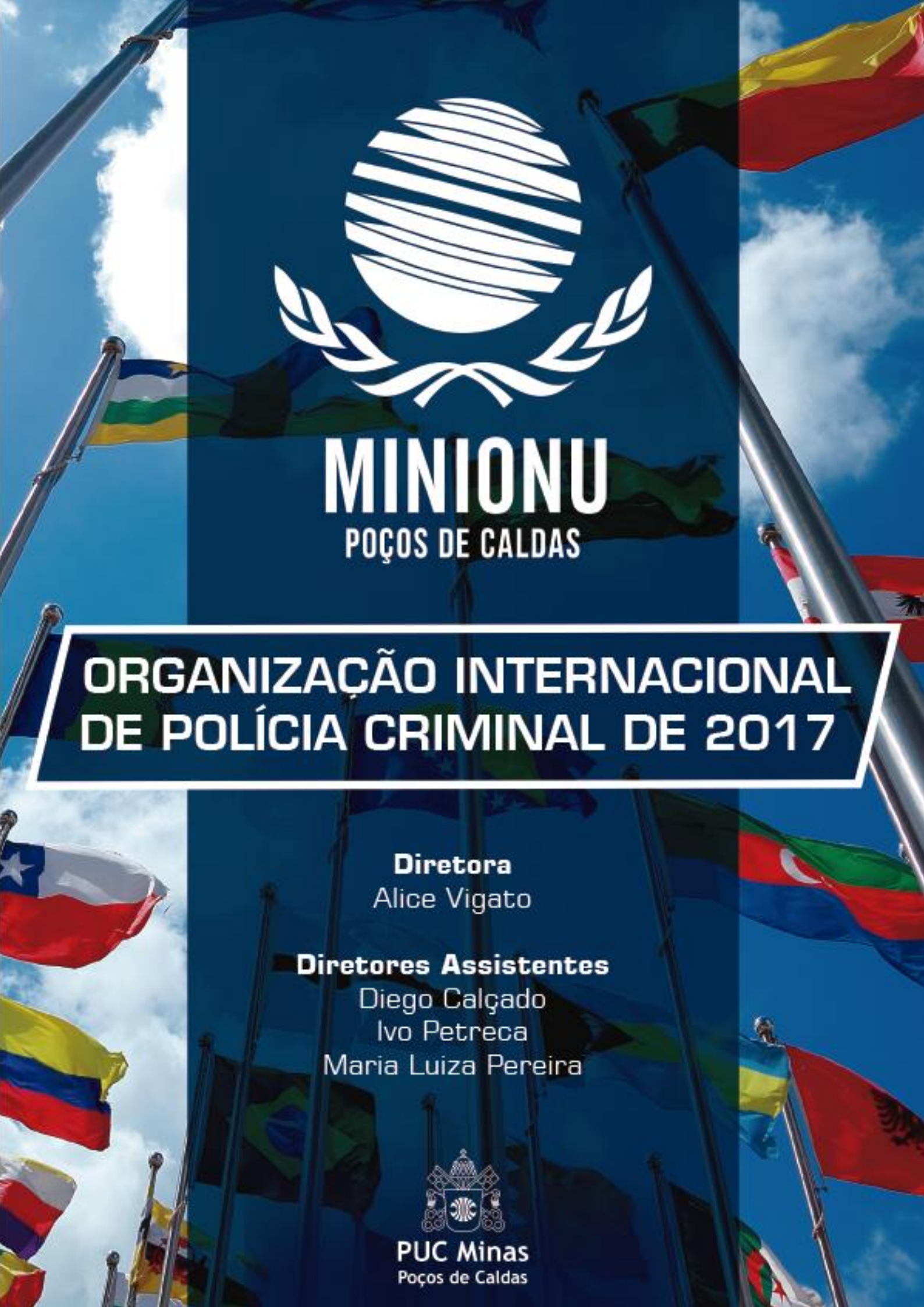

MINIONU
POÇOS DE CALDAS

ORGANIZAÇÃO INTERNACIONAL DE POLÍCIA CRIMINAL DE 2017

Diretora
Alice Vigato

Diretores Assistentes
Diego Calçado
Ivo Petreca
Maria Luiza Pereira

PUC Minas
Poços de Caldas

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Departamento de Relações Internacionais

Organização Internacional de Polícia Criminal

Conferência sobre Ciberterrorismo e Ciberespionagem de 2017

Alice Vigato Araújo

Guia de estudos do comitê INTERPOL para a 2º MINIONU – Poços de Caldas 2017

Poços de Caldas
2017

SUMÁRIO

1. APRESENTAÇÃO DO TEMA

1.1 A INTERPOL **3**

1.2 Relevância do Tema **6**

1.3 Segurança Cibernética **7**

1.4 Crimes Cibernéticos **7**

1.5 Terrorismo **8**

1.6 Ciberterrorismo **8**

1.7 Ciberespionagem **10**

1.8 Guerra Cibernética **11**

2. APRESENTAÇÃO DO COMITÊ **12**

2.1 Conceitos Importantes **12**

2.2 O Comitê **13**

3. POSICIONAMENTO DOS ATORES RELEVANTES **14**

4. QUESTÕES RELEVANTES **20**

5. INFORMAÇÕES COMPLEMENTARES **21**

5.1 *Darknet* **21**

5.2 *WikiLeaks* **21**

5.3 Sistema de Avisos da Interpol **22**

6. REFERÊNCIAS **24**

1. APRESENTAÇÃO DO TEMA

1.1 A INTERPOL

A ideia de se ter uma Polícia Internacional nasceu em 1914 com o primeiro Congresso Internacional de Polícia Criminal, realizado em Mônaco. Nele, oficiais de polícia, advogados e magistrados de 24 países se reuniram para discutir procedimentos de prisão, técnicas de identificação, registros criminais internacionais e processos de extradição. Inicialmente, pela iniciativa do Dr. Johannes Schober, presidente da Polícia de Viena, criou-se, em 1923 a Comissão Internacional de Polícia Criminal (CIPC), com sede em Viena, Áustria.

Em 1949, As Nações Unidas (ONU) concedem a CIPC o status de Organização Não Governamental. Assim, após a adoção de uma Constituição mais moderna composta por “metas e objetivos”, em 1956 surge a INTERPOL - Organização Internacional de Polícia Criminal. Uma Organização autônoma, que cobria as contribuições dos países membros e apoiava-se nos investimentos como principal meio de apoio.

Atualmente a INTERPOL é a maior organização policial internacional do mundo, com 190 países membros. Seu papel é garantir que a polícia em todo o mundo tenha acesso às ferramentas e serviços necessários para fazer o seu trabalho de forma eficaz e em conjunto para tornar o mundo um lugar mais seguro. Sua infraestrutura de alta tecnologia de apoio técnico e operacional ajuda a enfrentar os crescentes desafios da luta contra a criminalidade no século XXI. A organização também fornece treinamento direcionado, suporte de investigação especializado, dados relevantes e canais de comunicação seguro, sua missão é prevenir e combater a criminalidade através de uma maior cooperação e inovação no âmbito policial e de segurança mesmo quando não existam relações diplomáticas entre países específicos.

As atividades da INTERPOL são dirigidas pelos países membros, num quadro claro de órgãos diretivos e reuniões estatutárias.

A Secretaria Geral da INTERPOL está sediada em Lyon, França, com o apoio do Complexo Global para a Inovação em Singapura, sete agências regionais e escritórios de Representação Especial na União Africana, na União Europeia e nas Nações Unidas.

Cada um dos países membros mantém uma Agência Nacional Central com seu próprio pessoal, agentes da lei altamente.

A Assembleia Geral e o Comitê Executivo formam a governança da Organização. A Assembleia Geral é composta por delegados nomeados pelos governos dos países membros. Como é o órgão supremo da INTERPOL, reúne-se uma vez por ano e toma todas as decisões importantes que afetam a política geral, os recursos necessários para a cooperação internacional, os métodos de trabalho, as finanças e os programas de atividades. De um modo geral, a Assembleia toma decisões por maioria simples na forma de resoluções, onde cada país membro representado corresponde a um voto.

Eleito pela Assembleia Geral, o Comitê Executivo é dirigido pelo Presidente da Organização. O Comitê Executivo (CE) se reúne três vezes por ano e define a política e direção organizacional. Os membros da CE ocupam nível superior do policiamento em seus próprios países e trazem muitos anos de experiência e conhecimento. Seu papel é supervisionar a execução das decisões da Assembleia Geral, preparar a agenda das sessões e submeter à Assembleia Geral qualquer programa de trabalho ou projeto que considere útil. O CE também supervisiona a administração e o trabalho do Secretário Geral.

A implementação diária das decisões estratégicas da Organização é realizada pela Secretaria Geral e pelas Agências Centrais Nacionais (NCB). Localizada em Lyon, França, a Secretaria Geral funciona 24 horas por dia, 365 dias por ano e é gerida pelo Secretário Geral . Reconhecendo o valor de reunir a polícia dentro de uma região para compartilhar experiências e lidar com questões comuns de criminalidade, a Secretaria tem sete escritórios regionais em todo o mundo: Argentina (Buenos Aires), Camarões (Yaoundé), Costa do Marfim (Abidjan), El Salvador (San Salvador), Quênia (Nairóbi), Tailândia (Bangkok) e Zimbabwe (Harare). Juntamente com representantes especiais na Organização das Nações Unidas em Nova York e na União Europeia (UE) em Bruxelas que permite a INTERPOL trabalhar em estreita colaboração com os departamentos e entidades das Nações Unidas e da EU na prevenção e combate a criminalidade transnacional e no reforço à segurança regional e global.

Cada país membro da Interpol mantém uma Agência Nacional Central (NCB) ligando a polícia nacional de cada Estado com a rede global da INTERPOL. A

Agência trata-se basicamente de uma divisão da agência nacional de polícia ou serviço de investigação e, serve como ponto de contato para todas as atividades da INTERPOL no território. Equipados por agentes nacionais de aplicação da lei altamente treinados, as NCB são a força vital da INTERPOL, contribuindo com as bases de dados criminais e cooperando em investigações, operações e prisões transfronteiriças.

A Comissão de Controle de Fichários da INTERPOL (CCF) garante que o tratamento de dados pessoais, como informações, nomes e impressões digitais, estejam em conformidade com as regras da INTERPOL, a fim de proteger tanto os direitos fundamentais dos indivíduos como a cooperação internacional.

A principal fonte de financiamento da INTERPOL é a contribuição estatutária anual fornecida por cada um dos 190 países membros da Organização. Os países membros podem também fazer contribuições voluntárias adicionais, que podem ser monetárias ou em espécie. As contribuições dos países membros entram no Orçamento Ordinário da Organização. Entretanto, recursos adicionais também podem ser fornecidos por doadores diferentes para atividades pré-determinadas. Esse financiamento externo é administrado separadamente em um Fundo Fiduciário e em Contas Especiais.

A INTERPOL coopera estreitamente com um número de parceiros no setor público, como com a Organização Mundial das Alfândegas, a Comunidade Econômica dos Estados da África Central e numerosas agências governamentais, também mantém escritórios de representação na Organização das Nações Unidas e na União Europeia. A INTERPOL também conta com parceiros no setor privado, englobando entidades com e sem fins lucrativos, como organizações não governamentais e fundações.

Como principal documento legal da INTERPOL, a Constituição define metas e objetivos da Interpol. Estabelece o mandato da Organização de assegurar a cooperação mais ampla possível entre todas as autoridades policiais criminais e de suprimir os crimes de direito comum. Além de definir a estrutura da Organização, o papel de cada órgão da previr o orçamento e as relações com outras organizações.

A INTERPOL age dentro dos limites das leis existentes em diferentes países e no espírito da Declaração Universal dos Direitos Humanos. Sua base jurídica bebe no Artigo 3 de sua Constituição, “É estritamente proibido para a Organização realizar

qualquer intervenção ou atividades de caráter político, militar, caráter religioso ou racial. ”. Essa característica é de suma importância para definir em quais conflitos ou ideias a INTERPOL poderá ou não interferir. (INTERPOL, 2017)

1.2 Relevância do Tema

Tecnologias em rede tocam todos os cantos do globo e todas as facetas da vida humana. Elas impulsionaram a inovação, fomentaram as liberdades e estimularam a prosperidade econômica. Mesmo assim, as próprias tecnologias que permitem esses benefícios oferecem novas oportunidades para atividades cibernéticas mal intencionadas e indesejadas.

O aparecimento da Internet e a vulgarização do seu uso veio alterar o paradigma do modo de funcionamento das sociedades. As sociedades industriais transformaram-se em sociedades da informação, onde o conhecimento e a informação são valorizados e têm um papel fulcral. A internet, primeiramente considerada como um espaço de liberdade absoluta e que possibilitava o acesso e compartilhamento de dados instantaneamente e a partir de qualquer ponto do globo, é hoje vista como um fator de insegurança. O ciberespaço está suscetível a novas formas de ameaça sobre a forma de crime no mundo virtual. Os ciberataques colocam em risco não só a privacidade e liberdade dos cidadãos, mas a soberania do Estado e a segurança nacional. (KOBEK, 2017)

No mundo virtual de hoje, onde a comunicação online é uma necessidade, governos e empresas compartilham o medo de ataques cibernéticos. O ciberespaço e sua infraestrutura subjacente são vulneráveis a uma ampla gama de riscos decorrentes de ameaças físicas e cibernéticas. De acordo com um relatório da *Cybersecurity Ventures*, de 2017 a 2021, o gasto mundial acumulado em segurança cibernética superará US$ 1 trilhão. Os danos causados pelo cibercrime custarão US$ 6 trilhões anualmente até 2021. (INVESTOR'S BUSINESS DAILY, 2016)

Atores cibernéticos sofisticados e estados-nação exploram vulnerabilidades para roubar informações e dinheiro e, desenvolvem capacidades para interromper, destruir ou ameaçar a prestação de serviços essenciais. Ainda, a Agência Nacional de Segurança dos EUA (NSA) sugere, em termos inequívocos, que o próximo grande conflito ocorrerá no ciberespaço. Os riscos associados à dependência das

nações em relação a essas tecnologias em rede levaram ao desenvolvimento de políticas de segurança cibernética. (KULIKOVA, 2015)

Como afirma o estrategista global, autor e consultor especializado no impacto disruptivo dos avanços tecnológicos sobre a segurança Marc Goodman (2015), “nesse mundo interconectado a capacidade de entrar em contato com 1 bilhão de pessoas para o bem ou para o mal é uma coisa que não estamos preparados para lidar. Antes tínhamos os crimes praticados um a um e agora os cibercriminosos atacam em massa”.

1.3 Segurança Cibernética

A tecnologia é uma das principais armas usadas para burlar as defesas das organizações e das nossas casas, provocando perdas financeiras ou consequências ainda mais desastrosas. A inovação é fundamental para combater essas ameaças em constante evolução.

A segurança cibernética envolve a proteção de informações e sistemas contra grandes ameaças cibernéticas, como o terrorismo cibernético, a guerra cibernética e a espionagem cibernética. Em suas formas mais destrutivas, as ameaças cibernéticas visam ativos secretos, políticos, militares ou infraestruturais de uma nação ou de seu povo. A segurança cibernética é, portanto, uma parte crítica da estratégia de segurança de qualquer governo. (PALOALTO, 2017)

1.4 Crimes Cibernéticos

O cibercrime é uma área de rápido crescimento da criminalidade. Cada vez mais criminosos estão explorando a velocidade, conveniência e anonimato da Internet para cometer uma diversidade de atividades criminosas que não conhecem fronteiras, físicas ou virtuais, causam sérios danos e representam ameaças reais para as vítimas em todo o mundo. Embora não exista uma única definição universal de cibercrime, a aplicação da lei faz geralmente uma distinção entre dois tipos principais: o *cybercrime* avançado (ou crime de alta tecnologia), que diz respeito a ataques sofisticados contra hardware e software de computador; E o *cyber-enabled crime*, que são aqueles crimes "tradicionais" com o advento da Internet, tais como os

crimes contra crianças, crimes financeiros e até mesmo o terrorismo. Um número crescente de criminosos é atraído por crimes cibernéticos, visto que estes são convenientes, anônimos, rápidos, diversos e relativamente de baixo risco.

Novas tendências no *cibercrime* estão surgindo o tempo todo, com os custos estimados para a economia global chegando a bilhões de dólares. No passado, a cibercriminalidade era cometida principalmente por indivíduos ou pequenos grupos. Hoje, vemos redes criminosas altamente complexas que reúnem indivíduos de todo o mundo em tempo real para cometer crimes em uma escala sem precedentes. Outra característica atual da cibercriminalidade é de natureza cada vez mais transnacional. (INTERPOL, 2017)

1.5 Terrorismo

O terrorismo representa uma grave ameaça à segurança nacional e às vidas dos indivíduos em todo o mundo. Na INTERPOL, os peritos da Secretaria Geral coletam, armazenam e analisam informações sobre indivíduos e grupos suspeitos e suas atividades, a INTERPOL também divulga alertas e avisos sobre terroristas, criminosos perigosos e ameaças de armas à polícia nos países membros e outras organizações internacionais. (INTERPOL, 2017)

1.6 Ciberterrorismo

O termo foi cunhado na década de 1980 por Barry Collin, que discutiu essa dinâmica do terrorismo como a transcendência do físico para o reino virtual e “a interseção e a convergência desses dois mundos”. (COLLIN, 1996)

Até agora, a comunidade internacional não decidiu uma definição exata de "ciberterrorismo" que possa ser aplicada universalmente. No entanto, de acordo com a OTAN (2008), o ciberterrorismo é "um ataque cibernético usando ou explorando redes de computadores ou de comunicação para causar destruição suficiente para gerar medo ou intimidar uma sociedade em um objetivo ideológico".

Para Wilson (2003), segundo a *US National Infrastructure Protection Center*, ciberterrorismo é "um ato criminoso perpetrado por computadores resultando em

violência, morte e/ou destruição, e criando terror com a finalidade de coagir um governo para mudar suas políticas."

James Lewis (2002) define o termo como "A intimidação da empresa civil através do uso da alta tecnologia para produzir objetivos políticos, religiosos ou ideológicos, ações que resultem em desativar ou excluir dados ou informações de infraestrutura crítica".

Há uma diferença entre crimes cibernéticos e ciberterrorismo. O termo ciberterrorismo geralmente se refere a atos que se assemelham, em certa medida, aos que são característicos de ataques terroristas por meios convencionais. Já os crimes cibernéticos geralmente incluem uma atividade ilícita na Internet como um todo. Para que os casos de ciberterrorismo sejam considerados de forma semelhante ao terrorismo clássico, os atos do primeiro devem suportar, pelo menos em partes, o caráter e a magnitude do último, significando morte/lesão a seres humanos ou destruição física/danos às propriedades e, ser infligido através dos meios da Internet.

A Internet torna-se uma poderosa arma digital na mão dos ciberterroristas. Vários países atentam para o perigo dos ataques virtuais. Visto que os ciberterroristas conseguem acessar qualquer informação dos sistemas do governo, o terrorismo pela Internet também é considerado uma ameaça para a integridade do Estado.

Segundo Brickey (2012) podemos identificar três objetivos principais do ciberterrorismo: Objetivo Organizacional, no qual inclui funções como recrutamento, treinamento de instigação, captação de recursos, comunicação, planejamento, espionagem, etc; Objetivo de Debilitar, ou seja, dificultar o funcionamento normal de sistemas de computador, serviços ou sites. Os métodos utilizados são desfigurar, negar e expor. Uma vez que os países ocidentais são altamente dependentes de estruturas online que suportam serviços vitais, estes métodos são de mérito comprovado; E, por fim, Objetivo Destrutivo, no qual busca alcançar os mesmos ou, resultados semelhantes ao terrorismo clássico. Este é rotulado de ciberterrorismo puro.

O ciberterrorismo vem afetando várias nações soberanas. Em Janeiro de 2011 o governo canadense informou um grande ataque cibernético contra suas agências, incluindo a *Canada Defence Research and Development,* uma agência de

pesquisa do Departamento de Defesa Nacional do Canadá. O ataque forçou o *Finance Department* e *Treasury Board*, principais agências econômicas do Canadá, a se desconectar da Internet. (OTAN, 2017)

Em Outubro de 2012, a empresa russa *Kaspersky* descobriu um ataque cibernético mundial chamado *"Red October"*, que estava operando desde 2007. Os hackers reuniram informações através de vulnerabilidades nos programas Word e Excel da Microsoft. Os principais alvos do ataque parecem ser países da Europa Oriental, da antiga URSS e da Ásia Central, embora a Europa Ocidental e a América do Norte também tenham relatado vítimas. O vírus coletou informações de embaixadas do governo, empresas de pesquisa, instalações militares, fornecedores de energia, infraestrutura nucleares e outras críticas. (OTAN, 2017)

1.7 Ciberespionagem

Ciberespionagem é uso de redes de computadores para obter acesso ilícito a informações confidenciais, geralmente aquelas detidas por um governo ou outra organização. (OXFORD, 2017). Ou seja, é o ato ou prática de obtenção de segredos sem a autorização do titular da informação (seja ela pessoal, de propriedade ou natureza sigilosa), a partir de indivíduos, concorrentes, rivais, grupos, governos e inimigos. Isso pode ser utilizado em seu benefício pessoal, econômica, política ou militarmente usando métodos na Internet, redes ou computadores individuais através do uso de técnicas de rachaduras e software malicioso (MESSMER, Ellen, 2008).

A espionagem como uma arma de guerra foi utilizada em todos os grandes países, tanto durante a Segunda Guerra Mundial quanto na Guerra Fria. Segundo a lei internacional, em tempos de guerra, a espionagem é frequentemente reconhecida como legítima e admissível por muitas nações; No entanto, em tempos de paz, esse tipo de ação é rotulado como um crime na maioria dos países.

Em meados de 2013, Edward Snowden, ex-funcionário da CIA (Central Intelligence Agency) vazou informações sobre o monitoramento da segurança dos Estados Unidos. Snowden revelou que a NSA (National Security Agency) monitorava não só as ligações de milhões de cidadãos americanos, mas que o governo também tinha acesso aos servidores de nove empresas de internet, incluindo *Facebook*, *Google, Microsoft* e *Yahoo*. A agência britânica de escuta eletrônica *GCHQ* também

foi acusada de coletar informações sobre as empresas online via *Prism*. Em Junho de 2013, o jornal *The Guardian* publicou que a agência de espionagem do Reino Unido estava usando cabos de fibra óptica que transportam comunicações globais e compartilham grandes quantidades de dados com a NSA. Ainda, após fugir para Hong Kong, Edward Snowden disse *ao South China Morning Post* que a NSA havia liderado mais de 61.000 operações de hackers em todo o mundo, incluindo muitas em Hong Kong e na China continental.

Mais tarde, Edward Snowden informou ao *The Guardian* que a NSA tinha monitorado os telefones de 35 líderes mundiais. Em Julho do mesmo ano o jornal O Globo, revelou que a NSA dirigia um programa de vigilância em todo o continente. Alguns aliados dos EUA na América Latina como México, Brasil, Colômbia e Chile ficaram indignados com as revelações no jornal e exigiram respostas dos Estados Unidos.

Os vazamentos provocaram debates nacionais e internacionais sobre os “poderes secretos” da NSA e como lidar com os imprevistos do mundo cibernético. (G1, 2013)

1.8 Guerra Cibernética

A guerra cibernética envolve estados-nações que usam a tecnologia da informação para penetrar nas redes de outra nação para causar danos ou destruição. Nos EUA e em muitos outros estados-nações, a guerra cibernética foi reconhecida como o quinto domínio de guerra (depois de terra, mar, ar e espaço). Os ataques de guerra cibernética são principalmente executados por hackers que são bem treinados na exploração das complexidades de redes de computadores e operam sob os auspícios e suporte de estados-nações. Em vez de "desligar" as principais redes do alvo, um ataque de guerra cibernética pode invadir as redes com o propósito de comprometer dados valiosos, degradando as comunicações, prejudicando serviços de infraestrutura, como transporte ou serviços médicos ou interrompendo o comércio. (PALOALTO, 2017)

2. APRESENTAÇÃO DO COMITÊ

2.1 Conceitos Importantes

Quando dois ou mais países/Estados têm suficiente contato entre si, com suficiente impacto reciproco nas suas decisões, de tal forma que se conduzam, pelo menos ate certo ponto, como partes de um todo, se tem um Sistema Internacional. (DUNNE, 2007) Assim, podemos dizer que o Sistema Internacional é uma arena na qual os países se relacionam uns com os outros por meio de acordo de vontades.

A soberania é a autoridade suprema do poder público, ou seja, uma excelência não superada em qualquer ordem imaterial. A soberania do Estado é considerada geralmente sobre dois aspectos: o interno e o externo. A soberania interna significa que o poder do Estado é o mais alto existente dentro do Estado. A soberania externa significa que, nas relações recíprocas entre os Estados, não há subordinação nem dependência, e sim igualdade. (JUSBRASIL, 2017) Assim, cada estado tem direito a sua integridade territorial, independência política e autonomia para tomar suas decisões no plano interno e no internacional. Quando os países atuam no Sistema Internacional, eles agem de forma a reforçar a sua soberania e respeitar a soberania dos outros.

Nenhum país é totalmente autossuficiente, o que quer dizer que eles precisam manter uma relação de troca uns com os outros. Economicamente, por exemplo, países precisam importar alguns bens escassos assim como exportar aqueles que têm em grande quantidade em seu território. Essa relação de trocas dos países cria certa interdependência entre eles, pois os países precisam uns dos outros para suprir todas as suas necessidades. Os países são mutuamente dependentes, entretanto essa relação quase nunca é simétrica. (KEOHANE E NYE, 1998)

O poder é um dos conceitos mais complexos dentro da área de estudo das Relações Internacionais. As atuais mudanças tecnológicas e a emergência de um espaço cibernético ampliam a complexidade e a intangibilidade do mesmo. Poder é outro fator de influência no comportamento dos Estados no Sistema Internacional, assim, aquele país que detém de mais poder terá mais vantagens do que outros, por isso a busca por pode cibernético se tornou tão relevante no campo das relações internacionais. (MAIER, 2015)

2.2 O Comitê

Em 2001 aconteceu a Convenção de Budapeste sobre Crimes Cibernéticos, adotada pelo Conselho da Europa. A convenção foi o primeiro tratado internacional sobre crimes cometidos via Internet e outros tipos de redes de computador. Seu objetivo foi buscar uma política penal comum que visasse a proteção da sociedade contra o cibercrime, especialmente através da adoção de uma legislação apropriada e a promoção à cooperação internacional.

Devido fatos recentes e a crescente ameaça *cyber*, que saiu do âmbito doméstico para internacional, ameaçando não só civis, mas também empresas transacionais e governos. E, percebendo o crescimento dos cibercrimes, tanto em termos de frequência como de impacto econômico, e, acreditando que a cooperação internacional é um requisito indispensável para prevenir e combater eficazmente tal ilicitude, a INTERPOL realiza sua 1ª Conferência sobre Ciberterrorismo e Ciberespionagem de 2017 em Berlim, Alemanha.

Aqui, avaliar-se-á o que precisa ser feito para resolver a potencial ameaça que é o ciberterrorismo. Alguns especialistas em terrorismo advertem que, por mais que carros bomba e armas biológicas aparentem ser uma ameaça maior do que o ciberterrorismo atualmente, este não pode ser subestimado devido suas peculiaridades.

Com o intuído de dar suporte e apoio operacional aos países membros, a INTERPOL encoraja a discussão de tópicos como a detecção e a prevenção de crimes digitais; o desenvolvimento de tecnologias inovadoras, assim como a capacitação dos países para o combate a cibercriminalidade; uma possível militarização do ciberespaço; a avaliação de tendências regionais e ameaças atuais e formulação planos de ação e operações transnacionais a fim de formular leis que sejam aplicadas e internalizadas pelos países membros; formulação de estratégias para quebrar as redes criminosas por trás de diferentes tipos de crimes cibernéticos, de ciberterrorismo e ciberespionagem.

A Assembleia Geral da Interpol é atualmente formada por delegados representando cada um dos 190 países-membros da Organização. Cada um deles é apontado pelo governo de sua nação para lhe representar a cada seção, no presente comitê os delegados serão membros de suas forças policiais.

Na Conferência sobre Ciberterrorismo e Ciberespionagem delegados representarão os chefes de polícia e ministros de 36 Estados. Os países participantes serão os atores mais relevantes dentro do tema. As decisões serão tomadas por maioria qualificada, salvo os casos em que a Constituição da INTERPOL pede uma maioria simples.

O sistema de resoluções adotado no presente comitê será o de múltiplas resoluções, nas quais, pontualmente, serão abordados os tópicos pré-estabelecidos, assim como os surgidos nos debates.

Espera-se que os países participantes tomem consciência da vulnerabilidade cibernética e se comprometam a comum acordo a fim de cumprir o principal objetivo da conferencia que é encontrar uma forma de tornar o "*cyber world"* mais seguro.

Vale ressaltar que o comitê tem caráter recomendatório, assim, seu objetivo é auxiliar e assessorar as delegações presentes da melhor maneira possível para que estas tomem decisões baseadas em suas capacidades individuais e em consenso coletivo. As decisões aqui tomadas influenciarão todas as esferas dos estados dos países participantes, afetando assim, não somente a arena internacional, mas também a doméstica - de leis governamentais até o dia-a-dia dos civis.

3. POSICIONAMENTO DOS ATORES RELEVANTES

ESTADOS UNIDOS

Os Estados Unidos possuem uma política de vigilância do ciberespaço bastante forte através da Agência Nacional de Segurança (NSA). O país é um ator altamente relevante no mundo cyber, e já acusou e foi acusado inúmeras vezes de cometer ciberataques. Em 2013, Edward Snowden, ex-funcionário da CIA vazou informações confidenciais alegando que o país monitorava diversos sites, empresas e ate governos em todo mundo. Os Estados Unidos também já relatou ser alvo de inúmeros ataques cibernéticos dentre os quais alegam que grande parte é de cunho terrorista. (O GLOBO, 2017)

O país ainda conta com o Comando Cibernético dos Estados Unidos (USCYBERCOM), um comando sub-unificado das forças armadas, subordinado ao

Comando Estratégico dos Estados Unidos com o intuito de proteger a rede de computadores militar do país.

A coordenação de Incidentes Cibernéticos dos Estados Unidos, que estabelece os princípios que regem a resposta do Governo Federal a qualquer incidente cibernético do setor privado é responsabilidade da Diretriz de Política Presidencial 41 (PPD-41).

Washington e Londres trabalham em um projeto de desenvolver exercícios conjuntos de cibersegurança e defesa de redes, assim os serviços de informação dos dois países vão formar uma célula conjunta para coordenar uma resposta contra ciberataques.

BRASIL

Em 2010, foi criado no Brasil o Centro de Defesa Cibernética (CDCiber), por determinação do Comando do Exército. Esse órgão tem como objetivo coordenar e integrar os esforços dos vetores da defesa cibernética. Para atuar neste segmento tão específico, iniciou-se, entre outras atividades, o processo de capacitação de recursos humanos, possibilitando o domínio de temas multidisciplinares. Foi destinado um enfoque especial ao desenvolvimento da doutrina de proteção dos próprios ativos, bem como na capacidade de atuar em rede, implementar pesquisa científica e de coordenar relações com instituições civis acadêmicas e empresariais. Produtos como sistemas de segurança da informação, programas de detecção de intrusão, hardware para a composição de laboratórios e simuladores de defesa e guerra cibernética, além de estímulo à produção de software nacional, como antivírus, a realização de seminários e programas de treinamento especializado são alguns exemplos das ações adotadas para a identificação e o desenvolvimento das capacidades mencionadas. Em virtude desse conjunto de ações, o Projeto Estratégico de Defesa Cibernética incluiu o Exército Brasileiro no restrito grupo de organizações, nacionais e internacionais, que possuem a capacidade de desenvolver medidas de proteção e mitigar ataques no campo cibernético. (EPEX, 2017)

A Estratégia Nacional de Defesa (END), aprovada pelo Decreto no 6.703, de 18 de dezembro de 2008, considera que existem três setores estratégicos da

Defesa: o nuclear, o cibernético e o espacial. A partir de então, a defesa do setor cibernético foi considerada prioritária para o Exército Brasileiro. A fim de se atender os objetivos da END referentes à defesa cibernética, visualiza-se a implantação do Sistema Brasileiro de Defesa Cibernética. (IME, 2017).

A Lei nº 12.737 (Lei dos Crimes Cibernéticos) de novembro de 2012 caracteriza como crimes invadir computadores para conseguir, destruir ou alterar dados, ou instalar vulnerabilidades a fim de obter vantagens. A pena pode varia de 3 meses a um ano, e multa, e pode ser aumentada se a invasão levar a prejuízo econômico, ou se o crime for praticado contra a Presidente, governadores, Presidente do STF, e afins. (BRASIL, 2012).

O Brasil se comprometeu em mais de uma cúpula à cooperação internacional para o combate a crimes cibernéticos, como na VI Cúpula BRICS e na III Cúpula da ASPA. (BRICS, 2014; ASPA, 2012).

ALEMANHA

Ciberataques são bastante frequentes na Alemanha, conforme dados do Centro de Tecnologia de Informação (TI) são registrados, em média, de três a cinco ataques das mais diversas formas a sistemas de computadores do governo. Ainda, conforme a *Rogall-Grothe*, a maioria dos ataques é proveniente da esfera civil e se relacionam à espionagem econômica.

Na 47ª Conferência de Segurança de Munique, de 2010, a premiê alemã, Angela Merkel, afirmou que a ciberguerra seria tão perigosa quanto uma guerra convencional. Em 2011 foi inaugurado em Bonn, o centro de defesa cibernética do país com o intuito de melhorar o combate e intensificar a investigação de ataques provenientes do ciberespaço, criando uma estrutura de cooperação entre órgãos estatais alemães. (CW, 2011).

Desafiado por uma crescente ameaça terrorista e pelo aumento do nível de ataques cibernéticos, o gabinete alemão adotou uma estratégia de segurança cibernética e criou o chamado *Mobile Incident Response Teams* (MIRT) dentro do Escritório Federal de Segurança da Informação para combater ameaças online. Também serão criadas unidades cibernéticas especiais. A Agência de Inteligência Estrangeira (BND), anunciou que terá, em meados de 2022 seu próprio satélite de

espionagem. A Alemanha, ainda adota um conjunto de leis que exigem que instituições financeiras reportem ao governo as ocorrências de ataques cibernéticos ou de violações de dados.

RÚSSIA

Em 2011 a Rússia lançou um documento intitulado “Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no Espaço da Informação”. O documento valoriza o respeito ao Estado de direito e os princípios da legalidade. Reconhece a complexidade do novo paradigma e as várias dimensões envolvidas em torno do tema. Reconhece que, apenas por meio de interação e cooperação com outros países, é possível evoluir, na velocidade necessária, no campo dos sistemas de proteção. Entretanto, destaca a possibilidade de utilização da força em um eventual conflito cibernético. (IPEA, 2013).

O país vem se preocupando bastante com o tema. Ainda em 2013 o presidente russo Vladimir Putin lembrou que os chamados "ataques cibernéticos" já estão sendo utilizados para solucionar problemas de caráter político-militar. Ele também observou que o "poder de destruição” desses ataques poderá ser maior do que o das armas convencionais. (GAZETA RUSSA, 2013). Assim a Rússia aposta em estratégias para aumentar seu nível de proteção.

Na Declaração de Fortaleza (VI Cúpula do BRICS), a Rússia se comprometeu a explorar “a cooperação no combate a crimes cibernéticos”, e também com a “negociação de um instrumento universal juridicamente vinculante nesse campo" (BRICS, 2014). No entanto, o país se recusou a assinar a Convenção Europeia sobre Cibercrime. (CYBERCRIME LAW, 2015).

Importantes órgãos norte-americanos classificam a Federação Russa como uma das principais potências no ciberespaço. O país ainda é apontado por usar seu grande poder cibernético de maneira ofensiva no sistema internacional. (MEDVEDEV, 2015)

A Rússia também coopera com a China no domínio da segurança cibernética, fato que, alguns vêm como uma tentativa de reduzir a influência americana no campo da tecnologia da informação.

REINO UNIDO

O Reino Unido se empenha bastante quando o assunto são os crimes que ocorrem no ciberespaço, principalmente a espionagem. Por possuírem um histórico de ataques contra computadores do departamento de defesa britânico, tem investido milhões de libras em programas de segurança nacional para o ciberespaço. Assim, o governo britânico deseja a criação de regras internacionais que regulamentem o ciberespaço.

Reconhecimento o risco que os ataques cibernéticos representam, a Avaliação Estratégica de Defesa e Segurança do governo de 2015 classificou a ameaça *cyber* como de Nível 1 para o Reino Unido, o mesmo nível do terrorismo ou do conflito militar internacional. Para tal, foi lançada, em 2016 uma nova estratégia que se baseia em três pilares fundamentais: Defender, ou seja, reforçar as defesas do governo e dos setores críticos de infraestruturas nacionais, como a energia e transportes e economia; Dissuadir, de forma a reforçar as capacidades de aplicação da lei garantindo que se possa acompanhar, apreender e processar aqueles que cometeram crimes cibernéticos; Por fim, desenvolver uma capacidade de contra-ataque cibernético totalmente operacional e operacional. (GOV.UK, 2016)

CANADÁ

Após os ataques cibernéticos sofridos pelo Canadá em janeiro de 2011, o país passou a se engajar mais no causa.

O Centro de Segurança das Comunicações (CSE) presta aconselhamento, orientação e serviços para ajudar a garantir a proteção da informação eletrônica e das infraestruturas de informação de importância para o Governo do Canadá. Para conseguir isso, o CSE possui conhecimentos cibernéticos e técnicos reconhecidos internacionalmente que os permitem responder a ameaças e ataques contra redes e sistemas de computadores do governo do Canadá. (COMMUNICATION SECURITY ESTABLISHMENT, 2015).

A economia canadense depende fortemente da Internet, tanto as empresas quanto o governo se tornaram cada vez mais dependentes da Internet. Em função disso, o país conta com a Estratégia Canadense de Segurança Cibernética, que tem

três objetivos principais: Proteger os sistemas governamentais, fazer parcerias para assegurar sistemas cibernéticos vitais fora do governo federal e, oferecer suporte aos canadenses para estarem seguros online. (PUBLIC SAFETY CANADA, 2016)

IRÃ

Pesquisadores reconhecem que o Irã está entre os países mais avançados no que diz respeito às capacidades cibernéticas. Assim como muitos Estados, o Irã não tem uma estratégia cibernética abrangente e publicada.

O Irã vem trabalhando para desenvolver e implementar estratégias para operar no ciberespaço. Em termos gerais, suas atividades cibernéticas têm dimensões ofensivas e defensivas. As capacidades cibernéticas ofensivas do Irã oferecem uma opção teoricamente de baixo custo aos líderes iranianos por dissuadir e administrar ameaças estrangeiras. Sua estratégia do ciberespaço é parte da “Doutrina da Guerra Assimétrica”, um princípio central no conceito iraniano do uso da força. A guerra do ciberespaço, como outras táticas assimétricas clássicas, como o terrorismo, é vista pelo Irã como uma ferramenta eficaz para infligir sérios danos a um inimigo com superioridade militar e tecnológica.

Defensivamente o regime toma medidas para fortalecer a infraestrutura da Internet do país para evitar a "corrupção" da sociedade iraniana por valores ocidentais, simplificar o monitoramento de cidadãos iranianos e bloquear ataques cibernéticos por atores estrangeiros. (INSS, 2012)

O Estado iraniano conta com uma Sede Cibernética dentro de suas Forças Armadas (AFGS) que coordena a política cibernética nas forças armadas iranianas. Os ministérios da Inteligência, Defesa, Tecnologia, Informação e Comunicação também cooperam com a Sede Cibernética para identificar deficiências e acompanhar as ameaças à infraestrutura cibernética do Irã. Sua orientação é, portanto, principalmente de natureza defensiva (CRITICAL THREATS, 2015).

4. QUESTÕES RELEVANTES PARA A DISCUSSÃO

É importante que, ao final das discussões, algumas questões sejam debatidas. De modo geral, sugere-se a discussão do atual cenário criminal no mundo, bem como a

elaboração de propostas para o desempenho da INTERPOL na melhoraria das capacidades da comunidade global em lidar com a ameaça *cyber*. Além da promoção da interação desta com outras Organizações, sejam internacionais ou nacionais, visando uma maior ênfase às organizações policiais de cada Estado, e, sugerindo diretrizes para que estes implementem um efetivo combate à prática delitiva.

Deste modo, propõem-se as seguintes diretrizes:

1. É possível que se estabeleça um programa abrangente de cibersegurança e cibercrime de parcerias que reconheçam as perspectivas nacionais e regionais dos países membros e que, em conjunto com a INTERPOL, possa promover os esforços nacionais e internacionais contra a cibercriminosos?
2. Ate que ponto os estados estão dispostos a abrir mão de sua soberania em prol de uma maior segurança cibernética global, permitindo que a INTERPOL auxilie na investigação, detecção e fiscalização de crimes cibernéticos?
3. De que forma a INTERPOL pode auxiliar os países de maneira igualitária, tendo em vista as diferentes capacidades de cada país?
4. Até que ponto é pertinente a militarização do ciberespaço?

5. INFORMAÇÕES COMPLEMENTARES

5.1 *Darknet*

Quando se procura algo em um mecanismo de busca, ele verifica a Internet para encontrar uma correspondência. Entretanto, há grandes seções da Internet que os motores de busca não podem detectar, o que é conhecido como a *"*Deep Web". Algumas informações existentes na Deep Web podem ser deliberadamente mal utilizadas, assim, os criminosos agem nessa parte escondida da Internet sem ser detectados.

Usando software especializado para esconder suas atividades e garantir o anonimato, os criminosos podem conduzir empresas ilegais, vender drogas ou armas, jogos ilícitos, trocar documentos e material de abuso infantil.

Estas atividades criminosas subterrâneas vieram à atenção do público em 2013 quando o Departamento Federal de Investigação dos Estados Unidos (FBI) fechou o site de mercado negro *Silk Road*, que estava operando na *Darknet.*

As ferramentas complexas de criptografia usadas para acessar e comunicar na *Darknet* criam muitos desafios para a aplicação da lei e na identificação e localização dos criminosos que se escondem no anonimato. (INTERPOL, 2017)

O papel da INTERPOL nessa questão é de auxiliar no monitoramento da *Deep Web* e dar aos países uma base de dados confiáveis para o melhor aproveitamento das investigações lá feitas.

5.2 *WikiLeaks*

WikiLeaks é uma organização de mídia multinacional e uma gigantesca biblioteca que contem os documentos mais procurados do mundo. Foi fundada pelo seu editor Julian Assange em 2006 na Suécia. Sem fins lucrativos, a organização publica fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. Assim, a WikiLeaks é especializada em análise e publicação de grandes conjuntos de dados e materiais oficiais censurados ou restritos que envolvem guerra, espionagem e corrupção. Até agora, publicou mais de 10 milhões de documentos e análises e nos últimos anos vem publicando matérias de repercussão global.

A WikiLeaks tem relações contratuais e plataformas de comunicação seguras com mais de 100 grandes organizações de mídia em todo o mundo. Isso permite que a WikiLeaks tenha grande poder de negociação, impacto e credibilidade no mundo. A organização tem como marca registrada a autenticação de documentos e resistência à censura.

A plataforma do WikiLeaks se tornou mais popular quando o ex-consultor de inteligência americano Edward Snowden, autor do vazamento de dados sobre o programa de grampos do governo dos EUA divulgou informações no site.

5.3 Sistema de Avisos da INTERPOL

A INTERPOL tem um sistema de avisos que é usado para pedidos de cooperação ou alertas que permitem aos policiais dos países membros partilharem informações críticas relacionadas com o crime. Os avisos são publicados pela Secretaria-Geral da INTERPOL, a pedido dos Escritórios Nacionais Centrais (NCB) e entidades autorizadas, e pode ser publicada em qualquer um dos idiomas oficiais da Organização: Árabe, Inglês, Francês e Espanhol.

Red Notice - para buscar a localização e a prisão de pessoas procuradas com vista à extradição ou ação legal similar.

Yellow Notice - para ajudar na localização de pessoas desaparecidas, muitas vezes menores, ou para ajudar a identificar as pessoas que são incapazes de se identificar.

Blue Notice - para coletar informações gerais de uma pessoa como identidade, localização ou atividades em relação a um crime.

Black Notice - para buscar identificação de corpos não-identificados.

Green Notice - para divulgar avisos sobre pessoas que cometeram crimes e provavelmente os cometerão novamente.

Orange Notice - para divulgar pessoas, lugares, ou objetos que represente uma ameaça séria e iminente à segurança pública.

Purple Notice - para procurar informações sobre atividades, equipamentos, objetos e métodos usados por criminosos.

INTERPOL-United Nations Security Council Special Notice - é emitida para grupos ou indivíduos que sofreram alguma sanção por parte do Conselho de Seguranca das Nacoes Unidas.

Um Aviso é publicado apenas se ele preenche todas as condições para o processamento da informação.

No caso dos Avisos Vermelhos, as pessoas em causa são procuradas por jurisdições nacionais para serem processadas ou para cumprir uma sentença baseada num mandado de detenção ou decisão judicial. O papel da INTERPOL consiste em ajudar as forças policiais nacionais a identificar e localizar essas pessoas com vista à sua detenção e extradição ou a acções legais semelhantes.

A INTERPOL ainda faz uso de um alerta similar ao Aviso, conhecido como Difusão, que é outro pedido de cooperação ou mecanismo de alerta. A Difusao é menos formal do que um aviso, mas também é usado para solicitar a prisão ou localização de um indivíduo ou informações adicionais em relação a uma investigação policial. Uma Difusão é lançada diretamente por um NCB aos países membros de sua escolha. Tal ação é simultaneamente registada no Sistema de Informação da INTERPOL.

6 REFERÊNCIAS

Barry, Collin, “The Future of CyberTerrorism,” Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996. Retrieved also on 12/12/2012 from http://afgen.com/terrorism1.html

BBC*. Edward Snowden: Leaks that exposed US spy programme*. United States, 2014. From: http://www.bbc.com/news/world-us-canada-23123964

Brickey, J. (2012). *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*. Combating Terrorism Center at West Point. Retreived on 12/12/2012 from http://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

Bucala, P. *Iranian Cyber Strategy: A View from the Iranian Military, 2015*. From: https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military#_edn265398264b80259a64a107844869bb5c1

César, S*. A segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual*, Brasília, 2013. From: http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf

Communication Security Establishment. *The Government of Canada’s centre for cyber threat detection, mitigation, response, and defence*, 2015. From: https://www.cse-cst.gc.ca/en/group-groupe/cyber-defence .

CYBERCRIME LAW. *Cybercrime laws: Russia*, 2008. From: http://www.cybercrimelaw.net/Russia.html.

Departamento de Estado dos EUA, Gabinete do Coordenador de Combate ao Terrorismo, *Relatórios dos Países sobre o Terrorismo*, 30 de Abril de 2007.

DW. *Alemanha inaugura centro de defesa cibernética em Bonn*, 2011. From: http://www.dw.com/pt-br/alemanha-inaugura-centro-de-defesa-cibern%C3%A9tica-em-bonn/a-15161206

EPEX. *Defesa Cibernética*, 2017, From: http://www.epex.eb.mil.br/index.php/defesa-cibernetica

G1. *Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.* São Paulo, 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em 01/06/2015

Gazeta Russa. *Exército russo terá comando responsável pela segurança cibernética*, 2013. From: http://gazetarussa.com.br/ciencia/2013/07/11/exercito_russo_tera_comando_responsavel_pela_seguranca_cibernetica_20363

Goodman, Marc. *O futuro dos crimes cibernéticos*, 2015. From: https://cryptoid.com.br/banco-de-noticias/o-futuro-dos-crimes-ciberneticos-no-terceiro-dia-da-hsm-expo-management-2015/

GOV.UK. *Chancellor speech: launching the National Cyber Security Strategy*, 2016. From: https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy

Interpol, (2012). Cybercrime. Retreived on 12/12/2012 from http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Investor's Business Daily. *"As Russia Hacks, Is The Best Cyber Defense A Terrifying Cyber Offense?",* 2016. From: http://www.investors.com/news/preventing-cyberattacks-is-the-best-defense-an-almighty-offense/

Jusbrasil. Soberania Nacional, 2017. From: https://www.jusbrasil.com.br/topicos/366256/soberania-nacional

Keohane Robert and Joseph Nye,Power and Interdependence in the Information Age: Foreign Affairs, Vol. 77, No. 5 (Sep. - Oct., 1998), pp. 81-94

Kobek, Luisa Parraguez. *The State of Cybersecurity in Mexico: An Overview*, 2017. From: https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview

Kulikova, Alexandra*. Is A Cyber Arms Race Between The US And Russia Possible?.* 2015. From: http://www.russia-direct.org/analysis/cyber-arms-race-between-us-and-russia-possible

Laboratório de Defesa Cibernética. *Defesa Cibernética*, 2017. From: http://defesacibernetica.ime.eb.br/

Lewis, J. *Assessing the* Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Washington, DC, 2002. From: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Maier, Friedrich. Um poder cibernético? Dificuldades metodológicas em Nye para a compreensão do poder no ciberespaço, 2015. From: http://www.marilia.unesp.br/Home/Eventos/2015/xiiisemanaderelacoesinternacionais/um-poder-cibernetico_friedrich-maier.pdf

Medvedev, Sergei A. Monterey. *Offense-defense theory analysis of Russian cyber capability. California: Naval Postgraduate School*, 2015. From: http://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf?sequence=1

Nato Review Magazine. *Cyber Timeline*, 2013. From: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Nato, (2008). Cyber defence concept MC0571. Brussels, Belgium.

PALOALTO, *O Que É A Segurança Cibernética?*. From: https://www.paloaltonetworks.com.br/resources/learning-center/what-is-cyber-security.html

Pladna, B. (2008). Cyber terrorism and information security. Retrieved on 12/12/2012 from http://www.infosecwriters.com/text_resources/pdf/BPladna_Cyber_Terrorism.pdf

Public Safety Canada. *Canada's Cyber Security Strategy*, 2016. From: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx

Siboni, G. Kronenfeld, S. *Iran's Cyber Warfare*, 2012. From: http://www.inss.org.il/index.aspx?id=4538&articleid=5203

The Guardian. *NSA monitored calls of 35 world leaders after US official handed over contacts.* United States, 2015. From: https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

United States Government Accountability Office (GAO), (2007). *CYBERCRIME Public and Private Entities Face Challenges in Addressing Cyber Threats*. Report to Congressional Requesters. Retrieved on 12/12/2012 from http://www.gao.gov/new.items/d07705.pdf

Wilson, C. (2005). Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress.Retreived on 12/12/2012 from http://www.history.navy.mil/library/online/computerattack.htm