Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Relações Internacionais

EDUARDA MACIEL TRAVASSOS

SEGURANÇA CIBERNÉTICA INTERNACIONAL: O Terrorismo e a Internet das Coisas

BRASÍLIA
2021

EDUARDA MACIEL TRAVASSOS

SEGURANÇA CIBERNÉTICA INTERNACIONAL: O Terrorismo e a Internet das Coisas

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Lucas Soares Portela

BRASÍLIA
2021

EDUARDA MACIEL TRAVASSOS

SEGURANÇA CIBERNÉTICA INTERNACIONAL: O Terrorismo e a Internet das Coisas

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Lucas Soares Portela

BRASÍLIA, 08 ABRIL 2021

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

Dedico este trabalho a todos que me acompanharam ao longo dessa jornada acadêmica.

AGRADECIMENTOS

Agradeço aos meus pais, avós e demais familiares que me acompanharam e me apoiaram nesta jornada acadêmica.

Aos meus professores, em especial Dr. Edo Korljan, Dra. Imène Ajala, Dr. Alfred de Zayas, professor Frederico Seixas Dias, professor Oscar Medeiros Filho, e professor Lucas Soares Portela, meu orientador que foi muito paciente e me auxiliou durante todo o processo de escrita e formatação deste trabalho.

Aos meus amigos que sempre me deram apoio moral, foram minhas companhias em momentos difíceis e nunca deixaram que eu me sentisse solitária.

“It’s the small things, everyday deeds of ordinary folk that keep darkness at bay. Simple acts of love and kindness” - J.R.R. Tolkien, The Hobbit

RESUMO

Este trabalho tem como tema geral a segurança internacional, focando-se na segurança cibernética e na internet das coisas, fazendo-se também um estudo de caso da utilização do espaço cibernético para disseminação de propaganda terrorista pelo grupo Daesh. O objetivo desta monografia é expor a importância deste assunto sob a ótica das Relações Internacionais, trazer opiniões de diversos pesquisadores para um melhor entendimento sobre o assunto, além disso, faz-se objetivo deste trabalho, também, manifestar a importância deste tema não apenas para especialistas da área, mas também para leigos que podem ser afetados direta ou indiretamente. O método utilizado foi: revisão de literaturas de Relações Internacionais e segurança cibernética, além de breves consultas a literaturas de engenharia de softwares para fazer-se mais completo e coerente; realizou-se, também, um estudo de caso da utilização do espaço cibernético pelo grupo terrorista Daesh para a disseminação de propaganda terrorista e recrutamento. Concluiu-se que o tema estudado é, deveras, de grande importância para a academia e para a população geral, que requer atualizações constantes devido a rapidez da evolução das tecnologias; conclui-se também que os Estados necessitam de mais aparatos e especialistas na área, pois as ameaças tendem a crescer e se tornarem cada vez mais complexas.

Palavras-chave: Segurança Internacional; Relações Internacionais; Cibersegurança; Terrorismo; Territorialização; Internet.

LISTA DE ABREVIATURAS E SIGLAS

ABIN	**Agência Brasileira de Inteligência**
ACL	**Lista de Controle de Acesso**
DoS	**Sistema Operacional em Disco**
ECU	**Unidade de Controle Eletrônico**
EUA	**Estados Unidos da América**
FARCS	**Forças Armadas Revolucionárias da Colômbia**
FBI	**Federal Bureau of Investigation**
GFW	**Grande Firewall da China**
GPS	**Sistema de Posicionamento Global**
IdC	**Internet das Coisas**
ISIS	**Estado Islâmico do Iraque e da Síria**
NFV	**Infraestrutura de Virtualização de Funções**
NSA	**Agência de Segurança Nacional**
ONU	**Organização das Nações Unidas**
P2P	**Peer to Peer**
PLC	**Controlador Lógico Programável**
QOS	**Qualidade de Serviço**
SDN	**Rede Definida por Software**
TPMS	**Monitoramento da Pressão de Pneus**
VPN	**Rede Privada Virtual**

SUMÁRIO

INTRODUÇÃO

Este trabalho, que tem como tema a segurança internacional cibernética com foco em especial à propaganda terrorista disseminada pela internet e o conceito de Internet das Coisas, busca entender como o fenômeno da globalização e disseminação da internet afetam a segurança e a soberania dos Estados. Além de analisar possíveis ferramentas e soluções para que a segurança nesse novo espaço seja realizada da forma mais eficiente disponível atualmente, esse trabalho busca reunir opiniões diversas de especialistas da área e colocá-las sob a ótica das Relações Internacionais e facilitar seu entendimento para todo tipo de público que possa, de alguma forma, ser afetado pelos perigos, problemas, legislações e tratados citados ao longo do texto.

Para a realização deste trabalho foram utilizadas pesquisas bibliográficas de política e segurança internacional, linguagem de programação e segurança da internet, além de um estudo de caso de disseminação de propaganda terrorista utilizado pelo grupo estado islâmico. A pesquisa de tecnicidades da computação fez-se necessária para uma melhor compreensão de como o espaço cibernético opera e assim facilitar, não apenas o entendimento do leitor sobre o assunto, mas também auxiliar o entendimento de quais estratégias de segurança seriam as ideais para diversas situações, quais se tornaram obsoletas e quais ainda necessitam refinamento ou até mesmo quais situações ainda se encontram sem solução.

No primeiro capítulo são abordados os significados do termo espaço cibernético pela história até o consenso da atualidade. É abordado também o aspecto técnico da cibernética para que facilite o entendimento de termos e demais assuntos tratados ao longo do trabalho. Por fim, o último assunto do primeiro capítulo elenca os principais agentes da segurança espaço cibernético e como atuam no espaço supracitado. No segundo capítulo são estudados conceitos e dificuldades da territorialização do espaço cibernético, bem como possíveis ferramentas para auxiliar a demarcação e securitização desse espaço, são estudados também conceitos teóricos sob as óticas realistas e construtivistas sobre a segurança da internet.

No terceiro capítulo é estudada a definição e teoria das propagandas terroristas disseminadas pela internet, com um estudo de caso sobre o Daesh (também conhecido como estado islâmico) e seu sucesso em recrutamentos no exterior. No quarto e último capítulo, é estudado o conceito de Internet das Coisas e como essa nova tecnologia, que está cada vez mais presente no cotidiano de cidadãos comuns, pode ser um fator desafiador para legisladores e demais atuantes da área de segurança cibernética. São citados exemplos de

ataques ciberfísicos, suas complexidades e como são evitados (ou não) na atualidade. No quarto capítulo é explicado o conceito do termo Internet das Coisas (IdC). É contado brevemente o surgimento da tecnologia supracitada e em seguida são expostos diversos exemplos de brechas de segurança e ataques sofridos por intermédio da IdC. São abordados, então, mecanismos e estratégias utilizados atualmente para evitar tais ataques e reforçar a segurança de possíveis brechas do sistema.

1 ABORDAGEM CONCEITUAL DE ESPAÇO CIBERNÉTICO

As pessoas estão familiarizadas com o espaço físico tradicional, por exemplo o oceano, que é o vasto espaço aquático conectado na superfície da terra e composto de água salgada. Conceitos como mar territorial, alto-mar (ou mar internacional), recursos marítimos entre outros, já são amplamente conhecidos e juridicamente estruturados, o que demonstra ser um espaço concreto e familiar.

Espaço, para a matemática, refere-se a uma coleção multidimensional com uma natureza especial e algumas estruturas adicionais. Sabe-se que "Dimensão" mostra uma direção no espaço, ou seja, um espaço determinado por múltiplas direções é chamado de espaço multidimensional. Por exemplo, um modo linear determinado por uma direção é um espaço unidimensional; um modo plano estabelecido pelas duas direções é um espaço bidimensional; e um o modo estéreo composto de três direções é chamado de espaço tridimensional; um espaço que flui determina a direção tridimensional, e a direção do tempo é um espaço quadridimensional, também conhecido como espaço-tempo. Em suma, a compreensão do espaço deve ser baseada na realidade humana comportamental e prática, bem como sua abrangência e direções em que a ação pode ser empreendida. Dessa forma, os chamados objetos e os movimentos do sujeito são dois atributos centrais da conotação de espaço.

Assim, entender o chamado espaço cibernético demanda compreender essa dimensão espaço, que para tal faz-se necessário navegar pela origem do que é esse ambiente. A palavra "cibernética" vem do trabalho de Norbert Wiener (1948). Sua ideia básica é de que as pessoas podem "se acoplar" a uma máquina, e que o resultado pode fornecer um ambiente alternativo para a interação. Assim o autor estabelece uma base para o que posteriormente seria chamado de espaço cibernético. Em um segundo momento, a palavra "cibernético" foi considerada como um prefixo. Por exemplo, a Finlândia em sua "*Cyber Resolution*" de janeiro de 2013, componente da estratégia de segurança finlandesa, descreveu o cibernético da seguinte forma:

> A palavra 'cibernético' é quase invariavelmente o prefixo para um termo ou o modificador de uma palavra composta, em vez de uma palavra autônoma. Sua inferência geralmente se refere ao processamento eletrônico de informações (dados), tecnologia da informação, comunicações eletrônicas (transferência de dados) ou sistemas de informação e informática" (FINLÂNDIA, 2013, p. 12).

Compreendido o termo e “espaço” e o termo “cibernético”, cabe agora adentrar na conjugação conceitual dessas duas palavras. O ciberespaço, um conceito cunhado na década de 1980, foi visto inicialmente como um espaço fundamentalmente separado do mundo físico. Alguns teóricos chegaram a afirmar que o ciberespaço transcende as fronteiras geográficas e nacionais e, portanto, força noções tradicionais de soberania e segurança, como, por exemplo, o pesquisador Abraham M. Denmark (2010), que propôs os seguintes conteúdos:

> Hoje existem quatro grandes bens comuns globais: marítimo, aéreo, espacial e ciberespaço; cada bem comum é fundamentalmente diferente dos outros; os bens comuns globais compartilham quatro características gerais: (1) eles não são propriedade ou controlados por qualquer entidade única; (2) sua utilidade como um todo é maior do que se dividido em partes menores; (3) atores estatais e não estatais com as capacidades tecnológicas necessárias são capazes de acessá-los e utilizá-los para fins econômicos, políticos, científicos e culturais; e (4) atores estatais e não estatais com as capacidades tecnológicas necessárias são capazes de usá-los como um meio para movimento militar e como teatro de conflitos militares; o ciberespaço é agora uma parte integrante da vida moderna; pessoas ao redor do mundo interagem, cooperam e competem por meio de uma série de conexões em redes que abrangem o mundo todo (DENMARK, 2010 p. 27).

No entanto, Greg Rattray (DENMARK E KAPLAN, 2010) menciona que o ciberespaço é fundamentalmente um ambiente físico, criado pela conexão de sistemas físicos e redes, e gerenciados por regras definidas em protocolos de *software* e comunicações - todos localizados nos limites soberanos de estados-nações, e que, embora muitas das informações no ciberespaço sejam consideradas públicas, os elementos físicos do ciberespaço - os desktops, os laptops, os servidores, as geladeiras habilitadas para Internet, os roteadores, os telefones, os celulares, cabos de LAN, cabos de fibra ótica - têm proprietários claros.

Dessa forma, infere-se desse altar, que o espaço cibernético não se sustenta sem seus elementos físicos. Embora Denmark (2010) tenha alegado que cada bem comum se diferencia dos demais, existem características comuns, que o próprio autor constrói. Uma característica adicional aos quatro pontos elencados pode ser a existência de um elemento constitutivo. No caso do espaço terrestre seria o solo, no marítimo a água, no aéreo o ar, no espacial a gravidade. O elemento que constitui o espaço cibernético, portanto são os equipamentos e estruturas físicas, chamadas de *hardwares* e considerado por Daniel Ventre (2011) a estrutura que baseia todo esse novo ambiente geográfico.

Na mesma linha, Wolff Heintschel von Heinegg (2013), do Instituto de Direito Europeu da Goethe Universidade de Frankfurt, apontou os seguintes conteúdos em Soberania Territorial e Neutralidade no Ciberespaço: o ciberespaço requer uma arquitetura física para existir; o equipamento conectado a uma rede de transmissão proprietária geralmente está

localizado dentro do território de um Estado; é propriedade do governo ou de empresas; a integração de componentes físicos de infraestrutura cibernética localizada dentro de um estado território para o "domínio global" do ciberespaço não pode ser interpretado como uma renúncia do exercício da soberania territorial.

Os Estados têm enfatizado continuamente seu direito no ciberespaço, incluindo aqueles para exercer controle sobre a infraestrutura cibernética localizados em áreas de seu território soberano, para fazer valer sua jurisdição sobre atividades em seu território e para proteger sua infraestrutura cibernética contra interferência transfronteiriça por outros Estados ou por indivíduos. Na verdade, os Estados têm exercido, e continuarão a exercer, sua jurisdição sobre crimes cibernéticos e continuarão, também, a regular as atividades no ciberespaço, pois tal controle faz parte da natureza da soberania estatal.

Antes da fundação das Nações Unidas em 1945, as teorias da soberania eram originárias principalmente da Europa. Desde que os países europeus assinaram a Paz de Vestfália em 1648, teorias sobre a soberania nacional foram levantadas, praticadas, repensadas e alteradas até que um consenso global fosse alcançado.

O significado jurídico do conceito de soberania moderna está contido na Carta das Nações Unidas de 1945, porém, para que o conceito seja aplicado no espaço cibernético é preciso, primeiramente, que os países entrem em um consenso sobre como e quais normas seriam aplicadas a essa realidade. Um exemplo de divergência de jurisprudências seria o caso do Brasil e Estados Unidos, enquanto em 2014 com a lei 12.965 - o Marco Civil da Internet - o Brasil garante a neutralidade da Internet no inciso IV do 3º artigo da referida lei, os Estados Unidos já não garantem a neutralidade da rede, permitindo que empresas privadas estipulem a distribuição de dados aos seus clientes (VALENTE, 2017). Assim a teoria e a prática da soberania do ciberespaço variam de Estado para Estado, em especial pela ausência de um entendimento comum na comunidade internacional. Em virtude disso, elas têm sido um campo quente atraindo mais e mais atenção, seja no aspecto técnico, quanto no aspecto político e internacional.

A ordem de igualdade de soberania pode ser classificada por universalidade ou por logicidade. A legítima defesa, independência e igualdade de soberania são classificadas de acordo com a lógica produtiva da soberania nacional. Uma vantagem da discussão ordenada desta forma é deixa claro os seguintes fatos: a igualdade internacional de soberania nacional é igualdade de diferentes níveis, ao invés de igualdade absoluta ou igualdade real; a utilização prática da soberania nacional depende mais da história da geopolítica, o ponto de vista da ordem mundial e a constitucionalidade interna e externa de cada país.

Em 1999, um cientista político britânico, Tim Jordan, elaborou sistematicamente, pela primeira vez, o conceito de ciberpoder a partir das perspectivas da política e da sociologia: ciberpoder é a forma de poder da política e da cultura no ciberespaço e na Internet. O estudioso americano Joseph Nigro também observou esse conceito, explicando-o da seguinte forma:

> O poder cibernético depende de uma série de recursos relacionados à eletrônicos e computadores utilizados para a criação de informações, controle e comunicação, incluindo infraestrutura de hardware, rede, *software* e habilidades humanas; definido da perspectiva do comportamento, o ciberpoder se refere a capacidade de obter os resultados desejados usando recursos de informação interconectados no ciberespaço; o ciberpoder pode ser usado para produzir os resultados desejados no ciberespaço, ou para produzir os resultados desejados além do ciberespaço usando ferramentas de rede. (NIGRO, 2012. p. 94).

Quer sejam exageros, quer sejam realmente preocupantes, as ameaças cibernéticas alcançaram uma projeção indiscutível no pensamento de segurança no pós-Guerra Fria, particularmente entre os analistas e os formuladores de políticas de segurança e defesa. Enquanto as forças armadas convencionais e os orçamentos militares diminuíram com o fim da Guerra Fria, a nova ênfase dada na segurança da informação e nas ameaças cibernéticas foi uma exceção notável.

1.1 A segurança cibernética na teoria de Relações Internacionais

Uma questão principal nos estudos de segurança orientados teoricamente é o verdadeiro significado do conceito de segurança. Há basicamente duas visões sobre isso: a dos tradicionalistas e a dos que defendem a ampliação do conceito de segurança (BUZAN e HANSEN, 2009). Os tradicionalistas são oriundos da visão Realista das Relações Internacionais, e praticam os Estudos Estratégicos centrados no Estado e orientados militarmente. Independentemente da perspectiva teórica, há uma lacuna óbvia a ser preenchida nos estudos de segurança: de abordar o impacto da revolução da informação para o entendimento geral da segurança no mundo contemporâneo, assim como para explicar a variação nas relações e políticas de segurança pelo mundo afora.

As teorias de Relações Internacionais são úteis no sentido de suprimir essa lacuna. O que as perspectivas de Relações Internacionais podem dizer sobre a segurança na idade digital? Serão abordadas duas visões das Relações Internacionais e o que elas podem afirmar sobre segurança: realismo e construtivismo.

As premissas centrais do realismo são basicamente três: (1) o Estado é a principal unidade de análise; (2) o Estado atua de maneira racional em busca de seu interesse nacional; (3) o poder e a segurança são os valores fundamentais do Estado. Além dos três pressupostos mencionados, em todas as versões do realismo, a visão de mundo se distingue por ser essencialmente pessimista. A anarquia, isto é, a falta de um poder supremo, caracteriza o sistema internacional, o que obriga os Estados a agirem conforme seus próprios interesses, visando à sua sobrevivência. As condições anárquicas e o egoísmo por parte dos Estados, estabelecem o chamado dilema de segurança. O poder, mensurado principalmente em termos de capacidades militares, associado à busca pela segurança, é a principal força motriz da política mundial.

Em princípio, os realistas não acham necessário revisar as suas teorias para entender a segurança na idade digital. O Estado continua a ser visto como o principal e, muitas vezes, único ator importante. Uma definição restrita de segurança é mantida, negando que atores não-estatais possam exercer algum tipo de poder (militar). Os realistas, presumivelmente, combateriam o desafio da revolução da informação da mesma forma como enfrentaram desafios anteriores, isto é, a transnacionalização, a interdependência complexa e a globalização. Assim, para essa corrente teórica, essas tendências são vistas como fenômenos secundários, que podem afetar as políticas e as estruturas domésticas dos Estados, mas que não enfraquecem o sistema anárquico da política internacional, e assim não afetam a primazia do Estado como a unidade política suprema.

Os realistas podem considerar as ameaças de segurança relacionadas à tecnologia da informação como sendo uma questão econômica, não necessariamente afetando a segurança dos Estados e não sendo elas uma ameaça à segurança. Entretanto, não há discordância de que assim como outros instrumentos, o espaço cibernético é mais um domínio em que o poder pode ser projetado visando ganhos relativos.

Por sua vez, os construtivistas em Relações Internacionais, e nas Ciências Sociais como um todo, enfatizam a inevitabilidade da interpretação e, assim, a distorção da realidade, especialmente no que diz respeito à compreensão das atividades social e política. Se há algo semelhante a um teorema central sobre quais forças moldam a política mundial ou a realidade social em geral, seria algo mais ou menos como o que será descrito a seguir. No nível mais básico, os atores têm um conjunto de normas – crenças sobre o que é certo e errado. As normas moldam as identidades, isto é, a separação de “nós” e “eles”. As identidades, por sua vez, moldam os interesses. Diferentemente do racionalismo, dentro do qual estão o realismo e o liberalismo, todos estes elementos são vistos como inerentemente dinâmicos. Se os

interesses mudam, é porque há uma mudança nas identidades e nas normas. Os fatores sociais não são vistos apenas como dinâmicos, mas também fortemente condicionais.

Diferentemente do realismo e do liberalismo, o construtivismo não busca uma teoria universal, mas sim generalizações condicionais, quer dizer, os construtivistas dão algumas orientações sobre o que as teorias de Relações Internacionais devem atentar. Tal visão pode ser considerada uma contribuição importante do construtivismo à segurança é a teoria da securitização, desenvolvida pela Escola de Copenhagen. Trata-se de como, quando e com quais consequências os atores políticos percebem algo como ameaça à segurança.

A ênfase é nos "atos de fala", nos quais se encontram os discursos políticos, e as implicações disso para o estabelecimento da agenda política e das relações políticas. A securitização implica na identificação de uma "ameaça existencial", evidenciado por meio do ato da fala, que prioriza a questão na agenda política, legitimando medidas extraordinárias como confidencialidade, uso da força e a invasão da privacidade.

Apesar da Escola de Copenhagen advogar um entendimento mais amplo para segurança, tal corrente de pensamento também não levou em conta a revolução da informação, principalmente porque sua existência como uma Instituição findou ainda no século XX. Mas a análise construtivista tem muito a oferecer para projeção dos conceitos dessa instituição sobre o ambiente ciberespacial.

A análise construtivista do poder e da segurança no mundo virtual implica enfatizar o significado das imagens e dos símbolos em adição à realidade material dos computadores e cabos. O estudo da política simbólica, isto é, o uso e abuso de símbolos para manipular o discurso político e a opinião pública, é bastante relevante para estudar a segurança na idade digital. A desfiguração de um site na web, por exemplo, é uma prática notável de política simbólica, menos antagonista, embora comparável, à queima da bandeira de um inimigo.

1.2 A tecnicidade da segurança cibernética

Adentrando o lado prático do espaço cibernético e suas ameaças, Tong Zhang explica que muitos programas de *software*, como servidores da web, bancos de dados e sistemas operacionais, são frequentemente desenvolvido usando linguagens de programação C/C++, que permitem manipulações arbitrárias de ponteiro e acessos de memória não gerenciados. Embora isso seja eficiente e flexível, os programadores são responsáveis por evitar acessos indevidos à memória. Se os programadores não forem cuidadosos, o *software* pode ter duas

formas de *bugs* de segurança de memória: segurança de memória espacial e temporal violações.

Uma violação de segurança de memória espacial ocorre quando um programa acessa uma região de memória além do limite designado do objeto, conhecido como estouro de *buffer*, que consiste em um transbordamento de dados. Esse problema ocorre quando um aplicativo excede o uso de memória reservada pelo sistema operacional. Com isso, esse programa começa a escrever informações nos setores de memória contíguos. Por meio dessas brechas, os cibercriminosos conseguem executar códigos maliciosos nos computadores e dispositivos da rede, o que pode levar à substituição de outro objeto ilegalmente ou à leitura de dados potencialmente confidenciais sem permissão.

Por outro lado, uma violação de segurança da memória temporal acontece quando um programa acessa um objeto desconectado (por exemplo, use-after-free ou use-after-return). Cabe ressaltar também, que algumas programações são construídas com vulnerabilidade intencionais, utilizadas por diversos fins, algumas vezes para permitir uma intervenção do próprio programador em prol do programa, ou em outras por má fé, de forma a gerar defeitos no produto a ponto de ser requisitado um suporte técnico. Independente da intenção do programador, essas também são brechas que são exploradas pelos cibercriminosos.

Infelizmente, muitos *exploits* de segurança tiram vantagem das violações de segurança de memória como um primeiro passo na obtenção do controle de um programa. O primeiro vírus de computador, conhecido como Morris, explorou um bug de estouro de buffer na ferramenta do UNIX. O infame vírus Blaster, que danificou milhões de estações de trabalho do Windows, também explora um bug de estouro de buffer. Um *bug* "*use-after-free*"[1] no kernel Darwin é usado para fazer o jailbreak do iOS e conseguir escalonamento de privilégios locais no macOS.

Tratam-se, portanto, de atores estatais e não-estatais como espiões, hackers, criminosos e terroristas cibernéticos que atuam em esquemas altamente organizados, capazes de orquestrar ataques sofisticados sem que sua presença seja notada até que a ação tenha ocorrido e os danos causados. Um estudo realizado pelo Instituto Nacional de Padrões e Tecnologia em 2002 aponta que *bugs de software*[2] custaram à economia dos EUA cerca de US $59 bilhões em perdas a cada ano, ou cerca de 0,6% do PIB. Em 2018, esse número saltou para US $1,7 trilhão, que é cerca de 8% do PIB.

---

[1] Refere-se especificamente à tentativa de acessar a memória depois que ela foi liberada, ou seja, a memória foi "desprendida" de sua origem e pode ser acessada em outro aparelho.

[2] Qualquer erro de código em programação.

Ressalta-se também que tais ações não são limitadas apenas às questões mais técnicas, muitos crimes e litígios que acontecem nos ambientes tradicionais – terrestre, marítimo e aéreo – também são projetados no ambiente virtual. Assim, mesmo sem conhecimento técnico, uma pessoa pode por exemplo praticar de *bullying,* de estelionato, entre outros. Embora esses sejam crimes mais tangíveis para o usuário comum, que gera um nível de preocupação, o uso de instrumentos técnicos como os descritos também deveriam ser frutos de preocupação da população.

Não é só uma questão de controle da máquina ou de informação, que por si só é por vezes ignorada pelo senso comum como um recurso de poder, mas também uma real ameaça a condição física do usuário. Exemplo dessa interação entre vulnerabilidades cibernéticas e ameaças físicas foi o ataque me 2017 ao hotel austríaco Romantik Seehotel Jaegerwirt, que teve seu sistema de fechaduras dos quartos e saguão hackeado, sequestrando todos os hóspedes e requerendo pagamento em moeda virtual para liberação (DEMARTINI, 2017).

1.3 Agentes da segurança cibernética (Estatais, proxy e não-estatais)

No que tange a segurança cibernética, nas últimas duas décadas a China, os Estados Unidos e a Rússia propuseram medidas substantivas como o aprimoramento das capacidades dos órgãos de comando e controle, o aumento do poder de serviços de inteligência, e a criação de novas divisões especializadas em segurança e defesa cibernética para conter esse tipo de ameaça. Ameaças advindas de Estados são reconhecidas como prioridades de ponta e críticas para focos de mérito de recursos e resposta nacionais. Uma lacuna, no entanto, diz respeito a informações sobre atores não estatais e atores estatais substitutos, também chamado de *proxy*, em relação aos mecanismos de cumprimento e fiscalização. Ambos os tipos de atores apresentam desafios cibernéticos interessantes devido às dificuldades de atribuição e responsabilidade.

Maurer define proxies cibernéticos como "intermediários que conduzem ou contribuem diretamente para um ação cibernética ofensiva que é ativada conscientemente, seja ativa ou passivamente, por um beneficiário." Por exemplo, os atores proxy fornecem um desafio de governança porque eles podem estar supostamente agindo sob o comando de um estado ator, mas o ator estatal recusa o reconhecimento e a reivindicação de suas ações.

Rússia e China são dois dos mais importantes atores adversários no domínio cibernético face aos Estados Unidos, seguido pela Coreia do Norte. Suas prioridades são obter informações para fornecer vantagens sobre os Estados Unidos e seus aliados nas

negociações e tomadas de decisões. Os ciberataques estatais incluem ciberespionagem, guerra cibernética, interferência em eleições, campanhas de desinformação, conhecidas como *fake news*[3], phishing[4], negação de serviço, malware, roubo de informações e outros tipos de interferências em governos, setores privados e civis. Em julho de 2019, a Microsoft observou que 8.000 de seus clientes foram atacados por países durante o ano anterior.

Um dos ataques cibernéticos mais significativo cometido por um Estado foi o vírus Stuxnet em um centro iraniano de enriquecimento de urânio, visando controle de supervisão e aquisição de dados, bem como centrífugas de urânio. Em 2012, o New York Times publicou um artigo afirmando que o vírus era parte de um programa de guerra cibernética dos EUA - Israel chamado "Operação Jogos Olímpicos", que repetiu ataques por vários anos. O ataque resultou na "disseminação de um modelo para o qual especialistas em segurança da computação consideram a arma cibernética mais perigosa de todos os tempos."(NEW YORK TIMES, 2012, n.p.). Stuxnet é um ataque significativo porque mudou o cenário cibernético no que diz respeito aos atores do estado com o primeiro ataque direcionado como arma a um sistema que até então parecia estar isolado de ataques cibernéticos.

Esse não foi um fato isolado dos Estados Unidos, sendo comum a utilização de uma variedade de relações de *proxy* para os Estados projetarem poder coercitivo no ciberespaço. As relações de proxy normalmente se enquadram em três categorias: delegação, orquestração e sanção – aprovação ou permissão –, com diversos usos de poder coercitivo. A intrusão da Sony em 2014 e o ataque cibernético do *ransomware*[5] WannaCry em 2017 são exemplos recentes de atividade cibernética de *proxy* de Estado.

A Coreia do Norte melhorou significativamente seus recursos cibernéticos ofensivos nos últimos anos, tirando proveito dos atores do Estado *proxy*. O ciberataque em todo o estúdio da Sony de 2014 vazou filmes inéditos online; postou salários e senhas dos executivos; e ameaçou funcionários com mensagens intimidadoras. O ataque projetou a evolução da Coreia do Norte como uma grande ameaça no ciberespaço.

---

[3] Cabe ressaltar que as *Fake News* apresentam dupla ameaça, a primeira a desinformação, já comentada, e a segunda seria o seu uso como instrumento da espionagem cibernética. Pois essa atividade não consiste apenas em adquirir informações, mas injetar outra de tal forma que resulte em um comportamento esperado pelo espião.

[4] Phishing é um termo originado do inglês (fishing) que em computação se trata de um tipo de roubo de identidade online. Essa ação fraudulenta é caracterizada por tentativas de adquirir ilicitamente dados pessoais de outra pessoa, sejam senhas, dados financeiros, dados bancários, números de cartões de crédito ou simplesmente dados pessoais.

[5] Ransomware é um software malicioso que infecta seu computador e exibe mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar. Essa classe de malware é um esquema de lucro criminoso, que pode ser instalado por meio de links enganosos em uma mensagem de e-mail, mensagens instantâneas ou sites. Ele consegue bloquear a tela do computador ou criptografar com senha arquivos importantes predeterminados.

No entanto, o ataque de ransomware WannaCry de 2017, possibilitado pelas vulnerabilidades dos Estados Unidos e da própria NSA, mudaram o jogo da segurança cibernética. O último ataque acelerou uma evolução em direção a variações mais sofisticadas de ataques cibernéticos em escala global, multivetoriais e patrocinados pelo estado. Mais de 300.000 computadores em 150 países foram infectados, causando bilhões de dólares em danos e paralisação das operações comerciais em todo o mundo. A NSA emitiu uma nota interna afirmando que os atores do Lazarus foram patrocinados pelo Reconnaissance General Bureau, escritório de inteligência da Coreia do Norte para operações clandestinas. Binxing Fang ainda observa que o ataque de 2017 "marcou a mudança em direção ao uso de nível militar armas, ferramentas de hacking que são poderosas o suficiente para uma agência nacional de defesa cibernética usar na ciberguerra internacional" (FANG, 2018 p.97).

A Rússia também utiliza amplamente os cibermercenários para ações de estado *proxy*. Turla é um grupo de ciberespionagem patrocinado pela Rússia que realiza campanhas contra instituições governamentais usando táticas criadas internamente, bem como táticas de exploração de código aberto em suas operações. Em outubro de 2019, o grupo foi responsável por comprometer um grupo de hackers apoiado pelo Irã, OilRig ou APT34, explorando suas técnicas e ferramentas e utilizando-as para atacar mais de 35 países. Inicialmente, os ataques foram atribuídos aos grupos iranianos; no entanto, mais tarde foi determinado que Turla mascarou sua identidade por meio dos iranianos, sequestrando seus endereços IP e acessando sua infraestrutura de comando e controle. Este caso demonstrou que comprometer indicadores - dados forenses - e identificar locais de acesso à infraestrutura podem ser úteis para determinar a atribuição correta.

Atores não-estatais, apesar de não estarem na vanguarda das discussões sobre regulamentação cibernética, freqüentemente conduzem uma preponderância das atividades cibernéticas malignas. O agente Ari Baranoff do Serviço Secreto dos Estados Unidos declarou que "muitos dos atores [não estatais] que verificamos diariamente e semanalmente têm capacidades que realmente excedem as capacidades da maioria das nações" (TRAUTMAN, 2016 p.230). O Conselho Nacional de Inteligência dos Estados Unidos define atores não-estatais como "entidades não-soberanas que exercem poder e influência econômica, política ou social significativa em uma política nacional e, em alguns casos, internacional" (JOSSELIN, WALLACE, 2001. p. 12).

Terroristas e simpatizantes do terrorismo também são considerados atores não-estatais. O FBI define o terrorismo internacional como "atos violentos e criminosos cometidos por indivíduos e/ou grupos que são inspirados por, ou associados a, designados

estrangeiros organizações ou nações terroristas" e terrorismo doméstico como atos semelhantes para "promover objetivos ideológicos decorrentes de influências domésticas, como as de caráter político, religioso, natureza social, racial ou ambiental." Para os fins deste trabalho, a categorização não-estatais será alinhada com o *National Intelligence Council, Journal of Military Ciência* e FBI, que incluem hackers, hacktivistas, terroristas, cibercriminosos e organizações relacionadas, que agem de acordo com sua própria agenda e ideologias sem qualquer laço ou apoio de estados (JOSSELIN, WALLACE, 2001).

Embora seja um ator estatal, os Estados Unidos atuam, também, como um componente integral da governança cibernética não estatal. A Divisão Cibernética do FBI é a agência federal dos EUA líder na investigação de ataques cibernéticos e intrusões em redes governamentais e privadas por atores não estatais, como organizações criminosas, terroristas e outros adversários cibernéticos. Em janeiro de 2015, supostos hackers pró-islâmicos do Daesh, grupo terrorista popularmente conhecido como ISIS, comprometeram o Twitter do The United States Central Command (USCENTCOM) e diversas contas do YouTube. Os simpatizantes de terroristas apelidaram o ato de "CyberCaliphate" e acessaram Servidores comerciais do CENTCOM por aproximadamente 30 minutos, postando uma foto de um lutador do ISIS com as palavras, "I love you isis" e "AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK " (AWAN, 2017).

O Pentágono confirmou o ataque, chamando-o de "pegadinha" e rotulando-o de vandalismo cibernético. Embora o USCENTCOM afirme que nenhuma informação classificada foi postada, números de telefones e endereços de e-mail da equipe foram listados durante 30 minutos antes de serem derrubados. Dúvidas foram levantadas com relação à atribuição; independentemente do ataque ter sido conduzido pelo CyberCaliphate ou outros atores não estatais, isso demonstra a facilidade e o baixo custo que são o suficiente para fazer um estrago na infraestrutura cibernética.

Outro exemplo do envolvimento dos Estados Unidos na medida de regulação cibernética não estatal foi o caso Avalanche de 2016. O Departamento de Justiça dos EUA anunciou em Dezembro de 2016 que sua Divisão Cibernética, juntamente com a Divisão Criminal do FBI, *Western District of Pennsylvania U.S. Attorney's Office*, Ministério Público da Alemanha e polícia local, Europol, investigadores e promotores de mais de 40 jurisdições globais, e várias outras entidades fizeram parceria para desmantelar uma infraestrutura criminosa — Avalanche — por meio de uma operação multinacional que resultou em prisões em quatro países. Era uma rede cibercriminosa, acessada através de fóruns on-line clandestinos, que forneciam uma infraestrutura segura para campanhas e transações

criminosas, como malware, esquemas de “mula de dinheiro”, lavagem de dinheiro fora do alcance da aplicação da lei (FANG, 2018).

Desde 2010, quando o Avalanche se tornou operacional, a rede redirecionou, diariamente, dados financeiros e informações roubadas de até 500.000 computadores infectados pelo *malware*, causando em todo o mundo perdas monetárias estimadas em centenas de milhões de dólares. Este caso é um exemplo da colaboração dos Estados Unidos com parceiros internacionais para derrubar o crime cibernético organizado. Neste caso, a jurisdição foi determinada com base na localização das vítimas de ataque de *malware*.

GozNym foi um dos *malwares* usados pelos criminosos do Avalanche. Em 8 de setembro de 2016, Krasimir Nikolov foi preso na Bulgária e extraditado para os Estados Unidos por sua conexão com o *malware* GozNym. Em 4 de outubro de 2016, Nikolov foi indiciado no Tribunal Distrital da Pensilvânia como um conspirador de acesso não autorizado de um computador para obter informações financeiras, fraude e conspiração criminosa. A rede Avalanche dava suporte a mais de 800.000 domínios que facilitavam transações criminosas de dinheiro entre as vítimas de malware e os cibercriminosos.

O caso Avalanche demonstra a necessidade de um sistema multilateral e multifacetado com um mecanismo regulador para atividades cibernéticas não estatais. Indivíduos, assim como os Estados, enfrentam uma infinidade de ameaças significativas desde países, Estados proxy e atores não estatais de várias origens, várias culturas, crenças e etc. É preciso haver maior cooperação e coordenação entre Governos, setores privados e parceiros acadêmicos para lidar com essas ameaças complexas.

2 A TERRITORIALIZAÇÃO DA INTERNET

A popularização do uso da Internet em meados dos anos noventa, foi acompanhada pelo discurso sobre ciberespaço, que argumentou-se, constituía um novo reino nele mesmo. Em um nível técnico, arquiteturas de rede - uma malha flexível que pode redirecionar o tráfego a qualquer momento através de qualquer nó - parecia diametralmente oposto ao estado-nação e seus limites rígidos. No entanto, essa arquitetura também conduziu facilmente em uma reivindicação política convincente de estar livre dos legados do Estado e das fronteiras. O desenvolvimento deste "novo e excitante domínio" prometia um espaço global ou internacional que era "Potencialmente livre de políticas convencionais, ordem social e regulação social" (WALL, 1997 p. 208).

Para muitos, este mundo sem fronteiras não iria e não poderia ser governado. Exemplo marcante dessa crença, o "Manifesto do Ciberespaço" de John Perry Barlow (1996) fornece a representação quintessencial desta visão. "Governos do Mundo Industrial", escreveu ele "O ciberespaço não está dentro de suas fronteiras [...]. Seu conceito legal de propriedade, expressão, identidade, movimento e contexto não se aplica a nós [...]. O nosso é um mundo que é ao mesmo tempo em toda parte e em lugar nenhum" (BARLOW 1996, np).

Embora as opiniões de Barlow certamente emergiram de uma tendência política mais radical, sua visão da internet como ingovernável foi adotada por políticos considerados mais tradicionais. Em 2000, o presidente dos EUA, Bill Clinton, observou que as autoridades chinesas já estavam tentando reprimir a Internet. "Boa sorte", brincou Clinton (WU, 2020 p. 180), "isso é meio que tentar pregar gelatina na parede". A internet sintetizou a livre circulação da liberdade de expressão. Qualquer esforço para impor um conjunto nacional de valores neste domínio, para forçá-lo a um molde nacional, apenas terminaria em fracasso.

Junto com o ciberespaço, termos como "a superestrada da informação" também postulavam uma ausência de fronteiras, mesmo que enquadrados em termos diferentes. Nessa visão da internet, o que divide uma vez impedido o acesso ao conhecimento - seja financeiro, geopolítico ou ambos - seria dissolvido. Nas palavras de Tim May (1999 p.09): "as fronteiras nacionais não são nem mesmo redutores de velocidade na rodovia da informação".

Por meio da digitalização, organização e conexão, a internet tomaria o depósito da informação do mundo. Isto a superestrada da informação permitiria que os dados fluíssem para qualquer lugar era necessário, tornando as fronteiras do estado-nação cada vez mais supérfluas. O novo mundo sem fronteiras foi caracterizado por fluxos globalizados de

informação, argumentou Ohmae (1990 p. 20) “é um absurdo acreditar que linhas desenhadas em mapas podem ter qualquer impacto em seus movimentos”.

Duas décadas depois, essas visões têm sido cada vez mais corroídas a ponto de parecer um tanto ingênuas. No lugar deles está uma visão da soberania cibernética, "uma extensão natural da soberania nacional no ambiente de rede" (WANG, 2014). Nessa visão, a Internet singular deve gradativamente se transformar em “nossa” internet, um território nacional onde as normas devem ser definidas, as ameaças devem ser contra-atacadas, e as fronteiras devem ser aplicadas. “Atrás das brumas e da magia da Internet reside uma ordem mais antiga e mais forte”, afirmaram Tim Wu e Jack Goldsmith (2006, p. ix), um pedido com base nas leis nacionais e governança soberana - um território de ordem. Ao longo de vinte anos, uma série de técnicas foram desenvolvidas para ajudar os Estados a imporem essa ordem na Internet supostamente global e ingovernável. Embora a territorialização sempre tenha sido desejável, estas técnicas agora parecem torná-la viável ou até mesmo inevitável.

2.1 Territorialização por geolocalização

A retórica imaterial do ciberespaço discutida anteriormente neste trabalho não será ensaiada aqui novamente. Mas, mesmo a linguagem muito mais recente da "nuvem" postulou um domínio arejado onde os dados circulavam livremente, um espaço dissociado da política restritiva de soberania e solo. Para empresas de nuvem, se os dados certamente foram armazenados em algum lugar, esse “onde” era efetivamente “qualquer lugar”. Forçado a construir novos centros de dados domésticos para armazenar dados para a Iniciativa GovCloud, a Amazon Web Services reclamou sobre a exigência, argumentando que “a localização física não tem influência” (OTTENHEIMER, 2018 np). Para empresas de nuvem e sua visão de uma web distribuída e descentralizada, os dados “fixos” eram um anátema.

Ao lado de fornecedores de tecnologia, juristas também questionaram como as informações poderiam ser vistas como fixas, dado as condições da Internet. Lutando com novas tecnologias, pesquisadores argumentaram que a conectividade de rede fundamentalmente desafiou paradigmas antigos, como a territorialidade. Em um artigo que explora a jurisdição e a nuvem, Andrews e Newman (2013 np.) sugerem que “a concepção baseada no território de Estados e Estados-Nação pode estar rapidamente se tornando arcaica em um mundo cada vez mais conectado”. Da mesma forma, no artigo intitulado The Un-Territoriality of Data, Jennifer Daskal (2015, p. 326) argumentou que, devido à facilidade

e velocidade dos dados viajar além das fronteiras, em essência, “os dados estão em toda parte e em qualquer lugar”.

Essa visão está cada vez mais em desacordo com o impulso liderado pelo estado para uma compreensão territorial dos dados. Leis transfronteiriças procuram controlar quando e como os dados podem ser transferidos para outra jurisdição. Informações de acordo com essas estruturas não estão girando em algum reino nebuloso "lá fora", mas estão alojados em centros de dados localizados dentro das fronteiras do Estado-Nação. Como escreveu Duggal (2018), essas leis transfronteiriças desafiam “os países a adaptarem os modos pré-digitais de soberania nacional e competição econômica para uma indústria digital que prospera na troca de informações sem fronteiras e contínua”. Embora a internet possa ser global, "sua" rede tem limites claros.

Na verdade, um dos aspectos centrais das leis transfronteiriças examinados por juristas são seus "efeitos”, as propriedades que especificam quais tipos de dados são cobertos e em que condições esses dados podem ser transferidos fora da nação. Os próprios dados têm uma localização geográfica, um lugar que fica dentro ou fora da linha pontilhada do Estado-Nação. Da Malásia à Coreia do Sul, Filipinas e Japão, uma série de países asiáticos já passaram ou estão atualmente considerando a legislação transfronteiriça (GIROT, 2018 np.).

Como resultado desse entendimento, os governos estão colocando empresas sob crescente pressão para armazenar e processar estes dados em centros de dados domésticos. A Lei de cibersegurança da China, que é muito próxima do Regulamento Geral de Proteção de Dados da Europa, requer dados de infraestruturas críticas para permanecer dentro de seus territórios. De acordo com o Artigo 37 da lei, “todas as informações pessoais e outros dados importantes produzidos e recolhidos pela CII operadores (e agora também operadores de rede) devem ser armazenados em servidores localizados na China continental” (FANG, 2018 p.362). Na União Estados, GovCloud promete cibersegurança, oferecendo dados infraestrutura do centro "operada por funcionários que são cidadãos dos EUA em solo dos EUA" (AMAZON, 2020 np). A linguagem da terra e dos cidadãos, rejeitados como desatualizados ou irrelevantes há duas décadas, aponta para o ressurgimento da territorialidade dentro do contexto da internet.

Um site, serviço ou plataforma é ainda mais acoplado à nação pelos dados pessoais que aproveita. Esses dados não são genéricos nem abstratos, mas representam dados altamente íntimos com detalhes altamente valiosos de seus cidadãos. Esses dados podem ser usados ou intencionalmente mal utilizados, especialmente se escapar à jurisdição do governo.

Como tal, a proteção desses dados está sob a tutela do Estado e sua missão de apoiar a vida e os meios de subsistência desses sujeitos.

Como um breve exemplo desse forte apego à nação, considere Singapura. De acordo com sua Lei de Proteção de Dados Pessoais, esta regra internacional se aplica a uma organização ou corporação "formada sob a lei de Singapura" ou qualquer residente "com um escritório ou local de negócios em Singapura" (CHIA, 2018, p. 327). Em Chander e Le 's (2015), essas estratégias de localização constroem coletivamente uma espécie de "nacionalismo de dados". Quadros de legislação transfronteiriça dados como um recurso tangível e soberano, informação que é tanto dentro da nação quanto vinculada a um sujeito nacional.

2.1.1 Geolocalização

As ferramentas de geolocalização permitem que os agentes da Internet localizem dispositivos conectados à rede e identifiquem a localização física em tempo real dos usuários.

Inicialmente, os tribunais eram céticos quanto à precisão e confiabilidade da geolocalização, os tribunais consideraram inadequados para fins de cumprimento legal. Em 2002, por exemplo, o Supremo Tribunal da Austrália opinou em Dow Jones v. Gutnick que "não [havia na época] tecnologia adequada que permitiria aos provedores de conteúdo sem assinatura isolar e excluir acesso total a todos os usuários em jurisdições específicas". (Dow Jones & Company Inc. v. Gutnick, 2002 p.263). A decisão da Yahoo! de 2006, e particularmente a concordância do juiz Fisher, revelou a ambivalência do Nono Tribunal do Circuito sobre geolocalização naquela época (9th Cir., 2006).

Os tribunais também estavam preocupados com a precisão da geolocalização porque os usuários podem, e o fazem, utilizar ferramentas de fraude que fazem sua localização aparecer em um local diferente de física real.

Melhorias substanciais nas tecnologias de geolocalização devem agora aliviar preocupações dos tribunais sobre a precisão e o custo das ferramentas de geolocalização e bloqueio geográfico. Métodos simples de geolocalização que dependem de auto relatos não confiáveis ou da detecção mais confiável de endereços de protocolo de Internet (BASSETT, 2006) estão sendo substituídos por métodos avançados que combinam dados de várias fontes, como sinais de GPS e *wi-fi* para fornecer uma precisão significativamente maior com maior granularidade (FANG, 2018).

Muitas motivações levam os atores da Internet a localizar geograficamente os usuários; as informações de localização podem ser usadas para coletar estatísticas para marketing e outros fins, fornecer conteúdo localizado, apoiar a segurança cibernética medidas, dividir mercados a fim de discriminar preços e cumprir outros propósitos, como a instrumentos contra fraudes na compra de conteúdo, como ocorre com os jogos digitais. Gradualmente, a geolocalização está deixando de ser uma questão de escolha e está se tornando uma necessidade para conformidade na Internet. Conforme as ferramentas de geolocalização melhoraram, os países tornaram-se menos hesitantes em regular a conduta na Internet com base nos efeitos da conduta; eles agora estão substituindo regulação baseada na fonte da conduta com regulação baseada no local de consumo (TRIMBLE, 2016 p. 266-70).

2.1.2 Geobloqueio

Juntamente com a geolocalização de dados, o uso crescente dos geobloqueios representam uma forma rudimentar, mas poderosa, de soberania. Essas interrupções intencionais tornam a Internet “inacessível ou efetivamente inutilizável, para uma população específica ou dentro de um local, muitas vezes para exercer controle sobre o fluxo de informações” (ACCESS NOW, 2019 np). Certamente desligamentos praticamente totais ocorrem em países tipicamente considerados autoritários: Chade, a República Democrática do Congo, Iraque, Cazaquistão e Rússia (FANG, 2018).

No entanto, o líder mundial em paralisações é uma nação amplamente considerada como uma democracia, a Índia. Mais de 381 desligamentos foram registrados pela Lei de Liberdade de Software Center (2020), que mantém uma página que rastreia desligamentos em todo o país. Essas estatísticas mostram que a Índia não só desliga sua Internet mais do que todos os outros países combinados, mas está fazendo isso com mais frequência, com o número de desligamentos aumentando nos últimos anos para se tornar o “novo normal” (SURESH, 2019).

Para a Índia, a internet não é um bem público que deve estar constantemente disponível, mas uma infraestrutura nacional que pode e deve ser ligada e desligada conforme estrategicamente necessário. Como um caso específico, por exemplo, a paralisação mais longa do mundo foi imposta na Caxemira. Em 4 de agosto de 2019, o parlamento revogou o Artigo 370 da Constituição, dividindo o território administrado e privando-o de direitos anteriores. Antecipando ativismo e agitação civil, uma paralisação foi instigada.

Funcionários justificaram a paralisação afirmando ser necessária para “manter a paz” na região (NAZMI, 2019). A paralisação continuou por 176 dias, com ambos os serviços fixos e móveis restritos. Finalmente, em 26 de janeiro de 2020, o desligamento foi parcialmente suspenso quando o acesso aos serviços móveis de segunda geração (2G) foi restabelecido. No entanto, junto com velocidades incrivelmente lentas, os serviços acessíveis incluem apenas uma lista de permissões altamente seletiva: uma lista minúscula de 300 sites, incluindo bancos, alguns portais de notícias, instituições educacionais, serviços públicos, viagens e aplicativos de entrega de comida (AL JAZEERA NEWS, 2020).

Os governos frequentemente falham em fornecer qualquer tipo de explicação pública para decretar uma paralisação. Quando as razões são dadas, muitas vezes giram em torno da prevenção da disseminação prejudicial de informações, neutralizando a tensão e mantendo a ordem. Em 2018, as justificativas mais comuns foram segurança pública, notícias falsas ou discurso de ódio e violência relacionada à segurança nacional (TAYE, 2018).

Claro, se tais desligamentos são eficazes nesses objetivos é discutível. Em um estudo sobre as paralisações da Índia, Rydzak (2019) descobriu que eles encorajam os ativistas a substituir protesto não violento, que muitas vezes requer coordenação via comunicação online, com mais intervenções violentas *ad hoc*[6]. No entanto, independentemente de sua capacidade de reprimir a agitação civil, o ponto-chave aqui é que o desligamento enquadra a internet como “nossa”. Em vez de uma extensão de recurso universal em todo o mundo, a internet se torna uma infraestrutura doméstica, um território que segue a pegada do estado-nação e termina na fronteira. Junto com este link geográfico para da nação, há também um vínculo de poder.

As paralisações são uma demonstração concreta de controle soberano, demonstrando a capacidade de exercer uma força bruta, mas devastadora, sobre sua infraestrutura, desligando-a completamente. A Índia enquadra a internet como um espaço que deve ser ditado por decisões soberanas. As paralisações estabelecem um plano de intervenção nacional.

Para Selva (2019), o uso crescente desta técnica pela Índia tem levado outras nações a "descobrir o interruptor de desligar", incluindo o Sudão, após uma brutal derrubada do governo protesto, e Benin e Malawi, coincidindo com parlamentares e eleições presidenciais. Especificamente na Ásia-Pacífico, Nauru, uma ilha pequena, mas significativa, usada para detenção e processamento de pedidos de asilo, anunciou uma paralisação temporária em

[6] O termo “Ad Hoc” vem da língua latina e significa “para isso” ou “para este efeito”.

2015. A nação impôs uma proibição ao Facebook e outros sites como um mecanismo de proteção para "garantir que os Nauruans não sejam deixados expostos e vulneráveis às ações de criminosos, e cyber bullies"; a paralisação atendeu a novas leis imposição de pena de prisão por discurso que foi considerado uma ameaça à segurança nacional (OLUKOTUN, 2015 p.2335). Mais recentemente, a Indonésia impôs uma paralisação que buscava "acelerar os esforços do governo para restaurar a ordem em Papua Ocidental, após contínuos protestos violentos" (FIRDAUS, 2019 p.195). Esses desligamentos demonstram a soberania do estado, flexionando sua autoridade sobre a Internet.

2.2 Territorialização por filtro

Se as paralisações são uma exibição contundente do território da internet como território nacional, também são grosseiras. Filtrar informações é mais intervenção sofisticada que busca construir uma internet moldada à imagem do Estado. Filtrar, bloquear ou censurar informações cai sob o mesmo guarda-chuva, com técnicas variando de bloqueio de porta e filtragem de palavras-chave para pesquisa e alterações no motor (HAMADE, 2008). A ideia, como em qualquer *firewall*[7], é que a inspeção dos pacotes que passam pelos programas sinalize quais informações o usuário está solicitando, seja um site ou um termo de pesquisa controverso. O controle nesta "fronteira digital" permite que os pacotes sejam acessados, modificados, desviados ou ignorados completamente.

Um dos exemplos mais recentes de filtragem é a "Lei Russa da Internet" aprovada em maio de 2019, uma lei que "exige provedores de serviços de internet para filtrar todo o tráfego por meio de "nós" sob o controle de Roskomnadzor, o censor da Internet do Kremlin (FINANCIAL TIMES, 2019 np). Um domínio russo de serviço de nomes, combinado com legislação que obriga as empresas a armazenar dados internamente, poderia teoricamente observar todos os tráfegos no país. Pedidos de sites "estrangeiros" e os serviços poderiam ser bloqueados ou transformados em seus equivalentes nacionais, garantindo que as informações sempre permaneçam dentro das fronteiras do Estado-Nação.

Como Epivanova (2020) sugere, apesar da retórica da cibersegurança, o objetivo da emenda não é sobre defender a Rússia de ataques externos, "mas sim um passo pró-ativo para

[7] Firewall é uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo. os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede mas também a confidencialidade deles.

separar seu próprio segmento nacional da infraestrutura da Internet global, a fim de ganhar a soberania do estado sobre ele" (EPIVANOVA, 2020, p. 09).

O principal exemplo em qualquer discussão sobre filtragem é a China. Já em 1997, a *Wired* descrevia um conjunto de mecanismos técnicos e legislativos que coletivamente apelidado de Grande Firewall da China, agora frequentemente abreviado para GFW. Filtrando o material poluente "destinado a minar a unidade e a soberania da China", os engenheiros procuraram criar sua própria versão distinta da internet, "uma rede que tem características" (Barme, 1997). Tecnicamente, isso foi decretado *peering*[8] com o pequeno número de *gateways*[9] nas bordas da rede chinesa.

Conforme os dados passavam por esses pontos, eram identificados e alterados. Alguns pedidos foram atendidos e outros recusados, bloqueando esses sites e serviços dos usuários. Desde o seu início, este projeto só se tornou mais sofisticado. Nos últimos vinte anos, novas funcionalidades foram gradualmente integradas, resultando em um grau de controle altamente articulado e extenso.

Na primeira fase, o GFW bloqueou nomes de domínio e endereços IP; na segunda etapa, implementou censura de palavras-chave; na terceira etapa, passou a detectar VPNs (redes privadas virtuais) e outras ferramentas de evasão; e no quarto estágio, esses mecanismos de *hardware* e *software* foram complementados por legislação que visava ao anonimato e VPNs (CHANDEL et al. 2019).

A filtragem de informações visa remover ou bloquear mídia que é considerada questionável de acordo com a legislação e as normas sociais. Nesse sentido, a filtragem enquadra inerentemente a internet como extensão do território nacional. Para combater a informação perigosa e não filtrada "lá fora", os mecanismos de *hardware* ou *software* controlam o tipo de informação permitida "em" um país. O objetivo é alinhar o território digital da China com seu território físico, para eliminar qualquer tipo de disparidade quando um assunto muda entre offline e ambientes online. Para Xi Jinping "não há nenhuma distinção entre o mundo virtual e o mundo real: ambos devem refletir os mesmos valores políticos, ideais e padrões " (ECONOMY, 2018 np).

O que inspira essa territorialização da internet por meio de desligamentos, localização e filtragem? Com certeza uma motivação é controle. Para os estados, essas técnicas visam

---

[8] Em redes de computadores, o peering é uma interconexão voluntária de redes de Internet separadas administrativamente com o objetivo de trocar tráfego entre os usuários de cada rede.

[9] Gateway pode ser classificado como "portal" ou "portão". Em resumo, uma passagem entre dois ambientes distintos. Em outras palavras, é um sistema ou equipamento encarregado de estabelecer a comunicação entre duas redes. ... Ele faz o papel de ponte entre as redes.

agarrar apoio a um grau de autoridade sobre um domínio visto como frustrante e escorregadio. Quando a internet se torna uma caixa inflamável que pode instigar tensões - ou mais cinicamente, um site de contra-protesto ou constrangimento para o establishment político - então evidencia-se a busca pela capacidade de restringir essas comunicações.

Citando as paralisações na Índia discutidas anteriormente, o Estado alinhado ao Diário do Povo da China afirmou que tais medidas são um "Regulamentação necessária" da internet, uma "escolha razoável de países soberanos com base nos interesses nacionais, e uma natural extensão da soberania nacional no ciberespaço" (WANG, 2014 p.305). Seja por meio de legislação ou *hardware*, esses movimentos buscam regular "sua" internet da maneira que acharem melhor.

No entanto, talvez mais justificadamente, essas medidas também contestam uma visão "universal" da Internet, há muito reconhecida como implicitamente liderada pelos Estados Unidos. Para algumas nações, o suposto a internet global parece mais com o domínio americano desfrutado por um punhado de gigantes tecnológicos: Google, Facebook, Apple, Amazon e outros. Essas corporações estão alinhadas com as ideologias tecno libertárias do Vale do Silício e os valores ocidentais mais amplos de consumismo e individualismo.

Para Kalev Leetaru (2019), este *cluster* de empresas representa uma nova geração de "colonialismo cultural" na medida em que reforçam um conjunto global de normas estabelecidas pelo Vale do Silício; essas "ditaduras digitais transcendem as fronteiras nacionais tradicionais, impondo suas crenças, narrativas e regras sobre o mundo em geral"(LEETARU 2019, np). Para Estados com tendências mais autoritárias, uma mudança global da Internet para uma Internet nacional permite que eles eliminem esses valores indesejados e começam a incorporar seus próprios ideais.

Para os críticos, essas medidas colocam a Internet em risco de balcanização. Chamadas urgentes para evitar a balcanização podem ser cada vez mais encontradas nos principais meios de comunicação, em blogs de tecnologia, organizações civis, e revistas políticas. "Não podemos permitir que a Internet se torne balcanizada", defendeu Sascha Meinrath (2013 np) em um artigo amplamente citado; tal fragmentação transformaria a futura Internet de um "bem comum global a uma colcha de retalhos fragmentada severamente limitada pela política limites em um mapa".

Embora essas ligações tenham se tornado mais frequentes, sua retórica também foi acelerada, com urgência linguagem procurando apontar as enormes apostas. Fragmentação, somos informados, sinaliza nada menos do que a morte da Internet. "Os governos quebraram

a rede mundial de computadores", lamentou Mark Scott (2017), “criação de regras digitais regionais ameaça inviabilizar os avanços econômicos, sociais e políticos da era da Internet”.

No entanto, examinando a literatura, o mundo se posicionou à beira do precipício de balcanização por vinte anos. Ansiedades em torno da fragmentação surgiu já em 1997 e tem continuado ininterruptamente desde então, com cada acadêmico proclamando o fim da internet “livre e aberta”. Claro, a conversa certamente mudou com o tempo. Preocupações iniciais eram principalmente comerciais e técnicos, com foco, por exemplo, sobre os provedores de serviços de Internet recusando-se a “fazer pares” entre si (SAGAWA 1997; FRIEDEN 1998). Mais tarde, as preocupações assumiram uma matriz marcadamente mais geopolítico, enfatizando como a web “global” estava sendo fragmentada por inimigos antiamericanos como China e Rússia (EARLE, MADEK 2002; WU 2004; WERBACH 2008; KUNER ET AL. 2015; CATTARUZZA ET AL. 2016).

Apesar da angústia desses críticos, a internet sempre foi balcanizada. O singular “Internet” implica uma rede coesa e abrangente que abrange o globo. Mas a internet é melhor entendida como um sistema de sistemas, uma rede de redes. “Toda a Internet é uma coleção de *links* de longa distância entre redes discretas e conectadas localmente”, conforme Jack Goldsmith (2019, p.54), que nos lembra ainda que enquanto aparece “Suave e sem características, é na verdade um grupo de ilhas com ligações entre eles”.

Cada rede está conectada às outras por meio de uma complexa variedade de cabos, gateways e “nós” de interconexão. A Internet é o resultado desse funcionamento links. Nada revela mais essa ilusão de unidade do que interrupções de conectividade em nível nacional ou regional. Quando desligamentos ocorrem ou cabos são quebrados, este efeito coesivo é também quebrado.

Mesmo em um nível mundano, o "fluxo livre" de informações tem sido um mito desde o início. As redes nunca foram domínios onde vale tudo, mas, em vez disso, impuseram um conjunto estrito de controles sobre as solicitações de dados que foram atendidas, os usuários e portas que foram habilitadas, e as comunicações que poderiam ser divulgadas (MUELLER, 2019). Por razões de segurança e eficiência, a filtragem era integral, incorporada em ambas as camada de rede e como um recurso básico em roteadores de rede.

Na verdade, foi precisamente essa funcionalidade que permitiu a rede filtragem no âmbito da empresa para traduzir para o nível nacional ou geopolítico. “Ninguém questiona a autoridade e o direito de uma corporação para gerenciar, controlar e monitorar rigidamente ãa comunicação dentro e fora da rede de uma empresa”, documenta James Griffiths em sua história do Grande Firewall (2019, p.75), e continua: “essa tecnologia foi construída desde o

início para atender o mercado de clientes corporativos. Tudo que a China fez foi ligar esses interruptores para todo o país ”.

Junto com essa fragmentação técnica, cada rede também possui um grau de autonomia emergente de seu desenvolvimento social, cultural e histórico. É por isso que os estudiosos podem narrar o surgimento da internet chinesa (NEGRO, 2017; GRIFFITHS, 2019), a internet cubana (HARRIS, 2015), a tentativa e o fracasso de construir a internet soviética (PETERS, 2017) e assim por diante. Como um estudioso argumenta), assim como não existe uma televisão singular, mas sim "esta televisão, nossa televisão”, também não existe uma internet singular; em vez disso, “A Internet chinesa é uma forma cultural muito parecida com a televisão americana ou a televisão britânica” (YANG, 2012, p.49). Embora os padrões e protocolos globais certamente devam ser respeitados, cada uma das redes é uma internet “nacionalizada” no sentido de que sua construção exigiu mão de obra de engenheiros nacionais, documentação na língua nacional e decisões particulares tomadas no interesse nacional.

Essas observações mostram como a fragmentação sempre tem sido parte integrante da internet, tanto na arquitetura técnica quanto no desenvolvimento histórico. Mas talvez o aspecto mais prejudicial da "balcanização" como um espectro é que ela substitui um mito da internet sem fronteiras com outro mito da Internet limitada. Com base em um modelo westfaliano (idealizado), o mundo é dividido em “unidades espacialmente exclusivas” sem jurisdições sobrepostas (CAPORASO, 2000). Nesta visão, a internet de cada nação se ajusta perfeitamente ao pontilhado linhas de suas fronteiras nacionais.

Cada nação estabelece *gateways* nas bordas desta zona cibernética, de forma abrangente, para isolar as informações e comunicações que levam a colocar dentro deles. Cada nação pega informações “globais” e as delineia de forma limpa em doméstica e estrangeira, nacional e internacional. A Internet torna-se a Internet deles, um espaço governado com precisão absoluta.

Conforme discutido acima, certamente há uma mudança em direção à territorialização, com as nações enquadrando essas redes como uma extensão do espaço soberano. No entanto, esses territórios são confusos e suas bordas são permeáveis. O sonho estatal de territorialização permanece incompleto, e isso não se deve apenas à incapacidade técnica, mas porque a nação deriva sua identidade de entidades fora dela.

Esta visão ecoa a glocalização, um conceito introduzido em reconhecimento ao fato de que "muito de a promoção da localidade é feita de cima ou de fora”; mesmo nas “formas mais agressivas de nacionalismo contemporâneo”, observa Robertson (2002, p. 26), “ainda há um

fator translocal em ação". A territorialização está sendo constantemente moldada por práticas, narrativas e instituições que ocorrem no espaço "extraterritorial" em torno de suas fronteiras. Para demonstrar essa dinâmica de uma forma mais concreta, volto à China - sem dúvida o exemplo mais forte de soberania cibernética - para examinar como as atividades além do *firewall* são capazes de ambos intensificar e minar a internet como espaço nacional.

3 TERRORISMO E A INTERNET

Como visto no capítulo anterior, atores não-estatais conseguem gerar grande impacto com severas consequências tanto para indivíduos quanto para Estados no espaço cibernético. Consequências que afetam direta ou indiretamente o "mundo real". A Internet é um ambiente único e desafiador no qual a radicalização e o recrutamento terrorista ocorrem com frequência, e que a compreensão e penetração neste ambiente é essencial para prevenir o terrorismo local (STEVENS, 2009).

Neste capítulo haverá uma breve definição (ou tentativa) do que é terrorismo e como grupos terroristas agem e recrutam pessoas pelo mundo usando o espaço cibernético.

3.1 Definições de terrorismo

O terrorismo continua sendo um conceito ambíguo com desacordo entre acadêmicos e governos sobre a natureza do conceito do termo. A subjetividade não pode ser totalmente evitada e os dados sobre o terrorismo refletem inelutavelmente algumas entre as várias igualmente razoáveis interpretações do conceito (PYTHON, 2020). Ademais, há tentativas do uso do conceito para fins políticos, como por exemplo quando o governo colombiano tentou incluir as ações da FARCS como oriundas de um grupo terrorista.

Visando a universalização do conceito, em 2000, foi estabelecido um Comitê Especial no âmbito da Assembleia Geral da Organização das Nações Unidas (ONU) a fim de negociar uma Convenção Global sobre Terrorismo Internacional, entretanto ainda não foi estabelecido um critério único para todos os países. Tendo em vista que uma determinada definição de terrorismo adotada pode servir a interesses políticos, algumas vezes, desfavoráveis a outros Estados, o estabelecimento de um consenso acerca do tema fica prejudicado. O Art. 2º do projeto da referida Convenção prescreve a seguinte definição universal de terrorismo :

> Quando o propósito da conduta, por sua natureza ou contexto, é intimidar uma população, ou obrigar um governo ou uma organização internacional a que faça ou se abstenha de fazer qualquer ato. Toda pessoa nessas circunstâncias comete um delito sob o alcance da referida Convenção, se essa pessoa, por qualquer meio, ilícita e intencionalmente, produz: (a) a morte ou lesões corporais graves a uma pessoa ou; (b) danos graves à propriedade pública ou privada, incluindo um lugar de uso público, uma instalação pública ou de governo, uma rede de transporte público, uma instalação de infra-estrutura, ou ao meio ambiente ou; (c) danos aos bens, aos locais, às instalações ou às redes mencionadas no parágrafo 1 (b) deste artigo, quando resultarem ou possam resultar em perdas econômicas relevantes. (PANIAGO, 2007 p.14)

O terrorismo é comumente assumido como sendo politicamente dirigido, ao contrário de outros crimes, que encontram sua motivação em diferentes razões. Por exemplo, o crime passional é motivado principalmente por motivos pessoais, e não por motivos políticos (primeiro critério: objetivo político). Além disso, o terrorismo muitas vezes visa gerar medo per se (segundo critério: Medo), como sugerido por sua raiz latina terrere, que significa literalmente "para amedrontar". Outras formas de crime, como roubo, por exemplo, não possuem como objetivo principal gerar medo. Em vez disso, o roubo é principalmente movido por questões econômicas e materiais. Mesmo que as vítimas de roubo possam também ter medo, essa é geralmente uma consequência indireta de roubo (PANIAGO, 2007).

Mesmo entre categorias que possa inocentemente ser comparada, quando observada a questão medo e os alardes que provocam, como guerrilha e organizações criminosas, ainda assim há diferenças entre eles para com o conceito de terrorismo:

Quadro 3.1 – Diferenças entre grupo guerrilheiro, grupo terrorista e organização criminosa

	Grupo Guerrilheiro	Grupo Terrorista	Organizações Criminosas
Modo de atuação	1. Guerrilha rural e urbana; 2. Aniquilamento seletivo de autoridades; 3. Seqüestro; e 4. Atos terroristas.	Atos terroristas de modo geral.	Emprego de violência generalizada, podendo abranger, algumas vezes, atos que visem a aterrorizar a população.
Motivação	Política ou ideológica.	Política ou ideológica.	Econômica.
Área de atuação	Nacional ou Regional	Internacional e Nacional	Internacional e Nacional
Estrutura	Hierarquia militar centralizada	Células descentralizadas	Hierarquia centralizada

Fonte: Revista Brasileira de Inteligência. Brasília: Abin, 2007

O terrorismo é um tema que vem pouco a pouco ganhando seu espaço na academia brasileira, seja pela crescente atenção que o país despertou no cenário internacional, sediando tanto a Copa do Mundo em 2014 como os Jogos Olímpicos em 2016, sendo que, no caso deste último evento, foi elaborada a Lei Brasileira Antiterror, em vigor desde sua publicação em 2016. Sendo assim, ainda é preciso certo amadurecimento da abordagem da matéria pelo poder público, tendo em vista que, infelizmente, verificou-se pouco amadurecimento desde a Lei de Segurança Nacional de 1983, com a repetição de erros conceituais e a ausência de um controle central para tais políticas públicas nacionais, como no exemplo das leis americanas e de Hong Kong (ROCHA e SCHUBERT, 2020).

O Brasil é um país que historicamente não sofreu um ato terrorista em mais de 30 anos e detém uma cultura "pacifista" que termina por ocasionar em posição negativa do Estado sempre que surgem boatos de atuação de grupos armados no país. Alia-se a isso o fato de que o país geralmente surge como um dos países menos prováveis de ocorrência de grandes atentados nos rankings mundiais sobre o tema (ROCHA e SCHUBERT, 2020).

3.2 O terrorismo do espaço cibernético

O que torna os terroristas diferentes do usuário geral do espaço cibernético é o propósito para o qual eles estejam online. Gabriel Weimann (WEIMANN, Terror on the Internet: The New Arena, the New Challenge, 2006), distingue as ações terroristas entre atividades que visam construir, apoiasm e gerar publicidade (comunicativa), e aquelas que facilitam atos de terrorismo (instrumental). Ressalta-se que terroristas usam a Internet a muito tempo para essas atividades, inclusive para divulgar suas ideologias virulentas e recrutar indivíduos vulneráveis para seus grupos. Este uso da Internet, entretanto, escalou para o ponto no qual é possível recrutar indivíduos para o terrorismo exclusivamente por contato pela internet.

Como isso é possível? Existem muitas razões; o primeiro entre eles é que, no caso de grupos jihadistas militantes, como Al Qaeda, Boko Haram e outros passaram décadas espalhando suas ideologias e convencendo muitos de que o terrorismo suicida é um tipo de martírio islâmico, que construir um Califado, seria uma meta a ser alcançada posteriormente. Ademais, tentam convencer que fazer hijrah - isto é, viajar para terras regidas pela lei sharia - e participar na jihad militante são obrigações de todos os muçulmanos.

Além disso, a internet tem evoluído a um ponto em que os mecanismos de *feedback* imediato das mídias sociais tornam possível para os terroristas cobrirem a internet com suas propagandas e mensagens de recrutamento e apenas esperar obterem respostas de usuários interessados. Eles podem, então, focar sua energia para aperfeiçoar aqueles que mostram interesse - "amam bombardear" - e enxameiam informações e propagandas ideológicas sobre eles (MENDELSOHN, 2011).

Da mesma forma, a Internet criou um ambiente em que o mundo se tornou menor e mais interconectados, com a possibilidade de visualizar vídeos e imagens emocionalmente evocativos de partes distantes do mundo em tempo real. Isso joga com as crenças islâmicas já existentes sobre a interconexão da ummah muçulmana, algo que terroristas jihadistas militantes são rápidos para capitalizar. O sofrimento de outros muçulmanos é o sofrimento de

todos, de acordo com suas reivindicações, e a jihad é o dever de vir em seu socorro (MENDELSOHN, 2011).

Embora a humanidade por vezes tenha dificuldade de aceitar, a intimidade e aproximação pelo espaço cibernético é diferente, mas possível. Isso foi demonstrado durante o ano de 2020, com a pandemia do COVID-19, ocasião que obrigou as pessoas a buscarem meios de continuar a vida, e consequentemente suas relações.

Esse pequeno exemplo demonstra que quando um indivíduo mostra interesse e é contatado por um recrutador de terroristas, a possibilidade de um relacionamento real e íntimo agora é possível, dada a capacidade de vídeo e áudio, mensagens de texto, chat e e-mail. Os recrutadores terroristas agora podem chegar aos quartos dos vulneráveis jovens, e passar horas de investimento em treinamentos, tempo esse que poucos pais teriam para lidar com os filhos. Assim, preparam seus jovens recrutas para acreditar que ingressar no grupo terrorista é a melhor maneira de encontrar propósito, significado, dignidade, prosperidade, aventura, respostas aos problemas e para garantir sua vida após a morte (MENDELSOHN, 2011).

Mostrar imagens gráficas de sofrimento na ummah muçulmana para motivar os espectadores têm sido há muito tempo a ação principal de recrutadores jihadistas militantes. Com a capacidade atual da Internet recrutadores conseguem atingir e manipular as emoções de seus recrutas em potencial, mostrando-os graficamente eventos em tempo real, através de *livestreams,* ocorrendo em todo o mundo, enquanto os convence de que eles têm a missão de acabar com esse sofrimento. Da mesma forma, a recém-descoberta intimidade em conexões de Internet, ao lado da possibilidade de criptografar a comunicação através de aplicativos como WhatsApp e Telegram, tornam as relações de recrutamento de terrorista baseado na Internet relações reais, vívidas e ocultas ao mesmo tempo (PYTHON, 2020).

As plataformas de mídia social têm um grande alcance ao público global, com o YouTube ostentando mais de 1 bilhão de usuários por mês. Isso se divide em 6 bilhões de horas de vídeo que estão sendo assistidas a cada mês e 100 horas de vídeo que são enviadas para YouTube todos os meses (YOUTUBE STATISTICS, 2014). Similarmente, o Twitter tem em média 350.000 tweets enviados por minuto e 500 milhões de tweets por dia (TWITTER, 2014), enquanto o Facebook continua a ser a maior rede de mídia social com 500 milhões ativos usuários e 55 milhões de pessoas enviando atualizações (FIEGERMAN, 2014). Isso sem contabilizar estruturas como Instagram e Tik Tok que tem um potencial de conexão superior às demais plataformas.

Como mencionado anteriormente neste capítulo, grupos terroristas como Daesh (também conhecido como estado islâmico ou ISIS), tem usado essas plataformas como ímãs que atraíram milhares de visualizações, comentários, fóruns e postagens. Por exemplo, por meio do uso de vídeos postados no YouTube, o Daesh começou sua campanha de um bilhão, que chamou que os muçulmanos se juntem ao grupo.

Os vídeos atraíram um grande público e foram acompanhados com as palavras: ‘Apoie com orgulho a Causa muçulmana’ (IRSHAID, 2014). O centro nervoso da mídia social desse grupo terrorista é o centro Al Hayat de Media que envia muitas dessas mensagens que acabam revelando as ferramentas de propaganda que estão sendo usadas. Vários desses vídeos também retratam os integrantes do Daesh como lutadores com uma "consciência moral" e mostram-no ajudando a proteger os civis. Alguns dos vídeos também mostram membros do ISIS visitando combatentes feridos em hospitais e oferecendo doces para crianças (RICHARDS, 2014).

FIGURA 3.1 – Capa de Vídeo mostrando ISIS oferecendo doces para crianças

Fonte: YOUTUBE (2013)

Esses vídeos também fazem parte de uma série mais ampla chamada *'Mujatweets'*[10] que são produzidos em alta definição HD de qualidade com imagens poderosas. Na verdade, isso é reforçado por *podcasts* online feitos por lutadores britânicos solo (chamados também de *lone wolves*) como Abu Summayyah al-Britani. Falando de um Cibercafé no noroeste da Síria, Abu Summayyah descreve em detalhes a natureza do conflito. Ele afirma que o grupo obteve sucesso até agora em empurrar para trás o regime e também descreveu o combate na Síria como melhor do que jogar Call of Duty (LUCAS, 2014).

[10] Vídeos curtos realizados especialmente para serem compartilhados no Twitter pelos apoiadores do Daesh.

Além disso, o Daesh lançou um aplicativo de download gratuito que manteve os usuários atualizados com as últimas notícias da organização. O aplicativo, intitulado: "*The Dawn of Glad Tidings*", era promovido online e disponível no sistema google android, antes de ser detectado e suspenso. O aplicativo uma vez baixado permitia que os usuários vissem e monitorassem tweets, links, hashtags, imagens, vídeos e comentários postados em suas contas específicas das redes. A maior parte do conteúdo foi regulado pelo braço responsável pelas mídias sociais do Daesh (CHASMAR, 2014).

O uso de mídias sociais e da Internet por terroristas para conseguir alcançar seus objetivos ideológicos estão bem documentados. Isso inclui grupos terroristas como o Daesh que usam a Internet e as redes sociais como ferramenta de propaganda por meio de compartilhamento de informações, mineração de dados, captação de recursos, comunicação e recrutamento (CONWAY, 2003). Para Weimann (2004), no entanto, significa que terroristas estariam utilizando a Internet para guerra psicológica, publicidade, propaganda, arrecadação de fundos, recrutamento, networking, compartilhamento de informações e planejamento (LACHOW E RICHARDSON, 2007; WHINE, 1999).

Os recrutadores, portanto, podem usar mais tecnologia de Internet interativa (KOHLMANN 2008; 2006) para, por meio de salas de chat online e cyber cafés (FURNELL E WARREN, 1999), conseguir possivelmente recrutar apoio de pessoas vulneráveis. Marc Sageman (2018) afirma que esta forma de interação em salas de chat ajuda a construir relacionamentos e são uma ferramenta fundamental para radicalizar os jovens. Schmid (2005), argumenta que o terrorismo online, portanto, tornou-se a nova guerra psicológica e Arquilla e Ronfeldt (2001) argumentam que grupos terroristas agora estão usando redes online para criar e causar ambientes virtuais hostis. A natureza da participação na Internet e da participação na discussão online através das redes sociais é o novo ativismo. Este é o processo de se voltar para a violência política de forma ativa, e não passiva.

Sites de mídia social como o Twitter tem sido usado constantemente por grupos terroristas como meio de recrutar os que seriam considerados jihadistas (KLAUSEN, 2015). Eles têm sido usados não apenas para recrutar pessoas, mas para criar uma postura ideológica que visa intimidar e causar medo. Apesar do Twitter permitir apenas 140 caracteres para postar uma mensagem, essas contas enviam mensagens, declarações religiosas e pequenos comentários que maximizam o apelo do grupo. O objetivo de usar e transmitir mensagens no Twitter, significa que o grupo é capaz de criar um clima de medo e ansiedade. Além disso, isso também permite que o Daesh reforce suas mensagens e use sites de mídia social como o Twitter para agir como uma câmara de eco.

Por exemplo, os lutadores Isis foram relatados como tendo usado o Twitter para postar fotos de decapitações. Em um desses casos, simpatizantes e combatentes do Isis usavam a hashtag *#WorldCup* com as palavras que acompanham: "This is our ball… it has skin on it". Para a ala de mídia do Daesh, Al-Furqan, o Twitter, portanto, permite que eles forneçam mensagens com velocidade e reforcem essa narrativa com retuítes para milhares de seguidores. O Twitter, portanto, atua como um megafone pelo qual o grupo terrorista é capaz de enviar atualizações ao vivo de lutadores tweetando sobre como é estar na Síria.

Assim, o objetivo do Daesh é conquistar corações e mentes e manter as organizações atraentes para os jovens, como qualquer outro grupo terrorista. Katz (2014) afirma que o Twitter permite que o Daesh mantenha um forte foco global que se estende além da Grã-Bretanha e da Europa:

> Além de suas páginas gerais e locais, ISIS é apoiado por aproximadamente trinta outras mídias online grupos. Por exemplo, o Al-Battar Media Group, com 32.000 seguidores, trabalha constantemente para mobilizar os seguidores do Twitter para apoiar o ISIS traduzindo os lançamentos do ISIS e pela produção independente de mídia. (KATZ, 2014, np.)

Além disso, Katz argumenta que (2014) *The Billion Muslim campaign* gerou mais de 22.000 postagens em quatro dias desde seu lançamento em 13 de junho de 2014. Em 20 de junho de 2014, usuários do twitter começaram a distribuir imagens exibindo palavras de incentivo ou as frases *"All Eyes on ISIS"* e "We are all ISIS" nas postagens do Twitter que apresentam a hashtag *"#AllEyesOnISIS"*. A hashtag agora totaliza mais 30.000 tweets. Enquanto o Twitter tem estado ativamente suspendendo muitas das contas do Daesh, o grupo terrorista continua a ter uma presença online.

Como consequência dessa presença, simpatizantes, lutadores e grupos do Daesh também começaram a criar várias contas do Twitter, como a página *al-I'tisam* que estão sendo usadas para promover a "marca" Daesh. Além disso, há uma série de contas proeminentes, como @Minbar_s, @hashtag_isis, @mghol1122, @Nnewsi, @alfurqan2013, @raqqa98, @w_raqqa e @ShamiWitness contas que transformaram o Twitter em um megafone do Daesh. A maioria das contas têm atualizado suas postagens com atividades do grupo e também promovendo a marca da organização, apesar de muitas delas agora terem sido removidas (BERGER, 2014).

Uma série de contas do Twitter que foram examinadas e são usadas para propagar ideologias terroristas foram removidas ou suspensas. Na verdade, de todas as contas do Twitter que propagam para o Daesh, a conta @ShamiWitness no Twitter foi uma das as contas mais ativas e bem-sucedidas com mais de 17.700 seguidores. De acordo com uma

investigação de notícias do Canal 4, os tweets foram vistos 2 milhões de vezes por mês, e pelo menos dois terços de todos os recrutados estrangeiros no Twitter também seguem esta conta.

No entanto, após uma investigação recente do Channel 4, a identidade de @ShamiWitness foi revelada e a polícia indiana prendeu um homem chamado Mehdi Masroor que se acredita ter sido o criador da conta @ShamiWitness. Apesar disso, apoiadores do Daesh exigiram sua libertação por meio do uso da hashtag *#FreeShamiWitness*. A conta foi então reativada (CHANNEL 4 NEWS REPORT, 2014).

Awan (2017) propõe sete tipos de características do ofensor que podem facilmente serem encontradas em usuários de redes sociais como o Twitter e o Facebook, tais características os tornam mais suscetíveis a radicalização. Esses sete tipos são; *Cyber Mobs,* um grupo de pessoas que se auto perpetuam realizando campanhas de assédio online que geralmente inclui ridicularizar, praticar bullying ou espalhar discurso de ódio e ameaças; Loners, pessoas solitárias*; Fantasists,* pessoas que constantemente contam mentiras sobre suas vidas e conquistas para que pareçam mais empolgantes do que realmente são*; Thrill Seekers,* pessoas que possuem tendência a buscar novas e diferentes sensações, sentimentos e experiências. O traço descreve pessoas que perseguem sensações novas, complexas e intensas, que amam a experiência pela experiência e que podem correr riscos para buscar essas experiências*; Moral Crusaders*, pessoas que participam de um movimento social que faz campanha em torno de uma questão simbólica ou moral, como álcool ou pornografia; Narcisistas, O transtorno de personalidade narcisista envolve um padrão de pensamento e comportamento egocêntrico e arrogante, falta de empatia e consideração pelas outras pessoas e uma necessidade excessiva de admiração; e Buscadores de Identidade, os buscadores de identidade acreditam fortemente na importância de seu eu essencial, e que é de extrema importância discernir sua verdadeira natureza. Eles veem o autoconhecimento como o pré-requisito crítico para tudo o mais em suas vidas. Curiosamente, esses sete tipos de comportamento do agressor são encontrados entre aqueles que simpatizam diretamente com o Daesh e pessoas que estão realmente transmitindo as propagandas do grupo em diferentes plataformas. Além disso, uma alta proporção de pessoas que caíram na categoria de '*thrill seekers*' e '*moral crusaders',* indicaram, de alguma forma, que estavam indo ou pretendiam lutar com o Daesh (AWAN, 2017).

3.3 As Teorias da Propaganda Terrorista na Internet

A Internet e mídias sociais atuam como um banco de dados sobre como vídeos do YouTube da campanha de um bilhão promovem a violência e sua utilização como estratégia por meio da teoria do aprendizado social ou aprendizagem social (FREIBURGER E CRANE, 2008). Esta teoria afirma que indivíduos aprendem comportamento desviante de outros grupos, que podem levar à aprendizagem extremista que é categorizada por associação, definições, reforço diferencial e imitação.

Freiburger e Crane (2018) argumentam que os mecanismos da teoria da aprendizagem social são usados por grupos terroristas na Internet como uma ferramenta para facilitar ataques e recrutamento. Esta perspectiva de comportamentos desviantes oferece uma visão instigante dos processos que transformam indivíduos ingênuos como Andrew Ibrahim, que foi detido em 2008, em violentos extremistas (DESMOND, 2002). Freiburger e Crane (2018) também referem-se a um estudo europeu, onde Peter Cherif, também conhecido como Abu Hamza, um militante islâmico francês que foi membro da Al-Qaeda no Iraque e da Al-Qaeda na Península Arábica e teria ajudado no planejamento do tiroteio no Charlie Hebdo, e foi recrutado pela Al-Qaeda por meio da Internet em um processo de aprendizagem semelhante (POWELL et al.,2005). Eles argumentam que se os grupos se tornarem marginalizados, eles tornam-se mais suscetíveis ao uso da Internet para finalidades terroristas.

O uso do construcionismo social como mecanismo para entender as definições concorrentes de ciberterrorismo é crucial para obter uma melhor compreensão dos fenômenos. Claramente, as práticas sociais e o comportamento social mudam com o tempo e, portanto, nossa compreensão do extremismo online também evolui. Dentro deste contexto, o construcionismo social oferece a ambos criminologistas e sociólogos um meio de examinar os vários processos sociais que emergem quando se olha para as interpretações do extremismo online (FELSON, 2002).

A pesquisa de McKenna e Bargh (1998) sugere que o ciberespaço e o terrorismo convergiram, permitindo que os terroristas usem a Internet para fins terroristas. Como resultado de tal opinião conflitante, existe um medo real e presente, que críticos argumentam que significa que a Internet e os sites de mídia social têm se tornado um porto seguro para extremistas em potencial para "preparar" pessoas vulneráveis. Além disso, Tsfati e Weimann (2002) argumentam que grupos terroristas estão usando a Internet para preparar pessoas vulneráveis indivíduos justificando a violência contra civis inocentes como uma retribuição

pelas invasões e crimes cometidos contra muçulmanos em todo o mundo (VERTON, 2003). Eles têm um alto nível de conhecimento tecnológico, gastando horas intermináveis aprimorando suas habilidades, que simplesmente gostam do desafio de tentar entrar no ciberespaço. Seus objetivos não são os mesmos dos extremistas (FURNELL E WARREN, 1999).

Klausen (2015) argumenta que os sites de mídia social estão sendo usados pelo Daesh e outros como uma tática de guerra cibernética global em alguns lugares como a Síria. No estudo de Klausen (2015) sobre redes de mídia social, o autor descobriu que o Twitter estava sendo usado por membros do Daesh como meio de criar a ilusão de que o grupo era mais poderoso do que realmente era. Isso estava sendo feito, como este jornal descobriu através de contas do Twitter e diariamente *feeds* como um meio de angariar suporte. Na verdade, em um anterior estudo de Klausen (2012) ele também descobriu que grupos jihadistas estavam usando o YouTube como meio para fins de propaganda. Ele examinou o grupo, a conta do YouTube de Al-Muhajiroun utilizada para a Campanha de Propaganda e descobriu que o grupo estava usando canais de mídia do YouTube para politizar o apoio e criar poderosas redes terroristas.

A teoria social cognitiva, proposta por Bandura (2001) nos fornece alguns pontos importantes a serem considerados atenciosamente, como a comunicação online pode ser afetada pelo ambiente social. Segundo Bandura (2001), o uso dessa teoria ajuda a informar os grupos e cria fatores "motivadores”:

> A teoria cognitiva social fornece uma estrutura conceitual de agente dentro da qual examinar os determinantes e mecanismos de tais efeitos. O comportamento humano tem sido frequentemente explicado em termos de unidirecional causação, na qual o comportamento é moldado e controlado por influências ambientais ou por disposições internas. (Bandura, 2001, p.265)

Dentro da construção de motivação e comportamento do Daesh, o grupo tem sido proativo na exploração do ambiente online e estava utilizando de eventos mundiais, como a crise no Iraque, para formular ideias. Para que a teoria social cognitiva funcione aqui, vemos como membros de grupos podem atuar como produtores dentro de um ambiente social online. Bandura argumenta que:

> A extraordinária capacidade de simbolização fornece aos humanos uma ferramenta poderosa para compreender seu meio ambiente e criação e regulação ambiental de eventos que afetam praticamente todos os aspectos de suas vidas. A maioria das influências externas afetam o comportamento por meio de processos cognitivos, e não diretamente. (Bandura, 2001, p.267)

Esse uso de fatores emocionais são símbolos de como o Daesh e outros grupos de ódio online também podem transformar e galvanizar grupos online e transferir o poder do ambiente para criar modelos cognitivos de julgamento. Meyrowitz (1985) defende que a mídia eletrônica tem mudado significativamente a maneira como interagimos uns com os outros ao longo do tempo e que a internet, portanto, tem um impacto no comportamento social. Além disso, Meyrowitz (1985) argumenta que esses comportamentos online são determinados por diferentes estágios da socialização online.

No caso dos comportamentos observado neste estudo, que grupos como o Daesh jogam com essas crises de identidade como meio de criar apoio. Meyrowitz afirma que "[...] a mídia eletrônica tem cada vez mais invadido as situações que ocorrem em ambientes fisicamente definidos" (MEYROWITZ, 1985 p.07). Mais e mais, a forma de comunicação mediada passou a se assemelhar à forma de viver face a face. Este é claramente o caso ao examinar o uso, de grupos como o Daesh, do poder da mídia social para construir diferentes padrões de recrutamento.

Lietsala e Sirkkunen (2008) argumentam que o poder das mídias sociais significa que agora somos produtores e não simplesmente o público, o que significa que estamos tomando um papel proativo em nossas interações na Internet. Além disso, Pennebaker e King (1999) argumentam que a linguagem em sites de mídia social pode ser usada para criar perfis. Selfhout (2010) argumenta que as redes sociais são construídas por esses traços de personalidade e amizades que são criadas nas redes sociais.

Usando os cinco grandes modelos de personalidade que consistem em cinco fatores de personalidade, ou seja, abertura, consciência, extroversão, amabilidade e neuroticismo. Dentro deste paradigma, conforme discutido acima, grupos como o Daesh são capazes de usar as redes sociais para criar amizades importantes e selecionar "amigos" online dentre os usuários. Com base na tipologia o autor propôs neste estudo, então que claramente estamos a ver um nível dos cinco fatores de personalidade desempenhando um papel na em particular no que diz respeito à "abertura" e "agradabilidade", traços que mostram uma seleção de amizades online emergentes nas redes sociais por grupos terroristas (SELFHOUT, 2010).

4 A INTERNET DAS COISAS

No passado, a introdução de tecnologias avançadas como mecanização, informatização, automação e digitalização nas indústrias levou a diversas revoluções industriais. O cenário atual da industrialização, que pode ser considerado como a quarta revolução industrial ou Indústria 4.0, é composto por tendências atualizadas de tecnologias, mantendo a compatibilidade intacta para integrar sistemas inteligentes interativos com o conceito de *big data*. Nos dias de hoje, quase todas as organizações estão com pressa para a digitalização, o que as levou a enfrentar diferentes desafios e lutas (PATNAIK, 2020).

O principal objetivo da quarta revolução industrial em qualquer setor é servir sem riscos, operações sem esforço e entrega pontual de serviços, conforme definido anteriormente ao início da produção. Os conceitos de sistemas físicos cibernéticos e Internet das Coisas (IdC) são a espinha dorsal da indústria 4.0. Quanto mais eficiente a tecnologia, maiores são as chances de grande geração de dados. Então, o conceito de *big data* com o conceito de armazenamento de dados em nuvem colaborou com a indústria 4.0 para lidar efetivamente com este problema (PATNAIK, 2020).

4.1 O que é a Internet das Coisas

A Internet das Coisas (IdC) é conhecida como um paradigma da computação para permitir a conexão entre mundos físico e virtual, dando poder de processamento das coisas do dia a dia. A ideia básica da IdC é realizar a incorporação de rede móvel e capacidade de processamento de informações em gadgets e itens diários. Portanto, tornando-se possível uma nova forma de comunicação entre pessoas e coisas, e entre as próprias coisas. Assim, a IdC é uma nova oportunidade de criar um mundo onde todas as coisas ao nosso redor estão conectadas à Internet e se comunicam entre si. Deve-se observar que essa comunicação ocorre sem a necessidade de interação humano-humano ou humano-computador (SERPANOS, WOLF, 2018).

Recentemente, as casas inteligentes estão se tornando cada vez mais populares (JACOBSSON, 2015). O Ciclo de promoção de TI da Gartner em relatório de 2016 identifica a tecnologia emergente de casas inteligentes conectadas. Em 2022, uma casa típica pode conter 500 ou mais dispositivos inteligentes. A casa inteligente visa adicionar inteligência artificial e comunicar-se com infraestruturas cibernéticas existentes para objetos domésticos, como eletrodomésticos, fechaduras, câmeras, móveis e portas de garagem. A adição de

inteligência aos objetos físicos oferece muitas vantagens para uma melhoria da vida humana, incluindo maior conveniência, segurança e eficiência de recursos. Por exemplo, a casa inteligente pode ajustar as cortinas para economizar energia com base nas mudanças ambientais, abrir a porta da garagem automaticamente quando um veículo autorizado abordar sua entrada ou solicitar serviços médicos automaticamente quando emergências são detectadas.

Os eletrodomésticos físicos tradicionais são parte da extensão da Internet existente na casa inteligente. Se os dispositivos estiverem danificados, o impacto pode ser severo, por exemplo, o hackeamento bem-sucedido de fechaduras inteligentes permitirá que estranhos entrem em sua casa, ou como visto no primeiro capítulo deste trabalho, permite que um hacker te mantenha em cárcere em sua própria casa sem a necessidade do mesmo estar nela fisicamente; um hacker poderá assustar bebês remotamente por aparelhos de monitoramento ligados à internet ou conversar e dar ordens para crianças como foi detectado por diversos usuários de câmeras da amazon que reportaram terem suas câmeras invadidas por hackers que conversavam e insultavam os proprietários dos aparelhos invadidos (THE GUARDIAN, 2020); hackear um microondas ou um fogão inteligente pode causar incêndio em sua casa. Além disso, a coleta contínua de dados de dispositivos inteligentes domésticos podem revelar as atividades privadas dos proprietários, representando sérias ameaças para a privacidade.

4.2 Ataques Ciberfísicos

O impacto da segurança cibernética na segurança do mundo físico é facilmente notado - os invasores obtêm acesso não autorizado a um sistema físico cibernético e comandam-o a realizar qualquer tarefa danosa. No entanto, as medidas de segurança advindas da engenharia da computação ainda dependem fortemente de atualizações para corrigir ameaças recém-encontradas. Os sistemas físicos não podem ser interrompidos arbitrariamente - um avião não pode ser interrompido no meio do voo para uma atualização de software. Até mesmo um desligamento planejado de uma planta física pode levar horas devido às restrições físicas na operação do sistema.

Ataques ciberfísicos são diferentes dos ciberataques porque ameaçam diretamente sistemas físicos: infraestrutura, estruturas civis e pessoas. Ataques ciberfísicos podem matar pessoas e causar danos às plantas físicas que podem levar meses para serem reparados. Danos em grande escala à infraestrutura civil - aquecedores de água, refrigeração, equipamentos,

etc. - podem sobrecarregar a produção padrão e resultar em longos atrasos para substituições e reparos.

Ataques cibernéticos e físicos podem ser usados em conjunto para criar um ataque ciberfísico. Problemas de segurança demonstram os danos físicos que podem ser infligidos por sistemas ciberfísicos. E, em alguns casos, eles expõem falhas que podem também ser usadas por invasores.

Leveson e Turner (LEVESON e TURNER, 1993) analisaram as causas de uma série de acidentes relacionados com o dispositivo de radiação médica Therac-25. Eles identificaram vários problemas com o Projeto do Therac-25, incluindo sistemas mecânicos, projeto de interface do usuário e projeto de software. Esses dispositivos administraram várias overdoses de radiação, algumas das quais foram fatais. Esses múltiplos acidentes parecem ter resultado de várias causas distintas. Leveson e Turner identificaram vários fatores contribuintes: falta de procedimentos para reagir a incidentes relatados, excesso de confiança no software, engenharia de software e avaliações de risco irrealistas. O *malware* HatMan ataca os controladores de segurança da Triconex. Controladores de segurança são PLCs usados para procedimentos de segurança, como desabilitar equipamentos ou inibir operações. O HatMan pode ler e modificar a memória e executar código arbitrário em um controlador; acredita-se que seja projetado não apenas para reconhecer sistemas industriais, mas também para implementar ataques físicos.

Rouf (USENIX, 2010) demonstrou vulnerabilidades no monitoramento da pressão dos pneus (TPMS) que são legalmente exigidos para muitos tipos de veículos em vários países. Dispositivos TPMS diretos são montados em rodas e enviam dados sobre a pressão dos pneus para unidades de controle eletrônico (ECUs) do carro usando sinais de rádio. Rouf mostrou que os pacotes podem ser recebidos a uma distância de 40 m, que podem ser falsificados para o ECU, e que os pacotes não foram criptografados.

Checkoway (USENIX, 2011) identificou uma série de vulnerabilidades em um carro teste, com cada ataque fornecendo controle completo sobre os sistemas do carro. As vulnerabilidades incluíam o CD player do carro, a porta OBD-II[11] (diagnóstico *on-board*) exigidos nos EUA, links telemáticos, como aqueles usados para serviços de emergência, e portas Bluetooth.

[11] Sigla para a expressão em inglês *On Board Diagnostics*, que significa “diagnóstico de bordo”. Trata-se de um sistema que, ligado à central eletrônica do carro, permite a leitura e transmissão dos mais diversos tipos de dados mecânicos.

O Stuxnet, citado no primeiro capítulo deste trabalho, foi implantado em pelo menos duas fases. Stuxnet 0,5 (DOHERTY, CHIEN, 2013) estava na selvagem em novembro de 2007. Ele foi projetado para manipular válvulas em equipamentos de enriquecimento de urânio na instalação de Natanz, Irã, a fim de danificar centrífugas e outros equipamentos. Ele usou um ataque de repetição para ocultar suas alterações nas configurações da válvula durante um ataque físico. Esta versão difundiu os arquivos do projeto da Etapa 7.

W32.Stuxnet (FALLIERE, MURCHY, CHIEN, 2013) conduziu ataques mais extensos. Ele se propagou usando vulnerabilidades no Spooler de Impressão do Windows e vulnerabilidades em unidades removíveis. Isto usou computadores Windows infectados para modificar o código PLC. Seu ataque físico causou o aceleramento de centrífugas, causando-lhes danos. Acredita-se que os ataques tenham causado danos significativos ao equipamento de Natanz e reduzido sua produtividade.

O grupo Dragonfly (JOHNSON, 2014), foi identificado como espião de um grande número de alvos em diversos países. Os alvos da campanha incluem empresas de energia, operadores de oleodutos de petróleo e indústria de energia, fornecedores de equipamentos, bem como empresas de defesa e aviação. Espionagem e reconhecimento eram considerados os principais objetivos da campanha. Phishing e ataques watering hole foram usados para obter credenciais de usuários autorizados. Malware instalado em sistemas de destino reuniu uma variedade de dados. Symantec identificou uma Campanha Dragonfly 2.0 ativa nos EUA, Turquia e Suíça, começando como no início de dezembro de 2015 (JOHNSON, 2014).

A rede elétrica da Ucrânia foi atacada no início de 2016 (GOLDIN, 2016). O ataque físico fez com que subestações elétricas fossem desconectadas, causando a perda de centenas de milhares de casas de potência. O Centro Nacional de Integração de Segurança Cibernética e Comunicações (NCCIC) identificou o *malware* CrashOverride como sendo o vírus usado para atacar a infraestrutura crítica na Ucrânia em 2016 (CISA, 2017).

Reunindo estes exemplos de ataques ciberfísicos citados com os assuntos já abordados nos capítulos anteriores, principalmente nos capítulos 1 e 3, pode-se entender a gravidade que uma brecha de segurança significa no espaço cibernético. Desde roubo de dados aparentemente “insignificantes”, até ataques a estruturas estatais o espaço cibernético se mostra de complexo manejo de segurança versus liberdade, adicionando o fator da Internet das Coisas estar cada vez mais presente no dia dia de cidadãos comuns é nítida a necessidade de uma legislação que acompanhe essa modernização de sistemas, casas inteligentes e até mesmo cidades inteligentes.

4.3 Segurança na Internet das Coisas

A segurança deve ser garantida por sistemas IdC para que dados confidenciais e físicos, como por exemplo de infraestruturas, não caiam em mãos maliciosas. Os usuários não podem usar muitos sistemas e aplicativos IdC sem um bom nível de proteção. Apesar da segurança em sistemas de rede tradicionais continuar sendo um desafio, os sistemas IdC apresentam aos pesquisadores desafios maiores e mais complexos devido aos diferentes recursos especiais dos sistemas IdC. Para o desenvolvimento de novas soluções de segurança, uma compreensão completa desses desafios é essencial.

O diário *The News* colocam a segurança no topo das preocupações: vazamento de dados pessoais e econômicos, espionagem, infecção de sistemas informáticos confidenciais, roubo de identidade e receios sobre pagamentos com cartão são apenas alguns exemplos de ameaças (KOUICEM, BOUABDALLAH, LAKHLEF, 2018). Geralmente, a segurança de redes de computadores e sistemas de informação consiste em fornecer os seguintes serviços: (1) Integridade: garante que um terceiro não modificou os dados (acidentalmente ou intencionalmente). (2) Autenticação: verifica a suposta identidade da fonte de dados. (3) Irrecusabilidade: Garante que o remetente da mensagem não pode negar que enviou a mensagem no futuro. (4) Disponibilidade: Garante que os serviços do sistema estão disponíveis para usuários legítimos. (5) Privacidade: garante que as identidades dos usuários não sejam identificáveis ou rastreáveis a partir de seu comportamento e ações do sistema. (6) Confidencialidade: garante que as informações sejam tornadas ininteligíveis para pessoas não autorizadas, indivíduos, entidades e processos (KOUICEM, BOUABDALLAH, LAKHLEF, 2018).

A IdC é mais suscetível a ataques do que a Internet comum pois, bilhões de dispositivos a mais produzem e consomem serviços, os mais vulneráveis são os dispositivos altamente restritos, como por exemplo câmeras de segurança. Entidades maliciosas estão tentando, diariamente, controlar pelo menos um dispositivo diretamente ou indiretamente. Neste contexto, a tolerância a falhas - no sentido de, caso aconteça alguma falha no serviço de segurança ou no próprio *software* isso não comprometa os dados ou o próprio dispositivo - é essencial para a confiabilidade do serviço, mas qualquer solução deve ser especializada e leve para levar em conta o número limitado e facilmente acessível de dispositivos IdC. Três esforços colaborativos são necessários para alcançar a tolerância segura de falhas na IdC. A primeira é proteger por padrão todos os objetos, para projetar protocolos e mecanismos seguros, os pesquisadores devem trabalhar na melhoria da qualidade da implementação do

software, pois um patch de software pode não ser compatível para bilhões de dispositivos (ROMAN, NAJERA, LOPEZ, 2011).

O segundo esforço é fornecer a todos os objetos conectados a IdC a capacidade de saber o status e os serviços da rede. Este sistema teria que dar feedback a muitos outros elementos; um sistema de vigilância, por exemplo, poderia adquirir dados como parte do fornecimento de dados de segurança qualitativos e quantitativos. Neste segundo esforço, uma tarefa importante é criar um sistema de responsabilização que ajude a monitorar a conexão. Objetos deveriam, finalmente, serem capazes de se proteger de falhas e ataques de rede. Todos os protocolos devem incluir mecanismos que respondam a situações anômalas e permitir que o objeto degrade seu serviço normalmente. Os objetos devem ser capazes de prevenir invasores usando sistemas de detecção de intrusão e outros mecanismos de defesa. Elementos da IdC devem ser capazes de agir rapidamente para se recuperar de qualquer dano quando um ataque afetar seus serviços. O feedback de outros mecanismos e entidades conectados a IdC podem ser usados para mapear a localização de áreas inseguras onde um ataque causou falhas de serviço e áreas confiáveis sem falhas de serviço. Essas informações podem formar a base para várias recuperações de serviços, como acesso a objetos em uma área confiável. Além disso, os mecanismos poderiam informar as pessoas em qualquer área danificada e, em seguida, realizar as operações de manutenção. Esta infraestrutura para autogerenciamento é uma política chave de segurança da IdC (ROMAN, NAJERA, LOPEZ, 2011).

4.3.1 Rede Definida por Software (SDN)

Este é um novo paradigma de rede que revolucionou o mundo das redes nos últimos anos. Tem como objetivo fornecer um ambiente para desenvolver soluções de rede mais flexíveis e para facilitar o gerenciamento de recursos de rede usando um controlador SDN centralizado. Muitas soluções de segurança da IdC baseadas em SDN foram propostas na literatura. Devido à sua programabilidade e inteligência, SDN é um novo paradigma que revolucionou o mundo das redes. A ideia principal por trás deste conceito, que começou em 2011, ocorre na separação do plano de gerenciamento da rede e do plano de dados. É possível centralizar o gerenciamento e a configuração da rede e o tráfego de rede dinâmico gestão usando este paradigma (HU,2015).

Dispositivos (roteadores, switches, gateways e dispositivos conectados a IdC em geral) em arquiteturas SDN não tomam decisões de controle, como tabelas de transmissão e regras

ACL. Em vez disso, eles aprendem essas regras com um componente central chamado controlador SDN, que usa protocolos como o Openflow para tomar todas as decisões de rede. Dispositivos de arquitetura SDN lidam com pacotes com base em Tabelas de fluxo do controlador. SDN é uma solução eficiente para alguns desafios no Ambiente da IdC, com recursos de rede limitados para a maioria dos dispositivos. Como resultado, a implantação da SDN em conjunto com *Network Function Virtualization* (NFV) pode otimizar com eficiência a alocação de recursos em dispositivos da IdC. Ele oferece uma série de oportunidades para superar certos desafios de confiabilidade, segurança, escalabilidade e QoS em Aplicativos da IdC de maneira mais eficiente e flexível (HU, 2015).

4.3.2 Tecnologia *Blockchain*

É a tecnologia por trás das ferramentas de criptomoeda, como Bitcoin, que visa fazer transações entre entidades em uma arquitetura distribuída (ponto a ponto) sem referência a um servidor central confiável. Além disso, essa solução não exige que as empresas confiem umas nas outras. Nesta tecnologia, é praticamente impossível negar transações quando são validadas. Além de sua aplicação no domínio da criptomoeda nos últimos anos, muitos pesquisadores começaram a lançar luz sobre esta tecnologia para abordar soluções de segurança da IdC, como privacidade de dados, controle de acesso, e assim por diante (BAHGA, MADISETTI, 2016).

O blockchain é uma tecnologia eficiente que revolucionou o mundo criptomoeda. Consiste principalmente em um banco de dados seguro (também conhecido como biblioteca pública) contendo todas as transações realizadas por todas as entidades participantes. Transações são feitas e validadas em uma infraestrutura ponto a ponto distribuída em criptomoedas, soluções baseadas em blockchain, como bitcoin e ethereum. Basicamente, se uma entidade deseja realizar uma transação com outra entidade B, ele envia uma solicitação de transação a todos os colegas na rede do blockchain. Em seguida, cada nó coleta periodicamente um conjunto de transações (10 minutos para Bitcoin) e as agrupa em um bloco. Finalmente, o processo de validação de cada bloco é realizado de forma distribuída usando um algoritmo de consenso executado por certos nós da rede chamados *miners*. Novos aplicativos emergentes baseados na IdC se beneficiarão de transações e mensagens seguras e privadas, descentralização de comunicações e privacidade de design, todos os quais são recursos muito importantes para a indústria e para a IdC em geral (BAHGA, MADISETTI, 2016).

Conforme a IdC continua a crescer, sensores e dispositivos se tornam locais de informações, controle de temperatura e outros recursos mais comuns. Essas informações geralmente precisam ser compartilhadas entre diferentes entidades e usado em alguns aplicativos críticos para análise de big data e também para fins de monitoramento. Blockchain pode ajudar a criar registros resistentes à adulteração que permitem que todos os objetos inteligentes participantes acessem os mesmos dados de forma mais consistente e segura. Blockchain é uma maneira eficiente de automatizar negócios e criar contatos inteligentes entre dispositivos inteligentes sem redirecioná-los para entidades centrais, além disso para gerenciamento de fluxo de dados mais dinâmico, em suma, todos os tipos de contatos digitais criam "contratos inteligentes". Um contrato inteligente consiste em um programa de computador que é executado automaticamente por objetos inteligentes e define um conjunto de regras e condições com base em termos contratuais. Blockchain pode ajudar a garantir que os contratos sejam distribuídos sem problemas e de maneira mais eficiente (CHRISTIDIS, DEVETSIKIOTIS, 2016).

A tecnologia Blockchain tem recebido muita atenção de cientistas de diferentes áreas. Até agora, sua aplicação tem tido muito sucesso em aplicações financeiras e contratos inteligentes, mas alguns pesquisadores argumentam que vale a pena investigar até que ponto esta tecnologia eficaz pode melhorar significativamente a IdC e a segurança dos domínios. Já temos exemplos de aplicações não financeiras, como sistemas de registro de identidade globais(*namecoin, block stack*, entre outros), aplicativos de seguros, votação online, proveniência da cadeia de suprimentos, armazenamento P2P descentralizando plataformas, etc. Além disso, algumas soluções baseadas em blockchain foram recentemente propostas na literatura para resolver alguns problemas de segurança e privacidade na IdC (CHRISTIDIS, DEVETSIKLOTIS, 2016).

Alguns valores que a tecnologia blockchain pode trazer para a IdC e domínios de segurança são: 1. Descentralização: Por causa da arquitetura IdC descentralizada, o blockchain é a melhor solução de segurança IdC. A arquitetura de blockchain descentralizada torna a segurança escalável e pode resolver um único problema de ponto de falha e se tornar mais robusto em ataques DoS; 2. Pseudoanonimato: Os nós do blockchain são identificados com suas chaves públicas (ou chaves *hash*). Esses pseudônimos não vinculam nenhuma informação sobre a identidade dos participantes; 3. Segurança da transação: toda transação é assinada pelo nó antes de ser enviada para a rede blockchain e deve ser verificada e validada pelos *miners*. Após a validação, as transações que já foram salvas no blockchain não podem ser forjadas ou modificadas (CHRISTIDIS, DEVETSIKLOTIS, 2016).

Todos os dispositivos em uma rede de IdC geram e requerem espaço para armazenar certos tipos de informação. A segurança do manuseio desses dados, incluindo transferências e manutenção, e a sincronização de todos os dados de diferentes dispositivos sem comprometer nenhuma parte do sistema, requer atenção e esforço consideráveis (HOSSAIN, FOTOUHI, HASAN, 2015). Diversos problemas e desafios relacionados à segurança ainda são enfrentados. A pesquisa nesta área é muito necessária para resolver esses problemas de segurança e desafios da IdC em ambientes heterogêneos para que os usuários possam usar dispositivos IdC para se comunicar e compartilhar informações globalmente com garantia de segurança. Faz-se necessária tal segurança, também para que governos e entidades internacionais tenham a garantia de que documentos sensíveis e assuntos estatais não estejam sendo acessados por terceiros, visto que tecnologias conectadas a IdC estão cada vez mais presentes não apenas nas casas mas também em prédios governamentais, parlamentos e etc. E caso haja uma brecha de segurança seja possível identificar sua extensão e sua origem.

CONSIDERAÇÕES FINAIS

Esta monografia possibilitou uma análise da segurança cibernética sob a ótica das Relações Internacionais, com foco na territorialização do espaço cibernético e a Internet das coisas foi possível expor a importância desse assunto, não apenas para a política internacional mas, também para indivíduos da sociedade civil que estão cada vez mais expostos a tecnologias de ponta e, com isso, mais expostos a suas ameaças.

Fez-se possível analisar diversos casos de ataques a civis e órgãos estatais que, apesar de serem realizados por meio cibernético, refletiram consequências graves no espaço físico. Além dos casos de ataques ciberfísicos diretos, foi demonstrado no capítulo 3 que ataques indiretos ao espaço físico também são possíveis e de consequências igualmente catastróficas, como é o caso da disseminação de propaganda terrorista e o recrutamento online para grupos extremistas, vale-se notar que, apesar deste trabalho focar no grupo terrorista daesh, existem diversos grupos na internet, de diversas origens, que reproduzem pensamentos de supremacia racial, religiosa, de gênero, etc que não devem ser esquecidos ou minimizados e que representam também uma grande ameaça para a população e para a segurança nacional.

Pode-se concluir que existe a necessidade de mecanismos estatais, sejam eles leis domésticas, tratados internacionais ou órgãos de organizações internacionais *ad hoc* para que não apenas sejam protegidas as soberanias de Estados, mas também para garantir a segurança e a liberdade da sociedade civil na internet. É necessário ressaltar, também, que este trabalho expõe a necessidade de se conhecer as tecnicidades do espaço cibernético para que sejam traçadas as melhores estratégias de segurança disponíveis, sendo assim, crucial a presença de técnicos e especialistas da área nos diversos setores do mercado de trabalho e em órgãos legislativos para que seja possível garantir ao Estado sua segurança e manutenção de soberania no espaço cibernético (que como foi demonstrado durante o trabalho pode interferir no espaço físico de diversas formas), garantir à sociedade civil a segurança de seus dados e sua liberdade para navegar na internet sem uma repressão ou censura do Estado.

Por fim, é possível concluir que dada sua complexidade, o espaço cibernético (apesar de já existir desde o século passado) ainda é um espaço de estudo novo e que se encontra em constante mutação, fazendo com que seja desafiador manejá-lo. Este espaço, que está cada vez mais presente em nossas realidades, mostra-se não apenas como uma porta de entrada de ameaças constantes, mas também como uma abertura para diversas possibilidades, de aprendizados, trocas de experiências, culturas e conexões, sejam elas técnicas ou interpessoais.

REFERÊNCIAS

ANDREWS, Damon C.; NEWMAN, John M. **Personal Jurisdiction and Choice of Law in the Cloud**. Md. L. Rev., v. 73, 2013.

ARQUILLA, John; RONFELDT, David. Networks and netwars: **The future of terror, crime, and militancy.** Rand Corporation, 2001.

AWAN, Imran. **Cyber-extremism: Isis and the power of social media**. **Society**, v. 54, n. 2, p. 138-149, 2017.

BAHGA, Arshdeep; MADISETTI, Vijay K. **Blockchain platform for industrial internet of things**. Journal of Software Engineering and Applications, v. 9, n. 10, p. 533-546, 2016.

BANDURA, Albert. **Social cognitive theory of mass communication**. Media psychology, v. 3, n. 3, p. 265-299, 2001.

BARLOW, John Perry. **Declaración de independencia del ciberespacio**, 1996. Disponível em: <http://homes. eff. org/% 7Ebarlow/Declaration-Final.> acessado em 20 de novembro de 2020.

BRILMAYER, R. Lea et al. **Conflict of Laws**: Cases and Materials. Aspen Publishers, 2019.

BUZAN, Barry et al. **The evolution of international security studies**. Cambridge University Press, 2009.

CAPORASO, James A. **Changes in the Westphalian order:** Territory, public authority, and sovereignty. International studies review, v. 2, n. 2, p. 1-28, 2000.

CHANDEL, Sonali et al. **The Golden Shield Project of China:** A Decade Later—An in-Depth Study of the Great Firewall. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE Computer Society, 2019. p. 111-119.

CHECKOWAY, Stephen et al. **Comprehensive experimental analyses of automotive attack surfaces**. In: USENIX Security Symposium. 2011. p. 447-462.

CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. **Blockchains and smart contracts for the internet of things**. Ieee Access, v. 4, p. 2292-2303, 2016.

CONWAY, Maura. **Code wars**: steganography, signals intelligence, and terrorism. Knowledge, Technology & Policy, v. 16, n. 2, p. 45-62, 2003.

DASKAL, Jennifer. **The un-territoriality of data**. Yale lJ, v. 125, p. 326, 2015.

DE SA, Christopher; RE, Christopher; OLUKOTUN, Kunle. **Global convergence of stochastic gradient descent for some non-convex matrix problems**. In: International Conference on Machine Learning. PMLR, 2015. p. 2332-2341.

DEMARTINI, Mariana. Hackers trancam quartos de hotel e exigem resgate em bitcoin. **Exame**. Disponível em: <https://exame.abril.com.br/tecnologia/hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/> acessado em 20 de novembro de 2020.

DENMARK, Abraham M. **Managing the global commons**. The Washington Quarterly, v. 33, n. 3, p. 165-182, 2010.

FALIH, Noor; FIRDAUS, Andhika. **Measuring performance, functionality and portability for mobile hybrid application**. In: 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE, 2019. p. 195-200.

FANG, Binxing; FANG; ZHANG. **Cyberspace sovereignty**. Springer Singapore, 2018.

FURNELL, Steve M.; WARREN, Matthew J. **Computer hacking and cyber terrorism**: The

real threats in the new millennium?. Computers & Security, v. 18, n. 1, p. 28-34, 1999.

GARNETT, Richard. **Dow Jones & (and) Company Inc v. Gutnick. Melb**. J. Int'l L., v. 4, p. 196, 2003.

GIROT, Clarisse (Ed.). **Regulation of Cross-border Transfers of Personal Data in Asia**. Asian Business Law Institute, 2018.

GLENNY, Misha. **A weapon we can't control**. The New York Times, v. 24, 2012.

GOLDSMITH, Jack; WU, Tim. **How governments rule the net**. In: Who Controls the Internet?. Oxford University Press, 2006.

GOODIN, Dan. **First known hacker-caused power outage signals troubling escalation**. Ars technica, v. 4, 2016.

GRAHAM, Stephen. **Olympics 2012 security**: welcome to lockdown London. City, v. 16, n. 4, p. 446-451, 2012.

GRIFFITHS, James. **The great firewall of China**: How to build and control an alternative version of the internet. Zed Books Ltd., 2019.

HAMADE, Samir N. **Internet filtering and censorship**. In: Fifth International Conference on Information Technology: New Generations (itng 2008). IEEE, 2008. p. 1081-1086.

HEINTSCHEL VON HEINEGG, Wolff. **Territorial sovereignty and neutrality in cyberspace**. International Law Studies, v. 89, n. 1, p. 17, 2013.

HOSSAIN, Md Mahmud; FOTOUHI, Maziar; HASAN, Ragib. **Towards an analysis of security issues, challenges, and open problems in the internet of things**. In: 2015 ieee world congress on services. IEEE, 2015. p. 21-28.

JACOBSSON, Andreas; DAVIDSSON, Paul. **Towards a model of privacy and security for smart homes**. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015. p. 727-732.

JOHNSON, Rebecca. **Dragonfly Damian Montano**. The Flutist Quarterly, v. 40, n. 1, p. 70, 2014.

JOSSELIN, Daphne; WALLACE, William. **Non-state actors in world politics**: a framework. In: Non-state actors in world politics. Palgrave Macmillan, London, 2001. p. 1-20.

KATZ-BASSETT, Ethan et al. **Towards IP geolocation using delay and topology measurements**. In: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. 2006. p. 71-84.

KATZ, Stefan P. **REFORMING THE COUNTER-TERRORISM WORKHORSE**: ENSURING THE NATIONAL STRATEGY FOR THE NATIONAL NETWORK OF FUSION CENTERS. 2014.

KLAUSEN, Jytte. **Tweeting the Jihad**: Social media networks of Western foreign fighters in Syria and Iraq. Studies in Conflict & Terrorism, v. 38, n. 1, p. 1-22, 2015.

KOHLMANN, Evan F. "**Homegrown" terrorists**: Theory and cases in the war on terror's newest front. The Annals of the American Academy of Political and Social Science, v. 618, n. 1, p. 95-109, 2008.

KOUICEM, Djamel Eddine; BOUABDALLAH, Abdelmadjid; LAKHLEF, Hicham. **Internet of things security**: A top-down survey. Computer Networks, v. 141, p. 199-221, 2018.

LACHOW, Irving; RICHARDSON, Courtney. **Terrorist use of the internet:** the real story.

NATIONAL DEFENSE UNIV WASHINGTON DC, 2007.

LEETARU, Kalev. **A Reminder That 'Fake News' Is An Information Literacy Problem—Not A Technology Problem**. Forbes. Extracted from https://www. forbes. com/sites/kalevleetaru/2019/07/07/a-reminder-that-fake-newsis-an-information-literacy-problem -not-a-technology-problem, 2019.

LEHTO, Martti. **Cyber security competencies**: cyber security education and research in Finnish universities. In: ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS. 2015. p. 179-88.

LEVESON, Nancy G.; TURNER, Clark S. **An investigation of the Therac-25 accidents**. Computer, v. 26, n. 7, p. 18-41, 1993.

LI, Hua et al. **Development of a remote monitoring system for henhouse environment based on IoT technology**. Future Internet, v. 7, n. 3, p. 329-341, 2015.

LIETSALA, Katri; SIRKKUNEN, Esa. **Social media**. Introduction to the tools and processes of participatory economy. 2008.

LUCAS, Edward R. **Countering the "Unholy Alliance"**: The United States' Efforts to Combat Piracy and Violent Extremism in the Western Indian Ocean, 2001–2014. 2017.

MAMALI, Catalin. Benjamin Peters, **How Not to Network a Nation**: The Uneasy History of the Soviet Internet. International Journal of Communication, v. 11, p. 5, 2017.

MCDONALD, Geoff et al. **Stuxnet 0.5:** The missing link. Symantec Report, v. 26, 2013.

MCKENNA, Katelyn YA; BARGH, John A. **Plan 9 from cyberspace**: The implications of the Internet for personality and social psychology. Personality and social psychology review, v. 4, n. 1, p. 57-75, 2000.

MEINRATH, Sascha D.; VITKA, Sean. Crypto war II. **Critical Studies in Media Communication**, v. 31, n. 2, p. 123-128, 2014.

MENDELSOHN, Barak. **Foreign fighters—recent trends**. Orbis, v. 55, n. 2, p. 189-202, 2011

MOGHADAM, Assaf; BERGER, Ronit; BELIAKOVA, Polina. **Say terrorist, think insurgent:** Labeling and analyzing contemporary terrorist actors. Perspectives on Terrorism, v. 8, n. 5, p. 2-17, 2014.

MOHANTA, Bhagyashree; NANDA, Pragyan; PATNAIK, Srikanta. **Management of VUCA (Volatility, Uncertainty, Complexity and Ambiguity) Using machine learning techniques in industry 4.0 paradigm**. In: New Paradigm of Industry 4.0. Springer, Cham, 2020. p. 1-24.

MUELLER-BADY, Robin et al. **An evolutionary hybrid search heuristic for monitor placement in communication networks**. Journal of Heuristics, v. 25, n. 6, p. 861-899, 2019.

MURPHY, Bill; CULP, Charles. **TC/TG/TRG MINUTES COVER SHEET**. TC, v. 404, p. 636-8400, 2012.

NAZMI, Shadab. **Why India shuts down the internet more than any other democracy.** BBC News, v. 19, 2019.

NEGRO, Gianluigi. **The global construction of the Chinese internet 1994–2014**. In: GigaNet: Global Internet Governance Academic Network, Annual Symposium. 2017.

NELSON, Okorie et al. **Global Media, digital journalism and the question of terrorism:** An empirical inquest on ISIS. Media Watch, v. 10, n. 2, p. 212-224, 2019.

OHMAE, Kenichi. **The borderles**s world. McKinsey Quarterly, n. 3, p. 3-19, 1990.

PANIAGO, Paulo de Tarso Resende. **Uma cartilha para melhor entender o terrorismo internacional:** conceitos e definições. Revista Brasileira de Inteligência, v. 3, n. 4, p. 13-22, Brasília DF, 2007.

PENNEBAKER, James W.; KING, Laura A. **Linguistic styles:** language use as an individual difference. Journal of personality and social psychology, v. 77, n. 6, p. 1296, 1999.

PYTHON, Andre. **Debunking Seven Terrorism Myths Using Statistics**. CRC Press, 2020.

RADHAKRISHNAN, Adi. **COVID-19:** Restricted Internet Impacts on Health in Kashmir. Health and Human Rights Journal, 2020.

RAHIMULLAH, Riyad Hosain; LARMAR, Stephen; ABDALLA, Mohamad. **Understanding violent radicalization amongst muslims:** A review of the literature. Journal of Psychology and Behavioral Science, v. 1, n. 1, p. 19-35, 2013.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. **Securing the internet of things**. Computer, v. 44, n. 9, p. 51-58, 2011.

ROUF, Ishtiaq et al. **Security and Privacy Vulnerabilities of In-Car Wireless Networks:** A Tire Pressure Monitoring System Case Study. In: USENIX Security Symposium. 2010.

SAGAWA, Paul I. **The balkanization of the Internet**. The McKinsey Quarterly, n. 1, p. 126, 1997.

SELVA RAJOO, Kukaneswaran. **INTERNET OF THINGS IMPLEMENTATION IN HIGH FREQUENCY MEASUREMENTS**. IRC. 2019

SERPANOS, Dimitrios; WOLF, Marilyn. **Industrial internet of things**. In: Internet-of-Things (IoT) Systems. Springer, Cham, 2018. p. 37-54.

TRAUTMAN, Lawrence J. **Managing cyberthreat**. Santa Clara Computer & High Tech. LJ, v. 33, p. 230, 2016.

TRIMBLE, Marketa. **Geolocation, Geoblocking, and Private International Law**. 2016.

VALENTE, Junia; CARDENAS, Alvaro A. **Security & privacy in smart toys**. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. 2017. p. 19-24.

VENTRE, Daniel. **Cyberespace et acteurs du cyberconflit**. Lavoisier, 2011.

VERTON, Dan. **Black ice:** the invisible threat of cyber-terrorism. Osborne, 2003.

WALL, David. **Policing the Virtual Community**: The Internet, Cyberspace and Cyber-Crime. In: Policing futures. Palgrave Macmillan, London, 1997. p. 208-236.

WANG, Shiguang et al. **Towards cyber-physical systems in social spaces:** The data reliability challenge. In: 2014 IEEE Real-Time Systems Symposium. IEEE, 2014. p. 74-85.

WEIMANN, Gabriel. **Terror on the Internet:** The new arena, the new challenges. US Institute of Peace Press, 2006.

WIENER, Norbert. **Time, communication, and the nervous system**. Annals of the New York Academy of Sciences, v. 50, n. 4, p. 197-220, 1948.

WU, Jiangxing. **Cyberspace mimic defense**. Springer International Publishing, 2020.

YANG, Guobin. **A Chinese Internet? History, practice, and globalization**. Chinese Journal of Communication, v. 5, n. 1, p. 49-54, 2012.

YANKELOVICH, Nicole; MEYROWITZ, Norman K.. ; DAM, Andries van . **Reading and writing the electronic book**. IEEE computer, v. 18, n. 10, p. 15-30, 1985.