FERNANDO LIRA RIGAMONTE

A SOBERANIA NA ERA CIBERNÉTICA

LAVRAS-MG
2017

FERNANDO LIRA RIGAMONTE

A SOBERANIA NA ERA CIBERNÉTICA

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharel.

Prof. Dr. Pedro Ivo Ribeiro Diniz
Orientador

LAVRAS-MG
2017

Ficha catalográfica elaborada pelo Sistema de Geração de Ficha Catalográfica da Biblioteca Universitária da UFLA, com dados informados pelo(a) próprio(a) autor(a).

Rigamonte, Fernando Lira.
A Soberania na Era Cibernética / Fernando Lira Rigamonte. - 2016.
39 p.

Orientador(a): Pedro Ivo Ribeiro Diniz.
.
TCC (graduação) - Universidade Federal de Lavras, 2016.
Bibliografia.

1. Soberania. 2. Internet. 3. Segurança. I. Diniz, Pedro Ivo Ribeiro. . II. Título.

FERNANDO LIRA RIGAMONTE

A SOBERANIA NA ERA CIBERNÉTICA
SOVEREIGNTY ON CYBERNETIC ERA

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharel.

APROVADA em:
Dr. Pedro Ivo Ribeiro Diniz UFLA
Dr. Leonardo Gomes Penteado Rosa UFLA

Prof. Dr. Pedro Ivo Ribeiro Diniz
Orientador

LAVRAS-MG
2017

Aos meus pais, Santo e Elizabete, que estiveram presentes em toda essa jornada e aos amigos mais próximos.

Dedico

RESUMO

O presente Trabalho de Conclusão de Curso (TCC), escrito sob a forma de um artigo científico, teve por objetivo demonstrar o modo com o qual a internet vem redimensionando o significado e a aplicação do conceito de soberania. Também pretendeu-se demonstrar que, por meio desse redimensionamento, os Estados ainda possuem grande relevância dentro do Direito Internacional, sobretudo pelo fato de que, a partir do estímulo a políticas de cooperação em cibersegurança, o papel dos atores estatais se tornou ainda mais relevante. Para que fosse possível o êxito desse propósito, recorreu-se à pesquisa bibliográfica em artigos científicos e livros de autores especializados nos temas de Direito Internacional, Relações Internacionais e Informática. Por meio desta bibliografia, foi perceptível a relação interdisciplinar que o tema do presente trabalho proporciona. Iniciando-se pela exposição do contexto histórico do surgimento e da evolução da internet , buscou-se explicar a relação desta com a soberania, uma vez que seu crescimento resultou no aparecimento de danos a cada dia mais graves causados por ciberataques. Para que fosse possível explicar como esses funcionam, recorreu-se à explicação conceitual da internet. Posteriormente, surge o debate de como a internet é gerida. Isso foi importante para explicar como o Direito Internacional pode auxiliar os Estados a combaterem os ciberataques: com a cooperação, a exemplo da Política de Ciberdefesa da OTAN, de onde chegou-se a conclusão de que a internet apenas redimensionou o significado da soberania, fortalecendo-a em muitos casos.

Palavras-chave: Soberania. Estado. Segurança. Internet.

ABSTRACT

This Course Conclusion Paper (TCC), is written in the form of a scientific paper, aimed to demonstrate the way in which the internet has been expanding the meaning and application of the concept of sovereignty. Also intended to demonstrate that, through this resizing, states still have great relevence within the international law, particularly due to the fact that, from the stimulous to cybersecurity cooperation policies, the role of state actors has become even more relevant. For the success of this propose it was possible, it resorted to the literacture of scientific articles and book expert authors on topics on International Law, International Relations and the Information Tecnology. Through this bibliography was clear the interdisciplinar relationship of this to the sovereignty, since its growth is resulted on increasemente on cases of every day damages, which is becoming more and more serious, caused by cyberattacks. To make it possible for explain how International Law can help States to face cyber attacks: with cooperation, such as the NATO cyber defense policy, of which he reached the conclusion that the internet only resized the meaning of sovereignty, strengthening the importance of a State in many cases.

Keywords: Sovereignty. State. Insurance. Internet.

SUMÁRIO

REFERENCIAL TEÓRICO

A discussão a respeito do modo com que o direito internacional pode contribuir para o combate às ameaças causadas pelos ciberataques perpassa, a princípio, pelas análises feitas por Jovan Kurbalija e Eduardo Gelbstein; por Hindemburgo Francisco Pires e por Michele Tanchman da Silva, no que tange à formação, à expansão e o modo de governança da internet.

Para Kurbalija e Gelbstein (2005), " um dos aspectos fascinantes da internet durante o seu desenvolvimento e crescimento iniciais foi a sua governança peculiar.". Para explicar o modo com o qual essa governança ocorre, o autor recorre ao contexto militar do surgimento da internet, que se deu na Guerra Fria (1945-1991). A Guerra Fria consistiu na disputa hegemônica do planeta entre Estados Unidos e União Soviética (PINHO,2000).

A partir desse ponto, as obras de Hindemburgo Francisco Pires (2012) e Michele Tanchman da Silva (2008) passam a se entrelaçar, uma vez que, em quanto aquele dispõe que Estados Unidos e União Soviética travaram uma disputa tecnológica para amedrontar a potência rival, esta alega que esse medo, por parte dos Estados Unidos, fez com que este elaborasse uma forma de comunicação militar eficaz em tempos de guerra (SILVA, 2008).

A parceria entre as obras é reforçada pela ideia de que a necessidade de proteger o território estadunidense fez com que um grupo de pesquisadores criassem a *Intergalatic Computer Network*, o embrião da internet (SANTOS, 2011). Isso possibilitou a conexão com as ideias de Hindemburgo Francisco Pires (2012, p.3), para o qual a posterior criação da ARPANET possibilitou a interconexão entre "as empresas privadas, as universidades, centros de pesquisas e laboratórios.".

No que tange ao desenvolvimento da internet, ambos os autores retratam o grande investimento financeiro , provindo da parceria entre universidades e empresas privadas, como fato de expansão da internet. A partir dessa expansão, surgiram conflitos pelo controle do sistema de nomes de domínio (DNS).

Esse conflito foi denominado por Kurbalija e Gelbstein (2005) como "Guerra do DNS". Inicialmente motivado por disputas econômicas atreladas ao controle dos servidores de zona-raíz, que controlam o tráfego de informações na rede, a disputa pelo controle do sistema de nomes de domínio acirrou-se com a ocorrência de ciberataques.

A questão do controle dos ciberataques envolve, a princípio, a elucidação de como funciona a governança atual da internet. Para isso, recorre-se aos aspectos conceituais. A respeito disso, Morais; Lima e Franco (2012) concebe a internet como um acoplamento de computadores e equipamentos que distribui geograficamente os recursos de comunicação.

Ainda segundo Morais; Lima e Franco (2012), esse acoplamento permite a distribuição geográfica dos recursos de comunicação e a consequente otimização dos recursos de *hardwere* e *software*..

Muller (2010) complementa que a internet globaliza o escopo de informação, além de distribuir o controle da administração por meio da descentralização de protocolos. Isso faz com que a geografia dos Estados nacionais, visto que dinamiza as relações comerciais , influencia na difusão cultural e catalisa as relações comerciais (SILVA,2008), além de reforçar o controle geográfico por meio do mapeamento dos servidores inter-regionais conectados no espaço (PIRES,2012).

A respeito do funcionamento, Pires (2012) afirma que a internet funciona atualmente por meio do protocolo TCP/IP (*Transmition Control Protocol/ Internet Protocol*), que permite o direcionamento da informação ao destinatário final e o HTTP (*Hyper Text Transmition Protocol*), que dinamiza a navegação entre as páginas.

Com o aumento da facilidade de navegação, aumentão os riscos de vulnerabilidades, falhas que, conforme Al-Shaer e Hamed (2004) são combatidas por um *firewell*, que, segundo Cheswick e Bellovin (2005), restringe o acesso de dados entre uma rede protegida e a internet.

Quando as vulnerabilidades não podem ser combatidas, ocorrem as ameaças. São elas o cibercrime, a ciberespionagem, o ciberterrorismo e a ciberguerra (PIRES,2012). Neste aspecto destacam-se os autores Moore; Clayton e Anderson (2009), que caracteriza o cibercrime como “dolo do agente, cuja qualificação o faz desejar tal conduta”; Hersh (2010), que define ciberespionagem como uma ciência que captura mensagens eletrônicas em segredo; Deening (2000), para o qual o ciberterrorismo é definido como ataque ilegal contra redes de computadores para intimidar governos. Já a ciberguerra é definida por Arquilla e Ronfeldt (1993) como operação militar de coleta de informações sobre o inimigo.

A questão conceitual sobre a internet termina com a digressão de Krapp (2005) sobre a necessidade de cautela no que tange ao conceito de hacktivismo e a constatação de que as ameaças virtuais são difíceis de combater em virtude de sua variabilidade (PORTUGAL,2013).

No que diz respeito à governança, parte importante deste trabalho, a fundamentação abarca a sua conceituação, à sua abordagem e à polêmica da administração dos nomes de domínio. A conceituação, complexa em virtude da abrangência dos termos que a compõem (KURBALIJA: GELBSTEIN, 2005), é feita por Roseneau (2000) como o conjunto de atividades realizadas por instituições governamentais, para atender a objetivos comuns.

Quanto às abordagens, Silva (2008) classifica-as em estreita, que diz respeito à estrutura física, relativa aos nomes de domínio e ao IP, que segundo Drezner (2004), assegura

o endereçamento dos pacotes de dados entre os computadores, e a ampla, relativa à legislação e aspectos sociais.

Quanto ao funcionamento da governança da internet, Muller (2010) afirma que seu estudo de como as ideias de gestão da internet podem ser traduzidas em ação ou não. Pires(2012), por sua vez, é mais objetivo, pois relaciona a governança com a administração dos nomes de domínio (DNS), o que leva à tese da existência atual de uma hegemonia unilateral estadunidense, que permite a disseminação de sua ideologia política.

Em seguida Pires (2012) constata que a hegemonia estadunidense, em termos geográficos, é explicada pela presença de 10 dos 13 servidores de zona-raiz. Esses, para Mockapetris e Dunlap (1988) facilitam a disponibilização do sinal aos clientes da internet. Ao estudar o tema, Kruger (2016) constatou que o *Verisign* é o principal servidor zona-raiz responsável pelo imperialismo digital dos EUA, uma vez que permite aos mesmo controlar os registros comerciais.

A respeito disso, Castells (2003), estabelece o inicio da hegemonia dos EUA com relação à internet a partir da criação da *Internet Society*, organizações sem fins lucrativos que, segundo os estudos de Goldsmith (2006), ao transferir a gestão dos nomes de domínio à *Internet Assigned Numbers Authority* (IANA), proporcionou o crescimento da internet, o que tornou possível a internacionalização da mesma e a negociação da administração dos nomes de domínio com toda a comunidade mundial (SILVA,2008).

Nesse sentido, os estudos realizados por Roberts (2001) apontam para a criação da *International Corporation for Assigned Names and Numbers* (ICANN), que, atualmente exerce a administração dos nomes de domínio (KLEIN, 2002).

Verifica-se neste aspecto a convergência de abordagens entre Silva (2008) e Pires (2012), na medida em que ambos, cada qual à sua maneira de abordar o problema, perceberam a necessidade de se propor um modelo de governança da internet plurilateral e descentralizado.

Ambos os autores falaram a respeito dos Fóruns sobre Governança da Internet (FGI), baseados no trabalho realizado por Kurbalija e Gelbstein (2005), no qual percebe-se a descrição minuciosa dos acontecimentos que antecederam as edições do FGI, bem como suas consequências. Ainda sobre este tema , Yoda (2006) especificou as discussões da primeira edição, que versaram sobre cibercrimes, privacidade , cibersegurança, censura , etc.

Com a falha da primeira edição, o IGF Forum (2008), site do FGI, relatou a criação de coalizões dinâmicas, formadas por *multstakeholders* , para, segundo o site NIC (2007), alcançarem o equilíbrio entre a proteção de direitos e a liberdade de expressão. A respeito do FGI ainda podem ser constatadas, por Silva (2008), as atividades dos grupos de trabalho.

Apesar do FGI ter sido constatado pelos autores que são referência para este trabalho como falho na tentativa de estabelecer a governança multilateral da internet, os estudos de Drezner (2004) indicaram grande possibilidade de diálogo aberta para que os Estados, por meio da cooperação, possam reduzir custos com regulamentações.

O referido tema está atrelado à questão da soberania. Para que a soberania possa ser discutida na era cibernética, o presente trabalho apresenta uma breve digressão histórica sobre a evolução do conceito e o modo com o qual é aplicado atualmente pelo direito internacional.

Para o desenvolvimento desta parte, foram consultados livros e artigos científicos de autores renomados do direito internacional, bem como das relações internacionais, da filosofia e outras áreas correlatas.

A princípio Koskenniemi (2006) remete a Jean Bodin e a Thomas Hobbes o destaque nos estudos do conceito de soberania, que para este era imposição de comportamento e para aquele, a não submissão do Estado às normas estrangeiras. Isso possibilitou a ideia de que a soberania atingiria a paz na ordem interna e garantiria a igualda de na ordem internacional.

Destaca-se ainda a classificação de ordem internacional feita por Bull (2002), para o qual esta é um padrão de atividade responsável por sustentar os objetivos elementares de uma sociedade internacional, isto é, que demanda o redimensionamento da soberania. Pereira (1999), ao fazer um leitura de Rousseau sobre o tema, indica a limitação da soberania pelo Direito.

Destaca-se também a ideia de que a soberania enfrenta o desafio, representado pela perda da detenção da hegemonia cultural sobre seu povo na era globalizada, bem como da descontrução das fronteiras territoriais pela internet, o que obriga o Estado tenha que se redimensionar, se adaptar para solucionar conflitos, por meio da cooperação.

No que tange ao combate aos ciberataques, a princípio demonstrou-se ,por meio dos estudos realizados em Portugal pelo Instituto de Defesa Nacional (IDN), pelo Senado Francês (SÉNAT), do Gabinete Real Inglês e por Muller (2010), que as ações unilaterais dos Estados no combate aos ciberataques se mostraram ineficazes.

Diante disso, a alternativa encontrada foi a cooperação em matéria de cibersegurança, feita com maior destaque pela OTAN, mas também pela União Europeia, para a qual , segundo o Conselho da Europa (2009), o ciberespaço tornou-se um espaço vital para a promoção de direitos humanos e pela ONU.

A Política de Ciberdefesa da OTAN é realizada por meio de um treinamento pelo *National Computer Response Capability* (NCIRC), que é responsável por treinamentos de vigilância e comunicação de vulnerabilidades (PORTUGAL, 2013).

Com relação à União Europeia, Militão (2014) dispõe sobre a *European Network and Information Security Agency* (ENISA), que é especializada em segurança da informação, enquanto que Pires (2012) aponta para o levantamento processual realizado pela *European Cybercrime Center* (EC3), também de acordo com o site da Europol.

Por fim, no que diz respeito à cooperação em cibersegurança pela ONU, destaca-se a constatação, feita por Kahona (2009) da existência de uma compilação digital de tratados feitos pela ONU sobre internet, bem como na descrição das 5 principais resoluções a serem abordadas neste trabalho e a definição feita por Martinez (2009) para ciberterrorismo, concebendo-o como uma coerção para intimidar grupos sociais.

Por fim, a UIT (2008) remete à resolução A/RES/58/199, da ONU, que estabelece a cooperação entre as estruturas das tecnologias de informação à própria UIT, bem como Pires (2012) reforça a necessidade de cooperação em matéria de cibersegurança, que na visão de Castells (2007), trata-se de uma reafirmação da soberania estatal.

METODOLOGIA

A princípio, concebeu-se o presente Trabalho de Conclusão de Curso (TCC), sob a forma de artigo científico, por meio de uma revisão bibliográfica estruturada em autores fundamentais e sites específicos para as questões conceituais e estruturais abordadas ao longo do trabalho.

Uma vez realizada a coleta dos dados das referências bibliográficas, iniciou-se o processo de elaboração dos objetivos principais e secuncários, já especificados na introdução. Em seguida, delimitou-se o tema, de modo a cumprir com os objetivos pretendidos.

1 INTRODUÇÃO

O presente trabalho apresenta como objetivo principal demonstrar que as ameaças cibernéticas decorrentes da expansão da internet, embora evidenciem os limites da lógica interestatal para enfrentar tais dilemas, ainda permanecem geridos e combatidos, no cenário internacional, sob esta mesma dinâmica, concretamente manifestada por tentativas de cooperação internacional entre Estados soberanos.

Para o atendimento desses objetivos, é preciso elucidar o contexto de nascimento, desenvolvimento e a expansão da internet. Nesse sentido, será explicado que a internet surge durante a Guerra-Fria (1946-1991), como uma forma de comunicação segura para o exército estadunidense.

Seu desenvolvimento se deu com o investimento do setor privado e do setor empresarial e a sua expansão a partir da gestão de John Postel à frente da *Internet Assigned Numbers Authority* (IANA) e com a terceirização dos nomes de domínio.

A terceirização dos nomes de domínio, por sua vez, gera discussões em torno dos aspectos conceituais e políticos da internet. Os aspectos conceituais são de vital importância para que se possa compreender como a internet funciona, como é gerida e como pode ser administrada.

Ao longo do trabalho, verificar-se-á que a administração dos nomes de domínio (DNS) permite o controle das informações que circulam na rede. Isso representa a possibilidade de vantagens comerciais e econômicas. Atualmente, a gestão da internet é classificada como unilateral, sob a chefia dos Estados Unidos.

No entanto, diante da expansão da internet, bem como da sua má utilização, por crackers, verifica-se que a atual forma de gestão não é suficiente para evitar danos causados aos usuários comuns e aos Estados diante dos ciberataques, cuja transnacionalidade desafia o exercício clássico da soberania estatal.

Contudo, as propostas de combate aos ciberataques e aos cibercrimes deles decorrentes, com efeito, reafirmam a dinâmica interestatal, mantendo os Estados no centro das abordagens e alternativas de respostas a este tipo de problema.

2 INTERNET NO CONTEXTO INTERNACIONAL

Este tópico tem por objetivo abordar o contexto histórico de surgimento da internet, bem como seu processo de desenvolvimento e expansão. Também serão abordados aspectos conceituais, necessários para o entendimento das questões atinentes à governança da internet. Essa, por sua vez, faz parte dos aspectos políticos por meio dos quais é possível perceber a manutenção do modelo interestatal nas tentativas de combater este problema que desafia as formas clássicas de relação entre os Estados.

2.1 Nascimento, Desenvolvimento e Expansão

A internet surgiu no contexto histórico da Guerra Fria, para proporcionar segurança às informações coletadas pelas forças armadas dos EUA (SILVA,2011). O seu crescimento deu-se a partir da colaboração financeira do setor empresarial e do apoio das universidades. A evolução até o estágio atual, por sua vez, ocorreu a partir da invenção do protocolo TCP/IP[1] (PIRES,2012).

Durante o processo de evolução da internet, os Estados passaram a perceber o valor comercial e político do controle das informações que circulam nessa rede. O interesse pelo controle da internet foi fortalecido com o crescimento da ocorrência de ciberataques, fato que estimulou os debates pela governança da internet (PIRES,2012).

A preocupação foi ocasionada perante os efeitos nocivos dos ciberataques para a segurança das informações estatais, das organizações e dos cidadãos que fazem uso da internet, bem como a luta por mais poder a partir da possibilidade de dominação, a partir do controle das informações circulantes na rede (KURBALIJA; GELBSTEIN,2005).

É importante ressaltar também que, em relação à segurança[2], a preocupação dos Estados se justifica pelo crescimento da ocorrência de crimes cibernéticos provocados por

[1] Vinton Cerf e Robert Kahn "inventaram" o protocolo TCP/IP, um dos sustentáculos da internet que conhecemos hoje. O protocolo TCP/IP A origem militar da internet é defendida por uma grande quantidade de tecnólogos. De qualquer modo, a ideia de uma rede de computadores interconectados nasceu disso, apesar de alguns especialistas realizarem diferenciação. A respeito de Vinton Cerf e Robert Kahn, vide CERF, Vinton G.;KAHN, Robert E. A Protocol for Pocket Network Intercommunication. Princeton University Press, Princeton, v.22, n.5, mai 1974. Disponível em: <https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf>.

[2]De acordo com Moore; Clayton; Anderson (2009,p.9), a "Segurança é um problema de ação coletiva". Neste caso, os autores se referem à necessidade de cooperação para resolver o problema da segurança cibernética. A justificativa para essa preocupação reside nos graves danos sociais e econômicos

crackers[3] (MOORE; CLAYTON; ANDERSON, 2009). Diante disso, o presente trabalho é justificado pela necessidade de responder a seguinte indagação: Como o Direito Internacional poderia combater os ciberataques ou contribuir para a melhorar a gestão da internet?

Para responder à essa pergunta, será necessário elucidar o contexto histórico da formação, do desenvolvimento e da gestão da internet. Depois, será verificada a compatibilidade da gestão da internet dentro da lógica do Direito Internacional, o que será feito por meio do relato da Política de Ciberdefesa da OTAN.

Também será realizada menção à Convenção de Budapeste, na medida em que esta tipifica as condutas criminosas praticadas por meio dos ciberataques. O surgimento do que se conhece atualmente como "internet" ocorreu a partir de um contexto histórico específico, o da metade final da Guerra Fria (1945-1991). Nesse período, Estados Unidos (EUA) e União Soviética (URSS) dividiram a hegemonia do planeta (PINHO, 2000).

Para isso, ambas as potências se utilizaram da ciência e da tecnologia para demonstrar poder perante o rival. Isso foi feito através de investimentos na indústria bélica, por exemplo, que teve como resultado, por exemplo, o lançamento do satélite Sputnik[4] pela URSS e a produção de radares pelos EUA, que consistiam em um sistema de telecomunicações capaz de prevenir ataques (PIRES, 2012).

A preocupação com a criação de um método seguro de comunicação entre os membros do exército estadunidense, fez com que as informações estratégicas não se perdessem na hipótese de uma de suas estruturas fossem atacadas, o que gerou a necessidade de se pensar em uma outra tecnologia (SILVA,2011).

---

provocados pelos ciberataques, fato muito bem abordado pelo artigo cuja citação é utilizada neste trabalho. Para mais informações, vide <http://www.jstor.org/stable/20202392>.
Na versão original, a citação é: "Security is a collective-actionproblem".

[3]Eis a diferenciação feita por Marques Filho (2010,p.3): Originalmente, o termo hacker é aplicado para aqueles indivíduos que possuem um conhecimento superior aos outros em determinada área e, ao contrário do que muitas pessoas imaginam, utilizam essa verdade para ajudar e não para destruir, como comumente é veiculado nas mídias. Desde o início da década de 90, este termo tem sido utilizado na área tecnológica, mais precisamente na área da informática. Os Crackers, termo utilizado para designar aqueles indivíduos que também possuem um conhecimento elevado relacionado à tecnologia, mas que não a utilizam de maneira positiva, são os que invadem sistemas e promovem ações com a intenção de prejudicar os outros, como desconfigurar páginas ou promover invasões de PC´s (Computadores Pessoais) de usuários leigos.[...]

[4]O Sputnik-1 foi o primeiro satélite artificial, criado pelo Homem a entrar em órbita ao redor da Terra. Representou o início da corrida espacial pelo fato de que, com o seu lançamento, a URSS ameaçaria a hegemonia dos EUA. Para maiores informações a respeito do contexto histórico e de dados referentes ao referido satélite, acessar UNESP. **o Sputnik** . Disponível em: <http://www.feg.unesp.br/~orbital/ sputnik/capitulo-1.pdf>. Acesso em: 15 nov. 2015.

Nesse contexto, um grupo de pesquisadores do Departamento de Defesa dos EUA começou a trabalhar, no fim da década de 1960, no desenvolvimento da *Intergalatic Computer Network*, uma forma embrionária de internet com a função de proteger o território estadunidense (SANTOS,2011).

Com os investimentos do capital estatal e privado, teve origem a grande rede, que "passou a ser chamada de ARPANET, essa rede interconectava empresas privadas, universidades, centros de pesquisas e laboratórios, utilizando redes de pacotes de rádio." (PIRES,2012, p.3).

A partir do contexto histórico do surgimento da internet e do modo pelo qual a mesma começou a se estruturar, compreende-se a pertinência de seu estudo para o proposito deste trabalho. Tal pertinência deve-se ao fato de que o nascimento da internet está relacionado com a preocupação dos Estados em defenderem sua segurança e sua soberania.

2.2 Aspectos Conceituais

A internet consiste no acoplamento de computadores e equipamentos por meio da distribuição geográfica dos recursos de comunicação, que permite a troca de dados entre sistemas que otimiza os recursos de *hardware* e *software* (MORAIS; LIMA e FRANCO, 2012).

Sua importância justifica-se pelo fato de globalizar o escopo da informação, facilitar o salto quântico da mesma e distribuir o controle da administração por meio da descentralização de protocolos. Ao atuar desse modo, a internet gera novas instituições reguladoras, o que influencia mudanças na política (MUELLER,2010).

Nesse sentido, a internet influencia a geografia dos Estados nacionais, visto que dinamiza as relações comerciais, bem como altera o modo com o qual as pessoas se relacionam. Essa influência, no âmbito social, diz respeito à difusão cultural e, no âmbito econômico, à aceleração das transações comerciais e na importância econômica do seu tráfego de dados (SILVA,2008).

Outra explicação para a influência da internet sob a geografia dos Estados consiste no fato de que os nomes de domínio reforçam o controle geopolítico. Isso ocorre por meio do mapeamento geográfico dos servidores regionais interconectados no espaço (PIRES,2012).

Quanto ao seu funcionamento, a internet opera por meio de regras, conhecidas como protocolos. Os principais protocolos envolvidos são o IP (*Internet Protocol*), responsáveis pelo direcionamento da informação até o destinatário final, além do TCP (*Transmition Control Protocol*), mais antigo e menos seguro (PIRES,2012).

A criação do TCP/IP e do HTTP (*Hyper Text Transmition Protocol*) possibilitou, respectivamente, que aumentasse o número de conexões entre as redes, bem como a facilidade de navegação entre uma página e outra. Apesar de proporcionar maior dinamicidade na navegação, a facilidade de acesso possibilitou a ocorrência de vulnerabilidades (PIRES,2012).

As vulnerabilidades são combatidas pelo *firewall*, um elemento da rede que controla a passagem de pacotes de dados através dos limites de uma internet segura, impostos por uma política de segurança específica (AL-SHAER; HAMED,2004). Em outros termos, o firewall restringe o acesso de informações entre uma rede protegida e a internet (CHESWICK; BELLOVIN,2005).

A restrição à circulação de informações pela rede faz com que se reduzam as ocorrências de ameaças, que podem decorrer de vários modos de ataques. Esses, por sua vez, podem ser simples, de baixo ou de médio impacto; bem como sob a forma de Ameaças Persistentes Avançadas, cujo impacto é forte, permanente, recorrente e em larga escala, realizado por especialistas (PORTUGAL, 2013)

Dentre as ameaças que se propagam pelo ciberespaço[5], destacam-se o cibercrime, a ciberespionagem, o ciberterrorismo, a ciberguerra e, de uma forma mais controvertida, o hacktivismo (PIRES,2012). O cibercrime[6], caracteriza-se pelo dolo do agente, cuja qualificação intelectual o faz desejar praticar essa conduta; bem como pela transnacionalidade dos danos de pequeno valor que provoca, o que demanda cooperação internacional na investigação (MOORE; CLAYTON; ANDERSON, 2009).

Por ciberespionagem, compreende-se a ciência que captura em segredo as mensagens eletrônicas, escritas, além de outras formas de comunicações eletrônicas para reunir informações relevantes para o setor comercial e militar (HERSH,2010).

O exercício da ciberespionagem é uma ação clandestina praticada por agente que se faz passar por alguém tenha autorização para manusear as informações, que serão posteriormente transmiti-las à parte inimiga (TALLIM MANUAL,2013).

O ciberterrorismo, por seu turno, consiste na convergência entre o ciberespaço e o terrorismo. Faz referência a ataques ou ameaça de ataques ilegais a computadores, redes e às informações nelas contidas, quando feito para intimidar governos ou sua população a cumprirem seus objetivos sociais e políticos, de modo violento. (DEENING,2000).

---

[5]Ambiente artificial criado por meios informáticos (DRAE,2003).

[6]Na versão original: "Online crime,(..) will force big changes, both because its transnational and also because it consists of a high volume of low-value offenses."

A ciberguerra, por sua vez, é definida como o preparativo ou a condução de operações militares conforme os princípios da informação, de modo que se possa obter todas as informações sobre o adversário. Essas informações permitem, no contexto bélico, conhecer o inimigo e evitar gastos demasiados com ataques militares diretos (ARQUILLA e RONFELDT,1993).

Com relação à conceituação do hacktivismo, há uma polêmica muito forte em relação às atividades desempenhadas por seus praticantes. Em razão disso, é necessária muita cautela em sua abordagem, visto que, apesar de em muitos casos ser uma ameaça, em outros, pode ser enxergada como uma forma construtiva de desobediência civil diante do protecionismo comercial e das violações de direitos humanos (KRAPP,2005)[7].

As ameaças aqui apresentadas decorrem de problemas com os *firewalls*, bem como por causa de vulnerabilidades, erros de projeto, implementação, operação ou gestão de sistemas que comprometem a segurança do sistema, que ocorrem de formas variadas, o que torna difícil sua classificação, catalogação e combate (PORTUGAL,2013).

A partir da exposição de aspectos conceituais da internet, é possível compreender os aspectos técnicos discutidos dentro dos Fóruns de Governança da Internet. Essa compreensão é a base para a percepção da importância da soberania nas discussões sobre governança da internet.

2.3 Aapectos Políticos

Os aspectos políticos envolvidos na organização e na gestão da internet permitem compreender o modo com o qual a soberania estatal é redimensionada para a possibilidade de combate às ameaças provocadas pelos ciberataques. Desse modo, nesse tópico serão abordados a governança da internet e suas implicações políticas.

2.3.1 Governança

A definição do conceito do conceito de governança da internet ainda é muito complexo, uma vez que os termos que a compõem são muito abrangentes. A governança pode ser entendida como governo ou conjunto de políticas públicas destinado à regulamentação da

[7]De acordo com a versão original, tem-se: “Hacktivism can be a politically constructive form of civil desobedience or an anarchic gesture; it can signal anticapitalist protesto or comercial protectinism”.

internet, enquanto que a internet não abrange todas as tecnologias da informação (KURBALIJA; GELBSTEIN,2005).

Para os fins deste trabalho, considerar-se-á como governança da internet todo conjunto de atividades, apoiadas em objetivos comuns, realizadas por instituições governamentais (ROSENEAU,2000).

A partir dessa delimitação conceitual, é interessante mencionar as abordagens da governança da internet: a estreita, que diz respeito a estrutura física (nomes de domínio e IP[8]) e administrativa (regulada pela ICANN) da internet e a ampla, referente à legislação e assuntos sociais, políticos e econômicos abordados na Cúpula Mundial sobre a Sociedade da Informação (SILVA,2008).

A governança da internet, que se dá pelo controle da administração dos nomes de domínio, é atualmente responsabilidade do governo estadunidense, de forma unilateral. Esse controle do sistema de nomes de domínio, DNS[9], pelos Estados Unidos ocorre pela presença de 10 dos 13 servidores-raiz do mundo que distribui as informações entre os chamados servidores-raiz (PIRES,2012).

Esses, por sua vez, distribuem cópias correntes de zonas aos servidores e, dessa forma, facilitam a disponibilização para os clientes da internet (MOCKAPETRIS; DUNLAP,1988). Dentre eles, o mais importante é o VeriSign, que permite com que os EUA controlem os registros comerciais e consolide sua hegemonia cibernética (KRUGER,2016).

A detenção da hegemonia cibernética da aos EUA o poder de disseminar a sua ideologia política e, dessa forma, convencer outros atores internacionais a aderirem ao seu modelo de governança cibernética. Essa hegemonia se verifica na liderança exercida no combate aos ciberataques e dos cibercrimes que daqueles decorrem (PIRES,2012).

A consolidação da hegemonia estadunidense teve por base a criação, m 1992, da *Internet Society*, organização sem fins lucrativos que , sob o comando de Robert e Kahn, delegou a gestão dos protocolos e códigos de internet à recém-criada *Internet Assigned Nembers Authority* (IANA) (CASTELLS,2003).

---

[8]IP, ou Internet Protocol, tem como finalidade assegurar o correto endereçamento dos pacotes de dados a serem transportados de um computador para outro. Em outras palavras, o "IP é funcionalmente igual ao endereço/CEP no envelope"(DREZNER,2004,p.491).

[9]De acordo com o trabalho desenvolvido por Mueller (2010, p.8), "Um estudo da governança da internet proporciona uma oportunidade de observar como essas ideias são traduzidas em ação (ou não) no contexto político real e para avaliar se elas fornecem ou não alternativas viáveis". Na versão original: "A study of Internet governance provides an opportunity to observe how these ideas are translated into action (or not) in a real political context, and to assess whether they provide viable alternatives".

A IANA, na gestão de John Postel, foi responsável pelo crescimento da internet (GOLDSMITH,2006). Isso fez com que fosse reconhecido o seu caráter internacional. Diante dessa internacionalização, a administração dos nomes de domínio passou a ser negociada com a comunidade da internet (SILVA, 2008).

A partir do consenso negocial entre o governo estadunidense e a comunidade da internet, que consistiu no conjunto de estatutos conhecido como "White Paper", surgiu a *International Corporation for Assigned Names and Numbers* (ROBERTS, 2001). Atualmente, a ICANN estabelece a concorrência e representa as comunidades da internet ao coordenar as negociações da concessão dos nomes de domínio (KLEIN, 2002).

Sobre o controle dos Estados Unidos, a ICANN foi criticada por países como a China, a Índia e a Tunísia, que desejavam uma governança multilateral. Tais países sugeriram que a ITU, a União Internacional de Comunicações da ONU fosse o responsável pela gestão da rede. No entanto, essa sugestão tornou-se inviável pelo fato de que as agências da ONU não tem por objetivo ser uma autoridade gestora, mas apenas órgãos consultivos, de elaboração de documentos, com soluções a serem implantadas. (SILVA, 2008).

Diante disso, a ICANN enviou um relatório ao governo estadunidense, no qual argumentou que os objetivos estabelecidos foram cumpridos. Dessa forma, a entidade teria condições de se tornar um órgão autorregulado, o que evitaria embates jurídicos dentro dos Estados Unidos, provocados por boatos de que a ICANN seria influenciada pelos interesses divergentes das empresas que a financiam (SILVA, 2008).

Nesse sentido, a terceirização da administração do DNS[10] sofreu forte oposição da Internet Societ (ISOC), do setor empresarial e dos governos nacionais. A Internet Societ (ISOC) reivindicava o domínio público, o setor empresarial, a regulamentação comercial e dos direitos autorais, enquanto os governos nacionais preocupavam-se com a segurança de seus cidadãos e das suas informações estratégicas (PIRES, 2012).

A partir desse descontentamento, decorrente do enorme fluxo econômico promovido durante a concessão de nomes de domínio, surgiu um conflito pelo controle das informações da rede, motivado pela disputa do setor empresarial com os Estados, que aspiravam à segurança de seus cidadãos e às vantagens políticas e econômicas da administração da internet. A esse conflito deu-se o nome de Guerra do DNS[11] (PIRES, 2012).

---

[10]Conceito retirado de PIRES,Hindenburgo, vide nota de rodapé nº 9.

[11] DNS é o Domain Name System, ou Sistema de Nomes de Domínio é "um sistema hierárquico distribuído concebido para realizar a tradução de nomes para números necessária ao estabelecimento de conexões entre computadores ligados à internet." Ver mais em: http://ftp.unicamp.br/pub/apoio/treinamentos/tcpip/dns/dns.pdf.

A fim de combater os problemas que originaram a Guerra do DNS, foram elaboradas algumas alternativas contrahegemônicas de governança da internet. A primeira delas foi a iniciativa da ONU de constituir um sistema de zona raiz alternativo para a internet, que fosse independente da gestão estadunidense (PIRES, 2012).

Por fim, o estudo do modo como é feita a administração dos nomes de domínio permite compreender como o direito internacional poderá oferecer respostas aos dilemas da era cibernética. Em outras palavras, o entendimento das questões referentes à localização dos servidores-raiz e da importância de sua propriedade é importante para identificar os problemas e propor soluções, tal como é feito nos Fóruns de Governança da Internet.

2.3.2 O FGI e a Gestão da Internet

Em virtude da necessidade de resolução das questões polêmicas em torno da governança da internet, teve origem a Cúpula Mundial sobre a Sociedade da Informação (CSMI), sediada em Genebra e celebrada no ano de 2003. Essa por sua vez, estabelece, no artigo 13b do seu Plano de Ação, a participação ativa e conjunta dos governos com a sociedade civil e o setor privado para a promoção de política públicas (KURBALIJA; GELBSTEIN, 2005).

Dentro da CSMI, foi criado o Fórum sobre a Governança da Internet, em 2005, em virtude do surgimento de políticas conflitantes com a Governança da Internet (KURBALIJA; GELBSTEIN, 2005). Diante da complexidade das questões, foi necessária a criação de um segundo Fórum sobre a Governança da Internet.

A continuidade do FGI justifica-se pelo fato deste ser “uma plataforma de discurso democrático sobre questões difíceis e sensíveis a respeito da maneira pela qual a internet estava sendo dirigida e viria a ser dirigida” (ANG; PANG, 2012, p.47), uma vez que lida com conflitos de interesses de vários grupos da sociedade civil e estatais, bem como monitora a influência dos mesmos sobre os usuários (KURBALIJA; GELBSTEIN, 2005).

O referido fórum tenta superar as polêmicas do beneficiamento dos interesses de alguns grupos sobre os outros e sua respectiva influência sobre os usuários, ao lidar com questões técnicas e políticas, e sua respectiva influência sobre os usuários, são desafios a serem superados (SILVA, 2008).

O Fórum da Governança da Internet foi realizado pela primeira vez em Atenas, na Grécia, em 2003. Dentro dele, foram discutidos temas como spam, multilinguismo, censura,

cibercrimes, cibersegurança, questões de gênero, privacidade e proteção de dados, direitos humanos, etc (YODA, 2006).

A discussão dos temas norteou-se à preocupação com a infraestrutura lógica da rede, que permitiria a implementação das medidas discutidas no fórum. Diante das poucas oportunidades de participação conferidas à sociedade civil, bem como da dificuldade sentida por muitos Estados e de ter suas demandas acolhidas, verifica-se a falha do 1º FGI no que tange ao seu propósito de proporcionar diálogo para, a partir disso, expedir recomendações (SILVA, 2008)..

Diante do fracasso do 1º FGI, o secretariado da ONU propôs a criação de coalizões dinâmicas, grupos pluralistas, ou *multistakeholders*, formados por organizações da sociedade civil, representantes de governo, entidades acadêmicas e empresas, que tinham como finalidade debater e formular propostas de soluções para os problemas apresentados pela governança da internet (IGF FORUM, 2008).

As coalizões dinâmicas estiveram presentes no 2º Fórum da Governança da Internet, realizado em 2007, na cidade do Rio de Janeiro, RJ. Esse evento tratou de temas como o acesso, diversidade, recursos críticos, assuntos emergentes e, sobretudo a segurança. Dado o expressivo crescimento da internet o 2º FGI buscou o equilíbrio entre a proteção dos direitos humanos e a liberdade de expressão (SILVA, 2008).

Na discussão do tema de abertura, esteve presente a preocupação com a dualidade entre a liberdade democrática e o dever de controle do Estado. Dentro dessa preocupação, dialogou-se a respeito da necessidade de se buscar o equilíbrio entre liberdade de expressão, segurança e proteção da propriedade intelectual. (NIC, 2007).

Em seguida, o grupo coalizão que tratava sobre a diversidade, estabeleceu a importância da elaboração de conteúdos acessíveis a todos. Nesse sentido, uma atenção maior deverá ser dada às minorias linguísticas e à criação de políticas públicas que ofereçam conteúdos adequados aos grupos marginalizados (SILVA, 2008).

Também merecem destaque os grupos de coalizão sobre recursos críticos e o de segurança. O grupo de coalizão sobre recursos críticos discutiu a transferência da administração dos nomes de domínio para autoridade da comunidade mundial. Já o de segurança possibilitou a criação de redes de cooperação, sobretudo no que tange à diferença de legislações sobre privacidade e o combate ao crime organizado e às fraudes na internet (SILVA, 2008).

Os desafios enfrentados pelo FGI devem-se, sobretudo, a uma diversidade de questões que são originadas no seio do território dos Estados, mas que, em face da globalização, tornaram-se internacionais, por meio da internet. Todavia, o referido fórum ainda é uma

esperança de diálogo em questões cruciais pelo fato de que muitos Estados pretendem se utilizar da governança da internet para reduzir os custos com ajustes e mudanças legislativas (DREZNER, 2004)[12].

Por fim, cumprido o objetivo deste tópico de tratar sobre aspectos mais aprofundados sobre o Fórum da Governança da Internet, torna-se possível dissertar a respeito de como a soberania evoluiu para se adaptar à era cibernética.

[12] Versão original: "This reduces the adjustment costs of any requisite legislative or regulatory changes for governments, as well as the costs for national firms to adhere to a new standard."(DREZNER,2004, p.482)

3 INTERNET E A SOBERANIA NA LÓGICA DO DIREITO INTERNACIONAL

Este tópico tem como objetivo relatar a evolução histórica da soberania e do modo com o qual o direito internacional a aplica atualmente. Desse modo, será possível abordar os dilemas que os Estados enfrentam para combater os ciberataques.

3.1 Evolução e Aplicação Atual da Soberania

A inserção da discussão a respeito do conceito de soberania resulta da importÂncia da compreensão deste conceito basilar para a análise de como o Direito Internacional pode contribuir para a solução no combate aos ciberataques. Procurar-se-á, portanto, demonstrar que a soberania do Estado não necessariamente se enfraqueceu em decorrência dos problemas decorrentes do mal-uso da internet.

Na abordagem do conceito de soberania, destacaram-se Jean Bodin e Thomas Hobbes. Enquanto este definiu a soberania como monopólio da força de imposição de comportamento, aquele considerava que o Estado não poderia se submeter a outras normas. Ambas as definições buscavam delimitar o que de fato é a soberania. Dentro dessa definição, a soberania seria usada para atingir a paz e a ordem social interna e a igualdade entre Estados na ordem internacional (KOSKENNIEMI, 2006).

A ordem internacional, por sua vez, consiste em " um padrão de atividade que sustenta os objetivos elementares ou primários da sociedade dos estados, ou sociedade internacional. " (BULL,2002, p.13). Dessa forma, para haver equilíbrio na ordem internacional, a soberania estatal não deve ser agredida, mas redimensionada.

A partir da apresentação de conceitos basilares, afirma-se que:

> Nessa linha, afirma Rousseau que, para a teoria clássica do Direito Internacional, a soberania é o poder absoluto e incontrolável do Estado de agir (tanto nas questões internas como nas externas). Contudo, as doutrinas contemporâneas não admitem como válidas as concepções tradicionais de soberania absoluta e, baseadas nas realidades do mundo atual, consagraram o princípio da soberania como poder *limitado pelo direito* (PEREIRA,1999, p.627)

O aprofundamento da discussão a respeito da natureza da soberania ganhou destaque com o embate entre Hans Kelsen e Karl Schimitt. Nesse sentido:

> No sistema de Schmitt, a soberania é a descrição de uma questão de fato e a lei uma consequência normativa da mesma. Em Kelsen, a lei é normativa e a "soberania" apenas uma abreviação descritiva para os direitos" (KOSKENNIEMI, 2006, p.229).

A soberania apresenta outras definições: significando independência nas relações interestatais, sendo o direito da pessoa ou Estado exercê-la dentro do território, sem interferência de outros Estados (KOSKENNIEMI, 2006); dizendo respeito à independência do país em relação a qualquer poder externo (político, econômico e jurídico) que limite sua autonomia externamente (MIRANDA, 2004).

Com a globalização, o enorme fluxo de informações tornou-se "um desafio significativo para o exercício da soberania dos Estados no contexto internacional" (MIRANDA,2004, p.89) , uma vez que o Estado passou a não deter o controle sobre a influência cultural exercida sobre seu povo.

Isso porque a desconstrução da relevância das fronteiras estatais, que se manifestou, *inter* alia, por meio da internet, fez com que o Estado soberano fosse redimensionado perante os dilemas existentes na sociedade internacional contemporânea, que demandam cooperação. Essa, por sua vez, provê caminhos para mitigar os conflitos e reconhece elementos da dinâmica interestatal que fundamentam as relações internacionais (MIRANDA, 2004).

É nesse sentido que o redimensionamento do Estado soberano frente ao Direito Internacional permite ao Estado continuar sendo a base para as decisões no Direito Internacional, fortalecendo-se. Isso significa que, no caso dos ciberataques, a cooperação interestatal e com outros Estados e com a sociedade civil se apresente como a principal alternativa viável e concreta no cenário atual.

3.2 Dilemas e Abordagens

Neste tópico serão abordados os problemas causados pelos ciberataques aos Estados. Estes, por sua vez, têm de rever a forma de exercício de sua soberania, para que seja possível a realização de um combate mais eficiente às ameaças cibernéticas. A justificativa para isso é a ineficácia das ações estatais de combate aos ciberataques, em especial aos cibercrimes. Isso faz com que a cooperação seja necessária.

3.2.1 Combate aos Ciberataques

Enquanto a segurança, a nível militar, sempre fora um tema de extrema relevância no cenário internacional, a nível virtual, enquanto cibersegurança, ganhou destaque após a globalização. A justificativa reside na necessidade de proteção dos dados confidenciais de órgãos governamentais, organizações e também de cidadãos comuns diante da ação dos *hackers*[13].

As ações dos crackers muitas vezes não recebem a devida punição por conta da falta de tipificação de grande parte de seus atos. Com a Convenção de Budapeste, no entanto, este cenário começou a se modificar, pelo fato de seu preâmbulo tipificar os crimes dentro do direito penal material e enfatizar os aspectos de direito processual (SOUZA; PEREIRA, 2009).

Desse modo, torna-se possível criar "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente através da adoção de uma legislação adequada" (CONVENÇÂO SOBRE O CIBERCRIME, 2001).

Sob o aspecto processual, a Convenção de Budapeste estabelece condições para a sua aplicação, bem como ressalvas para os casos em que forem necessárias. Além disso, estabelece também a interceptação dos dados investigados, bem como seu recolhimento em tempo real e sua busca e apreensão (SOUZA; PEREIRA, 2009).

A Convenção de Budapeste não é o único modo adotado pelo direito internacional para combater os ciberataques. A partir da dificuldade encontrada por grande parte dos Estados para regulamentar os ciberataques, houve a necessidade de que os chefes de governo pensassem em outra alternativa: a cooperação internacional em cibersegurança.

3.2.2 Ações Unilaterais

Dentre os exemplos de ações unilaterais tentadas, temos a Alemanha, membro da OTAN, que sofreu invasões em seus sites governamentais por *crackers* em decorrência do apoio concedido à Ucrânia em 2015. Para responder a esses ataques, o governo alemão montou um ciber-exército, no qual 76 soldados especializados investigavam possíveis ciberterroristas (PORTUGAL, 2013).

[13]Na verdade, os indivíduos responsáveis por essas ações criminosas são *crackers*, pois os *hackers* são pessoas conhecedoras de informática, que são capazes de diagnosticar e solucionar problemas de computadores, softwares e rede (JORGE, 2011).

A França foi alvo de ciberataques, como a invasão de sites institucionais e da Assembleia Nacional, que ficaram inacessíveis, em represália à adoção de uma lei que visava reprimir a contestação de genocídios, tal como o armênio. Em função disso, e de outros ciberataques sofridos depois de presidir a União Europeia, foi criada a *l'Agence Nationale de la securité des systèmes d'information*, responsável pela prevenção, detecção e reação aos ataques informáticos.(SÉNAT, 2012).[14]

O Reino Unido definiu, em novembro de 2011, uma Estratégia de Cibersegurança, para combater o cibercrime e tornar o Reino Unido mais resistente aos ciberataques. Durante quatro anos, o programa britânico de cibersegurança recebeu 755 milhões de euros. Vale ressaltar que, diante da transnacionalidade das ameaças digitais, o governo conta com a colaboração interna da iniciativa privada e, a nível externo, recorre à cooperação internacional (REINO UNIDO,2011).

A partir disso, diante do caráter globalizado da internet, que impôs aos Estados dificuldades para responder à velocidade da evolução tecnologia e da limitação estatal para impor sua competência territorial (MUELLER, 2010), tornou-se necessária a criação de políticas de cooperação em matéria de cibersegurança.

A justificativa para essa premissa é que a Governança da Internet[15] traduz a forma com a qual os Estados se relacionam. Logo, uma política de cooperação em cibersegurança, realizada pela iniciativa estatal, permite reafirmar sua soberania na era cibernética globalizada (MUELLER, 2010).

3.2.3 Política de Ciberdefesa da OTAN

Diante dos riscos inerentes à segurança de seus países membros por conta do ciberataques, a OTAN começou a formular a sua Política de Ciberdefesa, que contou com um plano de ação para melhor implementá-la. Objetivo desta política é de integrar os sistemas de defesa, ao centralizar as redes, para facilitar a comunicação entre os sistemas e, dessa forma, facilitar o recebimento de diagnósticos de vulnerabilidades.

---

[14]Relatório a respeito das atividades de ciberdefesa, desenvolvido pelo senado francês, vide SÉNAT. França. **Rapport d' information.** Disponível em:<https://www.senat.fr/rap/r11-681/r11-6811.pdf>. Acesso em:20 dez. 2016. Na versão original: "Les prerrogatives de l' ANSSI recouvrent les capacités em matiére de prévention, l' ANSSI, de detection et de réactionaux ataques informatiques."(SÉNAT,2012).

[15] PIRES, Hindenburgo. **Estados Nacionais, Soberania e Regulação da Internet.** Revista Electrónica de Geografia y CienciasSociales. Barcelona,2012. Disponível em: <http://www.ub.edu/geocrit/sn/sn-418/sn-418-63.htm>. Acesso em 02/09/2015.

A política de ciberdefesa da OTAN consiste num instrumento de cooperação que, por meio do NCIRC, proporciona aos seus membros um treinamento especializado em Direito e informática. Nesse treinamento, são fornecidos equipamentos de análise de vulnerabilidades, além de assistência jurídica por meio da investigação ou atualização normativa, que facilitam a detecção de vulnerabilidades (PORTUGAL, 2013).

A estrutura de comunicação dessa política de ciberdefesa possibilita aos membros da OTAN a vigilância e comunicação das vulnerabilidades pelo NCIRC. Este, por sua vez, possibilita a implantação das ações da NCSA (*NATO Communication andInformation Service Association*), responsável pela comunicação com os *Computer Emergency Computer Readiness Team* (CERT), que prima por adotar estratégias de combate às ameaças à cibersegurança (CERT, 2017) dos países membros (PORTUGAL, 2013).

A partir das ações desempenhadas pela OTAN em matéria de cibersegurança, é notável a limitação do Estado para resolver esse problema internamente. Dessa forma, o combate por meio da cooperação entre os Estados soberanos, embora limitado, ainda apresenta-se como o caminho mais concreto para o combate aos ciberataques, dada a fragilidade de estrutura tecnológica e legislativa da maioria dos Estados para enfrentar o problema.

3.3 Outras Opções de Cooperação

As ações conjuntas de combate aos ciberataques atualmente mostram-se mais eficazes em relação às ações isoladas. Além da política de ciberdefesa da OTAN, existem também a União Europeia (EU), a Organização das Nações Unidas (ONU), que reforçam a tese defendida neste trabalho.

3.3.1 União Europeia (UE)

O desenvolvimento de ação conjunta contra os ciberataques na União Europeia, iniciou-se com o relatório sobre a implantação da Estratégia de Segurança Europeia[16], no ano

[16]De acordo com o Secretário Geral da União Europeia à época de sua elaboração, a Estratégica Econômica Europeia, "foi adoptada em Dezembro de 2003, tornou-se um marco no desenvolvimento da política externa e de segurança da União Europeia". Essas palavras se justificam diante dos feitos desse plano de ação comum que conseguiu focalizar as principais ameaças. No relatório elaborado em 2008, estabeleceu propostas de melhoramentos dessas ações. Mais informações em: <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568PTC.pdf>.

de 2008. Tal providência decorreu de a União Europeia encarar o ciberespaço como espaço vital para a promoção de direitos humanos (CONSELHO DA EUROPA, 2009).

Para a promoção do combate às ameaças cibernéticas, além da Convenção de Budapeste, a União Europeia também age por meio do *European Cybercrime Center* (EC3)[17], que realiza o levantamento sobre a análise da capacidade investigativa e processual. (PIRES,2012).

A União Europeia também dispõe da *European Network and Information Security Agency* (ENISA), especializada em segurança da informação. Essa agência atua na elaboração de respostas coordenadas entre os membros da União Europeia. Para isso, elabora relatórios coordenadas entre os membros da União Europeia e de mapeamentos das capacidades operacionais dos chamados *Computer Emergency Response Teams (CERT)*[18]de todos os membros (MILITÃO,2014).

A realização do mapeamento permite à União Europeia incentivar investimentos na capacitação de CERT's. Esses investimentos, por sua vez, visam eliminar as barreiras impostas pelo financiamento alternativo envolvendo a indústria e a sociedade civil. Dessa forma torna-se possível integrar a proteção do ciberespaço (PIRES,2012).

Para que a integração seja possível, a União Europeia desenvolve uma política de cibersegurança baseada no modelo da OTAN. Por meio deste, o vínculo entre a ciberdefesa e as operações militares é estabelecido por meio da Política Comum de Segurança e Defesa (*Common Security and Defense Policy*) (PIRES,2012).

Visando aprimorar sua ciberdefesa, a União Europeia atualizou, no ano de 2011, o Plano de Desenvolvimento das Capacidades, que colocou a cibersegurança como o 5º domínio operacional das atividades militares. Os resultados do plano em questão são avaliados pelo Grupo de Projeto em Ciberdefesa, responsável por fiscalizar o desenvolvimento das capacidades de ciberdefesa. (PORTUGAL,2013).

---

[17]O Centro de Cibercrime Europeu, ou European Cybercrime Centre, na tradução em inglês, foi criado em 2013 para reforçar a aplicabilidade e a efetividade das normas que regulam o cibercrime, protegendo cidadãos, governos e a economia. Situado na Europol, esse centro de combate ao cibercrime é capaz de ampliar as capacidades analíticas e de operações dos sistemas europeus. Atua como um centro de informações, coordenando investigações criminais e as respectivas operações, além de oferecer apoio técnico-digital forense. Para maiores informações, vide site da Europol: https://www.europol.europa.eu/ec3.

[18]Os CERT, ou Computer Emergency Response Teams, consistem em equipes de profissionais especializados em monitorar as possíveis ameaças aos sistemas de computadores, bem como elaborar estratégias para o combate às mesmas. O principal CERT do mundo é o dos Estados Unidos. Este funciona por meio de operações realizadas 24 horas todos os dias. Essas operações envolvem também ações conjuntas com os CERT de outros países.

A partir da fiscalização, são possíveis a coordenação e a unificação das ações de desenvolvimento de capacidades, o que permite o compartilhamento das estratégias de defesa. Também torna possível a realização das campanhas de sensibilização.

3.3.2 ONU

Em razão dos danos proporcionados pela ação dos crackers[19] hacktivistas[20], cibercriminosos[21] e ciberterroristas[22] aos países membros da ONU, a proteção às tecnologias de informação e comunicação foi incluído na agenda da Assembleia Geral das Nações Unidas.

Da preocupação com as tecnologias da informação decorreram 5 resoluções: a A/RES/53/61, que pretende proteger a liberdade do fluxo de informação da utilização criminosa da internet; a A/RES/56/121, propõe cooperação legislativa e política; a A/RES/57/239, visa a uma cultura global de cibersegurança, a A/RES/64/211 pretende desenvolver a integração da infraestrutura crítica e A/RES/58/199 promove a cooperação e coordenação em cibersegurança a nível mundial (KAHONA,2009).

A resolução A/RES/58/199[23] teve por particularidade dar a missão de promover a cooperação entre as estruturas das tecnologias de informação à União Internacional das Comunicações (UIT). A UIT já havia recebido um mandato da ONU para implementar as suas resoluções, principalmente no que tange à cibersegurança (UIT,2008).

---

[19]KOHONA,P.T.B. **The United NationsTreatyon The Internet.** The American Journal of International Law, Vol.92,No 1,Jan.2009, p.140-148. Disponível em:<http://www.jstore.org/stable/2998074>. Acesso em: 31/05/2016. Além de ter participação ativa nas políticas de cooperação em cibersegurança, a Organização das Nações Unidas (ONU) também presidiu a celebração de vários tratados sobre a internet, ao ponto de criar uma verdadeira compilação digital, com a finalidade de facilitar a difusão do conhecimento de suas premissas, facilitando sua aplicabilidade.

[20]Praticantes do hacktivismo.

[21]Praticantes dos delitos pela internet.

[22] Uma proposta de definição do conceito de ciberterrorismo é feita por Martínez (2009, p.119): "... é a forma de terrorismo que utiliza as tecnologias da informação para intimidar, coercionar ou para causar danos a grupos sociais com fins político-religiosos.", ou, nos termos originais, "... es la forma de terrorismo que utiliza las tecnologias de informacíon para intimidar, coercionar o para causar daños a grupos sociales com fines políticos-religiosos.".

[23]A (UIT, 2016) afirma que a *World Summit of Information Society*, foi estabelecida para colocar a proteção global da cibersegurança na agenda da ONU, principalmente pelo fato do acesso à informação auxiliar no desenvolvimento do padrão de vida de milhões de pessoas pelo mundo e por facilitar a resolução de conflitos. Para isso, a WSIS, como é conhecida, foi instituída em duas fases. A primeira delas foi realizada em Genebra em 2013 e a segunda, em 2015, em Tunis. A WSIS recomendou que as discussões fossem feitas no Prepcom, um comitê preparatório intergovernamental, responsável pela definição da agenda, das modalidades de participação e dos princípios e do plano de ação.

A preocupação da ONU com a cibersegurança escancara a incapacidade de o Estado promover ações individuais de proteção de seu ciberespaço. A explicação se encontra no fato de que somente organizações como a ONU possuírem a infraestrutura necessária para a proteção dos Estados (PIRES,2012).

A partir dos exemplos de cooperação em matéria de cibersegurança, é possível afirmar que, com a dificuldade de combater os ciberataques isoladamente, os Estados podem cooperar entre si. A cooperação, contudo, não apresenta-se como uma superação da dinâmica de estados soberanos, mas , ao contrário, coloca-se como reafirmação da lógica interestatal, na sua compreensão contemporânea que, embora flexibilize a atuação em redes (CASTELLS,2007) e busque o devido cumprimento dos princípios de direito internacional, mantem os Estados como principais agentes e controladores do modelo de gestão e regulação do tema.

4 CONCLUSÕES

Da preocupação com o desenvolvimento de um meio de comunicação eficiente e seguro em meio aos conflitos bélicos, a internet surgiu, de modo rudimentar, em meio à Guerra Fria (1946-1989). Nesse período, Estados Unidos e União Soviética disputavam a hegemonia política, econômica e militar do planeta.

Com o início da atual fase da globalização, as relações políticas, econômicas e comerciais se dinamizaram. Como a internet começou a receber investimentos diversos, sua expansão foi rápida. A partir da criação do HTTP e da World Wide Web, a internet passou a atrair a atenção dos chefes de Estado e do setor empresarial, que passaram a disputar o controle dos servidores raiz, que administram os Nomes de Domínio (DNS), resultando na Guerra do DNS.

Para a resolução das polêmicas em torno da Guerra do DNS, começou-se a discutir, nos Fóruns sobre a Governança da Internet (FGI) o melhor modo de governança da internet. Isso porque o modelo unilateral gerido pelos Estados Unidos, deu-lhe um imperialismo digital com a sede de 10 dos 13 dos servidores de zona raiz em seu território, mas mostrou-se ineficiente para o combate aos ciberataques.

Depois da governança da internet ter sido discorrida, seus aspectos conceituais foram elucidados as questões relativas aos cibercrimes. Dentro dessa discussão, constatou-se que ainda há muitos Estados que não dispõem de estrutura tecnológica e legislativa para combater os ciberataques e os crimes deles decorrentes, de modo que a cooperação em cibersegurança mostrou-se mais viável.

O fortalecimento da soberania se justifica pelo fato do Estado ainda poder recorrer às suas prerrogativas de decisão, por meio da adesão a legislações internacionais como a Convenção de Budapeste. A participação em políticas de cooperação em cibersegurança, tal como a executada pela OTAN, é baseada numa rede de proteção centralizada, responsável pela promoção de assistência recíproca que permite a comunicação e a tomada de ações conjuntas.

Embora os dilemas oriundos da internet desafiem as premissas da soberania estatal, as propostas de combate a estes problemas ainda encontram-se inseridas na lógica interestatal. As propostas, portanto, reafirmam as premissas da soberania contemporânea (subjugada ao direito internacional), colocando-se sobre a forma de cooperação e inseridas no escopo de atuação das organizações internacionais tradicionais. Os dilemas são novos e inéditos, as respostas são tradicionais. Os limites do Direito Internacional são conhecidos e sua aplicabilidade mais concreta perpassa pela ideia dos Estados enquanto principais sujeitos (passivos e ativos). Diante

deste inimigo que não obedece parâmetros estatais, a cooperação internacional coloca-se, ao mesmo tempo, como a única alternativa concreta de combate e como resposta significativamente limitada para a complexidade dos problemas apresentados.

REFERÊNCIAS BIBLIOGRÁFICAS

AL-SHAER, E.; HAMED, H. **Firewall policy advisor for anomaly Discovery androgenizing**. Integrated Network Management, 2003.

ANG, P. H.; PANG, N. **Globalização da Internet, Soberania ou Democracia:** o Trilema do Fórum de Governança da Internet. Revista de Direito, Estado e Telecomunicações, v.6, n.1, p.45-62. Brasília, 2013. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/globalizacao_da_internet_soberania_ou_democracia.pdf>. Acesso em: 15 out. 2015.

ARQUILLA, J; RONFELDT, D. **Cyberwariscoming!** Santa Mônica: Rand Corporation. 1993. Disponível em: <http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf>. Acesso em: 18 dez. 2016.

AMERICAN SOCIETY OF LAW. **United States Supports World Information Summit Outcome on Internet Governance.** The American Journal of Law. v.100, n.1, p.227-229. 2006. Disponível em: <http://www.jstor.org/stable/3518849>. Acesso em: 13 jun. 2016.

BULL, Hedley.**A sociedade anárquica.** São Paulo: Imprensa Oficial do Estado. Editora Universidade de Brasília. Instituto de Pesquisa de Relações Internacionais. 2002.

CASTRO, T. **Teoria das Relações Internacionais.** Brasília: FUNAG, 2012. Disponível em:<http://funag.gov.br/loja/download/931-Teoria_das_Relacoes_Internacionais.pdf>. Acesso em: 05 fev.2016.

CASTELLS, M. **Fim do Milênio**. 4.ed. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v.3) in.: SOUZA, G.L.M.; PEREIRA, D.V. A Convenção de Budapeste e as Leis Brasileiras. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/a_convencao_de_budapeste_e_as_leis_brasileiras.pdf>. Acesso em: 26 set. 2015.

CERF, Vinton G.; KAHN, Robert E. **A protocol for pocket network intercommunication**. Princeton: Princeton University Press, v.22, n.5, Mai/1974. Disponível em: <https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf>. Acesso em: 20 set. 2016.

CERT. **About us**. Disponível em: <http://www.cert.org>. Acesso em: 29 jul. 2017.

CHESWICK, W. R; BELOVIN, S.M; RUBIN, A.D. **Firewalls e segurança na Internet:** repelindo o hacker ardiloso. 2.ed. Porto Alegre: Bookman, 2005.

CONSELHO DA UNIÃO EUROPEIA. **Estratégia Europeia em Matéria de Segurança** Uma Europa Segura num Mundo Melhor. Bruxelas, 2009. Disponível em: <www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568PTC.pdf>. Acesso em: 02. set 2015.

DENNING,D. **Cyberterrorism:** Testimony Before the Special Oversight Panel on Terrorism Commitee on Armed Service. U.S House of Representatives. Disponível em:

<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>. Acesso em: 10 dez. 2016.

DREZNER, D. W. **The Global Governance of the Internet:** How the State Back. The Academy of Political Science. Political Science Quarterly, v.119, n.3, p. 477-498, 2004. Disponível em: <http://www.jstor.org/stable/20202392>. Acesso em: 20 mai. 2016.

FILHO, G.L.M. **Hackers e Crackers na internet:** as duas faces da moeda. Revista Eletrônica Temática, ano.VI, n.1, Jan/2010.

GOLDSMITH, J. L., WUN, Tim. **Who Controls the Internet?** Illusion of a Borderless World. NewYork: Oxford University Press, 2006.

HERSH, S. M. **The Online Treat:** Should we be worried about a cyberwar? 2010. Disponível em: <http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all>. Acesso em: 24 dez. 2016.

IGF. Disponível em: <http://governanca.cgi.br>. Acesso em: 08 jun. 2017.

KLEIN, H. **ICANN and Internet Governation:** Leveraging Technical Coordination to Realize Global Public Policy. Atlanta: School of Public Policy, Georgia Institute of Technology, 2002. Disponível em:<http://indiana.edu/~tisj/readers/full-text/18-3%20Klein.pdf>. Acesso em: 5 dez. 2016.

KURBALIJA, J; GELBSTEIN, E. **Governança da Internet:** Questões, Atores e Cisões. Diplo Foundation, 2005. Disponível em: <https://www.diplomacy.edu/sites/default/files/IG-Portuguese-1st.pdf>. Acessoem: 26 set. 2016.

KOHONA, P.T.B. **The United Nations Treaty on The Internet.** The American Journal of International Law, v.92, n.1, p.140-148. Jan/2009. Disponível em: <http://www.jstore.org/stable/2998074>. Acesso em: 31 mai.2016.

KOSKENNIEMI, M. **From Apology to Utopia:** The Structure of International Legal Argument. Cambridge. 2006.

KRAPP, P. **Terror and Play, or What Was the Hacktivism?** The MIT Press, n.21, p.70-93, 2005. Disponível em: <http://www.jstore.org/stable/20442704>. Acesso em: 28 jun.2016.

KRUGER, L.G. **The Future of Internet Governance:** Should the United States Relinquish Its Authority over ICANN? Congressional Research Service. Disponível em: <https://fas.org/sgp/crs/misc/R44022.pdf>. Acesso em: 20 dez. 2016.

MARQUES FILHO, G.L. **Hackers e Crackers na internet:** as duas faces da moeda. Revista Eletrônica Temática, ano.VI, n.1, Jan/2010. Disponível em: <http://www.insite.pro.br/2010/janeiro/hackers_crackers_internet.pdf>. Acesso em: 06 fev. 2015.

MARTÍNES, R.O. **Ciberterrorismo.** Conferência ditada em la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Carabobo. Carabobo: Revista Relacíon Criminológica, n.21,

2009. Disponível em: <http://servicio.bc.uc.edu.ve/derecho/revista/relcrim21/art06.pdf>. Acesso em: 27 mai. 2016.

MOORE, T; CLAYTON, R.; ANDERSON, R. **The Economics of Online Crime.** American Economic Association. The Journal of Economic Perspectives, v.23, n.3, p.3-20, 2009. Disponível em: <http://www.jstor.org/stable/20202392>.Acesso em: 08 jun. 2016.

MORAIS, C.T.D; LIMA, J.V; FRANCO, S.R.K. **Conceitos sobre internet e web.** Porto Alegre: Editor da UFRGS, p.13, 2012.

MUELLER, M.L. **The Global Politics of Internet Governance.** Cambridge: The MIT Press. Massachusetts Institute of Technology, p.1-271, 2010. Disponível em: <http://pages.uoregon.edu/koopman/courses_readings/phil123-net/intro/mueller_networks-and-states.pdf>. Acesso em: 26 set. 2016.

MILITÃO, O.P. **Guerra da Informação:** a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional. 2014. 89 p. Dissertação (Mestrado em Ciência Política e Relações Internacionais). Universidade de Nova Lisboa. Faculdade de Ciências Sociais e Humanas. Lisboa. 2014.

MIRANDA, N. **Globalização, Soberania Nacional e Direito Internacional.** Brasília: R. CEJ, n.27, Out-Dez/.2004.

MOCKAPETRIS, P.V.; DUNLAP, K.J. **Developmentofthe Domain Name System.** Computer Communication Review, v.18, n.4, p.123-133, Ago/1988. Disponível em: <http://www.cs.cornell.edu/courses/cs615/2002fa/615/mockapetris.pdf>. Acesso em: 21 dez. 2016

GETSCKO, Demi. **Queremos interferência mínima e autonomia**. 2005. Disponível em: <http://www.nic.br/imprensa/clipping/2005/entrevista13.htm>. Acesso em: 08 jun. 2017.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. Disponível em: <http://www.nato.int/cps/en/natolive/topics_67656.htm>. Acesso em: 22 set. 2015.

PEREIRA, A. C. A. **Soberania e Pós-Modernidade**. O Brasil e os Novos Desafios do Direito Internacional. Rio de Janeiro: Forense, 2004.

PIRES, H.F. **Estados Nacionais, Soberania e Regulação da Internet.** Barcelona: Revista Eletrônica de Geografia y CienciasSociales, v.XVI, n.418, Nov/2012. Disponível em: <http://www.ub.edu/geocrit/coloquio2012/actas/12-H-Pires.pdf>. Acesso em: 26 set. 2016.

PINHO, J. B. **Publicidade e vendas na internet.** Técnicas e estratégias. 1.ed. São Paulo: Summus Editorial, p.354, 2000.

PORTUGAL. Instituto de Defesa Nacional. **Estratégia da Informação e Segurança no Ciberespaço.** Lisboa, 2013. Disponível em: <http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf>. Acesso em: 26 set. 2016.

REINO UNIDO. Cabbinet Office. **The UK Cyber Security Strategy:** Protecting and Promoting the UK in a digital world. London, 2011. Disponível em:

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>. Acesso em: 10 dez. 2016.

ROSENAU, James. **Governança, ordem e transformação na política mundial**. Brasília/São Paulo: Editora UNB/Imprensa Oficial do Estado, 2000.

ROBERTS, M. **ICANN´s "Unelected" Crisis**. Circled: The Internet Infrastructure. Set/ 2011. Disponível em: <http://www.circleid.com/posts/20110905_icanns_unelected_crisis/>. Acesso em: 18 dez. 2016.

SANTOS, J.L.A. **Contributos para uma melhor governação da cibersegurança em Portugal.** Lisboa. 2011. 127 p. Dissertação (Mestrado em Direito e Segurança). Universidade Nova de Lisboa. Faculdade de Direito. 2011.

SÉNAT. França. **Rapport d' information.** Disponível em: <https://www.senat.fr/rap/r11-681/r11-6811.pdf>. Acesso em: 20 dez. 2016.

SCHMITT, M.N. **Tallinn Manual on The International Law Applicable to Cyber Warfare.** New York: Cambridge University Press, 2013. Disponível em: <https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf>. Acesso em: 18 dez. 2016.

UIT. **World Summit on the Inf ormation Society**. Disponível em: <http://www.itu.int/net/wsis/basic/why.html>. Acesso em: 18 dez. 2016.

UNESP. **O Sputnik**. Disponível em: <http://www.feg.unesp.br/~orbital/sputnik/capitulo-1.pdf>. Acesso em: 15 nov. 2015.

YODA, Carlos Gustavo. **Governança Global da Internet:** Fórum cede a pressões e gerenciamento da rede fica fora da pauta. Agência Carta Maior Nov/2016. Disponível em: <http://www.cultura.gov.br/foruns_de_cultura/cultura_digital/na_midia/index.php?p=20516&more=1&c=1&pb=1>. Acesso em: 10 jun. 2017.