pelo menos da sensação de segurança, de sua sociedade. Não obstante, isso contribui para a dificuldade em se encontrar um framework teórico que possibilite a definição de crime, e o entendimento de suas causas, e, como será observado nas sessões subsequentes, está dificuldade também é transportada para a contraparte cibernética deste fenômeno.

Para os fins deste trabalho, a teoria chave usada para definir as ações criminosas será a "Teoria da Estrutura Social do Crime". Esta teoria não é a única interpretação correta deste tópico, mas é útil para entender, tanto crimes cometidos no mundo físico, quanto no mundo digital. Além disso, é uma teoria que permite interdisciplinaridade com outros frameworks da criminologia que contribuem para um entendimento sociológico dos crimes:

> "Sociologists envision crime, delinquency, and deviant behavior as the product of social forces rather than of individual differences. Most sociological theories fit the positivist mode in that they contend that these social forces push or influence people to commit crime. Even at this broad level of categorization, however, the perspectives are not pure. Sociobiology, for instance, combines social and biological variables to explain crime. Many sociologists incorporate psychological factors in their theories; and both economists and sociologists are currently pursuing classical explanations of crime. So despite the general dominance of sociology in criminological theory construction, all manner of cross-disciplinary perspectives and hybrid theories can be found. A major trend is toward integration of various theoretical perspectives..." (BROWN et al. 2010)

A teoria estrutural define os crimes como produtos da sociedade, tendo suas causas nos problemas enfrentados pelos indivíduos conectados às origens estruturais destes problemas como: fome, miséria, falta de educação de qualidade, racismo e patriarcado. Isso não significa, entretanto, que apenas pessoas pobres cometem crimes. Uma pessoa em condição de vulnerabilidade, por conta de não ter recebido uma educação digna por exemplo, pode se tornar vítima de muitos tipos de crimes, especialmente cibercrimes. Um indivíduo que nunca foi ensinado sobre a internet pode ser vítima de fraude, ou ter suas informações roubadas por empresas privadas, mulheres que são oprimidas e exploradas pela estrutura patriarcal podem ser vítimas de crimes de ódio virtuais que atacam suas imagens ou tráfico de seres humanos,

algoritmos e Inteligências Artificiais são capazes de discriminar pessoas baseado em sua raça, crimes de "colarinho branco" são muitas vezes executados por pessoas que sabem das deficiências que pessoas marginalizadas possuem. Isso também é válido para outros crimes fora do meio digital como corrupção e trabalho escravo.

Esta teoria também não significa que pessoas pobres, ou exploradas pela estrutura social são isentas de responsabilidade, ou não possuem escolha se não cometer atos criminosos. Crime não deve ser interpretado como um problema primariamente de classes sociais baixas, até mesmo hoje com a democratização e acessibilidade dos meios digitais. A maior incidência de crimes por essas populações apenas revela a estrutura discriminatória presente naquela sociedade, e por isso é tão importante um entendimento macroteórico sobre estas questões. O indivíduo e a sociedade são então co-constituídos, seguindo o Modelo de Consenso: os indivíduos moldam a sociedade, que por sua vez molda os indivíduos. A teoria estrutural, então, afirma que dentro da sociedade existem falhas, ou elementos sociais econômicos, políticos e culturais que podem ser entendidos como causadores dos crimes. Essa ideia de falhas dentro de um sistema social que possibilitam a ascensão de crimes também pode ser utilizada quando se observa o mundo digital, quando grupos de pessoas se organizam para disseminar discurso de ódio, ou para organizar atentados contra grupos de pessoas. A teoria da Estrutura Social busca revelar as deficiências existentes dentro da sociedade, e assim corrigi-las para otimizar a vida em sociedade.

Ainda mais importante do que entender a teoria do crime, é entender como, e porque os crimes se manifestam em uma civilização, quais os motivos que levam as pessoas a se tornarem criminosos, e como estes atos de violência são desenvolvidos. Essa tarefa pode ser mais simples do que aparenta, apesar de ainda ser desafiante. Neste âmbito, o trabalho de Johan Galtung merece destaque, pois seu entendimento sobre as manifestações da violência em uma sociedade é crucial tanto para o entendimento do crime. Em seu famoso artigo "*Violence, Peace and Peace Research*", Galtung define dois tipos de violência: Pessoal e Estrutural (GALTUNG, 1969). Violência Pessoal é entendida por ele como ato violento envolvendo um agente contra uma vítima, sendo assim quando um assassino mata uma ou mais pessoas, essa violência pode ser entendida enquanto pessoal. Entretanto, a ideia de Violência Estrutural possui implicações intrigantes, tanto para os tipos de crimes, quanto para as causas deles.

Nas palavras do autor, este tipo de violência pode ser chamado de "injustiça social", ao invés de pessoas estarem cometendo atos violentos, estes são construídos dentro da estrutura social dentro de um contexto específico:

> "*Thus, when one husband beats his wife there is a clear case of personal violence, but when one million husbands keep one million wives in ignorance there is structural violence. Correspondingly, in a society where life expectancy is twice as high in the upper as in the lower classes, violence is exercised even if there are no concrete actors one can point to directly attacking others, as when one person kills another*." (GALTUNG, 1969)

Assim como descrito na Teoria da Estrutura Social, os problemas derivados da violência estrutural propiciariam a criação de um terreno fértil para que as pessoas sejam levadas a cometer crimes, sendo estes problemas: pobreza, disparidade econômica, ausência de segurança, discriminação por conta de credo e raça, desigualdade de oportunidades de vida, disparidade entre as taxas de mortalidade entre elites e povo, falta de acesso à educação, entre outros. Em seu outro livro "*Pax Pacifica*", Galtung também disserta sobre o aparecimento do crime organizado como consequência de regimes político-econômicos globais, sobretudo com relação a *terceiromundialização* de países na América Latina, Sudeste Asiático e Ilhas do Pacífico, que se consiste em um fluxo imutável e contínuo de materiais brutos e bens agrícolas saindo destes locais, e indo para países centrais do sistema capitalista, como os Estados Unidos, que então vendem seus bens de alto valor industrial para estes locais.

Isso tende a causar uma pobreza massiva e levar a miséria, tanto na população empregada, quanto a desempregada, e a uma desigualdade econômica, caracterizada por uma grande elite financeira surgindo nestes países *terceiromundializados*, que servem como o elo de ligação com a elite do país explorador. À medida que a relação entre esses países aumenta a miséria, a fome, a corrupção e o acúmulo de riquezas nas mãos de uma extrema minoria, a população pobre do país que está sendo explorado não possui outra perspectiva que não seja a vida de crime, já que a própria estrutura contribui para que sua qualidade de vida seja ruim. Além disso, indivíduos em posições de poder dentro dessas sociedades podem se aproveitar do sistema de injustiças para manter seus privilégios e posições de poder, muitas vezes através de ações criminosas, com a diferença que os perpetradores destas gozam de proteção pelo sistema.

As ideias de Galtung fornecem um panorama lógico para o surgimento de criminosos, tanto em camadas altas, quanto baixas de uma sociedade. Ao invés da razão ser por conta de questões biológicas, psicológicas, ou ainda por uma questão altamente subjetiva como a natureza humana, é o contexto econômico, social e político que separa as pessoas que se tornam criminosos, de pessoas que não se tornam criminosos. Além disso, o conceito da injustiça social causada por este tipo de violência permite analisar outros meandros como a responsabilidade Estatal sobre os crimes, já que não necessariamente os crimes se manifestariam pela inação do

Estado, mas sim por agentes ou oficiais do Estado que contribuiriam para a continuação destes crimes. Um exemplo prático poderia ser a corrupção que ocorre dentro de um governo, ou a formação de organizações de crime organizado que contam com a participação de agentes do Estado, como as milícias no Brasil, ou a máfia dos Estados Unidos, que contava com aliados com cargos executivos, legislativos e dentro do sistema jurídico nacional. De novo, pode se observar um sistema de falhas sociais, que é responsável pelo comportamento criminal.

Estas falhas sociais podem ser tanto a falta de acessibilidade a bens indispensáveis para o indivíduo, como acesso à educação, saúde, trabalho, segurança, etc... quanto o tratamento com iniquidade por conta da sociedade, perante os problemas particulares de seu tecido social. Sendo assim, para testar o quão eficiente é uma sociedade, tanto no meio físico quanto no virtual, deve-se ter em mente a maneira pela qual a sociedade lida com seus crimes, tanto em questões punitivas, quanto preventivas. Deve ser observado também que em sociedades Ocidentais, o indivíduo possui direitos que são considerados superiores aos direitos da sociedade em si (IVINS, 1911). No ciberespaço isto é evidente quando um crime de discurso de ódio é cometido, mas o perpetrador se defende utilizando seu direito de liberdade de expressão, apesar de isto não ser uma defesa válida. Existem outras causas para a manifestação dos cibercrimes também, como a falta de monitoramento por parte das organizações, sejam elas estatais ou não, que fazem parte deste meio, e também a diferença de comportamento apresentado pelas pessoas dentro do espaço virtual. Portanto, agora é necessária uma análise mais profunda sobre este fenômeno.

1.2 Definindo Cibercrimes

Para garantir o entendimento dos temas tratados neste trabalho, algumas colocações devem ser feitas a respeito à natureza e aos atos de Cibercrime. A definição de Cibercrime em si é rotineiramente mal-entendida, e se torna um tópico de debates, especialmente em relação à legislação adotada para categorizar e julgar perpetradores de atos criminosos no meio digital. O termo é usado para se referir a múltiplos tipos de crimes, ou seja, a definição é muito ampla. O autor Neal Kumar Katyal define cibercrimes em duas amplas definições que podem ser subdivididas. A primeira destas é a definição pura de “cibercrime”, que seria o ataque a um computador executado eletronicamente, ou seja, situações em que o aparelho de computador é em si o alvo da ação criminosa que não é executada de forma física, a destruição de peças de computador, por exemplo. Ele desenvolve essa categoria em três formas distintas de crime:

> *“We may further subdivide this category by distinguishing among acts that involve (1) unauthorized access to computer files and programs, (2) unauthorized disruption of*

> *those files and programs, and (3) theft of an electronic identity. An example of the first category is a break-in to Defense Department Computers. An example of the second category is the ILoveYou Worm. The third category, identity theft, occurs when a person's or entity's identity is wrongfully appropriated" (KATYAL, 2001)*

A outra grande definição de cibercrimes que o autor explicita em sua obra são crimes em que os sistemas de computadores em si são usados para facilitar ações criminosas mais tradicionais, como distribuição de pornografia infantil, pirataria, fraude e outras formas sofisticadas de crimes de "colarinho branco". Nestes casos, computadores agem como um "facilitador" ou um "meio" por onde crimes tradicionais são executados. Estes crimes podem ser entendidos então como ações criminosas dentro das redes digitais de computadores, mas que possuem igual peso e consequências do que suas contrapartes do mundo físico, mas são exacerbados pela falta de monitoramento e de medidas de segurança para combatê-las. Este tipo de cibercrime vem se tornando mais comum, à medida que a tecnologia de informação torna o mundo mais conectado, e de certa forma também mais vulnerável.

A Convenção sobre Cibercrime, provavelmente possui as categorias mais sucintas para identificar cibercrimes. Essa convenção identifica quatro principais tipos de ofensas, sendo elas: "Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores"; "Ofensas relacionadas a conteúdo"; "Ofensas relacionadas a Direitos Autorais" e "Ofensas relacionadas a computadores" (GERCKE, 2012). A Legislação também aponta que a tipologia não é inteiramente consistente, sendo os três primeiros tipos de definições de Cibercrime focadas nos objetos de proteção legal, e em contrapartida, o quarto tipo enfatizando o método usado para se cometer os crimes. Sendo uma inconsistência que leva a uma sobreposição entre as categorias.

Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores podem ser exemplificadas como o acesso ilegal de computadores através de "*hacking*" ou "*cracking*"[5], onde um indivíduo consegue acesso às senhas de sites ou são capazes de invadir sistemas de segurança protegidos. Estes são alguns dos cibercrimes mais antigos já detectados, e desde a criação de sistemas de computador tem se tornado um problema global. As estratégias de "*Hacking*" também podem ser usadas como plataformas para cometer outros tipos de cibercrimes como espionagem de dados, onde hackers conseguem acesso a informações sensíveis de uma organização, e depois vendem estes dados no mercado negro através da internet. Além disso, a espionagem de dados pode ser alcançada por outros meios,

[5] O termo é geralmente usado por programadores para se referir à indivíduos que invadem sistemas de segurança. Apesar do termo hacker ser usado comumente, ele é visto como errôneo por programadores.

como a manipulação. Peter Gottschalk considera que a manipulação de indivíduos para compartilhar seus dados e assim permitir que cibercriminosos tenham acesso a eles é também um tipo de cibercrime (GOTTSCHALK, 2010). A Convenção sobre Cibercrime define este tipo de manipulação para aquisição indevida de dados como "*Phishing*"[6].

Outro tipo de crime nesta categoria seria a interceptação ilegal de comunicações e transferência de dados. Locais de acesso à internet sem fio, também conhecidos como "pontos de Wi-Fi", são especialmente vulneráveis e este tipo de ação criminosa. É possível localizar estes locais em bares, restaurantes, shoppings, lojas, escolas, academias, hotéis, e outros serviços de atendimento ao cliente. Existe um raio de 100 metros entre o aparelho roteador de internet e o aparelho conectado. O cibercriminoso pode operar em qualquer região deste espaço para interceptar comunicações e dados sendo mandados através da rede pela vítima. Várias organizações como o Escritório das Nações Unidas sobre Drogas e Crimes (UNODC) denominam os ataques de interceptação de mensagens como "*man in the middle attacks*"[7], fazendo alusão ao fato de que o perpetrador está se pondo no meio da comunicação entre a vítima e o servidor de internet, ou entre a vítima e outra pessoa (UNODC, 2019).

Os últimos dois tipos de subcategorias para este tipo de ofensa seriam "Crimes de Interferência", podendo ser divididos entre Interferência de Dados, e Interferência de Sistemas. O primeiro tipo ocorrendo quando há "o apagamento, a supressão, ou a alteração de dados de computador", e o segundo "quando os perpetradores são bem-sucedidos em prevenir que sistemas de computador funcionem eficientemente, causando grandes perdas econômicas para as vítimas" (GERCKE, 2012). Os crimes de interferência são geralmente executados através do uso de programas que danificam a eficiência de aparelhos de computador ou de sistemas interligados em uma rede de computadores. Estes programas são conhecidos como "Vírus de Computador" ou "*Worms*"[8]. A transmissão destes programas, também chamada de infecção, talvez seja o ato de cibercrime mais famoso, se não pelo menos aquele que os indivíduos que utilizam os meios digitais têm mais conhecimento sobre. Um vírus atacando um computador age de forma simples, tendo em vista os parâmetros de sua programação:

[6] Uma prática fraudulenta que se consiste em um criminoso enviar um email, ou outro tipo de mensagem para uma vítima alegando ser de uma companhia confiável, e assim manipular a vítima a compartilhar informações sigilosas.
[7] Literalmente: "ataque do homem no meio", devido ao perpetrador precisar se posicionar entre o ponto de wifi e o alvo.
[8] Literalmente: "minhoca", um programa malicioso que é capaz de se replicar constantemente, rapidamente se espalhando por toda a rede.

> "*Essentially, a virus has four phases: the dormancy phase (optional), the propagation phase, the trigger- ing phase, and the damage phase. A propagation phase is all that is necessary for the program to be a virus. The creator of a virus might use a dormancy phase to instill a sense of trust in the user since the virus does not propagate or do damage during this phase. The triggering phase is launched by some oc- currence, such as a certain date or a particular num- ber of replications. Finally, the damage phase does whatever harm the author intends the virus to do.*" (AZARMSA, 1991)

Estes vírus são capazes de modificar os dados e arquivos dentro de um aparelho de computador, assim impedindo sua utilização. Quanto aos crimes de interferência de sistemas, geralmente eles são executados através de *Worms* que, apesar de serem superficialmente similares aos vírus de computador, são focados em danificar redes de serviços e informação, ao invés de sistemas operacionais de aparelhos eletrônicos. Um exemplo deste tipo de fenômeno é em ataques de "Negação de Serviço" (DOS). Ataques desse tipo já foram definidos por inúmeros autores como: um ato intencional planejado para desintegrar serviços de computador, ou comunicação, causando sua interrupção, e assim negando acesso aos usuários (ARMSTRONG, 2001), ou seja, não devem ser confundidos com erros, ou "*bugs*"[9] que são de natural ocorrência dentro de sistemas, e ocorrem por conta de erros na programação.

Ofensas relacionadas a conteúdo são geralmente observadas quando o conteúdo disseminado na rede é considerado ilegal. Tendo em mente o que foi estabelecido na primeira parte deste capítulo, a noção de "ilegalidade" é variável para o contexto social de cada sociedade. A Legislação sobre Cibercrimes aponta que:

> "*The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies. The dissemination of xenophobic material is illegal in many European countries, but can be protected by the principle of freedom of speech in the United States. The use of derogatory remarks in respect of the Holy Prophet is criminal in many Arabic countries, but not in some European countries.*" (GERCKE, 2012)

O tipo mais comum de crimes de conteúdo geralmente tem a ver com compartilhamento de conteúdo sexual, no caso, conteúdos pornográficos. Cada Estado Soberano tem a capacidade de decidir qual tipo de conteúdo sexual pode ou não ser compartilhado, mas por via de regra pornografia infantil costuma ser um denominador comum entre conteúdos ilegais, e com boas

[9] Literalmente: "inseto", um erro inesperado encontrado dentro de um software ou hardware. O termo foi criado pela cientista da computação Grace Hopper quando em 1947 ela identificou um problema no computador Mark II da Universidade de Harvard. Ao investigar o problema, ela encontrou uma mariposa presa no aparelho de transmissão do computador, assim cunhando o termo.

razões para tal. Fotos com conteúdo sexual trocadas entre adultos com consentimento costuma não ser considerado um crime, a não ser que estas fotos sejam compartilhadas sem conhecimento. Há ainda a questão sobre acesso a sites pornográficos, alguns países os proíbem por completo, outros utilizam mecanismos de restrição de idade para impedir que menores acessem o conteúdo. Em um estudo comissionado pelo governo australiano, pesquisadores descobriram que a exposição de crianças à pornografia poderia levar a experiências sexuais prematuras, criar expectativas irreais sobre sexo, e sobre o parceiro, práticas sexuais sem proteção e, no caso de homens, tendência a ver mulheres como objetos sexuais e tendência a praticar violência contra mulheres, particularmente a violência sexual (QUADARA et al, 2017).

Outro tipo extremamente comum de cibercrime relacionado a conteúdo seria o "discurso de ódio". As Nações Unidas definem este fenômeno como um "discurso ofensivo que tem como alvo um grupo, ou um indivíduo baseado em características inerentes (como raça, religião ou gênero) e pode vir a ameaçar a paz social" (UN. 2021). Discurso de ódio pode ser disseminado, tanto através de mídias físicas como filmes, panfletos, cartazes e outros, assim como por mídia digital, e está intimamente ligado com a promoção da violência nas sociedades conectadas. Assim como com a criminalização da pornografia, um problema similar ocorre quando discurso de ódio é disseminado na internet. Nem todos os países decidem criminalizá-lo devido à "liberdade de expressão". Um caso famoso deste tipo de conflito, publicado no New York Times em 2001, foi durante uma ordem de censura feita pelo governo da França ao site Yahoo!, que possuía em seu acervo materiais nazistas. Como o site tinha sua base nos Estados Unidos, estava protegido pela primeira emenda da constituição, logo apesar da França ter a soberania para ditar quais materiais podem ou não ser compartilhados em seu território, ela não poderia interferir na política interna de outro país (GUERNSEY, 2001)

Nos últimos anos também foi possível observar a explosão de "*Fake News*", ou desinformação e notícias falsas. Este cibercrime de conteúdo tem tido mais abundância devido a certas falhas no sistema social da internet, como a falta de moderação em páginas ou sites da web, que permite que os autores publiquem informações sem verificação, e o fato de que muitas vezes não é necessário apresentar documentos de identificação para que se saiba a identidade que quem está por trás da publicação, visto que, na internet as fotos de perfil podem não ser do usuário da conta (GERCKE, 2012). Outros tipos de ofensas relacionadas a conteúdo incluem também serviços ilegais realizados por jogos online, onde a plataforma de jogo virtual pode ser usada para transmitir dados ilegais, como material pornográfico, ou utilizada para conseguir informações através da manipulação, e também a utilização de SPAM, que são mensagens

eletrônicas que chegam ao usuário sem o seu consentimento, e sem a intenção de querer recebê-las também.

Ofensas relacionadas a direitos autorais podem ser facilmente entendidas como "pirataria"[10]. Empresas que trabalham com mídia e outros tipos de companhia de entretenimento utilizam as redes para vender seus produtos e alcançar mais clientes. Isto acarreta o risco de que cópias de seus produtos possam ser feitas e vendidas ou distribuídas. No passado, criar cópias de mercadorias como DVDs era mais difícil devido a perda de qualidade que ocorria no processo. Entretanto, como a maioria dos produtos de mídia como filmes, jogos digitais, músicas, livros e revistas hoje pode ser distribuída em formato puramente digital, as cópias desses produtos são praticamente idênticas às originais, talvez a melhor forma de as definir seria que elas são as originais, mas estão sendo distribuídas sem permissão. Pirataria causa, principalmente, a perda de lucros para empresas que fabricam, ou vendem produtos pirateados, entretanto este tipo de crime tem outras consequências como o aumento dos preços dos produtos para usuários, a redução de inovação de produtos para a empresa, e processos civis mais e mais implacáveis contra pessoas que cometem o crime de pirataria (JAIN, 2008).

Outro tipo de crime de direitos autorais seria utilizar de uma "marca registrada" para enganar pessoas no ciberespaço. Geralmente criminosos tentam vender produtos online com logos de marcas famosas, ou então enviam e-mails para potenciais vítimas como sendo representantes destas marcas ou empresas, incluindo no corpo da mensagem o logo e alguma versão do "carimbo" oficial da marca. Um tipo específico da utilização de marcas registradas de forma fraudulenta seria "*cybersquatting*"[11]. Um tipo de crime em que o criminoso monta um site, também chamado de domínio, que se apresenta como site oficial da marca, ou é muito parecido com o site oficial, de modo a atrair usuários para tirar lucro deles, o autor H. Brian Holland define *cybersquatting* como um ato deliberado, de má fé e abusivo do registro do nome de um domínio de internet que viola os direitos dos donos da marca registrada (HOLLAND, 2005).

Finalmente, a última definição, **ofensas relacionadas a computadores**, são crimes primariamente realizados através de fraude, como falsificação de documentos, e roubo de identidade. Crimes de fraude são um dos mais populares tipos de cibercrimes existentes, se não

[10] Vender ou distribuir produtos sem autorização daqueles que detém os direitos de propriedade sobre a marca ou o produto em si.
[11] Literalmente: Ocupação Ilegal Cibernética, fazendo referência a processos de ocupação ilegal que ocorrem no mundo material.

o mais popular. Cibercrimes que envolvem atitudes fraudulentas são tão diversos como suas contrapartes no mundo físico:

> "*Financial crime is carried out via check and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud, payment (point of sale) fraud, currency fraud, and health care fraud, and they involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, and social engineering.*" (GOTTSCHALK, 2010)."

A Legislação sobre Cibercrime identifica os dois tipos mais comuns de fraude que podem ocorrer no meio digital: fraude de leilões online e fraude de gratificação adiantada. O primeiro tipo se tratando da exploração da vantagem de não se ter comunicação cara a cara com o leiloeiro para apostar em bens que estão sendo leiloados em uma plataforma digital. Geralmente o criminoso não possuí bem algum para dar em troca das apostas, e então rouba o dinheiro de usuários que estão dispostos a participar do leilão. O segundo tipo é um pouco mais complexo, e envolve uma comunicação direta entre o criminoso e a vítima, em que o criminoso pede ajuda para pagar uma grande quantia de dinheiro, afirmando que retornará parte do dinheiro para a vítima, caso a vítima concorde em processar o pagamento utilizando sua conta bancária pessoal. As vítimas muitas vezes são manipuladas para divulgar sua informação bancária confidencial, ou são manipuladas para pagar uma taxa menor, com o objetivo de "validar" sua conta para o criminoso. Depois que a transferência, ou as informações são enviadas, a vítima nunca mais será contactada pelo perpetrador.

Roubo de identidade também pode facilmente acontecer com a ajuda de tecnologia de computadores e acesso à internet. Roubos fraudulentos de identidade como roubo de seguro de vida, número de passaporte, RG, CPF, endereço, número de telefone e senhas de contas pessoais ou bancárias são alguns dos crimes mais antigos que estão sendo cometidos há quase um século. Entretanto, hoje os métodos são diferentes. Isso se deve ao crescente uso de tecnologias digitais para efetuar transações monetárias, como utilizado no pagamento via PIX[12] e em aplicativos de bancos, e também ocorre no armazenamento de informações pertinentes ao usuário, por exemplo, quando órgãos governamentais que utilizam de bancos de dados para preencher automaticamente informações dos cidadãos como no imposto de renda ou na saúde pública.

Entender os tipos de cibercrimes e como eles ocorrem é só um lado da moeda, entretanto, é necessário ir mais além para entender quem são os cibercriminosos e como eles operam no meio digital. Já é possível notar que com uma gama imensa de cibercrimes, as

[12] Pagamento instantâneo brasileiro, criado pelo Banco Central (BC).

motivações para executar esses atos também tendem a ser igualmente diversas, da mesma forma que as motivações tidas pelos criminosos do mundo físico. Apesar de poder se observar que a maioria dos cibercrimes é motivada por lucro, tratando-se então de crimes com simples objetivos materialistas, essa não é a única força motora por trás dos cibercrimes.

1.3 Tipos de Criminosos, e suas Motivações no Ciberespaço

Peter Gottschalk em seu livro: "Policing Cyber Crime" define estes tipos crimes como sendo primariamente "crimes financeiros". Ele então explicita 4 subcategorias de crimes financeiros: Fraude, Roubo, Manipulação e Corrupção (GOTTSCHALK, 2010). Os cibercrimes são, em sua grande maioria, crimes motivados por lucro que são facilitados pela utilização de computadores e de redes de informação digital, o termo em si e usado para se referir a ataques contra a infraestrutura de cibersegurança de grandes empresas. O criminoso pode ter diversos objetivos para fazer isso, como ter acesso a informações confidenciais sobre a empresa, algo muito sensível considerando que a maioria dos negócios e dependente de informações sobre propriedade intelectual, dos bancos de dados de informações de seus empregados, de suas tabelas de preço e de seus números de vendas (GOTTSCHALK, 2010).

A partir disso, o criminoso consegue diretamente de apropriar de recursos econômicos que lhe conferem benefícios, através do desvio de fundos, ou da venda de informações confidenciais para concorrentes de uma empresa específica, ou até a venda de dados particulares dos empregados das empresas para companhias de anúncios. Ele pode também causar dano ao sistema de informações, deletando ou modificando os dados presentes neste sistema resultando em terríveis consequências, para assim conseguir chantagear a empresa a lhe pagar para interromper os ataques.

Apesar de estes serem os tipos mais famosos de cibercrimes, a definição e muito mais extensa do que apenas ataques contra empresas dependentes de redes. Cibercrimes também podem ser executados através do uso da internet. Ironicamente a maioria dos perpetradores desses crimes são empresas que utilizam dados roubados de seus usuários para lucrar em cima de anúncios. Elas se apropriam de informações através de ferramentas já muito conhecidas como "cookies" que são pequenos pedaços de código que permitem quem informações sejam passadas entre um servidor e um computador cliente, e "web bugs"[13], gráficos invisíveis que são embutidos em páginas da web e e-mails para monitorar as atividades dos usuários (ZUBOFF, 2021). Nestes dois casos, os tipos de perpetradores se tratam de indivíduos ou

[13] Ao contrário dos *bugs*, que são erros inesperados, os *web bugs* são códigos maliciosos que são postos em sites para rastrear atividade dos usuários.

grupos criminosos, a serviço de si mesmos, ou empresas, explorando ilegalmente a tecnologia de computadores e o acesso à internet para realizar seus crimes, visando ganhos materiais imediatos. Entretanto, como afirmado ao fim da segunda parte deste capítulo, lucro imediato não é a única razão pela qual cibercrimes são cometidos. Existem também objetivos políticos.

Um exemplo disto é o aparecimento de hacktivistas, ou seja, ativistas que utilizam do meio digital para transmitir sua mensagem política. Obviamente, ativismo político não é um tipo de crime, já que se encontra protegido pela liberdade de expressão, e, de fato, não é este elemento que define hacktivismo como cibercrime, mas sim sua manifestação em ações ilegais no ciberespaço, como estratégias de *hacking*:

> "*When such activism manifests itself in the form of surreptitious computer access or the dissemination of potentially disruptive and/or subversive software, it is called "hacktivism." A hacktivist, therefore, uses the same tools and techniques as a hacker, but does so in order to bring attention to a larger, political or social goal.*" (MILONE, 2002)

Hacktivistas são então cibercriminosos que utilizam dos métodos já citados na segunda parte deste capítulo que podem ser enquadradas dentro de "Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores", para alcançar objetivos políticos e sociais. Isso pode ser entendido através das já citadas ideias da teoria social da criminologia. Hacktivistas em sua grande maioria procuram as ferramentas de *hackers* ou *crackers* por conta das falhas presentes dentro de uma estrutura social. Eles utilizam estes métodos como uma prática efetiva para a transformação da realidade, pelo menos de acordo com a sua própria interpretação do que a realidade poderia ser.

Grande parte dos *hackers*, mesmo aqueles que não defendem uma bandeira ou movimento social específico são hacktivistas. O autor Steven Levy afirma que os *hackers* possuem uma filosofia, uma ética e um sonho. Em sua obra: Hackers, Heróis da Revolução, ele expõe os elementos que fazem parte da ética hacker, sendo que a base do éthos *hacker* é fundamentalmente a crença em que: "*access to computers and anything which might teach you something about the way the world works should be unlimited and total. Always yield to the Hands-On Imperative!*" (LEVY, 1985).

Outras crenças também são partes da ética *hacker* como a ideia de que "toda informação deve ser gratuita", "descrença em autoridades e promoção da descentralização", "a capacidade de poder se criar arte e beleza em computadores" e "computadores podem mudar sua vida para melhor". É evidente que algumas delas, particularmente a última, partem de uma visão

tecnodeterminista da tecnologia de computadores, mas servem para ilustrar que hackers não são simplesmente ladrões, e apesar de serem criminosos possuem um código que honra, que pode ser seguido ou não, mas isto influência suas motivações para fazer o que fazem. A definição de hacktivismo como crime, assim como foi observado na primeira parte deste capítulo, também é dependente do contexto social em que este fenômeno está inserido, entretanto o consenso parece ser que tentativas não autorizadas de penetrar em um sistema de informações confidenciais são consideradas crimes.

Hacktivistas não são os únicos que possuem um objetivo político para suas ações no ciberespaço. Existem também outros tipos de cibercriminosos que são muito mais perigosos do que ativistas virtuais. São os chamados ciberterroristas. Eles são fundamentalmente diferentes dos hacktivistas por diferentes razões, mas para não correr o risco destas duas distintas definições se confundirem nesta análise, é necessária uma breve explicação sobre o fenômeno do ciberterrorismo. Em sua essência, o ciberterrorismo nada mais é do que a facilitação do uso do terror através da tecnologia de computadores e das redes de informação da internet. Apesar de existirem inúmeras interpretações do que exatamente constitui o uso do terror, a legislação sobre cibercrimes identifica elementos pontuais que podem ser usados para identificar ações de ciberterrorismo. Porém é importante ressaltar que, até o ponto atual que as tecnologias de informática se encontram, as organizações terroristas não foram capazes de executar um ataque puramente cibernético, sendo a maioria dos casos de ciberterrorismo ocasiões em que as redes de computadores foram usadas como um auxiliador para os ataques.

Uma pré definição de terrorismo deve ser compreendida, pois quando o Ciberterrorismo é analisado, pode-se notar várias semelhanças com o terrorismo em sua forma física, uma vez que o próprio terrorismo virtual é uma extensão ou adaptação do terrorismo clássico aos novos tempos. Entretanto Anna-Maria Taliharm chama a atenção em seu texto *Cyberterrorism: in Theory or in Practice?*, que a grande semelhança entre o Ciberterrorismo e outros tipos de Cibercrimes, somado a propria dificuldade de entender o terrorismo em si, leva a conclusões erradas sobre o ato criminoso perpetrado dentro da rede digital. A autora afirma:

> "*As has been already discussed, the term 'cyberterrorism` is widely used but sadly with great inconsistency regarding the meaning of the concept. The strong interrelation between the characteristics of cyberterrorism and various other cyberoffences, such as hactivism, has rendered drawing a clear line between the types of incidents to be and increasingly challenging task. The 'continuing failure' to distinguish different types of cyberincidents often derives from the difficulties in determining the intent and motivation of the attacker as well as fairly evaluating the level of damage caused*." (TALIHARM, 2010)

O Ciberterrorimo, sendo uma modalidade de Cibercrime, possui duas dimensões, uma que seria a facilitação através de sistemas de computadores para a perpetração de crimes terroristas que seriam cometidos no plano físico, e outra que seria a utilização de meios eletrônicos para cometer crimes dentro do ambiente virtual. Taliharm apresenta essas dimensões como "*Tool Oriented Cyberterrorism*" e "*Target Oriented Cyberterrorism*".

A primeira definição sendo a utilização de meios eletrônicos que agem como uma ferramenta para a facilitação dos atentados terroristas, podem ser citados: "*Data Mining*", recrutamento de pessoas, lavagem de dinheiro, e realização de propaganda, além de uma plataforma para a transmissão do atentado para sua audiência alvo, como feito pelo Estado Islâmico. Essas ações não são consideradas atos terroristas em si, porém por conta da facilitação proporcionada aos criminosos, devem ser devidamente analisados, julgados e prevenidos. Ignorar essa abordagem pode causar uma grande vulnerabilidade dentro de uma nação, já que recursos e propaganda são excelentes meios de se vender uma ideia, inclusive o terror.

A segunda diz respeito a ataques que são realizados dentro do ambiente digital, e como a própria autora cita previamente, é muito confundida com hactivismo, que seria um ativismo digital que utiliza de meios usados por Hackers. A autora apresenta exemplos como: Bloqueios virtuais a sites usando tráfego de informações, ataques a e-mails através de *flood*, invasão de computadores através de Hack, e utilização de vírus de computadores como *Worms*[14]. Estes métodos também podem ser usados por Ciberterroristas, por isso sua citação neste trabalho é importante, porém qual seria então a principal diferença entre um Hacktivista e um Ciberterrorista, visto que ambos possuem uma dimensão política bem definida? Taliharm nos aponta uma possível resposta:

> "*As a rule, hacktivism is all about political protesting using virtual methods and does not seek to cause great financial harm or injure people, therefore it should not be qualified as cyberterrorism. However, hacktivism gives us a glimpse of what could be done by cyberterrorists on a bigger scale as terrorists could use any of the abovementioned tactics to accomplish their politically motivated goals*." (TALIHARM, 2010)

Portanto a principal diferença seria o grau de violência utilizado pelos Ciberterroristas, assim como um terrorista é também um assassino, o que o define como um terrorista é como sua violência é projetada ao seu alvo. Um exemplo de Ciberterrorismo, que é inclusive citado

[14] Um malware mais perigoso que um vírus comum de computador. O *worm* tem a capacidade de se reproduzir sozinho em um ritmo constante, infectando outros computadores através da rede. O objetivo do *worm* é roubar dados dos usuários.

no texto de Taliharm, foi o ataque aos sistemas de informação da Estonia em 2007, durante a transferência de um memorial soviético da Segunda Guerra Mundial. Após essa transferência recebeu ataques Ciberterroristas coordenados para interromper seus serviços governamentais, bancários, midiáticos entre outros.

Desde os ataques do onze de setembro de 2001, foram observados usos das redes por terroristas com os propósitos de: promover propaganda, colher informações, preparar ataques físicos, publicação de material de treinamento, comunicação entre membros de diferentes células, financiamento dos ataques e ataques contra infraestrutura crítica (GERCKE, 2012). Este último tipo de ataque terrorista é potencialmente o mais perigoso, com exceção de ataques terroristas executados no mundo físico. A infraestrutura crítica, que pode ser identificada como sistemas de fornecimento de água ou energia por exemplo, está passando por uma transição de seus ambientes isolados para "sistemas de sistemas" (GENGE et al. 2015), ou seja, se tornando mais dependente da integração com tecnologias de informação e de comunicação. Ataques contra a infraestrutura podem ser extremamente danoso, não apenas para a segurança financeira das pessoas, como no caso de *hackers*, mas sim para seu próprio bem-estar físico.

Da mesma forma que hacktivistas, ciberterroristas podem usar os mesmos métodos de outros tipos de cibercriminosos, mas assim como no caso do terrorismo físico, e necessária uma motivação política para que o ciberterrorismo se manifeste. Ainda sobre a questão do ciberterrorismo e da infraestrutura crítica, a professora Dorothy E. Denning afirma que:

> "*Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*" (DENNING, 2000)

Neste capítulo foi definido o que são os cibercrimes, como sua definição é até certo ponto subjetiva e dependente do contexto social em que está inserida, tal qual os crimes que ocorrem no mundo físico, quais são os tipos de cibercrimes que foram detectados até agora, e quais são os tipos de cibercriminosos e suas motivações para cometer este tipo de ofensa. Porém nada foi afirmado sobre como prevenir, impedir e criar resiliência a este tipo de crime. A partir do próximo capítulo serão expostas as formas que os sujeitos, sejam eles indivíduos, empresas

ou governos possuem para se defender dos cibercrimes, também conhecidas como as medidas de cibersegurança.

Capítulo 2. CIBERSEGURANÇA E TECNOLOGIA.

2.1 Ciberisco

A próxima parte da pesquisa tratará sobre medidas preventivas para cibercrimes, começando pela relação entre estes conceitos e cibersegurança, que apesar de serem conceitos similares e se sobreporem em diversas situações, são distintos. Como previamente citado na sessão de Apresentação e Justificativa, a Cibersegurança é entendida por Serger como a proteção da confidencialidade, integridade e disponibilidade de dados de informática e sistemas para aumentar a segurança, resiliência e confiança na tecnologia de informação. Como visto no primeiro capítulo, cibercrime possui inúmeras definições como: Ciberbullying, Hacking, Roubo de identidade e antigas formas de crime como roubo de bancos ou carros, facilitadas pelo uso de computadores. Por conta disso suas estratégias de prevenção são extremamente variadas e muitas podem ser usadas nas políticas de Cibersegurança.

A segurança digital, como entendida pelo Conselho Nacional de Prevenção ao Crime dos EUA, não é responsabilidade apenas dos governos ou de grandes empresas privadas, mas também de indivíduos, o Conselho afirma que:

> "*Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. When armed with a little technical advice and common sense, many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.*" (NCPC, 2012)

A cibersegurança de um sistema operacional digital costuma ser averiguada através do processo de avalição de cyber risco (*Cyber Risk Assessment*). Três fatores são cruciais para a abordagem de avaliação: a ameaça, ou seja, o tipo de cibercrime que se antecipa, exemplos foram dados no capítulo anterior como *hacking*/*cracking*, fraude, ou roubo de recursos. O segundo fator seria o grau de vulnerabilidade, podendo ser traduzido em fraquezas específicas presentes no sistema, que acabam permitindo que um recurso digital ou uma organização possam ser vítimas de cyber ataques. E por fim a "probabilidade", que simplesmente é a chance de um cenário de cibercrime ocorrer. Todos esses fatores traduzem o risco como:

> "*The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences*" (CISA, 2022)

Através da condução das avaliações de cyber risco, organizações públicas ou privadas são capazes de identificar os pontos fracos de seus sistemas operacionais ou bancos de dados e assim produzir maior resiliência, entendida nos termos de Serger, contra diferentes tipos de cibercrimes. As avaliações também permitem que se tenha uma ideia da postura de segurança que a organização deve tomar contra possíveis explorações de criminosos. Esta postura se refere ao status da segurança das redes de informações, contatos e sistemas baseados em recursos de segurança de informações presente dentro da organização, ou seja, pessoas, hardware, software ou políticas de segurança. A postura de segurança também se refere à capacidade de uma empresa ou organização de reagir e se defender de situações de risco (JOHNSON et al, 2011).

A Agência de Cibersegurança e Infraestrutura da Segurança (CISA) propõe seis passos para avaliar o cyber risco. O primeiro, e possivelmente o mais simples, seria a identificação e documentação das vulnerabilidades presentes nas redes pertencentes à organização. Processos internos e externos ao cyberespaço devem ser considerados, pois os membros integrantes do corpo de funcionários das organizações também podem realizar ações acidentais que coloquem as redes em risco. Um exemplo de riscos dentro do mundo digital seriam plataformas de e-mail, que são rotineiramente utilizadas por cibercriminosos para obter dados sensíveis, portanto é necessário a utilização de um software de segurança robusto para impedir ataques. Geralmente, empresas privadas possuem o luxo de contratar companhias terceirizadas para realizar a instalação e manutenção de sistemas de e-mail confiáveis, que são mais resilientes do que os amplamente disponíveis ao público, como Gmail ou Hotmail.

O segundo passo seria a identificação da fonte das ameaças à cyber inteligência. De onde vem os ataques, e quem está por trás deles? A última sessão do capítulo anterior já foi capaz de fornecer uma ampla gama de perpetradores e motivações que eles podem vir a ter, mas somente listá-los não é suficiente. É necessário saber quem exatamente é o responsável. Será que quem está atacando é um Hacker que está roubando dinheiro da empresa, ou um Hacktivista, que não é movido por lucro? Quando se analisa os serviços públicos, também se abrem possibilidades para ataques ciberterroristas. Portanto a organização precisa ter em mente seus potenciais inimigos, dependendo de sua natureza. Saber quem são os mais prováveis de cometer atos cibercriminosos contra os sistemas garante uma maior chance de preparo contra diferentes formas de ataques, ao mesmo tempo que também economiza tempo e recursos contra outros tipos de ataques que serão praticamente improváveis.

O terceiro passo é a identificação de ameaças, tanto internas quanto externas, à organização. Como afirmado pela CISA no primeiro passo, funcionários podem realizar ações acidentais, ou mal-intencionadas, que colocam a organização em risco. Ao contrário do primeiro passo, que é focado na criação de sistemas resilientes contra possíveis ataques, este aqui busca mais precisamente identificar e averiguar a ameaça que certos indivíduos, ou plataformas apresentam para a organização. Através da identificação e monitoramento, é possível se precaver contra possíveis brechas de segurança. Como exemplo, supondo que a empresa tenha resolvido o problema do primeiro passo e instalado uma plataforma de e-mail confiável, isto não significa que não podem ocorrer brechas. É importante monitorar quais funcionários apresentam maior risco dentro da plataforma, por exemplo: se um funcionário está compartilhando informação sensível com outros indivíduos utilizando o e-mail da companhia. Um outro exemplo poderia ser: quais sites ou páginas da web devem ser evitadas por funcionário quando eles estão utilizando os terminais da empresa.

O quarto passo é a identificação de quais sistemas são dependentes de tecnologias específicas. Cibercriminosos são capazes de atacar a infraestrutura crítica de uma organização, causando uma interrupção em seus serviços e sistemas operacionais. Esta infraestrutura é dependente de sistemas de comunicação e de informação, que podem ser explorados pelos criminosos causando um efeito dominó nos sistemas dependentes. Portanto, ao atacar um sistema, é possível afetar outros simultaneamente. A avaliação permite que os recursos partilhados, e a dependência entre diferentes sistemas sejam identificadas, para assim impedir que brechas ocorram ao mesmo tempo em sistemas com recursos partilhados, e também possibilita que um plano de ação seja formulado caso ocorra um ataque.

O quinto passo é a utilização das ameaças, vulnerabilidades, probabilidades e impactos para determinar o risco. Para isso devem ser usadas as definições de “alto”, “médio” e “baixo”, para averiguar o nível do risco presente dentro dos sistemas. É preciso ter em mente o que qualifica um risco dentro dessas categorias, e quais sistemas estão postos no nível de alto risco. É necessário também identificar corretamente quais são as ameaças à organização utilizando os passos 1 e 3, e quais contramedidas estão postas em lugar para combater possíveis brechas na segurança. Entretanto, mais importante ainda é o entendimento de que estes problemas são contínuos, e não podem ser resolvidos por completo através de uma bala de prata, ou solução milagrosa. À medida que a tecnologia avança, novos tipos de risco surgem, e assim novas medidas devem ser tomadas para mitigá-los.

Por fim, o último passo é identificar quais respostas devem ser dadas ao ciberisco, e quais delas devem ser priorizadas. É crucial para garantir a cibersegurança que os tomadores de decisão e seus agentes saibam as respostas para ameaças cibernéticas específicas, como os cibercrimes, e também quais delas estão disponíveis para serem executadas. Por tanto é necessário manter uma lista com protocolos de ação e também de identificação de pessoas ou grupos aliados para fim de realizar contato caso uma brecha ou um ataque ocorram.

2.2 Cyber Awareness

Como pode ser observado nos 6 passos da CISA, grande parte das medidas preventivas ao ciberisco é baseada no reconhecimento das ameaças, tanto de ações acidentais, quanto de reais invasões aos sistemas. Saber reconhecer essas ameaças exige um treinamento de funcionários, tanto quanto de tomadores de decisão como Chefes de Estado, e políticos de carreira. Através do treinamento é possível aumentar a "*cyber awareness*" de um indivíduo, ou sua "percepção digital". Este tipo de treinamento pode ser facilmente encontrado para a disposição de empresas ou Estados, por exemplo no caso da companhia de consultoria em cibersegurança: Titan HQ, que oferece treinamentos para melhorar a "percepção digital" de funcionários atuando em diferentes ramos. Este serviço utiliza modelos de comportamento de funcionários para definir qual tipo de treinamento seria mais eficiente, somado com simulações de *phishing* e intervenções em tempo real (TITAN HQ, 2023).

Na seção 1.1, os parâmetros de entendimento do que constitui a ideia de um crime foram explicados. Crimes são até certo ponto dependentes de contextos sociais, culturais e econômicos, e baseadas nestes contextos surgem iniciativas de resposta e prevenção a estes crimes. Um indivíduo que desconhece o contexto pode ficar à mercê de criminosos. Por exemplo, para um nativo, pode ser muito natural não andar em certos bairros depois do pôr do sol, entretanto um estrangeiro não saberia disso. O primeiro indivíduo possui uma "percepção" que será uma vítima de um crime se realizar certas ações ou comportamentos: andar com o celular na rua, ir para certas partes da cidade, se vestir de uma determinada forma, entre vários outros.

Como poderá ser visto na próxima sessão, é possível aumentar a "percepção" das populações sobre crimes através de iniciativas educacionais por parte dos Estados, ou de empresas privadas para reduzir o risco de crimes. Porém no mundo digital, todos são estrangeiros. A realidade virtual ainda é muito nova e muito pouco explorada pelo grande número de usuários, e ainda pior é que iniciativas para aumentar a "percepção digital" carecem de acessibilidade e visibilidade. Com a crescente onda de cibercrimes, e a maior dependência

de tecnologias de informação e comunicação, não é mais possível atribuir a proteção de indivíduos, ou organizações para o "senso comum" de não clicar em um link, ou não acessar determinados sites. Como já foi visto nesta monografia, roubo de dados e informações são processos extremamente insidiosos e sutis, e as maiores empresas de redes sociais estão muitas vezes por trás destes tipos de cibercrimes, e não apenas hackers ou grupos de cibercriminosos.

A falta de percepção é um dos maiores desafios para a punição de cibercrime, pois as vítimas nem sequer sabem que foram vitimizadas, e também não possuem conhecimento dos protocolos corretos para denunciar os crimes, além da falta de confiança na capacidade dos órgãos de segurança de responder a esses crimes, devido a uma postura de segurança fraca em responder aos cibercrimes, ou até mesmo por sentirem vergonha de terem sido vítimas deste tipo de crime, e no caso de corporações: a perda de sua reputação enquanto organização confiável. Segundo o Escritório das Nações Unidades Sobre Drogas e Crimes:

> "In addition to transnational elements, significant underreporting of cybercrime acts in the first place can contribute to a limited picture of the underlying phenomenon. Of the 90 per cent of cybercrime acts that come to the attention of the police through victim reporting, countries estimate that the proportion of actual cybercrime victimization reported to the police ranges upwards from only one per cent. One survey conducted by a private sector organization suggests that 80 per cent of individual victims of core cybercrime acts do not report the crime to the police" (UNODC, 2013).

A "percepção digital" é um fator crucial na identificação de ciberisco e também na formulação de respostas preventivas. Como um exemplo prático, na questão do Ciberterrorismo, este fenômeno é entendido pelo Conselho Nacional de Prevenção ao Crime dos Estados Unidos, como um dos tipos de Cibercrime listados em sua definição: "*Cyber terrorism, which is violence, commonly politically motivated, committed against a civilian population through the use of or facilitated by computer technology.*" (NCPC,2012), sendo assim as medidas de prevenção para Cibercrimes são válidas para o combate ao Ciberterrorismo, e isto demanda que além do governo e empresas os cidadãos façam sua parte.

O problema encontrado aqui é que a definição de "senso comum" utilizada pelo Conselho é algo extremamente particular de um país do Norte Global, onde a tecnologia de informação foi devidamente internalizada e compreendida pela população civil, ou seja, a população possui um elevado grau de "percepção digital". Obviamente o senso comum de países onde a tecnologia de informação está presente, mas não foi devidamente compreendida pela população será diferente, o que abre espaço para mais atos cibercriminosos. Isto é um dos sintomas do Abismo Tecnológico. Este problema pode ser resolvido com campanhas

educacionais para auxiliar no entendimento da tecnologia pelos civis. Utilizando as medidas tomadas nos países do Norte Global como base, as próximas sessões tratarão das iniciativas de cybersegurança que foram bem-sucedidas.

2.3 Cibersegurança no Norte Global

Quando o problema de cibersegurança é observado através da lente da Territorialidade, é necessário destacar que não existem fronteiras, ou territórios dentro do mundo digital. O corretor seria afirmar que o ciberespaço é uma outra dimensão que, apesar de poder ser afetada pelo que transcorre no mundo material, possui suas próprias regras. Não é uma situação muito diferente da exploração espacial, por exemplo, onde o espaço sideral é considerado como águas internacionais, e não foi mapeado e dividido entre as nações ainda. Portanto quando se abordam os esforços de cibersegurança no Norte ou no Sul Global, a ideia não é afirmar que existe uma "ciberfronteira" entre países, uma vez que a tecnologia de informação e comunicação não está limitada às fronteiras geográficas entre os países. Uma pessoa no Brasil pode, com facilidade inclusive, conversar com outra pessoa que se encontra na Inglaterra, e o inverso também é verdadeiro. É por esta mesma questão que o cibercrime se torna um problema transnacional, já que é impossível para um único país de assumir controle efetivo sobre uma área específica da internet, sendo necessária uma abordagem similar ao tratamento da pirataria.

Portanto o que está sendo explicitado nesta pesquisa é que existem esforços feitos pelos países do mundo material para capturar os fluxos de informação imaterial do ciberespaço, e como o acesso à tecnologia afeta essas iniciativas em diferentes partes do mundo. Como dito antes, apesar do mundo digital ser sua própria dimensão, ele ainda pode ser afetado por tomadores de decisões e agentes que são primariamente do mundo material, mas podem possuir presença e influência dentro das redes, como Estados Soberanos e empresas privadas com poder político, e até mesmo grupos não estatais que estão usando das redes para conseguir realizar seus objetivos. Esta é uma questão sofisticada e complexa que não poderá ser respondida nesta dissertação, devido a insuficiência de material empírico e literatura sobre o tema de como a territorialidade, ou falta desta, afeta o ciberespaço. Independente disto, o potencial para futuras discussões sobre este tema em particular ainda torna estas observações dignas de atenção. Nesta sessão, e na sessão 3.3 do próximo capítulo, estas tentativas de se conter o "gênio na garrafa" serão expostas, assim como seu grau de desenvolvimento e sucesso.

Com relação à crimes ocorridos no mundo material, os Estado Unidos estão na liderança em termos de iniciativas de prevenção, e mesmo com relação aos cibercrimes, o país ainda é responsável por facilitar atividades de cibersegurança dentro de seu território nacional há mais

de uma década, como a empresa internacional de serviços profissionais Klynveld Peat Marwick Goerdeler (KPMG) afirma em sua pesquisa sobre os efeitos do cibercrime em diferentes governos:

> "*The US Federal Bureau of Investigation (FBI) has established a separate division to address cyber crime in a coordinated manner.60 In October 2010, the FBI arrested more than 90 people, who were believed to be engaged in an international crime syndicate that hacked into US computer networks to steal US$70 million. Hackers used spam email to target the computers of small businesses and individual users. By gaining access to users' passwords and bank account details, the hackers were able to transfer money from those accounts*" (KPMG, 2011).

Cibersegurança é uma das pautas prioritárias da política estado-unidense, isso não é nenhuma surpresa, considerando que o país é um dos principais alvos de ataques cibernéticos. Como afirmado ao final da sessão 2.1, a população civil está tão acostumada com as tecnologias de informação por conta da dependência que o país possui delas. Esta dependência não deveria ser vista como algo negativo, uma vez que os EUA são um país continental com uma população de 332 milhões aproximadamente, portanto sendo necessário o uso de tecnologias que venham a facilitar a administração da nação. Porém devido a isso, também é crucial entender as ameaças que surgem dessa dependência e devidamente respondê-las, tal qual está descrito nos passos de prevenção ao ciberisco.

Não obstante, os EUA têm tido algumas dificuldades para se reestabelecer como líder global dos esforços contra os cibercrimes, e isto está relacionado aos problemas internos do país, especialmente após a administração Trump. Em 2020, enquanto agências federais, estaduais e locais tomavam medidas para combater cibercrimes, a gestão do ex-presidente americano não forneceu recursos, não coordenou os esforços, e negou os riscos que foram expostos na infraestrutura eleitoral do país, riscos estes que podem ter contribuído para o resultado da eleição de Trump, onde há suspeitas de interferência externa (THIRD WAY, 2020).

Todavia, o país ainda se mantém como um dos principais provedores de cibersegurança globais, mesmo que, atualmente, sua habilidade de contra-atacar seja menor do que sua habilidade de se proteger de ameaças. Os principais desafios para o país agora são justamente melhorar as capacidades de identificação, prevenção e punição de ciberataques, visando diminuir o vão entre o número de ataques executados contra o país ao ano, e o número de prisões de cibercriminosos que são realizadas no mesmo ano, também conhecido como "*cyber enforcement gap*". Além disso, também é necessário tentar reduzir a interferência externa de

atores internacionais no país, como grupos terroristas, ou outro Estados que visem interferir com a infraestrutura crítica do país.

Porém esta analise não é focada apenas nas falhas ou dificuldades nos processos de prevenção ao cibercrime nos EUA, mas sim nos pontos positivos que podem ser aproveitados e replicados em outras nações ao redor do mundo, principalmente no Sul Global. Neste âmbito, vale ressaltar que por mais de 20 anos os EUA, assim como a Rússia, tem sido protagonista em rodadas de acordos internacionais que visam monitorar o espaço cibernético, e determinar o comportamento dos Estados com relação aos crimes cometidos dentro deste espaço. Em 2010 e 2013, o Grupo de Especialistas Governamentais (GGE) da ONU, elaborou relatórios que foram responsáveis por incorporar o ciberespaço e a cibersegurança dentro do *framework* já existente das Relações Internacionais, possibilitando a otimização do uso da soberania estatal e das leis internacionais dentro do ciberespaço, que passou então a não ser mais uma "terra de ninguém" sem fronteiras, e os Estados passaram a ter responsabilidades (LEWIS, 2017).

Cibercrimes devem ser vistos como uma ameaça transnacional, e como tal exigem uma solução internacional. Vários países podem se beneficiar de uma medida de segurança baseada nas experiências nacionais de uma nação específica, que podem ser usadas como parâmetro para garantir a segurança do grupo. É por esta razão que, apesar do abismo tecnológico existir e ser responsável pelas diferentes formas em que a cibersegurança se manifesta no binário Norte-Sul, é necessário observar como as nações do Norte estão lidando com este tipo de fenômeno, dentro e forra de suas fronteiras. Negociações e Organizações internacionais também oferecem um compartilhamento de informações que é muito benéfico para países menos desenvolvidos tecnologicamente, já que isto oferece uma oportunidade para aprender sobre a postura de segurança de outras nações, e como estas se protegem de ciberataques.

Quanto as providências tomadas dentro do território nacional dos EUA, a cibersegurança tem se tornado tópico de debates recentemente. No painel intitulado "*The Business of Cybersecurity*", realizado em 2018 durante a BEYA STEM *Global Competitiveness Conference* os palestrantes expressaram preocupações sobre a falta de "*cyber awareness*" da população, o que é realmente preocupante considerando que os órgãos de prevenção de cibercrimes no país estão constantemente exigindo que o público faça sua parte também, assim como é responsabilidade dos cidadãos cuidar de seu próprio bem-estar. Dentre os palestrantes estavam o coronel Terrence Adams que era o diretor de comunicações, e oficial chefe de informações da Força Aérea Americana na época. O vice-presidente da Universidade AT&T, uma organização de ensino que presta seus cursos inteiramente online, Gary Gadson também

era um dos palestrantes, e o quadro foi moderado por Mike Black, que foi comandante de comunicações da casa branca durante as administrações Bush e Obama (ZACHER, 2018)

Durante os debates estes palestrantes concordaram que o governo dos EUA deveria fazer mais por sua população em um estágio de formação de seu caráter e não esperar que organizações privadas fiquem encarregadas de treinamentos que envolvam o ciberespaço. Portanto os cidadãos americanos deveriam ser ensinados como se comportar dentro da internet desde a escola primária, através de aulas de informática que abordem os perigos do cibercrime. Há uma crescente demanda de companhias e organizações públicas em uma futura força de trabalho que seja minimamente competente para lidar com os desafios do ciberespaço, e seria benéfico que um programa de ensino básico fosse desenvolvido. Este tipo de medida proativa por parte do Estado pode também ser benéfica para outros países que desejam apresentar as ideias de cibersegurança e ciberisco mais cedo o possível para suas populações.

Além das propostas de medidas educacionais para aumentar a "cyber awareness" e das iniciativas internacionais para o combate ao cibercrime, os EUA também contam com mecanismos nacionais para o combate a esse fenômeno dentro de seu território, através do Poder Executivo, que possuem grandes benefícios para o sistema internacional também. Com relação aos órgãos de manutenção da lei e da ordem nacionais americanos, é importante ressaltar que o Departamento de Segurança Doméstica (DHS) trabalha com outras agências federais para garantir que as investigações de cibercrimes tenham o devido impacto, e possam interromper atividades cibercriminais. Além da previamente citada CISA, O DHS também possui dois componentes que têm sido essenciais para o combate à criminalidade digital: o Serviço Secreto e o Departamento de Imigração e Alfândega (DHS, 2023).

O Serviço Secreto americano mantém forças tarefas dedicadas à identificação e localização de cibercriminosos internacionais como a Força Tarefa de Crimes Eletrônicos (ECTF) que foi criada orginalmente como uma força tarefa local de Nova Iorque em 1995, porém devido ao seu sucesso o Congresso demandou que uma rede nacional para prevenção, investigação e detecção de crimes eletrônicos, incluindo potenciais ataques terroristas contra infraestrutura crítica e sistemas de pagamentos financeiros, fosse estabelecida (U.S. Secret Service, 2023). A seção de ciber inteligência do Serviço Secreto americano já contribuiu para a prisão de cibercriminosos transnacionais responsáveis pelo roubo de informações de cartões de crédito que causaram um prejuízo de 600 milhões de dólares para instituições de varejo e financeiras, além do Serviço Secreto também administrar o Instituto Nacional de Computação Forense (National Computer Forensic Institute), que é responsável pelo compartilhamento de

informações e treinamento de profissionais da polícia, de promotores e de juízes para combater o cibercrime (CISA, 2023).

O Departamento de Manutenção da Imigração e Alfândega (Immigration and Customs Enforcement) da Segurança Nacional (*Homeland Security*) possui dois parceiros que são extremamente eficazes em questões domésticas de segurança. Primeiramente, o Departamento de Investigações para a Segurança Doméstica (HSI), que é o principal braço investigativo da Segurança Nacional, e é responsável pela investigação de crimes transnacionais, especificamente aqueles que exploram a infraestrutura crítica global, ou seja, a missão deste departamento é interromper e punir atividades terroristas, e outras organizações que visem ameaçar ou explorar as leis de alfândega ou imigração dos Estados Unidos (ICE, 2023). O HSI possui autoridade para investigar crimes envolvendo tecnologia usada para facilitar atividade criminal como imigração ilegal, terrorismo, fraude, roubo de informações e tráfico de drogas. Junto com o ICE, estes parceiros também oferecem serviços técnicos de computador que apoiam, tanto investigações domésticas, quanto internacionais sobre crimes transfronteiriços.

O segundo parceiro é o Centro de Cibercrimes (C3), que é um componente especializado do HSI, e tem como prerrogativa supervisionar investigações de atividade criminal ciber-relacionada, e também provem apoio forense, de inteligência e investigativo para todos os órgãos relacionados com a Segurança Nacional. A missão do C3 pode ser resumida em: se manter atualizado com as novas tecnologias de computadores e ciber processos emergentes; usar estas novas tecnologias para proativamente combater a atividade cibercriminal e reduzir o ciberisco, através da redução das vulnerabilidades; disseminar informações sobre novas tendências, riscos, procedimentos, lições aprendidas e pistas que podem ser usadas em investigações para escritórios de investigação criminal, organizações transnacionais de inteligência, e outras agências de manutenção da lei ao redor do mundo; apoiar investigações sobre atividades cibercriminais e sobre possíveis vulnerabilidades, utilizando tecnologia de ponta para realizar métodos ciberinvestigativos e técnicas de computação forense (ICE, 2023).

Além dos Estados Unidos, outros países também criaram mecanismos internos para combater esta ameaça. No Reino Unido crimes cibernéticos são considerados ameaças de nível 1, igualando-os a incidentes de terrorismo internacional e outros incidentes de extrema magnitude, e superando a ameaça apresentada por armas nucleares. Em 2008, a unidade de e-crimes da Polícia Central (PCeU) foi estabelecida para combater cibercrimes dentro das fronteiras do país, colaborando com agências de segurança públicas e privadas (KPMG, 2011). Em um relatório publicado em 2013 pela Câmara dos Comuns do parlamento britânico, foram

reportadas: as definições de cibercrime, as estratégias governamentais de cibersegurança, o papel dos órgãos de manutenção da lei e da ordem e executivos, como provedores de serviços online podem proteger os dados de seus clientes e quão efetivas são as camapanhas públicas para o aumento do "cyber *awareness*".

As definições do Reino Unido para cibercrimes são baseadas nas definições clássicas já apresentadas no primeiro capítulo, e também são próximas em categoria das definições usadas pelos órgãos de monitoramento e segurança dos Estados Unidos, mas resumidamente, as definições são focadas nos parâmetros de crimes digitais "puros", ou seja, quando um sistema digital é ao mesmo tempo o alvo e o meio pelo qual o ataque é conduzido, crimes digitais "existentes", que já eram efetuados antes do advento da internet, mas que tiveram sua intensidade aumentada para uma escala industrial após a criação dela, e crimes "tradicionais" que são facilitados pelo uso da internet, como tráfico de drogas. A estas três definições, também foram incorporadas definições apresentadas pela Comissão Europeia em 2007 sendo elas: formas tradicionais de crimes cometidas utilizando redes de comunicação eletrônica e sistemas de informação, publicação de conteúdo ilegal utilizando mídias digitais e crimes específicos de redes eletrônicas (HOUSE OF COMMONS, 2013). É importante ressaltar que mesmo após a saída do Reino Unido da União Europeia pelo Brexit, as leis e definições da Comissão ainda são aplicáveis:

> "*The Withdrawal Agreement provides for rules on winding down ongoing police and judicial proceedings in criminal matters involving the United Kingdom*. *Any such proceedings should still be completed according to the same EU rules.*" (EUROPEAN COMMISSION, 2020)

A estratégia de cibersegurança no Reino Unido pode ser encontrada no Programa Nacional de Cibersegurança (NCSP) que foi lançado em 2010, e coloca em termos claros os objetivos de políticas de reforço da lei do ciberespaço, incluindo criar novas capacidades para Agência Nacional de Crimes de julgar cibercrimes, e tornar estes tipos crimes como parte do *mainstream* operacional da polícia metropolitana. Estas novas capacidades podem ser facilmente adquiridas através da contratação de especialistas em cibercriminologia pelas organizações de segurança, e pelo compartilhamento de informações pertinentes a investigações de cibercrime e cooperação entre organizações. Também é destacada a necessidade de se criar um sistema de denúncias simples e de fácil acesso para os cidadãos, já que grande parte dos cibercrimes não são reportados por falta de mecanismos de denúncia. Também são necessárias mudanças legislativas para atualizar as leis e garantir que permaneçam eficientes, levando em consideração o espaço virtual. Encorajar as cortes de justiça para usar

seus poderes para impor sanções e punições aos cibercriminosos, sejam eles indivíduos ou organizações.

O Reino Unido também precisou redefinir categorizações de crimes, que antes não eram vistos como cibercrimes. Um exemplo seria o crime de fraude executado através de computadores, que eram definidos como crimes de fraude, ao invés de serem interpretados como crimes digitais. Crimes de negação de serviço[15] seriam qualificados como crimes de extorsão por conta da intenção do criminoso, ao invés de levar em conta os métodos pelos quais o crime estava sendo realizado (HOUSE OF COMMONS, 2013). Todas essas interpretações incorretas afetam a *cyber awareness* da população civil, tornando difícil a denúncia desses tipos de cibercrime. Ilustrativamente, uma pessoa que teve suas informações bancárias fraudadas provavelmente iria no banco que a tem como cliente para tentar resolver esta situação, quando na verdade deveria estar indo à polícia. Este problema foi facilmente consertado através da criação de mais websites, e plataformas de denúncia que utilizam definições mais abrangentes para crimes digitais.

Outro problema também era a falta de cooperação com as agências bancárias que interpretavam como sendo mais fácil simplesmente reembolsar as vítimas de pequenos furtos, do que realizar uma investigação juntamente à polícia metropolitana. Assim como o primeiro problema, isto foi facilmente resolvido pelo governo tomando medidas para aumentar a cooperação com estas agências, e a imposição da obrigação dos bancos em denunciar e mostrar seus relatórios para as forças de cybersegurança, já que pequenos cybercriminosos muitas vezes acabam impunes, mas ainda são capazes de obter grandes lucros.

O governo britânico também monitora fortemente redes sociais, considerando a maioria delas incapazes de proteger as informações confidenciais de seus usuários, portanto sendo necessárias ações do Estado para lidar com as consequências da falta de segurança presente nestas redes. Como já exposto anteriormente por Shoshana Zuboff, as redes sociais possuem sua responsabilidade quando cibercrime é relatado, muitas vezes porque a ação de extrair padrões de comportamento de seus usuários é em si cibercriminosa, o Reino Unido aponta as descobertas da empresa de segurança digital americana RSA, como evidência de que as redes sociais também são responsáveis, ainda que sem intenção, de fornecer dados de seus usuários para cibercriminosos, permitindo que possam planejar um ataque com meses de antecedência, através de processos de Engenharia Social que as redes sociais tornam possíveis:

[15] Denial of Service (Dos)

> "(...) *attackers are increasingly gathering intelligence on their targets, sometimes months in advance of an attack, using social media and other means to understand which individuals possess the assets they want, and crucially how to tailor, or "socially engineer", their attacks to increase their likelihood of success. Indeed cyber attackers prefer using social engineering in this way because in so doing they are able to evade traditional perimeter controls more easily.*" (RSA, 2013, apud HOUSE OF COMMONS, 2013)

Por fim o Reino Unido possuí projetos de aumento da *cyber awareness* através de campanhas educativas que podem ter seu alcance ampliado graças a uma maior parceria com o setor privado, utilização de plataformas como televisão e cinema, para poder atingir um público maior, tecer campanhas específicas direcionadas a diferentes segmentos da sociedade, particularmente os mais vulneráveis e aumento da verba do governo para ser gasta na elaboração destas campanhas. O governo ainda recomenda que informações sobre como manter informações pessoais seguras sejam incorporadas a todos os serviços online que necessitem de informação pessoal de seus usuários, e também que se tenha um esforço maior por parte dos pais e das escolas para educar crianças que estão descobrindo o ciberespaço pela primeira vez, pois geralmente os cibercriminosos buscam explorar vulnerabilidades familiares utilizando as crianças da família.

Como último exemplo de iniciativas do Norte Global para conter o cibercrime, vale citar o trabalho da União Europeia que hoje abarca 27 nações ao todo no bloco, e cujas medidas segurança valem para praticamente todos os Estados-membros. Em 2010, a agência de manutenção da lei da UE, também conhecida como Europol, criou a Força Tarefa contra Cibercrimes da União Europeia, que incluiu membros da Europol, do corpo de justiça cooperativo da UE, o Eurojust, e da Comissão Europeia (KPMG, 2011). A organização se encontra duas vezes ao ano, e além de promover segurança para os Estados-membros do bloco, também pretende promover a disseminação de informações para países associados como Reino Unido, Dinamarca, Islândia, Noruega e Suíça.

A Força Tarefa tem a difícil e ambiciosa missão de promover uma abordagem harmoniosa dentro da União Europeia para o uso criminoso de informações, de tecnologia da informação e também quais ações os países do bloco devem tomar na luta contra o cibercrime. Mais importante ainda é transformar o território do bloco europeu em um local hostil para cibercriminosos, de fato, as medidas de prevenção e punição ao cibercrime realizadas pela União Europeia, parecem ser uma das mais agressivas respostas transnacionais ao fenômeno do cibercrime, pelo menos em termos de discurso. Entretanto, uma abordagem concisa dentro de

uma organização internacional deste calibre necessita de um alinhamento das prioridades e dos interesses dos países que fazem parte da união.

Isso parece ser uma tarefa de proporções quase impossíveis devido ao número maciço de serviços públicos prestados a uma quantidade enorme de cidadãos europeus por parte do bloco, o que também demanda uma manutenção enorme, e por conseguinte o ciberisco. As inerentes diferenças entre os próprios países também não devem subestimadas. O próprio Centro Europeu de Cibercrimes aponta que nem todos os países membros da União Europeia chegaram em um nível de conhecimento aplicado para começar a lutar efetivamente contra o cibercrime, tendo uma falta de hardware e software para realizar processos de cibercriminologia forense simples. Por conta disso, um dos principais objetivos da Força Tarefa é justamente o aumento dessas capacidades através de fundos adquiridos pelo bloco europeu, além de treinamento para os funcionários dos serviços de segurança que fica a cargo do Grupo Europeu de Educação e Treinamento contra o Cybercrime (ECTEG) em cooperação com a CEPOL (EUROPEAM CYBERCRIME CENTER, 2013).

A União Europeia baseia suas respostas ao cibercrime na Convenção Sobre Cibercrime, já citada neste trabalho, que foi assinada em 2001 em Budapeste, e permanece sendo considerada pelo Conselho da Europa como sendo o único instrumento internacional de natureza vinculante para o combate aos crimes digitais. Uma parte grande dos fundos da UE, cerca 80 milhões de euros, foi utilizada para criar o projeto Horizon 2020, que foi o oitavo programa de pesquisa e inovação, seguindo os moldes europeus, e foi ativo nos anos 2014 até 2020. A importância deste projeto é que dele foi criado um projeto auxiliar de pesquisa e inovação para segurança específico para lidar com respostas a crises chamado DARWIN (EUROPEAN COMMISSION, 2017). Este projeto foi responsável por desenvolver as Regras de Gerência da Resiliência Europeia (*European Resilience Management Guidelines*), que priorizam 5 ameaças à infraestrutura crítica do bloco europeu que estão em constante evolução, sendo elas: clima extremo, pandemias, acidentes ou falhas técnicas, atos de terrorismo, e é claro, ameaças cibernéticas (GAITANIDOU, BELLINI & FERREIRA, 2018). Com um orçamento de 5 milhões de euros, o projeto DARWIN foi responsável por elevar os cibercrimes como uma ameaça transnacional que deveria ser tratada com seriedade.

A UE também criou a Agência da União Europeia para Cibersegurança (ENISA), que foi aberta em 2005 para regular medidas de cibersegurança ao em todo bloco. A ENISA possui uma grande importância, sobretudo com relação a medidas que visam aumentar a *cyber awareness*, sendo esta organização responsável por campanhas educacionais direcionadas ao

público, como o Mês da Cibersegurança Europeia, que ocorre todos os anos durante todo o mês de outubro e inclui conferências, oficinas, treinamento, webnários, apresentações, e outros eventos que almejam promover a segurança digital e a cyber higiene. A ENISA considera que o maior fator que promove o cibercrime na atualidade é justamente a falta de percepção dos usuários da internet e de sistemas de informação sobre o ciberisco, e pretende então realizar uma mudança comportamental partindo das organizações transnacionais europeias, para os tomadores de decisões e chefes de Estado, até o público, e oferece ferramentas e instruções para aumentar a resiliência cibernética por toda Europa (ENISA, 2023).

Apesar do Norte Global estar na liderança das medidas contra cibercrime, e ter conquistado inúmeras vitórias para sua contenção, é importante lembrar que a dependência de conexões digitais é muito maior nesses países, o que torna necessário que quantidades enormes de recursos sejam alocadas para a proteção digital. No caso da União Europeia por exemplo, pode-se observar que o problema é considerado grave, e, portanto, os países do bloco foram capazes de utilizar suas reservas para fornecer verbas maciças para o programa de desenvolvimento Horizon em pouquíssimo tempo, e com resultados invejáveis. Porém, as medidas de cibersegurança ocorrem de forma diferente no Sul Global, assim como os próprios cibercrimes também. Se enganam aqueles que pensam que por conta dos países do Sul serem menos conectados, estariam eles melhor protegidos contra o cibercrime. Esta pesquisa já revelou que, apesar de isso talvez ser verdade para certos crimes, que o Reino Unido define como “puros”, utilizando o próprio sistema para atacá-lo, os países do Norte Global já perceberam que vários crimes tradicionais podem ser facilitados com a utilização de tecnologia de comunicação e informação, que tem se tornado mais e mais acessível nos últimos anos, inclusive em países do Sul. Para começar a entender como o cibercrime se manifesta, seus efeitos no Sul Global, e como podem ser prevenidos, primeiro precisa-se observar outro importante fenômeno: o abismo tecnológico.

Capítulo 3. O ABISMO TECNOLÓGICO

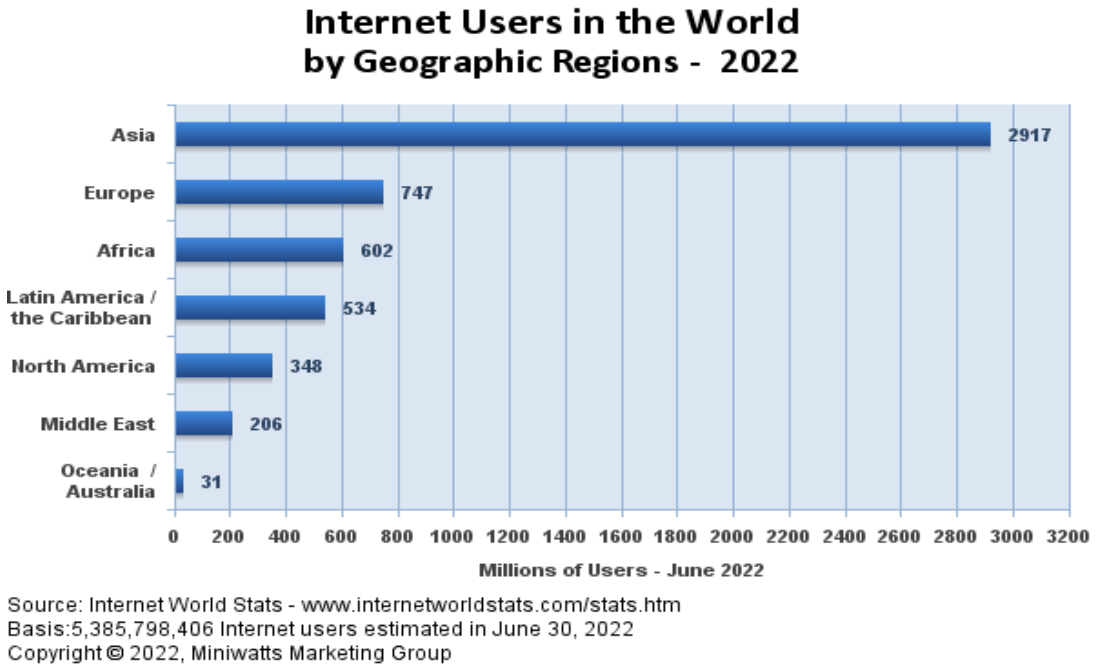
3.1 A Desigualdade Digital

O abismo tecnológico, também conhecido como abismo digital, em sua essência, é um termo utilizado para se definir a desigualdade existente entre indivíduos que possuem acesso de qualidade à tecnologia de informação, primariamente a internet, e a quantidade de pessoas que possuem esse acesso. Atualmente, o acesso a este tipo de tecnologia é de extrema

importância em diversas áreas do crescimento individual de uma pessoa, como o exercício da cidadania, por exemplo: durante processos eleitorais onde o eleitor pode ter acesso a seu título e seu comprovante de votação pelo celular; para questões de saúde, através da utilização de aplicativos como o Conecte SUS, que fornece informações sobre vacinações e alertas de segurança envolvendo epidemias; e também para o estudo e a inserção do indivíduo no mercado de trabalho, devido à aulas de modelo de educação à distância, procura por vagas de emprego e comunicação com empregadores.

É fácil entender, portanto, que se a desigualdade a este acesso vem de um sintoma estrutural, se caracterizará em um cenário onde as elites possuem tecnologia suficiente para realizar todas as suas obrigações e conquistas, em uma sociedade que se torna mais e mais conectada, enquanto as massas não possuem tecnologia e vão sendo deixadas ao relento a passos rápidos, pois o desenvolvimento tecnológico não dá sinais de reduzir sua velocidade em um futuro próximo. Porém a capacidade de acessibilidade da tecnologia não deve ser subestimada. No início dos anos 2000, especialistas se preocupavam com o grande abismo existente entre os principais polos tecnológicos do mundo: América do Norte, a Europa Ocidental e Japão; e os países da América Central e Sul, do Oriente Médio e do Sudeste Asiático. O site "*Internet World Stats*" que monitora o uso da internet ao redor do globo anualmente, afirma que em 2000 apenas 361 milhões de pessoas utilizavam a internet, o que representava de 4% a 5% da população mundial daquele ano, e mal representa 2/3 dos usuários do Facebook hoje em dia (SOLARWINDS, 2010).

Porém se comparado a 2010, pode-se observar um salto exponencial no número de pessoas que possuíam pelo menos algum tipo de acesso à internet, cerca de 1.967 milhões de usuários. Em dezembro de 2021, cerca de 5 bilhões de pessoas possuíam acesso à internet (INTERNET WORLD STATS, 2021). Para fins de comparação, a população mundial em 2023 é de 7.8 bilhões. O site vai ainda mais além apresentando suas estimativas para 2022 em forma de gráfico:



(Fonte: Internet World Stats, 2022)

Os 3 grandes polos globais em 2022 correspondiam a aproximadamente 24,4% dos usuários globais de internet, com outros países da Ásia, África e América Latina, superando com certa folga, a quantidade de pessoas que tinham acesso à internet. Então um argumento poderia então ser feito que o abismo tecnológico não representa mais o mesmo problema de antes, mas é aí que se encontra o erro. A quantidade de pessoas que possuem acesso à internet é apenas uma faceta de um problema mais complexo, especialmente quando cibersegurança e cibercrimes estão envolvidos. Não só as pessoas precisam ter acesso a internet, como este acesso também precisa ser de qualidade. Além disso, o que ocorreu fui uma mudança bruta no número de usuários por país, e apesar de 10, no caso de 2010 a 2020, corresponderem a uma quantidade de tempo considerável para um ser humano, isso não necessariamente se traduz em projetos competentes e impactantes para conter os malefícios trazidos por estas tecnologias, especialmente nas regiões do globo que tiveram acesso somente recentemente à internet.

Isto não é um argumento tecno determinista, no sentido de a tecnologia de informação ser puramente boa, ou ruim para a vida dos indivíduos. Pelo contrário, como dito anteriormente a tecnologia de informação auxilia na própria administração estatal de países continentais como Brasil, EUA, China e Rússia, permitindo o encurtamento das distâncias entre as pessoas, e a aceleração da burocracia, além de ser muito importante para a geração de novos tipos de emprego no setor privado e público. Entretanto ela também vem carregada de elementos que podem sim ser negativos. Como exemplo, a questão do "*cyber awareness*" explorada no

capítulo 2, que é crucial para o quebra cabeça da segurança digital, ainda é foco de inúmeras campanhas educacionais nos países do Norte Global, pois os cidadãos demoram a desenvolvê-la para aumentar sua segurança individual no ciberespaço. Nos países do Sul Global a situação pode ainda ser mais difícil. A diferença na qualidade de conexões internet também interfere nas tentativas dos Estados de monitorarem os cibercrimes, e sua ocorrência.

Primeiramente, para entender como o abismo foi constituído, e a situação atual, é necessário compreender como ele se relaciona com a divisão internacional do trabalho e com fatores geográficos. Existe uma falta de investimento nos setores de tecnologia e informação por parte dos países da América Latina e, apesar de países do Norte Global serem em parte culpados por isso, isto também ocorre por conta de fatores particulares da região, a abundância de recursos naturais por exemplo. Paulo Roberto Feldmann afirma que:

> "A abundância de recursos naturais na América Latina tem sido apontada como uma explicação importante para a baixa preocupação com a inovação que predomina na região. Fairbanks e Lindsay (2000) afirmam que os empresários locais tendem a pressupor que as vantagens em recursos naturais, matérias-primas abundantes e mão-de-obra barata proporcionam a eles posições de liderança nos mercados exportadores e, assim, deixam de criar condições para a inovação. Adotando essa filosofia, são constantemente ultrapassados por países da Ásia ou da África, que conseguem ou baratear ainda mais o custo de sua mão-de-obra, ou entram no mercado internacional vendendo um recurso natural a um preço ainda mais baixo do que vinha sendo praticado por eles." (FELDMAN, 2009)

É evidente que isto faz parte do fenômeno da "terceiromundialização" que assola os países do Sul Global, sendo, claro, uma consequência direta da colonização exercida por países do Norte Global, devido a criação de elites coloniais que até hoje moldam a economia e os processos de extrativismo dentro das ex-colônias. Ainda há também interesses de países que por décadas lideraram os mercados de informação de se manter no topo, às custas do desenvolvimento de países do Sul. Um exemplo recente e bastante prático disto é a atual disputa pelo 5G ocorrendo entre Estados Unidos e China. Apesar dos EUA usarem a retórica de que o 5G chinês é uma ameaça à segurança nacional devido a China utilizar essa tecnologia para monitoramento, vigilância e espionagem, o problema é ainda mais crítico para os americanos. Em 2020, o Procurador Geral William P. Barr afirmou que permitir que a China estabelecesse dominância no mercado de tecnologia de informação representaria uma ameaça direta para o futuro da economia do país (BENNER, 2020). Fora isso, em 2021 a economia digital já movimentava 25% dos negócios do mundo (INSIDE, 2021), e esse número só tende a aumentar.

É aqui que o trabalho do professor Ha-Joon Chang mostra seu valor inestimável para o entendimento do Abismo Tecnológico. Em seu livro "*Kicking Away the Ladder*", Chang explicita que a história do desenvolvimento econômico capitalista nos Estados Unidos e na Europa foi construída devido a políticas protecionistas e de restrição ao desenvolvimento dos países periféricos no sistema internacional. Neste caso, as políticas de desenvolvimento internacional, cujo establishment é controlado pelos países centrais do capitalismo, seria responsável pelo estabelecimento de "boas políticas", ou "boas instituições" para que estes países fossem capazes de promover seu desenvolvimento. "Boas políticas" sendo entendidas aqui como políticas macroeconômicas restritivas, liberalização do comércio e do investimento internacional, privatização e desregulamentação do Estado. Enquanto as "boas instituições", são aquelas encontradas dentro dos países centrais: democracia, boa burocracia, um poder judiciário independente, direitos de propriedade privada e intelectual fortemente protegidos, instituições financeiras, sendo de extrema importância a criação de um Banco Central politicamente independente, e uma governança coorporativa voltadas para o mercado financeiro (CHANG, 2002).

O que Chang tenta explicitar em seu livro, é que: os países centrais do sistema capitalista, foram capazes de encontrar uma escada para seu desenvolvimento econômico, tecnológico e social, entretanto para se manterem as condições necessárias para que eles continuassem em sua posição dentro do sistema, eles "chutaram" esta escada para que mais países não pudessem escalá-la. Na próxima sessão, vale a citação de certos acontecimentos recentes que mostram que é possível sim outros países subirem a escada do desenvolvimento, porém não sem suas dificuldades e desaprovação dos países que já se encontram no topo dela, pois o chute à escada é também movido pelo medo dos países centrais de serem suplantados, e uma vez que privilégios dentro do sistema são estabelecidos, dificilmente seus detentores abrirão mão deles. O autor propõe que, as políticas e instituições criadas pelos países centrais e que hoje são exportadas para os periféricos do sistema, o que é passível de críticas sim, porém geralmente os críticos se esquecem que as mesmas políticas e instituições não necessariamente eram adotadas pelos países centrais quando estes ainda estavam no seu processo de desenvolvimento. Na verdade, se observa exatamente o contrário nos casos de maior sucesso de países como Estados Unidos e Inglaterra que, apesar de serem vistos como a vanguarda do *laissez-faire*, utilizaram de políticas intervencionistas nas primeiras fases de seu desenvolvimento para alcançar sua posição atual.

Chang argumenta que as políticas de industrialização, comércio e tecnologia (ITT em inglês) utilizadas pelos países centrais, chamados pelo autor de NDCs (*Now Developed*

Countries), durante seu desenvolvimento foram exatamente opostas as que são afirmadas pela ortodoxia do pensamento econômico moderno, e que são recomendadas para serem utilizadas por países periféricos dentro do sistema. No caso da Inglaterra, por exemplo, que possui um histórico de proibição de importações de produtos superiores aos seus de países que muitas vezes eram suas colônias durante os séculos XVII e XVIII, permitindo assim seu próprio desenvolvimento industrial e tecnológico, ao mesmo tempo que impedia o florescimento de invenções e produtividade superior vindo de países como a Índia. Somente quando a Inglaterra já se encontrava na liderança dos processos tecnológicos, foi quando o regime de *laissez-faire* foi finalmente adotado pelo país. Como o autor aponta:

> "*It is important to note here that Britain's technological lead that enabled this shift to a free trade regime had been achieved 'behind high and long-lasting tariff barriers'. It is also important to note that the overall liberalization of the British economy that occurred during the mid-nineteenth century, of which trade liberalization was just a part, was a highly controlled affair overseen by the state, and not achieved through a laissez-faire approach.48 It should also be pointed out that Britain 'adopted Free Trade painfully slowly: eighty-four years from The Wealth of Nations to Gladstone's 1860 budget; thirty-one from Waterloo to the ritual victory of 1846'.*" (CHANG, 2002)

Chang também aponta que no caso dos Estados Unidos foram usadas várias tarifas ao longo do século XVIII, XIX e XX para proteger a nascente indústria americana e o desenvolvimento tecnológico do país, especialmente na década de 1930 com a tarifa Smoot-Hawley, vista por outros autores como uma grande medida antagônica para o livre comércio, ainda mais com os EUA sendo o principal credor internacional e inimigo das regulações comerciais. Porém, como mostrado pelo autor, isso não foi uma mudança brutal no paradigma comercial americano, visto suas tarifas passadas de viés protecionista. Como pode ser observado na imagem a seguir, a tarifa apenas aumentou marginalmente o nível de protecionismo da economia estado-unidense da época:

Table 2.1
Average Tariff Rates on Manufactured Products for Selected Developed Countries in Their Early Stages of Development
(weighted average; in percentages of value)[1]

	1820[2]	1875[2]	1913	1925	1931	1950
Austria[3]	R	15–20	18	16	24	18
Belgium[4]	6–8	9–10	9	15	14	11
Denmark	25–35	15–20	14	10	n.a.	3
France	R	12–15	20	21	30	18
Germany[5]	8–12	4–6	13	20	21	26
Italy[6]	n.a.	8–10	18	22	46	25
Japan	R	5	30	n.a.	n.a.	n.a.
Netherlands[4]	6–8	3–5	4	6	n.a.	11
Russia	R	15–20	84	R	R	R
Spain	R	15–20	41	41	63	n.a.
Sweden	R	3–5	20	16	21	9
Switzerland	8–12	4–6	9	14	19	n.a.
United Kingdom	45–55	0	0	5	n.a.	23
United States	35–45	40–50	44	37	48	14

(Fonte: BALROCH, 1993 apud CHANG, 2002)

Internacionalmente falando, o autor afirma que mesmo no presente, com o colonialismo e imperialismo sendo elementos internacionais do passado, ainda assim os países centrais (NDCs) podem exercer grande influência sobre os periféricos através das instituições econômicas internacionais e políticas de governança internacional, que tem como uma de suas consequências prejudicar o desenvolvimento tecnológico desses países, além do econômico, e o que por sua vez impede a alocação de recursos em áreas de infraestrutura crítica, complicando ainda mais a conectividade e a capacitação de seus cidadãos, lhes privando da habilidade de reconhecer e se prevenir de crimes tecnológicos, e também afetando a capacidade de resposta dos Estados em combater os cibercrimes.

O autor propõe a discussão de que, através políticas de governança, como leis de patentes, diretrizes da OMS e do FMI, e medidas anti-protecionistas, os Países Agora Desenvolvidos, ou NDCs, estariam "chutando a escada" do desenvolvimento que subiram e impedindo os outros países de escalar, já que os NDCs não foram submetidos a essas políticas durante seu desenvolvimento. O Abismo Tecnológico, poderia então ser uma consequência direta das políticas ditadas pelos NDCs para os países em desenvolvimento. Ou seja, a suposta "ineficiência" que os países em desenvolvimento apresentam para assimilar e conter ameaças virtuais, pode ser fruto de políticas comerciais e de desenvolvimento que são elaboradas para o controle do desenvolvimento destas nações. Apesar disso o professor aponta:

> "*I do accept that this "ladder kicking" may be done out of genuine (if misinformed) goodwill. Some of those NDC policymakers and scholars who make the recommendations may be genuinely misinformed: thinking their own countries developed through free trade and other "laissez faire" policies, they want developing countries to benefit from these same policies. However, this makes it no less harmful for developing countries.*" (CHANG, 2002)

As lições oferecidas por Chang, são importantes por outra razão. Ele conclui que a melhor opção seria deixar os países em desenvolvimento escolherem as políticas que sejam adequadas a seu nível de desenvolvimento, para assim avançar rumo ao fim da escada. Isto também se aplica as políticas de prevenção do Cibercrime, já que o Sul não deve almejar imitar políticas que deram certo no Norte, mas sim, de acordo com suas próprias necessidades e realidade, desenvolver políticas que se adequem aos problemas vividos dentro desses países. Isso já está acontecendo com certos países do Sul como a China, entretanto a probabilidade do ato de "subir a escada" ser respondido com hostilidade também é grande, vide o próprio caso chinês. Na próxima seção serão analisadas as formas que os países periféricos estão encontrando de reduzir, e até mesmo superar o abismo, e por consequência, promover medidas proativas de combate ao cibercrime e promoção da cibersegurança, que serão mais especificamente analisadas na seção 3.3.

3.2 Superando o Abismo

Apesar das pré-condições impostas pelos países centrais, já é possível observar que certos países estão encontrando suas próprias maneiras de abordar as questões derivadas da tecnologia, como direito de propriedade intelectual de tecnologia de comunicações, e é claro, cibercrimes e cibersegurança. O melhor exemplo atual é possivelmente a já citada disputa entre China e EUA sobre a liderança do 5G global. A China investiu enormes quantidades de capital político para se tornar um líder em tecnologia 5G. Os esforços do país de consistiam em um grupo de promoção da tecnologia que foi estabelecido por agências governamentais e contava com universidades chinesas, companhias e institutos de pesquisa (ROGERS, 2017). A China estipulou um plano de desenvolvimento chamado "*Made in China 2025*" utiliza quase todas as áreas da economia chinesa, incluindo: agricultura, equipamento para estradas de ferro, biotecnologia, farmacêutica, entre outras, para aumentar o valor interno de sua produção manufaturada, o que inclui como peça-chave o desenvolvimento tecnológico, o governo chinês estima que o valor incorporado de seus materiais brutos pode chegar a até 70% em 2025, pelo menos esta é a meta. (BERASALUCE apud GUERRERO, 2021).

Duas das maiores empresas do ramo das telecomunicações, Huawei e ZTE, são chinesas, e representam 40% de toda infraestrutura do 5G global, e será usada como o alicerce para a geração de trilhões de dólares em atividades econômicas e industriais na crescente economia digital global, e pela primeira vez na história os EUA não serão os líderes em um setor tecnológico massivo, que pode definir o futuro de inúmeras nações. Isso não necessariamente se caracteriza como uma mudança 100% positiva, pois para muitos isso pode ser apenas a troca de um tirano digital por outro. Mas ainda assim, é importante notar que o paradigma da tecnologia da informação global está sendo quebrado, e a América do Sul encontra-se no proverbial "olho do furacão", com relação às consequências deste processo. De qualquer forma, não será a ascensão chinesa no mercado das telecomunicações que acabará com o abismo digital, porém isto merece destaque por ilustrar a reação do Norte vendo uma potência do Sul chegar ao seu patamar, e tentar ultrapassá-lo. Com certeza, no sistema capitalista, existe um interesse em manter os países ao sul do Equador do outro lado do abismo.

O poder tecnológico das comunicações está intimamente conectado com as medidas de prevenção de cibercrime, como visto anteriormente nesta pesquisa. Com o controle comunicacional, um país é capaz de desenvolver medidas coercitivas dentro do mundo digital, além de ser capaz de aumentar a *cyber awareness* de sua população por meio de campanhas feitas na internet. Além disso, as tecnologias de comunicação oferecem alternativas de estudo, emprego, ou realização profissional, e também são capazes de melhorar outros setores de infraestrutura crítica do governo, como saúde pública e segurança, diminuindo assim os problemas estruturais que muitas vezes são responsáveis pela aparição de crimes e sua contraparte cibernética. O Conselho de Inteligência Nacional dos Estados Unidos afirma que:

> "*Technology, particularly military technologies, will continue to be central to a country's security and global influence, but going forward, cutting-edge artificial intelligence (AI), biotechnology, and data-driven decisionmaking will provide states with a range of advantages for economic growth, manufacturing, healthcare, and societal resiliency. With these technologies, there will be a first mover advantage, enabling states and nonstate actors to shape the views and decisionmaking of populations, to gain information advantages over competitors, and to better prepare for future shocks.*" (NATIONAL INTELLIGENCE COUNCIL, 2021)

O conselho também aponta que, no caso específico das redes de comunicação e dos nodos de informação, o controle de certos fatores importantes na área de comércio, telecomunicações, finanças, fluxos de dados e cadeias de apoio para a produção industrial, darão a países e corporações a habilidade para conseguir informações vitais, negar acesso a potenciais rivais e até coagir certos tipos de comportamentos. Além disso, muitas destas redes

estão desproporcionalmente localizadas nos EUA e na Europa, porém agora a China também se apresenta como um polo de concentração de redes. (NATIONAL INTELLIGENCE COUNCIL, 2021). Portanto pode-se perceber que, para utilizar as medidas coercitivas contra o cibercrime de forma efetiva, um país necessita ter, tanto o domínio das redes de comunicação e controle de áreas específicas, quanto o domínio tecnológico para aplicar as novas invenções e inovações que podem auxiliar na prevenção dos crimes tecnológicos, como o uso de softwares de rastreamento avançados. Este domínio dessas duas importantes tecnologias é um dos principais problemas causados pelo abismo tecnológico a serem enfrentados pelos países do Sul Global, especialmente na América do Sul, no contexto atual.

Além disso, os países precisarão enfrentar a grande disparidade de conectividade entre os espaços urbanos e rurais. Em um relatório feito pela Aliança pela Internet Acessível (A4AI) onde 9 países do Sul foram analisados, sendo eles: Colômbia, Gana, Índia, Indonésia, Quênia, Moçambique, Nigéria, Ruanda e África do Sul, foi constatado que somente 10% da população destes países tem algum tipo de conexão de qualidade com a internet, sendo que este número sobe para 14% quando zonas urbanas são analisadas, e caí para apenas 5% em zonas rurais (A4AI, 2022). Além de super o abismo tecnológico internacional, é necessário superá-lo internamente também.

De novo, um contra-argumento pode ser feito para afirmar que: “Se o cibercrime advém da interconectividade entre as populações, então seria melhor não estender as conexões para estas áreas e este países, assim poupando-os de se tornar vulneráveis a este fenômeno”. Este argumento é sinceramente muito fraco, além de desumano tendo em vista as condições atuais. Ao longo desta pesquisa foram apresentadas diversas vantagens para o uso da tecnologia de comunicações, que são importantes para assegurar direitos humanos básicos nas áreas de educação, trabalho e saúde, além de facilitar processos burocráticos estatais. Fora isso, também foi contatado que cibercrimes não estão apenas isolados ao meio digital, mas podem sim ser crimes que são facilitados utilizando tecnologia de informação, ou seja, em regiões com extrema disparidade entre pessoas que possuem tecnologia, ou não, pessoas que não tem acesso a estes bens tecnológicos se tornam vulneráveis a esses tipos de crime, por conta da falta de *cyber awareness* também. Um país ter mais ou menos tecnologia de informação ou desenvolvimento da indústria tecnológica, não o torna mais ou menos vulnerável aos efeitos do Ciberterrorismo. Entretanto ser detentor de menos tecnologia pode tornar as medidas preventivas contra atos de crimes virtuais mais difíceis de serem executadas.

Um outro problema também assola os países do Sul, mas este é mais atual. A pandemia de COVID-19, como mencionado na introdução, impulsionou uma rápida transição para o trabalho remoto, que ainda se mantém como uma opção viável, mesmo depois do fim da pior fase da pandemia. Isso criou uma maior dependência da tecnologia de comunicações nunca antes vista no mundo inteiro, mas nos países do Sul, especialmente da América Latina, o processo de adaptação foi truculento. O processo foi feito com pressa e sem planejamento. No caso do Brasil, as organizações perderam controle de seus ativos e de seus funcionários, logo foi necessária a adoção de contramedidas que ainda se mantém no pós-pandemia, como a utilização de múltiplos fatores de autenticação nos sistemas e plataformas, soluções de proteção e monitoramento de notebooks e computadores de mesa durante o home office. Além disso, as soluções convencionais que eram usadas dentro das organizações, como firewalls, acabaram se tornando defasadas uma vez que seus funcionários não estavam mais conectados a elas para trabalhar (BONATO apud INSIDE, 2021).

Ainda há outros problemas a serem enfrentados pelos países que estão do outro lado do abismo, como a abundância de *fake news*, do discurso de ódio nas redes digitais, do crime organizado cibernético, e da falta de recursos e divisões treinadas e especializadas em cibersegurança. Apesar disso, os países da América do Sul ainda lutam para conseguir lidar com a nova onda de crimes que ocorrem no mundo digital, com vários países como Brasil, Argentina e Chile são capazes de realizar iniciativas para o combate e a prevenção de cibercrime, através da criação da cibersegurança. Estas iniciativas são muitas vezes inspiradas nas realizadas pelos países do Norte Global, especialmente América do Norte e Europa, e é por isso que um entendimento prévio destas regiões auxilia no entendimento de quais medidas devem ser tomadas, e quais delas priorizadas, mas é claro que no caso do países citados, estas medidas são estabelecidas visando as características particulares de cada nação.

3.3 Cibersegurança na América do Sul.

Voltando para as ideias que foram estabelecidas na sessão 2.3 do capítulo 2, a territorialidade volta a aparecer nesta pesquisa apenas para ilustrar as tentativas de contenção do cibercrime, e promoção da cibersegurança, dentro de uma moldura teórica que pode ser facilmente compreendida, mas é necessário ressaltar novamente que todas as tentativas de criação de ciberesiliência, assim como nos países do Norte Global, são parte do fenômeno de tentar se conter algo que, por sua própria essência, não pode ser contido, pois não é tangível. Apesar disso, como demonstrado nas sessões anteriores deste capítulo, a aquisição de tecnologia de ponta é capaz de causar consequências positivas e duradouras, especialemnte com

relação a questões cibernéticas. Nesta sessão será apresentado como os países do Sul Global, especificamente na América do Sul, conseguiram conter o cibercrime.

Quando se fala em cibersegurança na América do Sul, geralmente se observa o histórico brasileiro sobre o tema. De fato, o Brasil é um pioneiro na área de cibersegurança na região, tendo criado o Centro de Estudos, Respostas e Treinamento de Incidentes no Brasil (CERT.br) em 1997, por iniciativa do Comitê Gestor de Internet no Brasil (CGI.br). Sua principal missão é aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à internet no Brasil (CERT.br, 2022). Cibercrimes são um problema gravíssimo no Brasil. Só em 2023, o país aparece em duas listas dos 10 países mais afetados pelo cibercrime no mundo, ocupando o quinto lugar, e também na lista de países que são os maiores alvos de ransomware do mundo, ocupando nesta lista o décimo lugar (IG tecnologia, 2023).

O CERT.br possuía diversas iniciativas para aumentar a *cyber awareness* dos brasileiros, contendo em seu site diversos fascículos da cartilha de cibersegurança que expõem informações sobre diversos temas pertinentes para a averiguação do ciberisco. Alguns destes merecem destaque especial como os fascículos para Boatos (*Fake News*), Códigos Maliciosos (*Malware*), *Phishing* e outros golpes, Privacidade, Redes e Redes Sociais (CERT.br, 2020). O único problema seria o marketing feito para essas campanhas, que não parecem ser interpretadas com o devido valor por seu público-alvo, ademais pode-se observar que o CERT.br também considera privacidade e redes sociais como temas centrais de suas políticas de cybersegurança, o que torna difícil o compartilhamento dessas informações pelas próprias redes em forma de anúncios.

Recentemente as questões de cibersegurança envolvendo grandes empresas também se tornou um tópico problemático para o Brasil, com o recente Projeto de Lei número 2630 que visa regulamentar e fiscalizar plataformas digitais. O chamado “PL das Fake News” colocou o Brasil em pé de guerra com diversas empresas do ramo das comunicações, mas principalmente a Google. O Brasil parece ser um dos poucos países que entendem a gravidade que é deixar uma empresa privada do ramo das comunicações sem ser responsabilizada pela sua influência política nas redes digitais. Justamente um dia antes da PL ser votada, as empresas Google, Meta, Spotify e Brasil Paralelo distribuíram informações e anúncios contra o projeto, inclusive burlando os próprios termos de uso (BBC Brasil, 2023), mas defendendo o discurso que estariam zelando pela “liberdade de expressão”. A já citada autora Shoshana Zuboff afirma que estas redes sociais e de informação são um dos principais responsáveis por crimes contra a

privacidade de seus usuários, isso sem contar o fato que estão usando suas ferramentas de alcance para ter influência dentro de governos locais.

Apesar disso, como apontado pelo procurador da República em Minas Gerais no ano de 2021, o Brasil ainda está muito atrasado em termos de legislação quando comparado a países como Estados Unidos e membros da União Europeia, onde grandes empresas foram multadas por não protegerem os dados de seus usuários (Senado Notícias, 2021), sendo algumas inclusive ameaçadas de banimento dentro do território do país, como foi com o recente caso da plataforma chinesa Tiktok. Essa demora em se criar uma legislação eficiente para a promoção de cibersegurança, é também um efeito do Abismo tecnológico, visto que por conta da tecnologia de informação demorar mais a chegar em países periféricos, e também nestes países haver poucos especialistas nestes tipos de tecnologia, há também uma demora considerável em suas aplicações e aspectos negativos de serem interpretados e internalizados pelos governos e organizações privadas nestes países. Resultando assim em uma inabilidade de combater o ciberisco oferecido pelas novas tecnologias de informação.

Apesar disso, o Brasil também possuí um histórico de combate a diferentes tipos de cibercrime, um dos exemplos disso foi descrito pelo autor Jorge Mascarenhas Lasmar em seu artigo: Legislação brasileira de combate e prevenção do terrorismo quatorze anos após o 11 de setembro: limites, falhas e reflexões para o futuro:

> "O Sr. Lorenz (Chefe da Divisão de Inteligência da Polícia Federal na época) confirmou em uma audiência pública em 7 de julho de 2009 (Brasil 2009) que o Sr. Khaled Hussein Ali, um indivíduo preso em março daquele ano por crimes de racismo em São Paulo, tinha conexões com a Al-Qaeda e era um dos líderes globais da Jihad Media Battalion (JMB), um dos braços de divulgação e recrutamento da rede Al-Qaeda. A importância deste fato é digno de nota. É importante destacar que tanto o recrutamento quanto a difusão de uma ideologia radical são centrais para a continuidade do terrorismo e, em parte, explicam a falha da Guerra Global Contra o Terror estadunidense." (Lasmar, 2014)

O país também conta com uma estratégia nacional de segurança cibernética conhecida como E-Ciber, que se baseia em um conjunto de ações realizadas pelo governo federal especificamente na área de cibersegurança, tendo sido iniciada em 2020 e com prazo até 2023, ano que este trabalho está sendo escrito. Essa estratégia é uma continuidade da Política Nacional de Segurança da Informação (PNSI) aprovada no ano de 2018, que abrange segurança cibernética, defesa cibernética, defesa física e proteção de dados organizacionais, em consonância com as políticas públicas e os programas do Governo Federal (Governo Federal,

2021). Outro braço do Governo Federal Brasileiro especializado em cibersegurança é o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) que é responsável por decretar alertas de ataques cibernéticos e detectar vulnerabilidades nos sistemas de informações governamentais e, a partir daí, definir recomendações para responder a este tipo de cibercrime ou aprimorar estratégias de cibersegurança. O Trabalho do CTIR é de extrema importância para a contenção do ciberisco nos canais oficiais do governo brasileiro.

Além de Brasil, a América do Sul conta com outros países que só agora estão desenvolvendo políticas de promoção da cibersegurança, e combate ao cibercrime. Um dos maiores exemplos é o Chile, que em 2017 publicou sua *Política Nacional de Ciberseguridad*, para atingir metas de proteção cibernética até o ano de 2022, porém esse plano foi massivamente afetado pela pandemia de COVID-19. A política era pautada nos moldes de outros tipos de projetos de cibersegurança que tiveram bons resultados, especificamente pode-se observar grande influência dos projetos executados por países do Norte Global, como Estados Unidos e Espanha. Por exemplo, o governo chileno foi capaz de observar e definir suas infraestruturas críticas de informação observando o meio internacional, como fica claro na passagem:

> "*Los sectores que componen la clasificación de ICI son muy similares y se repiten en varias clasificaciones a nivel internacional. En el caso chileno, mientras se adopta una política específica para infraestructuras críticas, la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras.*" (CICS, 2017)

Na publicação do governo, são apresentadas necessidades do país que tornavam necessária a criação de uma política especializada em regular o espaço cibernético, como a proteção das pessoas dentro do espaço virtual, promover a segurança das instituições do país, fomentar processos de colaboração e coordenação entre instituições públicas e privadas e a gestão do ciberisco. Entretanto, definitivamente a parte mais importante da política de cibersegurança, tendo em vista os efeitos do Abismo Tecnológico, é a criação de uma "Cultura de Cibersegurança" em torno da educação, boas práticas e responsabilidade com o manejo de tecnologias digitais, a fim de promover o *ciberawareness*. O governo chileno detectou que o acesso ao acervo tecnológico, cultural e econômico de um país é essencial para o desenvolvimento humano, ou seja, não apenas melhorar as tecnologias de informação utilizadas pelas instituições, mas também torná-las acessíveis a população (CICS, 2017)

Entretanto, apesar de já existirem algumas leis voltadas para o ciberespaço desde a década de 1990, foi somente no ano de 2023 desenvolveu uma legislação específica para a

proteção da infraestrutura crítica governamental. A "*Ley Marco sobre Ciberseguridad e Infraestrutura Crítica de la Información*" ainda está em trâmite na Câmara dos Deputados do Chile, mas já conta com aprovação do Senado, e é possível que no segundo semestre de 2023 a lei possa ser finalmente aprovada. A lei é um dos 31 projetos que são tidos como prioridade pela bancada da segurança no Senado chileno, e sua função é impulsionar a criação de uma agência governamental reguladora, nomeada de "*Agencia Nacional de Ciberseguridad*" (SEGURILATAM, 2023). Os principais objetivos da nova norma são 3; primeiro: determinar a institucionalidade, os princípios e os elementos normativos que permitam estruturar, regular e coordenar as ações de cibersegurança dos organismos do Estado, e também os privados; segundo: a norma pretende fixar os requisitos mínimos que contribuam para prevenir, conter, resolver e responder aos incidentes de cibersegurança; terceiro: enfatizar quais as contribuições e obrigações dos organismos do Estado, assim como os deveres das instituições privadas e dos mecanismos de controle, supervisão e responsabilidade frente as infrações (SEGURILATAM, 2023).

O Chile também possui uma Equipe de Resposta a Incidentes de Cibersegurança (CSIRT) que monitora constantemente o uso das plataformas de internet de organizações públicas. Este monitoramento é efetuado através de uma equipe técnica que se encontra disponível ao longo do ano inteiro. O CSIRT se concentra em detectar vulnerabilidades em sites e sistemas da web do Estado chileno, ou seja, são uma organização especializada na investigação do ciberisco. Somado a isso, também realizam gestão de incidentes envolvendo cibersegurança e difusão de medidas preventivas. Um elemento que o CSIRT preza para garantir a melhora em seus serviços de proteção é justamente a evolução contínua da tecnologia de informática utilizada pelo grupo (CSIRT, 2020), isto é muito importante quando se levam em conta as dificuldades proporcionadas pelo abismo tecnológico. O grupo foi criado em 2018, de novo pode-se observar a demora na criação de órgãos de cibersegurança eficientes quando em comparação com os países do Norte Global.

Em 2021, no auge da pandemia de COVID-19, a empresa estado-unidense Fortinet identificou que o Chile recebeu 410 milhões de tentativas de ciberataques no primeiro trimestre do ano, sendo que a América Latina recebeu um total de 7 mil milhões contando todos os países (FORTINET, 2021), um número absurdo para um espaço de tempo tão curto. O CSIRT, na época, atribui isto ao uso intensivo de modalidades de trabalho a distância durante a pandemia de COVID-19, que tiveram que ser implementadas com muita rapidez. Mais uma vez a falta de "*know how*" e *cyberawereness* com relação a estas tecnologias e seus riscos causada pelo abismo foi crucial para criar este ambiente de consequências negativas para a América Latina,

sem esquecer, claro, que as falhas de segurança também afetaram os países do Norte, mas visto que já existiam órgãos de segurança cibernética efetiva, e uma legislação robusta, estes incidentes foram resolvidos com agilidade e medidas preventivas foram executadas.

Outro país que merece destaque nos esforços de cibersegurança é a Argentina, que criou um programa de proteção em 2011 intitulado: Programa Nacional de Infraestruturas Críticas para a Informação e Segurança Cibernética, que tinha como finalidade a adoção de um marco regulatório para proteger a infraestrutura de organizações públicas e privadas. Em 2017, o país criou sua versão do grupo de respostas para cibercrimes ou CSIRT, tal qual pode ser visto no Chile (BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA, 2017). A criação de grupos de pesquisa e resposta já pode ser vista como uma medida padrão para a promoção de cibersegurança, e está sendo usado por diversos países do América Latina, como os supracitados. O CSIRT argentino se assemelha em muitas formas aos outros grupos de pesquisa, então para evitar repetições somente vale destacar que o grupo está inserido na legislação sobre cibersegurança do país.

Entretanto, apenas a criação de um grupo de resposta não é capaz de solucionar os problemas de cibersegurança por si só, como visto ao decorrer da pesquisa, a *cyberawareness* tem um grande impacto na identificação e prevenção ao ciberisco. Por exemplo, na seguinte citação do pesquisador Cícero Araújo Lisboa:

> "Mesmo com o trabalho desenvolvido pelo ICIC com o setor privado, um relatório apresentado pela consultoria Price Waterhouse Cooper em 2018 informa que 53% das empresas argentinas pesquisadas não possuem uma estratégia de segurança cibernética, e 61% não têm um plano de contingência sobre como responder a um incidente cibernético (PRICEWATERHOUSECOOPERS, 2018)." (LISBOA, 2022)

Isto acabou levando o governo argentino a atualizar sua *Estrategia Nacional de Ciberseguridad de la República Argentina* em 2019, que se consiste em uma abordagem multidisciplinar e multisetorial encabeçada pelo poder executivo argentino, que buscava estabelecer princípios básicos e objetivos fundamentais para que o país tivesse a capacidade de executar medidas de proteção ao ciberespaço. Assim como o Chile, a Argentina também busca super as adversidades proporcionadas pelo Abismo Tecnológico através da cooperação internacional e do desenvolvimento de capacitações e novas tecnologias. Por exemplo, em 2017 a Argentina fez uma parceria com os Estados Unidos para a criação de um grupo de trabalhos que forneça mecanismos de capacitação para os cidadãos argentinos com relação a cibersegurança, além disso, também foram estabelecidos acordos com a Espanha e o próprio Chile. A Argentina também contou com empréstimos do Banco Interamericano de

Desenvolvimento para conseguir recursos necessários para a implementação de sua estratégia (LISBOA, 2022).

Os objetivos da estratégia nacional de Cibersegurança Argentina foram estabelecidos da seguinte forma: primeiramente, e mais importante de todos, a conscientização do uso seguro do Ciberespaço, depois disso, a capacitação e a educação para o uso seguro do Ciberespaço. Em terceiro lugar, o desenvolvimento de um marco normativo jurídico, em quarto lugar o fortalecimento das capacidades de prevenção, detecção e resposta. O quinto objetivo seria a proteção e recuperação dos sistemas de informação do setor público, e o sexto, fomentar a indústria de cibersegurança. O sétimo objetivo seria a busca pela cooperação internacional para combater o cibercrime, e o último objetivo, a proteção das infraestruturas críticas de informação nacionais (REPÚBLICA ARGENTINA, 2019). Através desta estratégia, tem-se o panorama geral de como a Argentina aborda o ciberespaço, colocando o *cyberawareness*, a prevenção do ciberisco e a cooperação internacional como peças-chaves de uma boa política de cibersegurança.

Lisboa também aponta que o domínio do ciberespaço na Argentina é construído a partir de um framework político, ou seja, o país foca na criação de mecanismos estatais para a regulação da internet, e das tecnologias de comunicação, incluindo a criação de uma legislação específica, e um conselho de segurança governamental. O país também tem avançado no combate contra o ciberterrorismo, mas isto é compreensível, considerando o histórico dos argentinos de ter seu território atacado por diversos grupos terroristas ao longo do final do século XX e segunda década do XXI. A abordagem da Argentina com relação à cibersegurança pode até ser interpretada como "intervencionista", mas assim como no caso do Brasil, e diversos países que sofrem com os efeitos do abismo tecnológico, sem a regulação rígida do Estado, o ambiente cibernético se torna extremamente volátil. Uma estratégia de *laissez-faire* virtual pode ter sérios prejuízos, já que, apesar das empresas do ramo de informação terem seus mecanismos de regulamento e monitoramento, elas não estão acima de cometerem cibercrimes, ou de interferirem negativamente na política interna de nações.

CONCLUSÃO

A presente pesquisa pretendeu demonstrar que a exploração da dimensão cibernética pela humanidade ainda está em sua infância. A atual década dos anos 2000 será de extrema importância para a observação das questões cibernéticas dos crimes e da segurança digital, e

como as dinâmicas da tecnologia da informação as afetam em diferentes partes do mundo. O intuito deste trabalho é então servir como um ponto de início de discussões que possam ser desenvolvidas com estes elementos em mente. Esta dissertação teve como objetivo apresentar casos que possam ser usados como parâmetros investigativos, sobretudo na questão da cibersegurança, já que o estudo do ciberespaço deve continuar sendo feito para que novas interpretações sobre este tema surjam.

A humanidade sempre teve interesse em tornar o incompreensível capaz de ser compreendido, metaforicamente "prendendo um raio em uma garrafa", e é exatamente isso que deve ser entendido quando o mundo digital é analisado. É um mundo intangível, e para muitos ainda invisível e desconhecido, mas ainda capaz de trazer consequências consideráveis ao mundo material. Sendo assim, também é correto afirmar que o mundo material tem a capacidade de interferir nos fenômenos cibernéticos, apesar do desafio que os Estados, organizações e indivíduos possuírem para conseguir se entender enquanto agentes dentro do mundo cibernético. Somente através da educação, investimento e reponsabilidade, a nova categoria de crimes cibernéticos pode ser combatida.

A principal falha da segurança no mundo digital pode ser vista em uma falsa confiança dos usuários, tanto pela crença que eles são capazes de proteger suas informações sensíveis, quanto pela percepção errônea de que as empresas que controlam os fluxos digitais prezam pela segurança informacional de seus usuários. O mesmo é verdade no caso de Estados e organizações privadas. Foi-se o tempo em que o necessário para garantir a segurança de empresas era a proteção contra a espionagem corporativa, e os Estados podiam simplesmente vigiar suas fronteiras contra invasores e ameaças externas. A nova dimensão virtual abriu portas que só podem ser acessadas de forma indireta, através de um avatar, ou proxy, porém esta forma cibernética fugaz ainda existe porque ela foi criada por alguém no mundo físico. Da mesma forma, os crimes cometidos contra o avatar virtual têm consequências para sua contraparte física.

O ciberespaço também pode ser cooptado por criminosos que planejam cometer crimes no mundo físico. Já podem ser vistas tentativas de utilizar uma tecnologia que visa encurtar a distância e o tempo entre as pessoas, sendo utilizada para semear o caos e causar dor e sofrimento entre a humanidade. O mundo digital não pode ser deixado aos seus próprios mecanismos, ele precisa de seus guardiões. Mais importante ainda, as pessoas precisam de protetores que visem garantir seus direitos fundamentais de existência, tanto fora, quanto dentro da internet para a criação de uma sociedade mais justa e estável.

Da mesma forma, somente tendo em vista que a tecnologia de informação se encontra inserida dentro de um sistema socioeconômico específico, podem ser tomadas medidas para amenizar as injustiças e os danos causados pela exploração e expropriação que ocorrem dentro do meio digital, apesar de estar fisicamente separado, e de fato ser uma dimensão alternativa. É importante sempre não cair no discurso tecnodeterminista defendido por grandes companhias de informática que afirmam que a tecnologia não pode simplesmente ser monitorada de forma ética e crítica, da mesma forma isto não significa que a tecnologia de informação é sempre algo que trará discórdia e consequências negativas para a humanidade. A tecnologia, assim como inúmeros outros elementos, é uma ferramenta, e como tal pode ser usada de forma positiva ou negativa, para semear o conhecimento, ou manter pessoas na escuridão e para trazer o desenvolvimento ou manter as estruturas que o limitam.

REFERÊNCIAS BIBLIOGRÁFICAS:

AGÊNCIA SENADO. Combate ao cibercrime é urgente, afirmam especialistas na CCT. Senado Notícias, 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/combate-ao-cibercrime-e-urgente-afirmam-especialistas-na-cct. Acesso em: 06/06/2023.

ALLIANCE FOR AFFORDABLE INTERNET. Meaningful Connectivity for Rural Communities: Geographic Barriers & Policy Strategies for Digital Inclusion. **A4AI**, 2022. Disponível em: https://www.intgovforum.org/sites/default/files/webform/igf_2022_workshop_proposal_form/227863/MC-Rural-Report-English_1.pdf. Acesso em: 01/06/2023.

AZARMSA, Reza. Computer Viruses and Safe Educational Practices. **Educational Technology**, vol. 31, n. 11, p. 26-32, 1991.

ARMSTRONG, H. L. Denial of Service and Protection of Critical Infrastructure. **Journal of Information Warfare**, vol. 1, n. 2, p. 23-34, 2001.

BBC NEWS BRASIL. PL das Fake News: 3 pontos para entender disputa entre governo e Google. BBC.com, 2023. Disponível em: https://www.bbc.com/portuguese/articles/crg2jx75y40o. Acesso em: 06/06/2023.

BENNER, Katie. China's Dominance of 5G Networks Puts U.S. Economic Future at Stake. Barr Warns. **New York Times**, 2020. Disponível em: https://www.nytimes.com/2020/02/06/us/politics/barr-5g.html. Acesso em: 20/05/2023.

BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA. Ministerio de Seguridad: Resolución 1107-E/2017. **Argentina Presidencia**, 2017. Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/172434/20171018. Acesso em: 06/06/2023.

BROADHURST, Roderic, WOODFORD-SMITH, Hannah, MAXIM, Donald, SABOL, Bianca, ORLANDO, Stephanie, CHAPMAN-SCHMIDT, Benjamin, and ALAZAB, Mamoun.

Cyber Terrorism: Research Review, Australian National University, Cybercrime Observatory, Canberra, 2017, DOI: 10.13140/RG.2.2.19282.96964

BROWN, Stephen E.; ESBENSEN, Finn-Aage; GEIS, Glibert. **Criminology: explaining crime and its context**. Sétima Edição. Nova Jersey: Anderson Publishing, 2010.

CARVALHO, Victor. **App de videoconferência Zoom está sendo banido de escolas devido problemas com segurança**. Tudo Celular, abril de 2020. Disponível em: https://www.tudocelular.com/android/noticias/n154734/zoom-meeting-deixa-de-ser-usado-por-escolas-11265.html. Acesso em: 15/01/2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Cartilha de Segurança para Internet: Fascículos. Cert.br, 2020. Disponível em: https://cartilha.cert.br/fasciculos/. Acesso em: 06/06/2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Sobre o CERT.br. **Cert.br**, 2022. Disponível em: https://www.cert.br/sobre/. Acesso em: 06/06/2023.

CHANG, Ha-Joon. **Kicking away the Ladder**. Londres: Anthem Press, 2002.

CHANG, H-Joon. Kicking away the Ladder: An Unofficial History of Capitalism, Especially in Britain and the United States. **Challenge**, vol. 45, n. 5, p. 63-97, 2002.

CISCO SECURE. Security Outcomes Report volume 3: Achieving Security Resilience. **Cisco Secure**, dezembro de 2022. Disponível em: https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html. Acesso em: 15/01/2023.

COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD. Política Nacional de Ciberseguridad. **CISC**, 2017. Disponível em: www.ciberseguridad.gob.cl. Acesso em: 06/06/2023.

CSIRT CHILE. ¿Qué es CSIRT? **YouTube**, 2019. Disponível em: https://www.youtube.com/watch?v=56FrzoN1BV8&t=93s&ab_channel=CSIRTGobCl. Acesso em: 06/06/2023.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **Guide to Getting Started with a Cybersecurity Risk Assessment**. CISA, 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisa.gov/sites/default/files/2023-

02/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf. Acesso em: 22/02/2023.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **Combatting Cyber Crime**. CISA, 2023. Disponível em: https://www.cisa.gov/combatting-cyber-crime. Acesso em: 10/04/2023.

DENNING, Dorothy E. **Testemunho feito na Universidade de Georgetown**, 23 de maio de 2000, disponivel em: https://irp.fas.org/congress/2000_hr/00-05-23denning.htm. Acesso em: 11/03/2023.

EUROPEAN COMMISSION. **Interim Evaluation of Horizon 2020**. Luxemburgo: Escritório de Publicações da Comissão Europeia, 2017. Doi: 10.2777/220768. Acesso em: 09/05/2023.

EUROPEAN COMMISSION. **Questions and Answers on the United Kingdom's Withdrawal from the European Union on 31 January 2020**. Bruxelas: Comissão Europeia, 2020. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_104. Acesso em: 10/04/2023.

EUROPEAN CYBERCRIME CENTER. **Combating Crime in a Digital Era**. EC3 Europol, 2013.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **ENISA aims to raise cybersecurity awareness and promote behavioral change**. ENISA, 2023. Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-education. Acesso em: 09/05/2023.

FARAH, Paulo Daniel. **Abismo Tecnológico: estudo mostra que o acesso à rede está concentrado na América do Norte, na Europa Ocidental e no Japão. Nem 5% do mundo usa internet, diz ONU**. Folha de São Paulo, junho de 2000. Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft2306200001.htm. Acesso em: 15/01/2023.

FELDMANN, Paulo Roberto. O atraso tecnológico da América Latina como decorrência de aspectos e de fatores microeconômicos interligados. **SciELO – Brasil**, 2009. Disponível em: https://www.scielo.br/j/ecos/a/tXfhJY4QzCpcj8XVSFGYz8P/. Acesso em: 20/05/2023.

FORST, Brian. **Terrorism, Crime and Public Policy**, Cambridge: Cambridge University Press, 2009

FORTINET. Reporte Fortiguard Labs: Primer Trimestre 2021. **CSIRT Chile**, 2021. Disponível em:

https://www.csirt.gob.cl/media/2021/07/infografia_fortinet_fortiguard_q1_2021_chile.pdf. Acesso em: 06/06/2023.

GAITANIDOU, Evangelia; BELLINI, Emmanuele; FERREIRA, Paulo. **RESOLUTE D3.6 European Management Guidelines**. Horizon 2020 Framework Programme of the European Union, 2018.

GALTUNG, Johan. Violence, Peace and Peace Research. **Journal of Peace Research**, vol. 6, n. 3, p. 167-191, 1969.

GALTUNG, Johan. **Pax Pacifica: Terrorism, the Pacific Hemisphere Globalization and Peace Studies**. Londres: Pluto Press, 2005.

GENGE, Béla; KISS, István; HALLER, Piroska. A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. **International Journal of Critical Infrastructure Protection**, vol. 10, p. 3-17, 2015.

GERCKE, Marco. **Understanding Cybercrime: Phenomena, Challanges and Legal Response**. International Telecommunication Union (ITU), 2012. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx. Acesso em: 02/02/2023.

GOODWIN, Gabriel. **Cyberterrorism: How Real is the Threat?** United States Institute of Peace, relatório especial 119, dezembro de 2004. Disponível em: https://www.usip.org/sites/default/files/sr119.pdf. Acesso em: 15/01/2023.

GOTTCHALK, Petter. **Policing Cyber Crime**. Telluride: Ventus Publishing ApS, 2010.

GOVERNO FEDERAL. Política Nacional de Segurança da Infomação. **Gov.br**, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao. Acesso em: 06/06/2023.

GUERNSEY, Lisa. TECHNOLOGY; Court Says France Can't Censor Yahoo Site. **New York Times**, sessão C, p. 5, 9 de novembro de 2001. Disponível em: https://www.nytimes.com/2001/11/09/business/technology-court-says-france-can-t-censor-yahoo-site.html. Acesso em: 02/02/2023.

GUERRERO, César. China's Leadership in 5G networks: Economic and Geopolitical Implications. **Revista Comércio Exterior**, 2021. Disponível em: https://www.revistacomercioexterior.com/chinas-leadership-in-5g-networks-economic-and-geopolitical-implications. Acesso em: 01/06/2023.

G1. **“Não haverá retorno ao antigo normal em um futuro próximo”, diz diretor geral da OMS.** Matéria G1, julho de 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/07/13/nao-havera-retorno-ao-antigo-normal-em-um-futuro-proximo-diz-diretor-geral-da-oms.ghtml. Acesso em: 15/01/2023.

HOLLAND, H. Brian. **Tempest in a Teapot or Tidal Wave – Cybersquatting Rights and Remedies Run Amok**. Texas A&M University School of Law, 2005. Disponível em: https://scholarship.law.tamu.edu/facscholar/140. Acesso em: 02/02/2023.

HOUSE OF COMMONS HOME AFFAIRS COMMITTEE. **E-Crime Report**. Londres: United Kingdom Home Affairs, vol. 1, 2013.

IG. Brasil é o 5º País do mundo mais afetado por crimes cibernéticos. **IG Tecnologia**, 2023. Disponível em: https://tecnologia.ig.com.br/2023-04-15/brasil-quinto-pais-mais-afetado-crimes-ciberneticos.html. Acesso em: 06/06/2023.

INSIDE. Cyber Tech Report: Desafios da Cibersegurança no Brasil. **Cisco Secure**, 2021. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report1-distrito.pdf. Acesso em: 20/05/2023.

INTERNET WORLD STATS. **Internet Usage Statistics: The Internet Big Picture**. Year estimates, 2023. Disponível em: https://www.internetworldstats.com/stats.htm. Acesso em: 09/05/2023.

IVINS, William M. What is Crime? **Proceedings of the Academy of Political Science in the City of New York**, Nova Iorque, Vol. 1, N. 4, p. 531-558, 1911.

ITCHANNEL. *Ciberterrorismo:* **Hamas instala spyware em telemóveis de soldados israelitas.** It Channel, Segurança, julho de 2018. Disponível em: https://www.itchannel.pt/news/seguranca/ciberterrorismo-hamas-instala-spyware-em-telemoveis-de-soldados-israelitas-. Acesso em: 15/01/2023.

JAIN, Sanjay. Digital Piracy: A Competitive Analysis. **Marketing Science**, vol 27, n. 4, p.610-626, 2008.

JOHNSON, Arnold; DEMPSEY, Kelley; ROSS, Ron; GUPTA, Sarbari; BAILEY, Dennis. Guide for Security-Focused Configuration Management of Information Systems. **National Institute of Standards and Technology Special Publication 800-128**, 2011. Disponível em: https://doi.org/10.6028/NIST.SP.800-128. Acesso em: 20/03/2023.

KATYAL, Neal Kumar. Criminal Law in Cyberspace. **University of Pennsylvania Law Review**, Pensilvânia, vol. 149, n. 4, p. 1003-1114, 2010.

KLYNVELD PEAT MARWICK GOERDELER INTERNATIONAL. Cyber Crime – A Growing Challenge for Governments. **Issues Monitor – Government on Cyber Crime**, n. 11 – 008, vol. 8, p. 1-19, julho, 2011.

LASMAR, Jorge Mascarenhas. A legislação brasileira de combate e prevenção do terrorismo quatorze anos após o 11 de setembro: limites, falhas e reflexões para o futuro. **Revista de Sociologia e Política**, vol. 23, n. 53, p. 47-70, março, 2015.

LEVY, Steven. **Hackers: Heroes of the Computer Revolution**. Nova Iorque: Dell Publishing Group, 1984.

LEWIS, James A. Cibersecurity: A U.S. Perspective. **A Roadmap for U.S.-Russia Relations**, Center for Strategic and International Studies (CSIS), 2017. Disponível em: https://www.jstor.org/stable/resrep23179.12. Acesso em: 09/05/2023.

LISBOA, Cícero Araújo. A securitização do combate ao cibercrime no século XXI: um estudo sobre a América do Sul. Porto Alegre: **Universidade Federal do Rio Grande do Sul** Faculdade de Ciências Econômicas: Programa de Pós-Graduação em Estudos Estratégicos Internacionais, 2022. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/238889/001141287.pdf?sequence=1&isAllowed=y. Acesso em: 06/06/2022.

MILONE, Mark, G. Hacktivism: Securing the National Infrastructure. **The Business Lawyer**, vol. 58, n. 1, p. 383-413, 2002.

NATIONAL CRIME PREVENTION COUNCIL. **Cybercrimes**. Arlington, 2012. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://archive.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf. Acesso em: 11/03/2023.

QUADARA, Antonia; EL-MURR, Alissar; LATHAM, Joe. **The Effects of Pornography on children & young people: An evidence scan**. Melbourne: Australian Institute of Family Studies, 2017. Disponível em: <aifs.gov.au/publications/effects-pornographychildren-and-young-people>. Acesso em: 02/02/2023.

QUEIROZ, Breno. **Entenda a disputa pelo 5G na inovação, nos negócios e na geopolítica**. Invest News, novembro de 2021. Disponível em: https://investnews.com.br/geral/entenda-a-disputa-pelo-5g-na-inovacao-nos-negocios-e-na-geopolitica/. Acesso em: 15/01/2023.

REPÚBLICA ARGENTINA. Estrategia Nacional de Ciberseguridad de la República Argentina. **Governo da Argentina**, 2019. Disponível em: https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf. Acesso em: 06/06/2023.

ROGERS, Lilian. What is at Stake in China's 5G Push? **Apco Worldwide**, 2017. Disponível em: https://apcoworldwide.com/blog/whats-at-stake-in-chinas-5g-push/#:~:text=China%20has%20funneled%20enormous%20political,%2C%20companies%2C%20and%20research%20institutes. Acesso em: 01/06/2023.

ROLFINI, Fabiana. **Cibercrime: ataques no Brasil aumentam em mais de 300% com a pandemia.** Olhar Digital, julho de 2020. Disponível em: https://olhardigital.com.br/2020/07/03/noticias/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 15/01/2023.

SEGURILATAM. Agencia Nacional de Ciberseguridad de Chile: ¿cuáles son sus funciones? **Segurilatam**, 2023. Disponível em: https://www.segurilatam.com/actualidad/agencia-nacional-de-ciberseguridad-de-chile-cuales-son-sus-funciones_20230508.html. Acesso em: 06/06/2023.

SEGURILATAM. Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información: ¿cuál es su objetivo? **Segurilatam**, 2023. Disponível em: https://www.segurilatam.com/actualidad/ley-marco-sobre-ciberseguridad-e-infraestructura-critica-de-la-informacion-en-chile-cual-es-su-objetivo_20230504.html. Acesso em: 06/06/2023.

SERGER, Alexander. **Cybercrime Strategies**, Version 14 October 2011, Strasbourg. Disponível em: https://www.techtarget.com/searchsecurity/definition/cyberterrorism#:~:text=The%20threat%20of%20cyberterrorism%20is,acknowledged%20to%20have%20occurred%20earlier. Acesso em: 15/01/2023.

SOLAR WINDS PINGDOM. The Incredible Growth of the Internet since 2000. **Solar Winds Pingdom**: Tech Musings, 2010. Disponível em: https://www.pingdom.com/blog/incredible-growth-of-the-internet-since-2000/. Acesso em: 09/05/2023.

TALIHARM, Anna-Maria. Cyberterrorism: In Theory or in Practice. **Defense Against Terrorism Review**, vol. 3, n. 2, p. 59-74, 2010.

THIRD WAY. **2020 Thematic Brief: US Cybersecurity Efforts**. Third way, 2020. Disponível em: https://www.jstor.org/stable/resrep26169. Acesso em: 09/05/2023.

TITAN HQ. **SafeTitan Security Awareness Training**. Titan Hq, 2023. Disponível em: https://www.titanhq.com/safetitan/. Acesso em: 20/03/2023.

UNITED NATIONS. **Hate Speech: Undestanding Hate Speech**. Publicação feita pela Organização das Nações Unidas, 2021. Disponível em: https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech. Acesso em: 02/02/2023.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). **Offences Against the Confidentiality, Integrity and Availability of computer data and systems**. 2019. Disponível em: https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html#:~:text=An%20example%20of%20illegal%20interception,and%20communicate%20on%20their%20behalf. Acesso em: 02/02/2023.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY. **Cybersecurity**. Homeland Security, 2023. Disponível em: https://www.dhs.gov/topics/cybersecurity. Acesso em: 09/05/2023.

UNITED STATES NATIONAL INTELLIGENCE COUNCIL. Emerging Dynamics. **National Intelligence Council**, 2021. Disponível em: https://www.dni.gov/index.php/gt2040-home/emerging-dynamics/international-dynamics. Acesso em: 01/06/2023.

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT. **HSI Cyber Crimes Center**. ICE, 2023. Disponível em: https://www.ice.gov/partnerships-centers/cyber-crimes-center. Acesso em: 10/04/2023.

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT. **Homeland Security Investigations**. ICE, 2023. Disponível em: https://www.ice.gov/about-ice/homeland-security-investigations. Acesso em: 10/04/2023.

UNITED STATES SECRET SERVICE. **ECTF and FCTF**. Secret Service, 2023. Disponível em: https://www.secretservice.gov/contact/ectf-fctf. Acesso em: 10/04/2023

ZACHER, Christopher. The Business of CYBERSECURITY. **Hispanic Engineer and Information Technology**, Career Communications Group, n. 2, vol. 33, p. 20-23, 2018. Disponível em: https://www.jstor.org/stable/10.2307/26573742. Acesso em: 09/05/2023.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder.** Rio de Janeiro: Editora Intrínseca LTDA, 2010.