UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
CURSO DE RELAÇÕES INTERNACIONAIS

PAULO CÉSAR GOMES DE SOUZA SOBRINHO

A SEGURANÇA CIBERNÉTICA: UMA ABORDAGEM SECURITIZADORA E A ASCENSÃO DE UM REGIME INTERNACIONAL

JOÃO PESSOA
2017

PAULO CÉSAR GOMES DE SOUZA SOBRINHO

A SEGURANÇA CIBERNÉTICA: UMA ABORDAGEM SECURITIZADORA E A ASCENSÃO DE UM REGIME INTERNACIONAL

Trabalho de Conclusão de apresentado ao Programa de Graduação em Relações Internacionais da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais.

Área de concentração: Política Externa.

Orientadora: Prof. Dr. Cristina Pacheco.

JOÃO PESSOA
2017

S677s Souza Sobrinho, Paulo César Gomes de
A segurança cibernética [manuscrito] : uma abordagem securitizadora e a ascensão de um regime internacional / Paulo Cesar Gomes de Souza Sobrinho. - 2017.
67 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2017.
"Orientação: Profa. Dra. Cristina Carvalho Pacheco, Departamento de Relações Internacionais".

1. Segurança cibernética. 2. Organizações internacionais. 3. Regimes internacionais. I. Título.

21. ed. CDD 341.2

PAULO CÉSAR GOMES DE SOUZA SOBRINHO

A SEGURANÇA CIBERNÉTICA: UMA ABORDAGEM SECURITIZADORA E A ASCENSÃO DE UM REGIME INTERNACIONAL

Monografia apresentada ao Curso de Relações Internacionais da Universidade Estadual da Paraíba.

Aprovado(a) em 19 / 08 / 2017.

Cristina Carvalho Pacheco /UEPB
Orientador(a)

Fábio Rodrigo Ferreira Nobre/UEPB
Examinador(a)

Jeane da Silva Freitas /UEPB
Examinador(a)

Aos meus pais, Rozimar e Luiz por todo
o esforço imprescindível, DEDICO.

AGRADECIMENTOS

Primeiramente, agradeço a Deus, por estar presente em toda a minha vida e me dar suporte para concluir mais um ciclo, me auxiliando nos momentos mais difíceis.

Aos meus pais, Rozimar da Conceição e Luiz Carlos, pelo apoio incondicional e incentivo para começar e continuar essa jornada.

Aos meus irmãos, Carla Águida e Carlos Felipe, que sempre me incentivaram, me apoiaram e estavam ao meu lado, mesmo distantes fisicamente.

Aos meus familiares por toda a ajuda, carinho e dedicação fornecidos a mim no decorrer destes anos. Obrigado a minha madrinha Rosimary pelas palavras doces, minha tia Ana Paula pelos conselhos e meu padrinho Antônio por toda a ajuda.

Também agradeço de forma especial à Amanda Oliveira que me deu muito suporte, à Dona Socorro e sua irmã Valdenora que tornaram possível minha estadia em João Pessoa.

Aos meus amigos, que se tornaram minha família nesse tempo. Palavras não expressam a gratidão por todas as experiências vividas juntos.

Agradeço de forma especial à Amanda Arruda, Ana Cristina, Andresa Carrilho, Cassielly de Oliveira, Chris Alves, Késsio Lemos, Matheus Montenegro e Mayane de Araujo por todos os sorrisos, as lágrimas, as palavras de motivação e os conselhos, meu muito obrigado.

Agradeço também a Dignata Jr, por ter desenvolvido habilidades em mim tão importantes e ter possibilitado encontrar pessoas tão especiais, como Karina Oliveira e Mayara Clemente, obrigado por terem compartilhado experiências tão enriquecedoras e uma amizade tão solene.

A todo o corpo docente do curso de Relações Internacionais da UEPB, por sua dedicação diária na transmissão do conhecimento.

A Professora Cristina Pacheco, por seus direcionamentos, paciência, e conhecimentos compartilhados.

Em conclusão, a todos que estiveram presentes neste ciclo da minha vida, a minha eterna gratidão.

RESUMO

A segurança cibernética vem alcançando um foco maior com o passar dos anos no campo da política e do setor militar, encontrando-se em diversas decisões dos atores da sociedade internacional, tais como o Estado e as Organizações Internacionais (OI's). A necessidade de alianças e cooperação fez-se presente ao crescente número de eventos e conferências internacionais destinados ao debate do tema. Sendo assim, este trabalho propõe a identificar, num primeiro momento a utilização da securitização para a segurança cibernética através de 1) discurso, 2) políticas e 3) práticas, ressaltando os termos encontrados e a sua utilização em discursos. Para alcançar este objetivo, uma análise histórica da formação da Organização das Nações Unidas e do *Internet Governance Forum* e da ascensão da segurança cibernética nestes dois meios. Ao fim, delineia-se a construção de um regime internacional e as etapas já realizadas acerca do espaço cibernético e como os atores interagem sobre o tema. As considerações levantadas ao final, apontam para o a visibilidade que as alianças e parcerias tomam ao decorrer dos anos e acontecimentos pelo mundo, propiciando um ambiente conveniente para as discussões e debates acerca do tema somando as visões dos diferentes atores, como o Estado, OI's e o setor privado.

Palavras-Chave: Segurança cibernética, Organizações Internacionais, Regimes Internacionais.

ABSTRACT

Cybersecurity has been acquiring a greater focus over the years in the field of politics and the military sector, where occurs to been found in various decisions by actors in international society, such as the State and International Organizations (IOs). The need for alliances and cooperation was reflected in the growing number of international events and conferences for the discussion of the topic. Thus, this paper proposes to identify, at first, the use of securitization for cybersecurity through 1) discourse, 2) policies and 3) practices, highlighting the terms found and used in speeches. To achieve this goal, a historical analysis of the formation of the United Nations and the Internet Governance Forum and the rise of cybersecurity in these two actors. Finally, it outlines the construction of an international regime and the steps already taken on cyber space and how the actors interact on the subject. The considerations at the end point to the visibility that the alliances and partnerships take over the years and events around the world, providing a convenient environment for the discussions and debates about the theme, adding the visions of the different actors, such as the State, IO's and the private sector.

Keywords: Cybersecurity, International Organizations, International Regimes.

LISTA DE ABREVIATURAS E SIGLAS

AGNU	Assembleia Geral
ASEAN	Associação de Nações do Sudeste Asiático
CGI.br	Comitê Gestor da Internet no Brasil
CNCI	*Comprehensive National Cybersecurity Initiative*
DdD	Departamento de Defesa
EUA	Estados Unidos da América
FNISA	Rede Francesa e Agência de Segurança de Informação
GFCE	Forum Global em Cyber Especialidade
GGE	Grupo de Peritos Governamentais
IEC	Infraestruturas Criticas
IGF	Fórum da Governança da Internet
ITU	*International Telecommunications Union*
NETmundial	Encontro Multisetorial Global Sobre o Futuro da Governança da Internet
NSA	Agência de Segurança Nacional
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
QDR	*Quadrennial Defense Review*
TIC's	Tecnologias das Informações e Comunicações
WGIG	Grupo de Trabalho para a Governança da Internet
WSIS	Cúpula Mundial da Sociedade da Informação

SUMÁRIO

1 INTRODUÇÃO

A segurança cibernética é tratada em diversos eixos da política internacional. Faz parte das estratégias, políticas e operações no espaço cibernético, o que inclui uma gama de contenção de ameaças para garantir a estabilidade e a segurança universal. Neste trabalho é realizado uma análise da teoria de securitização, em que se pretende explanar o termo de origem e como está inserida nas políticas e tomadas de decisões governamentais de forma a relacionar a segurança cibernética como sendo fruto de um processo de securitização; além de exemplificar como a segurança cibernética encontra-se presente nos discursos de autoridades políticas e preocupações internacionais sendo elucidadas através das ações da Organização das Nações Unidas (ONU) e do Fórum da Governança da Internet (IGF); e por fim, explorar a dimensão de regimes internacionais e como a segurança cibernética esta intrínseca nas alianças internacionais resultando num trabalho conjunto de uma construção de complexo de normas.

As estratégias e a segurança do Estado tornam-se objeto de estudo das Relações Internacionais por constituírem um alguns dos temas basilares desde a criação dos Estados nacionais. As questões de segurança nacional e internacional encontram-se presentes nas prioridades dos governos, assim como o processo de formulação de estratégia, seja política, militar ou de segurança também, marcado por várias gerações de estudos das relações internacionais.

O estabelecimento da informação, comunicação e conhecimento tornou aqueles elementos essenciais para as decisões dos Estados, garantindo àqueles que as realizam bem, um crescente proveito no entendimento e tomadas de decisão tanto no âmbito nacional quanto internacional. O espaço cibernético é marcado por não existir fronteiras físicas, dando uma dimensão drástica de espaço que perpassa pelos outros domínios, como o terrestre, marítimo, aéreo. Com a evolução da tecnologia cibernética, a possibilidade de vários benefícios é conquistada, porém riscos à segurança conectam-se a este crescimento, o que não afeta apenas o Estado, mas atinge também outros atores da sociedade internacional. (HOLDORF, 2015)

As nações dependem gradativamente da informação e da tecnologia, as empresas dependem de computadores e diversos processos de negócios que estão ligados à Internet. O setor militar, por sua vez, utiliza armas que são controladas à distância em decorrência

do avanço tecnológico. Nesta dependência cada vez maior da tecnologia da informação, a segurança cibernética deixou de ser considerada um problema de computadores, e passou a ser considerada como uma política dos Estados e organizações. (MULLIGAN, SCHNEIDER. 2011) Discursos, conferências, estratégias nacionais são exemplos de meios dos quais a segurança cibernética se tornou um resultado da.

O espaço cibernético é um ambiente interconectado que propicia vários benefícios para as nações, empresas e indivíduos. Dessa forma, a segurança cibernética requer que governos, companhias privadas e organizações não governamentais trabalhem juntos para entender as ameaças oriundas do espaço cibernético e trabalhar o compartilhamento de informação e capacidades para que seja possível conter essas ameaças. (BUTLER, LACHOW. 2012)

Esta monografia tem como proposta analisar como se deu a utilização e adaptabilidade da securitização para a segurança cibernética com o avanço tecnológico, num primeiro momento, para, em seguida, verificar como organizações internacionais, com foco na ONU, posicionaram-se ao elaborar resoluções aos Estados membros de forma à inserir as preocupações internacionais na pauta global em busca de consensos. A última etapa pretende, analisar os regimes internacionais e como os países reagruparam para debater e realizar medidas acerca da segurança cibernética

Desta forma, o método de análise utilizado para este trabalho é o qualitativo, resultante da captação de informação coletada a partir de *papers, journals,* livros e documentos oficiais dos governos e organizações que tratam sobre o tema. O mesmo é construído a partir da abordagem indutiva, pois intenta em qualificar a segurança cibernética através de uma abordagem dos pontos centrais utilizados no meio político, sendo dividida em três momentos:

O primeiro capítulo, apresenta o conceito de securitização e, uma vez que esse conceito se desenvolve através do discurso, é realizada a classificação de termos utilizados no movimento de securitização na área cibernética, ressaltando também as formas que uma securitização bem sucedida está baseada em três etapas: 1) identificação, 2) ação e 3) efeitos. O passo seguinte consiste, ainda neste capítulo, em apresentar a estrutura da securitização e a sua aderência ao tema.

No segundo capítulo dois atores importantes para a segurança cibernética, A Organização das Nações Unidas (ONU) e o *Internet Governance Forum* (IGF). O

primeiro propõe resoluções e trabalha em consenso com seus Estados membros de forma a trabalhar o compartilhamento de informação de ameaças e capacidades entre si de modo a resultar em uma rede complexa de sugestões para o convívio internacional em paz. Assim, o seguinte é um fórum internacional que reúne atores governamentais, do setor privado, organizações e indivíduos para a discussão de tendências e preocupações que atingem os vários setores da sociedade para um trabalho em conjunto.

O último capítulo trabalha a definição de regimes internacionais e fatores subcorrentes para a resolução de dilemas do cenário internacional, para isso é necessário o trabalho cooperativo de todos os atores que incorporam o tema. Por isso, é exemplificado os atores mais recorrentes do espaço cibernético que tem o seu foco na segurança cibernética e as ações realizadas para o conhecimento e o trabalho da área através de conceitos, temas, ameaças e capacidades, tais como o Estado, a Organização do Tratado do Atlântico Norte (OTAN) e o Conselho Europeu.

2 TEORIA DA SECURITIZAÇÃO E A CIBERSEGURANÇA

A teoria de Securitização defende a existência um conjunto de regras linguísticas gramaticais que tanto caracterizam e mobilizam o campo de segurança, e podem incluir, por exemplo, o uso de expressões como "inimigo", "ameaça", "necessidade" e "emergência"[1]. Da mesma forma, a teoria da securitização sustenta que existem fatores empíricos estruturais, que limitam ou definem as estratégias securitizadoras e as opções disponíveis para os atores. Sendo assim, a teoria da securitização aceita fundamentalmente a linguagem conceitual e as suposições, estruturais institucionais da tradição de segurança clássica.[2]

Um ator securitizante é alguém, ou um grupo, que executa o discurso de segurança. Geralmente são líderes políticos, burocratas, governos e grupos de influência. O Estado tem regras explícitas sobre quem pode representa-lo, então quando um governo afirma que "nós precisamos defender nossa segurança nacional", trata-se de uma emergência de um problema que requer solução imediata. Não existe uma regra formal de representação para as Nações ou para o sistema internacional; consequentemente, o problema de legitimação é maior nessas áreas do que quando um dos atores é o Estado[3].

Myriam Dunn Cavelty[4], chefe da Unidade de Pesquisa em Novos Riscos (*New Risks Research Unit – Center for Security Studies*) da Universidade de Zurique, desenvolveu uma lista com palavras-chave que foram detectadas como movimento de securitização na área cibernética.

Tabela 1 – Palavras-chave para Ciberameaça

Threat framing keywords (for cyber-threats)
• Computer (-based) attack
• Computer intrusion
• Critical information infrastructures
• Critical infrastructures
• Cyber-attack

[1] TAURECK, Rita. 2006.
[2] WILLIAMS, Michael C. 2003.
[3] BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. 1998.
[4] Cyber-Security and Threat Politics (2008):38.

• Cyber-security
• Cyber-terrorism
• Cyber-threat
• Cyber-vulnerability
• Cyber-war(fare)
• Electronic Pearl Harbor
• Information operations
• Information warfare
• National security (in connection with information security, etc.)
• Vulnerabilities of information infrastructure

Fonte: Cyber-Security and Threat Politics - CAVELTY (2008)

A partir desta lista, tem-se palavras que se tornaram presentes nos discursos daqueles que realizam a securitização, no caso, os chefes de Estado, e para esta pesquisa, deve-se entender alguns conceitos, tais como: "cibersegurança ou segurança cibernética", "Ciberameaça" e "segurança nacional" e "Infraestruturas Críticas da Informação".

2.1 Cibersegurança ou Segurança Cibernética

Esta é uma definição ampla, por isso toma-se como exemplo o que foi delimitado no *Cyberspace Policy Review* (2009), que faz parte da *(Comprehensive National Cybersecurity Initiative - CNCI),* uma ação nacional com estratégias e implementações para assegurar o ciberespaço, que especifica

> Segurança cibernética inclui estratégias, políticas e normas relativas à segurança das operações no ciberespaço, e que englobam uma gama de redução de ameaças e vulnerabilidades, a dissuasão, engajamento internacional, resposta a incidentes, resiliência e políticas de recuperação; além de atividades, incluindo as operações de rede de computadores, garantia à informação, aplicação da lei, missões de inteligência, diplomáticas, ou militares, e como elas se relacionam com a segurança e a estabilidade da infraestrutura de informação e comunicação global. (COUNCIL on FOREIGN RELATIONS, 2009)

Para tanto, com a criação de políticas e estratégias para o espaço cibernético, o Estado desenvolve a perspectiva de proteção contra certas ameaças[5], que estão surgindo com o decorrer dos anos, e que preocupam os chefes de Estado.

[5] "Cybersecurity problems involves highly scalable, difficult to trace actions and distributed actors and attacks that easily cross national borders, which often exceeds the capabilities of national approaches to Internet Governance." MUELLER, 2010.

2.2 Ciberameaça

Desde a década de 1990 questões sobre as ameaças no campo cibernético têm sido colocadas em pauta, porém somente em 2008 o Presidente George W lançou a *Comprehensive National Cybersecurity Initiative – CNCI*, que caracterizou as ameaças cibernéticas como as que "produzem resultados indesejáveis, que podem incluir a intrusão não autorizada", seja para obter acesso aos computadores ou sistema e ver dados protegidos, como "roubar ou manipular informações contidas em base de dados" assim como são consideradas ameaças aqueles susceptíveis à "ataques aos dispositivos de telecomunicações, seja para danificar dados ou proporcionar a operação irregular dos componentes de infraestrutura"[6].

2.3 Segurança nacional

Não existe uma definição exata do que seja segurança ou uma visão teórica amplamente usada nas Relações Internacionais que defina e utilize o conceito de segurança nacional para todos os moldes. Para Nye[7], a maioria das políticas de segurança são desenhadas para garantir a autonomia social como um grupo, num patamar de *status* político, não se limitando à sobrevivência física dos indivíduos na fronteira do Estado. Haftendorn[8] afirma que as variações regionais do conceito de segurança podem ser explicados pelas prioridades nacionais específicas, e que o resultado das estratégias de segurança, são fatores determinantes pela cultura e geografia. Porém a maioria dos pesquisadores utiliza o paradigma nacional de segurança Hobbesiano, e na sua orientação normativa, o objetivo da segurança nacional é a sobrevivência[9].

2.4 Infraestruturas Críticas da Informação ou Infraestruturas Digitais

Por Infraestruturas Criticas (IEC) entende-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade[10]. Como exemplo, o governo brasileiro, considera que a infraestrutura crítica da informação

---

[6] WHITE HOUSE, 2008.
[7] Problems of Security Studies. 1988 p.6.
[8] The Security Puzzle: Theory-Building and Discipline-Building in International Security. 1991 p.4.
[9] HAFTENDORN, 1991.
[10] CANONGIA, C.; MANDARINO JR., R; GONÇALVES JR., A. 2010

é o "subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade"[11].

Vistos alguns conceitos importantes para o estudo de segurança, o passo seguinte consiste em exemplificar como a securitização está presente no meio internacional e a forma em que ela se conecta com a segurança cibernética.

A securitização pode ser vista como uma versão mais extrema da politização. Para Buzan e Waever (1998), uma exata definição de securitização é constituída pelo estabelecimento intersubjetivo de uma ameaça existencial com importância suficiente para efeitos políticos substanciais. Para evitar que 'tudo' se torne uma questão de segurança, uma securitização bem sucedida consiste em três etapas. Estas são: 1) identificação de ameaças existenciais; 2) ação de emergência; e 3) efeitos (práticas) sobre as relações entre unidades, quebrando as regras.[12]

2.5 Discursos

A maneira de estudar securitização é analisando discursos e arranjos políticos. Williams (1978) explica, em conceituação de Buzan e Wæver, que um dos passos para um ato de discurso bem sucedido é estruturar pelas capacidades dos atores (sua posição, autoridade, habilidade comunicativa, poder de persuasão, recursos, etc.) e posteriormente, pelos "fatores empíricos ou situações em que estes agentes podem fazer referência". Segurança é uma construção social e intersubjetiva [13].

O discurso do ex-presidente George W. Bush em 2001, pós ataques no World Trade Center, teve um posicionamento forte para medidas domesticas com um foco no externo.

> "We will come together to give law enforcement the additional tools it needs to track down terror here at home. We will come together to strengthen our intelligence capabilities to know the plans of terrorists before they act and to find them before they strike." (BUSH, 2001b)

Como um de suas primeiras medidas, numa manhã de outubro de 2001, o presidente Bush faz uma transmissão pela televisão para os cidadãos estadunidenses. O assunto abordado era a assinatura da USA PATRIOT ACT *2001*. Bush declarou que assinou essa nova lei, de forma a permitir a vigilância de todos os meios de comunicação, resultando na

[11] CANONGIA, C.; MANDARINO JR., R. 2009
[12] BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. 1998.
[13] NEAL, Andrew W. 1978.

identificação dos terroristas. Essa medida, para ele, proporcionaria melhores condições para enfrentar os desafios causados pela expansão dos meios de comunicação[14].

Com o aumento da preocupação acerca da segurança cibernética, a urgência em relação ao assunto, despertou o interesse dos *policy makers* e do público em geral quando, pouco tempo depois do *9/11*, em 2003, o presidente Bush lançou uma declaração autoritária e abrangente sobre a política da segurança cibernética estadunidense, o *The National Strategy to Secure Cyberspace*, no qual introduz com a seguinte afirmação: "nos últimos anos, as ameaças no ciberespaço aumentaram dramaticamente." (THE WHITE HOUSE, 2003: III) Apesar de um ataque cibernético não ter ocorrido nessa época, não era o momento de ser "muito otimista", porque as "ferramentas de ataque são amplamente disponíveis, assim como a capacidade técnica e sofisticação dos usuários propensos a causar estragos ou rupturas cresce" (HANSEN, L; NISSENBAUM, H. 2009: 1161).

Ao tomar como exemplo os discursos do governo pós *9/11*, que intercalaram entre a legitimação da vigilância digital e a busca de informações através da securitização referente à Guerra ao Terror, em contra ponto com grupos de cidadãos que lutam contra essa legislação em busca dos liberdade civil básica e questões relacionadas à privacidade, percebe-se que o caso da segurança cibernética é um link entre redes e o indivíduo e à sociedade. Não se trata de um caso em que o discurso de segurança privada constitui o indivíduo como o objetivo final, mas sim utiliza o indivíduo num discurso que o correlaciona com objetivos sociais e políticos[15].

Embora as eleições presidenciais tenham ocorrido apenas em novembro de 2008 Barack Obama, em julho do mesmo ano, Obama fez um discurso na Universidade de Purdue onde ele já apresentava três prioridades que modelariam seu governo uma vez eleito - ameaças nucleares, biológicas e do ciberespaço[16]. Já na presidência dos Estados Unidos da América (EUA), assumida em janeiro de 2009, Obama manteve o campo cibernético na agenda nacional, estabelecido pelo seu antecessor, Bush, responsável por ter começado a dar os primeiros passos na segurança cibernética[17]. Outra razão da

[14] Bush, 2001c
[15] HANSEN, L; NISSENBAUM, H. 2009.
[16] Obama, 2008
[17] Ver mais em: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

manutenção da agenda foi a necessidade de desenvolver uma proteção à economia estadunidense e aos cidadãos[18].

No primeiro semestre do mandato do ex-presidente Barack Obama, em 29 de maio de 2009, um pronunciamento teve o intuito de destacar a situação da "segurança das infraestruturas cibernéticas da nação"[19]. Na abertura do discurso na inauguração do escritório da segurança cibernética na Casa Branca, Obama ressaltava a importância do assunto quando afirma que "o ciberespaço é real, assim são os riscos que vem com ele [...] as mesmas tecnologias que nos capacitam para criar e construir, também fortalecem aqueles que buscam perturbar e destruir"[20]. Ele ainda aponta que "a nossa vantagem tecnológica é a chave para o domínio militar dos Estados Unidos; no entanto nossas redes militares e de defesa estão sob ataque constante"[21].

> Por todas essas razões, essa ameaça nos é clara, e é um dos desafios de segurança nacional e econômica mais graves que enfrentamos como nação […] Hoje estou lançando um relatório, e posso garantir que minha administração perseguirá uma nova abordagem abrangente para garantir a infraestrutura digital da América. Essa nova abordagem começa do topo, firmando um compromisso meu: a partir de agora, nossa infraestrutura digital – as redes de computadores dos quais dependemos todos os dias – será tratada como deveria ser, um ativo nacional estratégico. Vamos garantir que essas redes sejam seguras, confiáveis e resistentes. Vamos dissuadir, prevenir, detectar e se defender contra ataques, e nos recuperar rapidamente de quaisquer interrupções ou danos. (WHITE HOUSE, 2009, tradução livre).

A partir das afirmações, nota-se que os Estados Unidos estavam prontos para levar o campo cibernético para um patamar que atinge o âmbito nacional e econômico, posicionando a segurança cibernética no conjunto de estratégias do país, afim de assegurar sua soberania e liderança. Ao expandir as responsabilidades deste mandato, Obama direciona o comprometimento para a sua administração, e consequentemente, para outros atores presentes e responsáveis em auxilia-lo no movimento de elevar a segurança cibernética ao mesmo patamar da segurança nuclear. O objeto são os EUA, e durante o ato do discurso a preocupação é voltada para as ameaças à infraestrutura digital, que movem esse objeto para o campo da securitização.

---

[18] Ver mais em: https://www.whitehouse.gov/video/President-Obama-on-Cybersecurity#transcript
[19] THE WHITE HOUSE, 2009.
[20] *So cyberspace is real. And so are the risks that come with it [...] the very technologies that empower us to create and to build also empower those who would disrupt and destroy.* (OBAMA, 2009)
[21] *Our technological advantage is a key to America's military dominance, but our defense and military networks are under constant attack.*(*Idem)*

2.6 Política

A utilização da securitização está longe de ser uma opção para todas as unidades de segurança e as suas respectivas ameaças. Entretanto, esta medida governamental é amplamente baseada em poder e capacidade, e com isso, os significados para o social e político constroem uma ameaça. Desta forma, o estudo da segurança permanece amplo, mas com restrições a "quem" pode securitiza-la não é nem incontrolável nem incoerente.[22]

Na prática, a abertura para realizar a securitização é restringida por condições limitantes: a da estrutura do próprio ato de fala, e sua relação com a posição social do "agente de securitização" e a relação entre esse ator e o público a ser tratado. Para Buzan, Waever e Wilde (1998), as condições para um ato de discurso devem se encaixar em duas categorias: (1) a interna, a gramática linguística, que segue as regras do ato de discurso e (2) a externa, que é o contexto e o social, que correlaciona a posição de onde o ato pode ser feito[23].

Balzacq (2005) afirma que a securitização é melhor compreendida como uma prática estratégica (pragmática) que ocorre dentro e como parte de uma configuração de circunstâncias, incluindo o contexto, a disposição psicocultural do público, e o poder de quem faz o discurso para quem o ouve através das suas interações, no caso, a segunda categoria feita por Buzan.[24]

Enquanto a Escola de Copenhagen insiste em que o conceito de segurança modifica o contexto em virtude de uma aplicação bem-sucedida das regras constitutivas de um ato de fala, Balzacq sugere, que para conquistar uma audiência, as declarações de segurança devem estar relacionadas à uma realidade externa[25].

Pela primeira vez, desde 1997, o tema do ciberespaço foi mencionado no *Quadrennial Defense Review (QDR).* O QDR foi lançado em 2010 e é uma avaliação de estratégia que perpassar pelos tópicos de defesa, força, armas e operações que tinha por objetivos: rever as capacidades das Forças Armadas Americanas para prevenção das guerras atuais e para orientar uma reforma nas Instituições de departamento[26]. Para as

[22] BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. 1998.
[23] Williams apud Buzan, Wæver and Wilde, 1978
[24] BALZACQ, T. 2005
[25] Idem.
[26] DAGGETT, 2010

defesas no ciberespaço, o Departamento de Defesa (DdD) deveria fortalecer alguns recursos no ciberespaço, tais como:

> "Desenvolver uma abordagem mais abrangente para as operações do DdD no ciberespaço;
> Desenvolver um maior conhecimento e consciência sobre o ciberespaço
> Centralizar o comando das operações cibernéticas; e
> Melhorar as parcerias com outras agências e governos." (Quadrennial Defense Review Report, 2010. Tradução livre)

Ainda não se obteve êxito quanto ao reconhecimento entre os países de que a segurança cibernética é também um grande instrumento de poder, como também falta uma compreensão da melhor forma de utiliza-lo, quais interesses deve-se proteger, como barrar o seu uso pelos outros e as regras para os Estados. A característica "sem fronteiras" do espaço cibernético restringe uma criação de políticas e também de uma legalização. Uma das formas de organizar a infraestrutura do ciberespaço é através dos *policy makers* compreenderem não somente como as outras nações vêem a segurança cibernética, mas também as suas capacidades e intenções[27].

Para tanto, em maio de 2011, os Estados Unidos lançaram a "*International Strategy for Cyberspace"*, sendo este o primeiro documento político que promove normas internacionais. O objetivo consistia em

> "...trabalhar internacionalmente para promover uma aberta, interoperacional, segura e confiável estrutura de informação e comunicação que de suporte aos acordos internacionais e o comercio, fortaleça a segurança internacional e a promoção da liberdade de expressão e inovação." (INTERNATIONAL STRATEGY FOR CYBERSPACE, 2011. Tradução livre)

Essa estratégia foi desenhada para mostrar de que forma os Estados Unidos representa-se internacionalmente pelo ciberespaço e como pretende construir a prosperidade, aumentar a segurança e proteger-se de um mundo que está incessantemente conectado em rede, que perpassa pela diplomacia, defesa e desenvolvimento. Inclusive neste documento, os EUA garantem que haverá aplicação de leis para o campo cibernético, através de políticas para o crime cibernético[28].

[27] VISNER, 2013.
[28] SCHMIDT, 2011.

2.7 Práticas

Da mesma forma, Buzan, Waever e Wilde (1998) sustentam: "O que é essencial (à securitização) é a designação de uma ameaça existencial que exige ação de emergência ou medidas especiais e a aceitação dessa designação por um público significativo". Quanto às "medidas especiais" usualmente envolvem dobrar regras de governança de um Estado, e serem levantadas como questões de segurança nacional – mesmo que temporariamente - fora dos limites do procedimento político[29].

O Departamento de Defesa (DdD) dos Estados Unidos lançou um documento em julho de 2011, com cinco iniciativas de estratégia para o ciberespaço, chamado *Strategy for Operating in Cyberspace.* A primeira delas visava trabalhar com o ciberespaço de forma a considera-lo um domínio operacional para organizar, treinar e equipar de forma que o DdD tivesse um proveito potencial do campo. A segunda tratava de utilizar novos conceitos operacionais de defesa para proteger as redes e sistemas da DdD[30].

A terceira iniciativa se estendia em fazer parcerias com os outros departamentos dos EUA e as agências de modo que permitisse uma estratégia de segurança cibernética em conjunto com o governo. A quarta iniciativa intenta em construir relações sólidas com os aliados dos EUA para reforçar a segurança cibernética coletiva. Por fim, a quinta iniciativa destinava-se a alavancar a nação através da força de trabalho cibernética, assim como uma rápida inovação tecnológica[31].

Com essas iniciativas e estratégias, os Estados Unidos viam um futuro a ser estudado e decodificado. Através de normas, os EUA combinariam diplomacia, defesa e desenvolvimento para aumentar a prosperidade, segurança e liberdade, interconectando tudo para o uso benéfico da tecnologia. No século XX os EUA instauraram uma estrutura de pós guerra na economia internacional e cooperação para segurança; para o século XXI o trabalho para realizar a paz e um ciberespaço confiável no mesmo espirito de cooperação e responsabilidade coletiva[32].

---

[29] NISSENBAUM, H. 2005
[30] DEPARTMENT OF DEFENSE, 2011.
[31] DEPARTAMENT OD DEFENSE, 2011
[32] Ver mais em: <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

Para a segurança nacional de um país, quando reconhecem ameaças e fazem movimentos para securitiza-las, como por exemplo, ameaças on-line, exige respostas extraordinárias. O discurso de segurança não só aumenta a importância e a prioridade das ameaças designadas, mas também confere legitimidade a um determinado intervalo de reações, sejam elas no âmbito interno, como no externo[33].

Em teoria, esse movimento é uma opção a qualquer unidade, porque uma vez que um ator convenceu um público (relações entre unidades) da sua necessidade legítima de ir além de regras e normas, se constitui um caso de securitização. Um discurso que toma forma na apresentação de algo como uma ameaça existencial para algum objeto em referencial, não significa que ali há a securitização, acontece um movimento de securitização[34]

A utilização do conceito de "segurança" num discurso obriga o público a perceber o que está acontecendo seja no âmbito doméstico ou internacional, para identificar as condições (as ameaças presumidas) que justificam a articulação do discurso securitizante. Em outras palavras, o contexto "seleciona" ou ativa certas propriedades do conceito, enquanto outros estão escondidos[35].

Os eventos de 11 de setembro puseram uma atenção maior aos computadores, à tecnologia da informação e à segurança cibernética, principalmente com as questões relacionadas à proteção da infraestrutura digital, a vigilância eletrônica, *hackers* terroristas e a Internet como uma plataforma utilizada para comunicações entre Estados e contra eles[36].

A segurança doméstica não se restringe somente ao nacional, seja em seus aspectos ou em sua análise de dados, assim como as diferentes necessidades de segurança nacional dos outros Estados podem sem divergentes, causando desconfiança. A digitalização cria grandes volumes de dados recolhidos em escala transnacional, perdendo o sentido das fronteiras nacionais, bem como as limiar entre a aplicação da lei e a inteligência.

---

[33] Idem.
[34] TAURECK, Rita. 2006
[35] NISSENBAUM, H. 2005
[36] BALZACQ, T apud Latham. 2005

No jornal *The Guardian* foi publicado em junho de 2013 uma série de artigos revelando que o governo americano, através da Agência de Segurança Nacional (NSA), detêm acesso direto à provedores de serviços na internet, dentre eles, toma destaque a Microsoft, as redes sociais Facebook, Skype, YouTube e os sites de pesquisa Google, AOL e Yahoo. Através da NSA, o governo estadunidense reunia os mais variados dados de civis, desde a digitação, histórico de pesquisa, conteúdos de e-mail e chats online[37]

A revelações feitas por Edward Snowden não apenas trouxeram à tona os programas da NSA, mas também demonstraram que a Internet não é um lugar democrático e seguro. O modelo multisetorial e a Governança da Internet foram colocados em cheque. A privacidade e a soberania foram quebradas pela justificativa de combate ao terrorismo e estados inimigos[38].

Uma das estratégias para a coleta de dados do programa estadunidense era a coalizão com outros governos. O mais poderoso no âmbito da vigilância era o grupo dos Cinco Olhos, formado EUA, Canadá, Nova Zelândia, Austrália e Reino Unido possui a característica de que os EUA espionam junto com esses países, porem só fazem espionagem entre eles quando solicitado pelas autoridades dos próprios países parceiros[39].

Normalmente essas espionagens constituem-se em coleta de todos os dados ou espionagem econômica, e reúnem dados de comércio e da economia para obter vantagens para a indústria estadunidense[40]. As práticas de vigilância em larga escala, realizadas pela NSA e os seus parceiros, devem, portanto, ser compreendidas não como breves casos midiáticos, mas como fatores de uma transformação maior que afeta o modo de funcionamento dos limites de segurança nacional.

Visto alguns conceitos importantes para categorizar a segurança cibernética na securitização, o passo seguinte consiste em afirmar a importância do tema e a sua abrangência no campo internacional, seja contida por ameaças ou limites técnicos.

No desenvolvimento da estrutura de securitização, Buzan e Waever (1998) estavam mais preocupados na construção do conceito do que na garantia de que quando

[37] GREENWALD, MACASKILL; 2013
[38] Idem.
[39] GREENWALD; 2014
[40] GREENWALD; 2014

a securitização é legitimada ou garantida. Porém, Nissenbaum (2005) sustenta que, deve-se "começar a descobrir o quão terríveis, iminentes e quais são as ameaças. Assim como, deve-se questionar a adequação das medidas propostas e a sua proporcionalidade às ameaças."[41]

Crucialmente, as ameaças à segurança cibernética não surgem apenas de agentes (geralmente) intencionais, mas também de ameaças sistêmicas. Ameaças surgem de software, bem como falhas de hardware e não pode ser corrigido através do aperfeiçoamento de tecnologia digital e programação. Sendo assim, existe uma insegurança característica nos sistemas de computadores, que há abertura para ataques pelo constante desenvolvimento da tecnologia[42].

No contexto da segurança cibernética, a razão para a dificuldade desse tema, é que os técnicos peritos em segurança (cientistas e engenheiros da computação) buscam nas vulnerabilidades técnicas as possibilidades para o ataque e o dano, ao invés de ter um quadro mais completo das probabilidades e a incidência geral do dano a ser analisado[43].

Como observa Helen Nissenbaum (2005), a maioria dos cientistas da computação adotam um discurso técnico que se concentra no desenvolvimento de bons programas com um número limitado de bugs e sistemas (sérios) que são difíceis de penetrar por atacantes externos. Por isso, a problemática envolvida na segurança cibernética não se resume aos problemas técnicos, tendo um viés mais abrangente[44].

A securitização das redes não pode, nem deve parar na rede, deve-se entender as implicações das falhas de rede para outros objetos, como a sociedade, o regime ou a economia, que torna a securitização cibernética uma alternativa para atenção política. A característica multidisciplinar da securitização participa de uma articulação que relaciona os objetos do discurso, bem como as potenciais instabilidades em cada discurso e na situação e, no caso da segurança cibernética, relaciona as redes com o indivíduo e os problemas da sociedade[45].

[41] NISSENBAUM, H. 2005
[42] BALZACQ, T. 2005
[43] NISSENBAUM, H. 2005
[44] NISSENBAUM, H. 2005
[45] HANSEN, L; NISSENBAUM, H. 2009

3 O DESENVOLVIMENTO DA SEGURANÇA CIBERNÉTICA PELA ONU E O IGF

A governança é um termo abrangente, não se limita ao governo estatal. Em termos empíricos, o conceito de governança – relacionada diretamente ou não ao papel do Estado – diz respeito aos arranjos sociais distintos e às diferentes escalas, em que a responsabilidade de governar pode estar nas mão de diferentes atores sociais, considerando o fato de que o processo de governança pode ser hierárquico ou horizontalizado. Os arranjos sociais são medidas com fins variáveis e atendem a interesses diversos, relacionados a pratica política.[46]

A Internet por si só é uma plataforma tecnológica em que as outras tecnologias comunicacionais (principalmente a telefonia) convergem progressivamente, o que a coloca como uma rede de redes distribuída globalmente[47] A governança da internet é um termo definido pelo relatório da ONU "*Report of the Working Group on the Internet Governance*" como o "desenvolvimento e a aplicação, por governos, pelo setor privado e pela sociedade civil – em seus respectivos papeis – de princípios, normas, regras e procedimentos de tomada de decisão, bem como de programas, que devem determinar a evolução e o uso da Internet". (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2005.)

Este mesmo relatório listou os papeis e as responsabilidades de cada um dos atores (*stakeholders*) considerados reconhecidamente envolvidos no processo – seja o governo, o setor privado, a sociedade civil e as organizações internacionais – pertinentes aos dilemas da governança da Internet. Cada grupo tem interesses diferentes, papeis e participação, em que alguns casos, podem convergir. [48]

Esses fatores são relevantes para entender a relação dos atores apresentados a seguir e a sua influência na governança da internet. Para tanto, esta pesquisa utilizou-se de atores de cunho internacional que possuem uma relação direta, porém não específica, com a internet.

[46] CANABARRO, 2014.
[47] Idem.
[48] ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2005.

3.1 A Organização das Nações Unidas e a Segurança Cibernética

A Organização das Nações Unidas está baseada no princípio da igualdade soberana de todos os membros, voltados a garantir os compromissos da Carta das Nações Unidas, elaborada pelos representantes presentes na Conferência sobre Organização Internacional em 1945[49].

Para o funcionamento pleno desta Organização Internacional, foi estabelecido pela Carta das Nações Unidas, seis órgãos para atender os múltiplos mandatos, eles são: Assembleia Geral, Conselho de Segurança, Conselho Econômico e Social, Conselho de Tutela, Corte Internacional de Justiça e Secretariado[50].

Para esta pesquisa, foi escolhida a utilização da Assembleia Geral (AGNU) e suas resoluções, uma vez que possuem como principais funções de "Examinar e fazer recomendações sobre os princípios da cooperação internacional para a manutenção da paz e da segurança, inclusive os princípios que regem o desarmamento e a regulamentação dos armamentos" assim como "Discutir quaisquer questões que afetem a paz e a segurança", uma vez que questões ligadas a segurança cibernética – ou da informação – vem sido discutidas com o objetivo de mapear sobre possíveis ameaças e respostas aos países, como será visto no decorrer deste capítulo[51].

Para tanto, a AGNU realiza suas funções através de seis comitês principais, nos quais todos os membros têm direito a representação. Eles são:

- Primeiro Comitê (Desarmamento e Segurança Internacional);
- Segundo Comitê (Econômico e Financeiro),
- Terceiro Comitê (Social, Humanitário e Cultural),
- Quarto Comitê (Assuntos políticos especiais e descolonização),
- Quinto Comitê (Administração e Orçamento) e
- Sexto Comitê (Jurídico). (ABC das NAÇÕES UNIDAS, 2011.)

Em razão da proposta de estudo aqui envolvida, os três primeiros comitês da ONU tornaram-se o ponto de análise, já que cada um deles possui resoluções adotadas acerca do debate da segurança cibernética, tratando de diversos temas, entre eles, a ameaças iminentes no campo, a criação da cultura global do espaço cibernético e dos direitos humanos na internet, que serão abordados no decorrer deste capítulo.

[49] ABC das NAÇÕES UNIDAS, 2011.
[50] Idem.
[51] Idem.

O Primeiro Comitê lida com o desarmamento, desafios globais e ameaças à paz que afetam a comunidade internacional e busca por soluções aos problemas à segurança internacional. O Segundo Comitê é responsável pelos assuntos econômicos e financeiros, tais como o crescimento econômico e desenvolvimento, as questões políticas macroeconômicas, financeirização para o desenvolvimento, desenvolvimento sustentável, globalização e a erradicação da pobreza. Por fim, o Terceiro Comitê trata dos assuntos de âmbito social, questões humanitárias e dos direitos humanos que afetam as pessoas pelo mundo. Somado à isso, discute a proteção de crianças, a promoção das liberdades fundamentais através da eliminação do racismo e da discriminação racial e da privacidade[52].

No entanto, para entender melhor como funciona o processo de votação e os *sponsors* de cada resolução, faz-se necessário um pequeno esclarecimento sobre tais especificações, possibilitando um conhecimento sobre as atividades propostas nas resoluções.

3.1.1 Processo de Votação das Resoluções da ONU

Antes de agir sobre um projeto de resolução, os representantes dos Estados Membros passam horas discutindo cada palavra da resolução para chegar a um acordo sobre o texto. Quando se chega a um consenso sobre o texto, todos os Estados-Membros acordam em aprovar o projeto de resolução sem proceder à votação. A adoção de um projeto sem votação é a definição mais básica do consenso. Se 192 Estados-Membros concordaram com o texto, mas há apenas um Estado-Membro que solicita a votação, não se chega a um consenso[53].

Quando a ONU foi criada, em 1945, havia apenas 51 Estados membros e as resoluções eram aprovadas por votação. Hoje, em contraste, há 193 Estados Membros e cerca de 80% das resoluções da AGNU são adotadas por consenso, isto é, sem votação[54].

Ao se adotar as resoluções por votação, só é necessário obter uma maioria simples para concordar com o texto de uma resolução. Não precisa se preocupar ou tentar entender as perspectivas da minoria que discorda. Este processo é seletivo. Quando se adota

[52] GENERAL ASSEMBLY OF THE UNITED NATIONS.
[53] Model United Nations. Disponível em: http://outreach.un.org/mun/guidebook/introduction/how-decisions-are-made-at-the-un/>
[54] Idem.

resoluções por consenso, tem-se a preocupação com o ponto de vista de todos e se envolver em negociações que muitas vezes resultam em compromissos para que os diferentes pontos de vista são levados em consideração. Este processo é inclusivo[55].

Conforme mencionado acima, o consenso é alcançado quando todos os Estados Membros concordaram em adotar o texto de um projeto de resolução sem votação. No entanto, chegar a um consenso não é a mesma coisa que ser unânime. É importante notar que o consenso não significa que todos os Estados-Membros concordem com cada palavra ou até com cada parágrafo do projeto de resolução. Os Estados-Membros podem atingir um acordo sobre um projeto de resolução sem realizar a votação, mas ainda têm reservas quanto a determinadas partes da resolução. O ponto importante é que nada na resolução é tão desagradável para qualquer Estado-Membro que sentem que deve ser submetido a votação[56].

3.1.2 Patrocinadores (*Sponsors*) e Signatários (*Signatories*)

Os patrocinadores de um projeto de resolução são os principais autores do documento e concordam com seu conteúdo. Embora seja possível ter apenas um patrocinador, isso raramente ocorre na ONU, uma vez que os países devem trabalhar em conjunto para criar uma linguagem amplamente agradável para que o projeto de resolução seja aprovado. Os patrocinadores controlam um projeto de resolução e somente os patrocinadores podem aprovar mudanças imediatas. Já os signatários são países que podem ou não concordar com o conteúdo do projeto de resolução, mas que ainda assim querem que ele seja debatido para que possam propor emendas[57].

3.1.3 Histórico

3.1.3.1 Primeiro Comitê da ONU – Desarmamento e Segurança Internacional

A Rússia lançou um projeto de resolução para o Primeiro Comitê da Assembleia Geral, em 1998, direcionada aos Estados Membros da ONU com o intuito de desenvolver

[55] Model United Nations. Disponível em: http://outreach.un.org/mun/guidebook/introduction/how-decisions-are-made-at-the-un/>
[56] Idem.
[57] United Nations Association of the United States of America. Ver mais em: <http://www.unausa.org/global-classrooms-model-un/how-to-participate/model-un-preparation/resolutions/sponsors-and-signatories>

princípios internacionais, através da iniciativa de controle de armas cibernéticas, que viriam a ajudar no combate ao terrorismo de informação.[58]

Os elementos desta resolução para computar uma ameaça internacional na segurança da computação podem ser categorizados pelo surgimento da discussão sobre o potencial militar da tecnologia da informação e comunicação pela primeira vez, a necessidade para prevenir o terrorismo e o crime cibernético e por fim, convida os membros para analisar as definições e o desenvolvimento de princípios internacionais para a segurança cibernética[59].

Este projeto de resolução foi adotado e incorporado na resolução do Primeiro Comitê, sendo incluído também na agenda deste comitê, um item nomeado "*Developments in the field of information and telecommunications in the context of international security*"[60]; com o objetivo de tratar das questões da segurança de informação e problemas relacionados ao tema[61].

Com o avançar dos anos, os debates para as resoluções da ONU ganharam uma projeção de interesse entre a maioria dos países[62]. A busca pelas normas e princípios que tratassem da segurança no domínio cibernético fez com que a Rússia, novamente, lançasse um projeto de resolução[63] que propunha a formação de um Grupo de Peritos Governamentais (Group of Governmental Experts - GGE) formado por experts de 15 países[64] escolhidos por uma distribuição geométrica equitativa para 1) estudar as existentes e potenciais ameaças no domínio da segurança da informação, assim como possíveis cooperações, e 2) submeter um relatório do estudo à Assembleia Geral na sessão subsequente.

Com a Resolução da ONU de 2001[65], foi estabelecida a formação do primeiro GGE em 2004 com os objetivos sugeridos, porém não se chegou a um consenso sobre o

---

[58] GJELTEN, 2010.
[59] MAURER, T. 2011
[60] United Nations General Assembly, 1998
[61] Ver mais em: <https://ccdcoe.org/un.html>
[62] United Nations.
[63] Ver mais em: <https://ccdcoe.org/un.html>
[64] Belarus, Brasil, China, França, Alemanha, Índia, Jordânia, Malásia, Mali, México, República da Coreia, Federação Russa, África do Sul, Reino Unido da Grã Bretanha, Irlanda do Norte e Estados Unidos da América. Ver mais em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement>. Acessado em 10/01/2016
[65] United Nations General Assembly, 2001.

impacto das Tecnologias da Informação e Comunicação (TIC's) na segurança da informação associada à segurança nacional[66].

Para a formação do primeiro GGE houve um consenso da importância do desenvolvimento das Tecnologias das Informações e Comunicações (TIC's), porém durante as discussões em 2004 para a construção de um relatório que abordasse sobre os problemas e possíveis ameaças no campo da segurança cibernética, dois impasses foram os marcos para a não concretização do trabalho dos peritos. O primeiro problema encontrado respaldava no impacto em que as TIC's geram nas decisões militares e de segurança nacional[67].

Porém o problema maior se encontrava em definir se as discussões deveriam abordar os assuntos abordando o conteúdo da informação ou apenas concentrar-se na infraestrutura de informação. A principal discussão envolvia a alegação de que o conteúdo de informações transfronteiriças deveria ser controlado por questões de segurança nacional. A preocupação aqui é que as informações transmitidas pela internet poderiam ameaçar a estabilidade dos estados, em especial os regimes autoritários. A preocupação russa era o termo "segurança da informação", um conceito que as palavras podiam ser vistas como armas[68].

No entanto, houve a orientação para um novo grupo em 2009. O segundo GGE, com peritos de 15 Estados[69], foi capaz de produzir um relatório de consenso que destacou principalmente a necessidade de continuar a discutir mais normas para abordar ameaças existentes e potenciais na esfera da segurança da informação.

Neste período, preocupações sobre guerras cibernéticas tomavam espaço em manchetes pela primeira vez. O caso da Estônia, em 2007 e o da Geórgia, em 2008 são versões sofisticadas e poderosas de ataques cibernéticos. Na Estônia vários ataques foram utilizados para tirar sites governamentais, de bancos e de notícias do ar, de modo a infectar

[66] Geneva Internet Platform.
[67] UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS, 2015.
[68] GJELTEN, Tom. 2010.
[69] Belarus, Brasil, China, Estônia, França, Alemanha, Índia, Israel, Itália, Qatar, República da Coreia, Federação Russa, África do Sul, Reino Unido da Grã Bretanha, Irlanda do Norte e Estados Unidos da América. Ver mais em: < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement>. Acessado em 10/01/2016

vários computadores, os forçando a tentar acessar o sistema inúmeras vezes até que os computadores não pudessem processar e entrassem em colapso.[70]

No caso da Geórgia, as semelhanças com a Estônia se resumiram à etapa incial. Após atacar sites do governo e da mídia local, foram atacados sites de instituições financeiras, de ensino e empresas, gerando uma inundação no sistema bancário com transações falsas, fazendo com que bancos internacionais suspendessem operações com Geórgia e, por fim, houve um ataque ao serviço de telefonia do país, deixando-o ilhado. Para ambos casos a Rússia foi acusada, porém sem provas concretas[71].

Após estes casos, o avanço nas discussões obteve maior espaço, a partir de 2009, com o debate a respeito da criação de uma internet mais segura e transparente permite que o questionamento tome um direcionamento mais amplo. Apenas as lei e normas por si só não constroem uma rede de comunicação e informação mais segura. Os desenvolvedores de computadores devem trabalhar para fazer seu equipamento com um sistema seguro, porém é preciso que seja feito um trabalho em conjunto com os possuidores e operadores de tais, portanto se faz necessária a construção de confiança e segurança aliada na promoção de uma cultura global da cybersegurança[72].

3.1.3.2 Segundo Comitê da ONU - Econômico e Financeiro

Além das propostas feitas pela Rússia, na Assembleia Geral, e que resultaram no Grupo de Experts, a questão da segurança cibernética também foi discutida no âmbito do Comitê Econômico e Financeiro, que apresentou na Assembleia Geral três resoluções relacionadas com a Internet. As resoluções adotadas em 2002[73], 2003[74] e em 2009[75], são intituladas "criação de uma cultura global da cibersegurança".

O primeiro documento trata dos elementos para a criação desta cultura global reconhecendo que os espaços no acesso e ao uso da tecnologia da informação pelos Estados, pode diminuir a efetividade da cooperação internacional para o combate ao uso indevido da tecnologia da informação.

---

[70] Este ataque durou cerca de três semanas e só cessou quando a Estônia se desconectou totalmente da internet, afetando sites do governo, de jornais e emissoras de TV além de tirar os bancos do ar. (G1, 2007)
[71] AGOSTINI, 2014
[72] World Information Society Report: Beyond WSIS, 2007
[73] United Nations General Assembly, 2002.
[74] United Nations General Assembly, 2003.
[75] United Nations General Assembly, 2009.

Para tanto, na resolução é anexada princípios, elementos, para esta criação. Sendo requerido que adote nove elementos complementares, como consciência, responsabilidade, reação, ética, democracia, avaliação de risco, projeto e implementação de segurança, gerenciamento de segurança e reavaliação (ver anexo). Apesar do desafio da implementação destes elementos, podem ser analisados como um consenso para princípios internacionais básicos e sinais de um surgimento de normas.

Os dois últimos documentos tratam de elementos para proteção de infraestruturas críticas de informação, que vão desde problemas técnicos a serem resolvidos, como a promoção de parcerias e cooperação internacional[76] e um anexo (ver anexo) ressaltando uma "forma voluntária de auto avaliação dos esforços nacionais para proteger as infraestruturas críticas de informação" [77]. Essas recomendações não são voltadas apenas para os países, como também para os *stakeholders*[78], cooperação público-privado e a participação do processo político de tal forma que assegure a força para a segurança cibernética com o aumento do conhecimento da cultura global nesta área[79].

A declaração da Cúpula Mundial da Sociedade da Informação (WSIS) de 2003 recorreu à essa cultura global para fortalecer o cenário de confiança, incluindo a segurança da informação, das redes, privacidade e proteção ao consumidor, tidos como requisitos para o desenvolvimento de uma forte Sociedade da informação[80], como objetivo a ser alcançado mundialmente. [81]

Com o desenvolvimento das discussões acerca do tema, um terceiro GGE foi montado em 2011. As reuniões ocorreram nos anos de 2012-2013, contando com peritos

[76] United Nations General Assembly, 2003.
[77] United Nations General Assembly, 2009.
[78] A stakeholder refers to an individual, group or organization that has a direct or indirect interest or stake in a particular organization; that is, a given action has the ability to influence the organization's actions, decisions and policies to achieve results. (Multistakeholder Model, PATRICIO, N. S., 2016)
[79] United Nations General Assembly, 2009.
[80] O termo 'sociedade da informação' pode ser classificado como uma expansão da "comunidade mundial", porém concentrada nas TIC's onde a informação domina o novo modo de organização social. PYATI, 2005.
[81] DUNN; MAUER; KRISHNA-HENSEL, 2007.

de 15 Estados[82], sendo considerado o relatório como um marco no processo de definição de normas de segurança cibernética[83].

Com o decorrer dos debates, um assunto foi uma das pautas principais para a formação desse relatório; se o direito internacional existente aplicava-se ao ciberespaço ou não. Enquanto o Conselho de Direitos Humanos da ONU afirmou em 2012 que os direitos humanos que se aplicam off-line, deve-se ter a mesma proteção on-line, em particular a liberdade de expressão, aplicável independentemente de fronteiras e através de qualquer meio de escolha, indo de acordo com o Artigo 19[84] da Declaração Universal de Direitos Humanos[85], somente no relatório do terceiro GGE que a comunidade internacional entrou em acordo e considerou que as leis humanitárias são aplicáveis tanto no *on-line* quanto no *off-line*.

3.1.3.3 Terceiro Comitê da ONU - Social, Cultural e Humanitário

O Terceiro Comitê abordou principalmente as questões de crime cibernético e direitos à privacidade durante suas discussões relacionadas à segurança cibernética. As resoluções de 2000[86] e 2001[87] – intituladas "Combate ao uso indevido de tecnologias da informação" – têm destaque por conterem recomendações para os Estados utilizarem e possuírem segurança na esfera tecnológica.

Ademais em 2013, nesse mesmo comitê, foi aprovada a resolução titulada "O Direito à Privacidade na Era Digital"[88] cuja versão inicial foi elaborada em conjunto pelo Brasil e Alemanha, por resultado das revelações feitas por Edward Snowden, também em 2013. Esta resolução enfatizou a responsabilidade dos Estados de respeitar e proteger a privacidade e, sob o mesmo ponto de vista do Conselho de Direitos Humanos da ONU e

[82] Argentina, Austrália, Belarus, Canada, China, Egito, Estônia, França, Alemanha, Índia, Indonésia, Japão, Federação Russa, Reino Unido da Grã Bretanha e Estados Unidos da América. Ver mais em: <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/01/Information-Security-Fact-Sheet-Jan-2014.pdf>

[83] Freedom Online Coalition

[84] Artigo 19. Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão. (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948)

[85] United Nations General Assembly, 2012.

[86] United Nations General Assembly, 2000.

[87] United Nations General Assembly, 2001.

[88] United Nations General Assembly, 2013.

do terceiro GGE, afirmou que os mesmos direitos que as pessoas têm *off-line* devem ser protegidos *on-line*, incluindo o direito à privacidade[89].

O quarto GGE, formado em 2014, contou com peritos de 20 Estados[90] e produziu um relatório em 2015. O grupo produziu um relatório substancial sobre as normas, regras e princípios do comportamento responsável dos Estados no espaço cibernético que devem ser respeitadas por todas as nações, inclusive em tempos de paz[91].

Embora haja um consenso no relatório, houve propostas e opiniões divergentes durante a sessão. Excluída do documento se encontra uma proposta dos Estados Unidos acerca do relatório de 2013, por sugerir que o direito internacional geralmente se aplica ao ciberespaço, da mesma forma que em terra ou no mar. Essa proposta foi vetada por um grupo de países – incluindo a Rússia, China, Paquistão, Malásia e Belarus – afirmando que essa declaração apenas institucionaliza a hegemonia dos EUA no ciberespaço[92].

A proposição dos EUA fazia referência ao Artigo 51[93] da Carta das Nações Unidas, que autoriza o uso da força em casos de auto defesa conta um ataque armado, legitimando uma resposta militar a um ataque cibernético. O argumento chinês iria contra essa proposta porque objetivava militarizar o ciberespaço, deixando de ser uma zona de paz, afirmou James Lewis – relator do grupo de especialistas e diretor do Programa de Tecnologias Estratégicas do Centro de Estudos Estratégicos e Internacionais[94].

O Oficial do Departamento de Estado descreveu a seção de direito internacional do documento como "um passo muito importante a partir de 2013", mas também "mais ambígua do que gostaríamos". Para a Diretora de *Georgetown University's Institute for Law, Science and Global Security* e assistente geral do conselho da CIA, Catherine

---

[89] United Nations

[90] Belarus, Brasil, China, Colômbia, Egito, Estônia, França, Alemanha, Gana, Israel, Japão, Quênia, Malásia, México, Paquistão, Federação Russa, Espanha, Reino Unido da Grã Bretanha e Estados Unidos da América. Ver mais em:

[91] MARKS, 2015

[92] Idem.

[93] Artigo 51. "Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais." (CARTA DAS NAÇÕES UNIDAS E ESTATUTO DA CORTE INTERNACIONAL DE JUSTIÇA, 1945:30-31)

[94] MARKS, 2015.

Lorionte, "o desenvolvimento de normas em tempos de paz, tem uma importância maior do que estabelecer como o direito internacional age durante o conflito armado"[95].

3.2 *INTERNET GOVERNANCE FORUM*

Com o avançar das discussões acerca da segurança cibernética e da informação com um cunho eminentemente técnico, constatou-se que se fazia necessário ampliar a transparência quanto à governança da Internet. Além dessa ampliação, também foram traçadas funções dos vários atores interessados, envolvidos na governança da Internet e analisou como eles se reuniriam, em razão das suas diferentes representações e constituintes[96]. Tais questões tomaram forma global na Cúpula Mundial da Sociedade da Informação (WSIS).

A Cúpula foi resultado de uma sugestão da Conferência *Plenipotentiary* em Minneapolis, organizada pela União Internacional de Telecomunicações em 1998 e posteriormente aprovada em 2001 pela Assembleia Geral da ONU. A WSIS foi dividida em duas fases, a primeira foi sediada em Genebra, Suíça, em 2003; e a segunda ocorreu em Túnis, Tunísia, em 2005[97].

Como temática geral para a Cúpula, discutiu-se os princípios fundamentais que deveriam guiar a Sociedade da Informação, como, *por exemplo, o respeito aos direitos humanos e à liberdade de expressão, o direito à informação, o engajamento de múltiplos atores nos ciclos de políticas públicas (tanto nacionais quanto internacionais), relativas a informação, comunicação e telecomunicações, etc.* Como cúpula, o único poder que o WSIS passou a ter, para tomar decisões, é a partir de um consenso, ao contrário de uma organização intergovernamental permanente[98].

Ambas fases envolveram a discussão de diversos assuntos, como o regime da ICANN – por ser vinculada diretamente ao governo dos EUA e a falta de equilíbrio em seu modelo multisetorial –, mas o principal foco residia sobre a Governança da Internet. Durante a primeira fase foi adotada a Declaração de Princípios e reconheceu-se que o tópico destinado a governança da internet estava destinado aos governos, o setor privado, a sociedade civil e as organizações internacionais, em que tanto questões técnicas quanto

[95] Idem.
[96] ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2015
[97] United Nations General Assembly, 2002
[98] MALCOLM, 2008.

políticas públicas estão relacionadas ao uso das TIC. Desta forma, foram estabelecidos o papel de cada um desses atores[99].

> A autoridade para o desenvolvimento de políticas públicas conexas à Internet é direito soberano dos Estados. Eles têm direitos e responsabilidades pelas questões internacionais relacionadas às políticas públicas relativas à Rede. O setor privado tem – e deve continuar tendo – um importante papel no desenvolvimento da Internet, tanto em termos técnicos quanto em termos econômicos. A sociedade civil – que teve um importante papel em questões de Internet, especialmente no nível local, deve continuar a desempenhar tal papel. As organizações intergovernamentais facilitaram e devem continuar facilitando a coordenação da tomada de decisões relativas às políticas públicas conexas à Internet. E as organizações internacionais devem continuar a ter um papel importante no desenvolvimento de padrões e políticas técnicas e não técnicas relacionadas à Internet. [CÚPULA MUNDIAL PARA A SOCIEDADE DA INFORMAÇÃO, 2003b, par. 48.]

Ademais estes conceitos, foi requisitado ao Secretário Geral da ONU a formação de um Grupo de Trabalho para a Governança da Internet (WGIG) composto pelos atores mencionados anterioromente para um consenso do termo "governança da internet" – apresentado anteriormente – assim como a sugestão de desenvolvimento de um fórum *multistakeholder*[100], que permitisse uma discussão regular das questões relativas à governança da Internet.

O principal resultado da reunião de Túnis acerca da governança da Internet, estava relacionada à resolução solicitada ao Secretário Geral da ONU na primeira fase, para a organização do fórum a partir de 2006. Desta forma, neste ano, foi criado o Fórum da Governança da Internet (IGF) em que,

> [...]sua importância reside na sua habilidade de facilitar discursos entre governos, organizações intergovernamentais, empresas privadas, a comunidade técnica e as organizações da sociedade civil que lidam com ou são interessadas na Governança da Internet relacionadas aos assuntos da política pública. Os encontros do IGF abordam estruturas regulatórias, potenciais riscos, tendências globais, como também as melhores e piores praticas que tem sido adotadas ou estão em discussão. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2014)

Porém, apesar da criação e designação do fórum, alguns elementos ficaram em aberto, como a natureza do programa, a sua duração e a frequência das reuniões. Para tanto, a partir de reuniões com os stakeholders, decidiu-se sobre tais questões, assegurando uma

[99] CANABARRO, 2014.
[100] Em português, multisetorial ou pluriparticipativo

natureza inclusiva e aberta, como também ficou estabelecido que o IGF deve ser organizado uma vez ao ano, com duração de três a cinco dias de evento[101]

Ficou definido ainda que cada mandato do IGF teria a duração de cinco anos, no qual ocorreriam as reuniões, renovando – caso fosse necessário – para mais cinco anos nas resoluções da AGNU[102]. Para o período inicial do mandato do IGF, ocorrido entre os anos de 2006 a 2010, foram realizadas reuniões presenciais em Atenas, Grécia – 2006; no Rio de Janeiro, Brasil – 2007; em Hyderabad, Índia – 2008; em Sharm El-Sheikh, Egito – 2009 e por último em Vilnius, na Lituânia – 2010. No mesmo ano do evento na Lituânia, a Assembleia Geral decidiu renovar o mandado do IGF até 2015[103]. A reunião anual de 2011 foi realizada na cidade de Nairóbi, Quênia. Já em 2012, a reunião ocorreu em Baku, Azerbaijão. Em 2013 o Fórum aconteceu em Bali, Indonésia, enquanto em 2014 a reunião ocorreu em Istambul, Turquia e em 2015 João Pessoa, Brasil.

Para cada reunião estipula-se um tema e subtema que, geralmente, estão relacionados com as questões emergentes referentes à Internet[104]. Para tanto, sempre esteve presente um subtema em cada ano nomeado "*Security, Openness and Privacy*", em que cada reunião ou workshop é tratado sobre temas que circundam sobre a privacidade cibernética e seus derivados. Porém no ano de 2015, na reunião ocorrida em João Pessoa, PB, Brasil, aquele subtema foi renomeado para "*Cybersecurity and trust*" tratando de assuntos voltados para princípios da cooperação internacional, a segurança cibernética e como aumentar a confiabilidade digital e manter a privacidade, através de iniciativas bi e multilaterais[105]

Como já mencionado no início do primeiro capítulo, a definição de segurança cibernética está além da segurança dos computadores, ou de proteção de *hard* e *software*, e concerne preocupações que envolvem outros atores, como o Estado e empresas privadas, por exemplo.

Segundo Kramer (2011) as áreas que o governo deve tomar responsabilidade acerca da segurança cibernética nacional é para garantir que:

---

[101] ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2015
[102] United Nations General Assembly, 2006.
[103] United Nations General Assembly, 2006.
[104] Exemplos de subtemas recorrentes nos eventos do IGF: Governança da Internet, Acesso e Diversidade, Questões Emergentes e Administração de Recursos Críticos da Internet. (Internet Governance Forum, 2010-216)
[105] Internet Governance Forum, 2015.

> [...] o Departamento de Defesa (DdD) e a Comunidade de Inteligência (IC) operem eficazmente enquanto estiverem sob ataque; garantir, através de parcerias público-privadas, seja mantidas sem falhas as principais infraestruturas críticas – rede elétrica, financeira, telecomunicações e governamentais – mesmo sob ataque, podendo manter ou retornar ao serviço normalmente, e por fim, limitar a espionagem e o roubo de informações da segurança nacional. (KRAMER, 2011.)

Para tanto, na discussão no IGF 2015 sobre Cibersegurança e confiança, um dos assuntos principais levantados foi dos desafios enfrentados na manutenção da segurança cibernética, e David van Duren, Secretário-Chefe do Forum Global em Cyber Especialidade (GFCE), afirmou que o desafio principal é a construção de confiança entre os multistakeholders relevantes, confirmando por Paulo Sergio, o anfitrião do evento no Brasil, que adicionou a necessidade de uma colaboração intensa entre os atores[106].

A preocupação levantada por Van Duren foi justificada no Fórum pelo fato de que os computadores foram desenhados para executarem programas e guardarem dados, não para prover segurança; e as redes foram planejadas para transmitir informação, não para assegurar sua fonte ou segurança. Porém com o avançar do desenvolvimento tecnológico, programas foram aplicados para essas funções seja nos governos, setor privado ou para os indivíduos[107]. Ainda assim, a solução para manter a segurança cibernética de algo ou alguém não reside em soluções simples, nem em uma única solução, por isso se faz necessário o trabalho em conjunto dos atores relacionados à este assunto[108].

Uma das medidas multilaterais foi concretizada na reunião de várias Organizações Internacionais e *Stakeholders* no Encontro Multisetorial Global Sobre o Futuro da Governança da Internet (NETmundial), que logrou êxito ao trazer o conceito dos princípios da Governança da Internet[109]. O objetivo deste evento era promover e proteger o uso do espaço cibernético e a Internet como uma "plataforma para o desenvolvimento social, econômico e humano, e como catalisador para garantir os Direitos Humanos de todas as pessoas no mundo". (EUROPEAN COMMISSION, 2014.)

Ainda na discussão do IGF 2015, Michael Kaiser (2015), Diretor Executivo da National Cyber Safety Alliance, ressaltou que se faz necessária a criação da cultura da

[106] Internet Governance Forum, 2015b.
[107] KRAMER, Franklin D, 2011.
[108] Internet Governance Forum, 2015b.
[109] Os princípios são: Direitos Humanos e Valores Compartilhados; Proteção de Intermediários; Cultura e Diversidade Linguistica; Espaço Unificado e Desfragmentado; Segurança, Estabilidade e Resiliência da Internet; Arquitetura Aberta e Distríbuida; Fornecer o ambiente para a sustentabilidade, inovação e criatividade. http://www.netmundial.org/principles

cibersegurança, partindo da perspectiva em que o mundo globalizado demanda um conhecimento e uma educação sobre a tecnologia para todos os atores, seja para os governos como para as empresas e os cidadãos[110]. Em adição à essa afirmação, o Chefe de Estratégia da International Telecommunications Union (ITU)[111], Tomas Lamanauskas (2015), afirmou que a necessidade da educação e informação para a segurança cibernética se faz vital pois, segundo estudos, 80% das ameaças cibernéticas poderiam ser previstas seguindo passos de segurança, tais como a atualização do antivírus[112].

Acerca das ameaças no campo cibernético, a adaptação entre os Estados com a rede mundial e vice-versa, é tida como um grande impasse. A incorporação da dinâmica da segurança cibernética na segurança nacional mostra diferentes tipos de poderes surgindo, o que leva os Estados a buscar conciliar os seus interesses e adequar suas defesas e modos de ataque. A identidade e a origem das ameaças cibernéticas está categorizada como uma peça chave na adaptação por sua dificuldade de localização, o que implica diretamente nas relações entre países e atores[113].

As reuniões nos eventos e as discussões levantadas nas sessões, são de representantes diversos, seja de governos, empresas privadas, Organizações Não-Governamentais (ONG's) e tais conferências são realizadas para criar uma ponte sobre a divisão digital, incluir o próximo bilhão, e para enfatizar que tais assuntos levantados são de interesse internacional. Ainda que, esses eventos reúnem vários atores que são representantes oficiais seja de governo ou instituições, ele não tem força de decisão. O IGF identifica os problemas que precisam ser levados em consideração pela comunidade internacional e modela as decisões para que esses atores levem as ideias discutidas ondem fazem sua representação, seja nas instituições ou governos[114].

Para tanto, a preocupação acerca do ciberespaço seja dos papéis de cada ator, é causa de como cada país reage e atua. Com isso, as nações e os atores internacionais instauram suas preocupações em ações, alianças e participação em organizações internacionais para discutir sobre o espaço cibernético e como mantê-lo seguro. Na

[110] Internet Governance Forum, 2015b.
[111] A International Telecommunication Union é uma agência especializada nas Tecnologias da Informação e Comunicação, especializada em conectar os povos do mundo. (International Telecommunication Union, 2017)
[112] GRIMES, 2013
[113] MUELLER, 2010.
[114] ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2015

medida que alianças são formadas e as organizações colocam em pauta a segurança cibernética, tais atores desenvolvem um conjunto de procedimentos para a sua atuação no espaço, até porque, por ser considerado relativamente recente, o âmbito cibernético pode ser usado para o benefício quanto para o malefício, por isso a cooperação é um dos meios viáveis para a confiança internacional.

4 REGIMES INTERNACIONAIS E A SEGURANÇA CIBERNÉTICA

A definição mais recorrente de regimes internacionais foi expressa pelo Keohane (1982) através do contexto internacional que caracterizava-se por um mundo político em que faltava autoridade das instituições governamentais, marcado por uma desconfiança generalizada. Para tanto, Keohane (*idem*) definiu que a função central dos regimes internacionais é "facilitar o benefício mútuo da realização de acordos entre governos, dessa forma, a condição estrutural da anarquia não seria encaminhada para uma 'guerra de todos contra todos." (KEOHANE, 1982:332)

Desta forma, para Keohane (1993), algumas decisões negociadas, teriam um resultado eficiente se tomadas de forma coletiva, e não unilateral e individual, o que elucidava a demanda por regimes internacionais por parte dos Estados: "Os regimes facilitam a cooperação, propiciando regras, normas, princípios e procedimentos que auxiliam os agentes a superar barreiras à cooperação como a falha de mercado." (KEOHANE, 1993:182).

A partir desta definição, Krasner (2012) define os regimes como "princípios, normas e regras implícitos ou explícitos e procedimentos de tomadas de decisão de determinada área das relações internacionais em que convergem as expectativas dos atores". (KRASNER, 2012:94)

Para tanto, Krasner (2012) desenvolve os termos citados ao determinar que os princípios são "crenças em fatos, causas e questões morais. As normas são padrões de comportamento definidos em termos de direitos e obrigações. As regras são prescrições especificas para ação. Por fim, os procedimentos para tomada de decisão são práticas predominantes para fazer e executar a decisão coletiva." (KRASNER, 2012:94) Porém o cerne do Regime está contido entre os princípios e normas, uma vez que ocorre mudanças

nestes, há, ou a criação de um novo regime, ou o desaparecimento dos regimes em determinada área. Quando há mudança em procedimentos ou tomadas de decisão ou em regras o que ocorre são mudanças internas aos regimes.[115]

Como citado anteriormente, regimes propiciarem a realização dos acordos ao prover um conjunto de fatores para a negociação, tais como os princípios e as normas, porém, Keohane (1993) afirma que, embora os regimes forneçam essa plataforma facilitadora de acordos, ainda é preciso mencionar a distinção entre os atores num regime que realizam vários acordos, daqueles que se reúnem para um acordo *ad hoc.* Isto acontece porque num acordo *ad hoc* não há benefícios para todas as partes.

Os regimes são, em parte, desenvolvidos porque os atores políticos acreditam que a junção dos atores será capaz de fornecer benefícios mútuos, Coase (*apud* Keohane, *1993)* afirma que mesmo os Estados buscando um maior interesse entre as relações ou acordos, sob certas circunstâncias pode levar à soluções de problemas de forma efetiva. Os regimes funcionam provendo um conjunto de fatores para facilitar a resolução de algum dilema que necessite da participação de atores internacionais para sua solução ou normalização.[116]

A proposta de Coase, exemplifica o teorema em três circunstâncias: 1) estabelecer uma estrutura legal para ações, 2) informação precisa e 3) custos de transações zero. Se essas condições fossem alcançadas entre os atores, os acordos *ad hoc* seriam os mais viáveis e os regimes desnecessários. Porém Keohane (1982) ressalta que existe a falta nestas três orientações de Coase, ao exemplificar que um governo mundial não existe – logo não há uma legislação internacional, informação é muito valiosa e rara de se obter, assim como as transações custam caro. No entanto, essas variáveis levam a identificar os problemas no meio internacional e servir como soluções dentro dos regimes.

A característica marcante dos regimes é a sua eficiência, como afirma Krasner (1982), e o autor Carvalho (2005) explora que o conceito da funcionalidade dos regimes deve ser complementado e especificado para determinar os elementos que asseguram a autonomia e a relevância dos regimes. Para tanto, Carvalho (2005) apresenta uma análise de elementos básicos para os regimes, como os atores e a especificidade da área de interesses.

---

[115] KEOHANE, 1982
[116] *Idem.*

O estudo de regimes progrediu com os estudos das organizações internacionais após a Segunda Guerra Mundial, dessa forma, a característica desta época, os primeiros autores "institucionalistas" tiveram suas atenções para as organizações interestatais, como a ONU, e os processos de decisão dos Estados no foro destas organizações[117].

Com o avançar dos estudos, Keohane e Nye (apud Carvalho, 2005) posicionaram entre as duas perspectivas: modernistas – que tinham o caráter transnacional das relações e a relativização do Estado – e os tradicionalistas – identificados pelos realistas, que enfatizavam a continuação do Estado e a sua predominância em questões de política internacional -, procurando interagir entre estes prismas. Assim sendo, Keohane e Nye (apud Carvalho, 2005) sugerem que a ideia de atores não está relacionada diretamente aos atores estatais, pois podem ser atores não estatais também, ao levar em consideração que estas organizações fazem parte da sociedade internacional e, junto com os Estados, discutem e procuram soluções para os problemas de cunho mundial.

Por fim, Carvalho (2005) delineia a formação dos regimes, ao elucidar que se aplicam as áreas especificas de inter-relação entre os atores, nomeado como *issue-areas.* Keohane (1993) explana que os regimes formam-se em áreas de interesses delimitadas através da afinidade de temas e sua concordância de possuir um mesmo arranjo político e consoante nas regras.

Visto alguns conceitos importantes para a área dos regimes internacionais, o passo seguinte consiste em considerar pontos importantes para o cerne internacional, como interesse e poder Estatal, e como se conecta e relaciona à segurança cibernética mundial.

A segurança é um das preocupações básicas do Estado, e a sua providência é uma função clássica, por isso, o crescimento da insegurança leva ao crescimento de governos no espaço cibernético. O avanço do desenvolvimento tecnológico levou a dimensão espacial de soberania a um nível maior, como Nye (2014) afirmou que "vários Estados buscam expandir sua soberania pelo espaço cibernético, através da busca pelos meios tecnológicos para sua realização" (NYE, 2014).

Os regimes são um subconjunto de normas, que são expectativas compartilhadas sobre o comportamento apropriado. Gilpin (*apud* Nye, 2014) afirma que os regimes são criados e sustentados pelo estado mais poderoso e, na medida que seu poder cresce, a

[117] CARVALHO, 2005

manutenção dos regimes se torna mais difícil, isso porque os *hegemons* conduzem o incentivo do benefício desproporcional entre os *free riders* para apoio da maioria no regime. Nye (2014) sustenta que o declínio do controle dos Estados Unidos na internet pode levar a uma fragmentação futura.

Na medida que os Estados buscam representar o interesse nacional, e por vezes tendem a seguir pela ideologia ou barganha das potências, um dos fatores relevantes levantado por Nye é como os interesses são notados e implementados, principalmente no espaço cibernético. De acordo com Krasner (1991) a adaptação de poder junto com as TIC's, possibilitou a sua utilização por outros atores que não o Estado, e foram inseridos através das habilidades tecnológicas, seja domestica ou internacionalmente[118].

> In recent years, distributional issues have become more consequential. Third World statesmen have worried that the entire electromagnetic spectrum would be allocated without taking account of the future needs of their countries. The regime has responded to these concerns because in this case Third World countries have power conferred by their ability to interfere with other states' broadcasts and by their membership in the ITU. In the area of telecommunications, technological change has altered the capabilities of actors and increased distributional conflicts. International regimes, in turn, have changed in response to these changes in capabilities. More precisely, technological innovation gave some private actors, primarily domiciled in the United States, an incentive to press for a more competitive telecommunications regime both domestically and internationally. (KRASNER, 1991)

De acordo com Cavelty e Brunner (2007), a informação e a sua utilização como poder, transformam o sistema internacional ao elucidar que o crescimento tecnológico – e cibernético – leva a duas perspectivas que diminuem a importância dos Estados e assim a redistribuição de poder, sendo elas: a noção que a revolução da informação empodera novas formas de atores internacionais, tais como as ONG's e ativistas, e a noção que a emersão de um mercado global eletrônico pode entrar em colapso no pilar econômico de poder do Estado, na medida que as empresas *tomam* representatividade como cidadãos globais[119].

Apesar destas mudanças não ocorrerem em curto prazo, a primazia estatal sofre uma competição pelos novos atores de acordo com o avanço das TIC. Este fato ocorre principalmente pela demanda na proteção da segurança e da economia do público. Desta forma, duas das principais responsabilidades do Estado são parcialmente *suprimidas* por

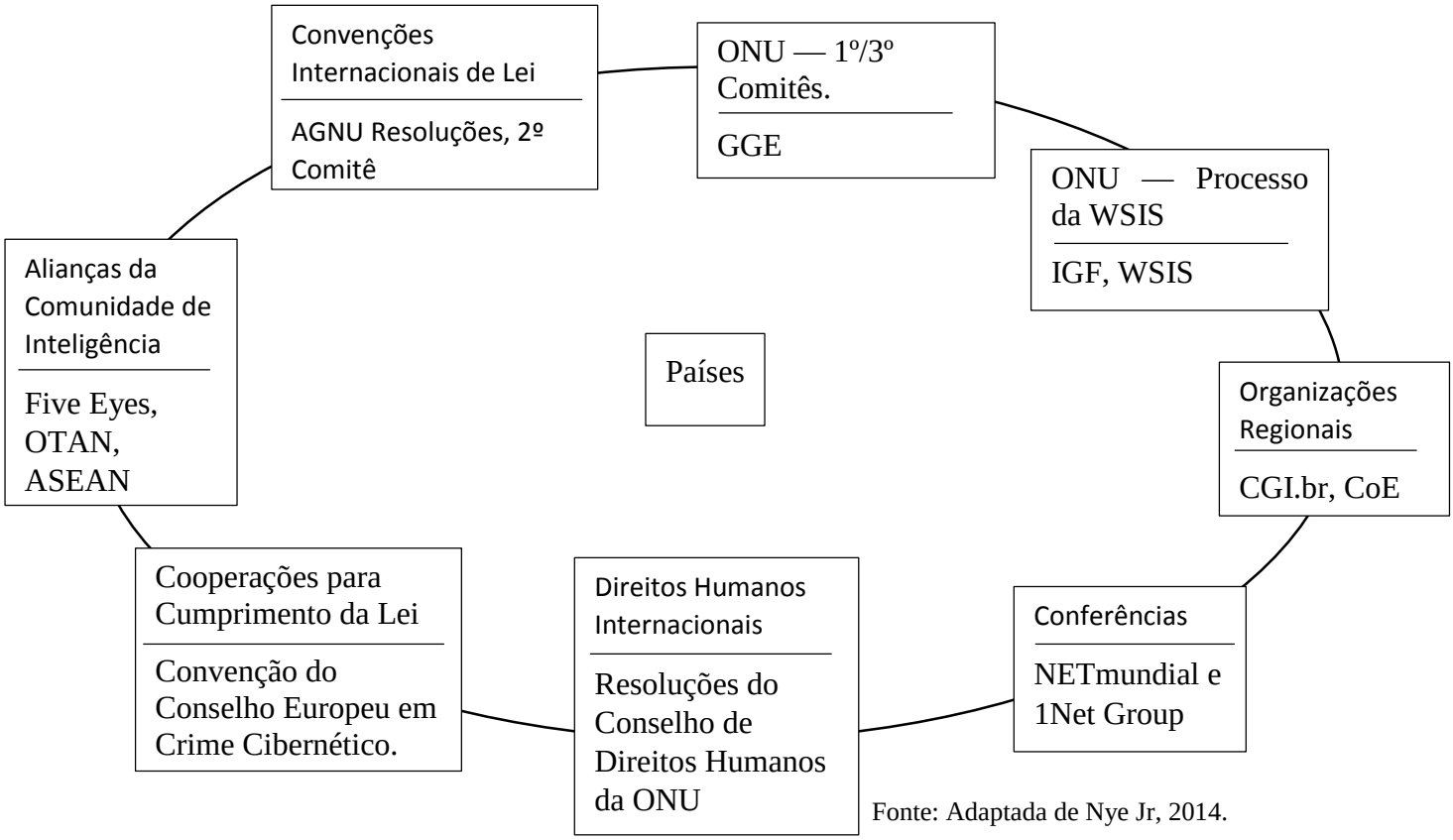
[118] KRASNER, 1991
[119] CAVELTY, BRUNNER. 2007

empresas multinacionais, uma vez que estas não são restritas geograficamente e podem interagir internacionalmente correspondendo às necessidades externas[120].

Na medida que as empresas tomam responsabilidades e proveem serviços e assim, o direito à proteção e a defesa, o setor privado não pode realizar ações que perpassem dos poderes legítimos e os papéis do governo sem que exista um mandato claro e diretrizes legais que demarquem comportamentos aceitáveis para com o Estado[121].

Não há um regime para o espaço cibernético ou para a segurança cibernética, existe um conjunto de normas e instituições que se encontram entre organizações integradas que impõem regulações sobre regras hierárquicas e práticas e instituições fragmentadas. A Figura 1 é um mapa de uma parte da governança cibernética que inclui normas, atores, procedimentos. Seu objetivo não é mapear todas as atividades no espaço cibernético, mas sim indicar uma grande extensão relacionada a governança que existe no espaço[122].

Figura 1: Mapa parcial da governança cibernética



Fonte: Adaptada de Nye Jr, 2014.

[120] *Idem.*
[121] BUTLER, LACHOW. 2012
[122] Nye, 2014

Acrônimos da Figura 1

AGNU	Assembleia Geral da ONU
CoE	Conselho da Europa
Five Eyes	Aliança da Austrália, Canadá, Nova Zelândia, o Reino Unido e os Estados
GGE	Grupo Governamental de Experts
IGF	Fórum da Governança da Internet
ONU	Organização das Nações Unidas
WSIS	Cúpula Mundial da Sociedade da Informação

4.1 ATORES

4.1.1 Estado-Nação

Os Estados são atores centrais na promoção de uma segurança no espaço cibernético, seja ao coordenar ou desenvolver ações seguradoras para seus cidadãos. Butler e Lachow (2012) acrescentam que, para o funcionamento da segurança cibernética multilateral funcionar, cada participante necessita desenvolver e pôr em prática seu próprio mecanismo de defesa cibernética.

Essa estrutura deve ser trabalhada continuamente através de operações militares, civis e redes comerciais que são os alicerces para o bom funcionamento da segurança nacional. Sem essa base cibernética, os atores encontram dificuldade em coordenar e desenvolver estratégias e práticas de acordo com o sistema internacional para o ecossistema cibernético[123].

Desta forma, deve-se nomear uma organização governamental que seja responsável pela coordenação da defesa cibernética nacional, podendo atuar com entidades governamentais e do setor privado, uma vez que a maioria das técnicas cibernéticas residem em empresas, as nações devem desenvolver parcerias com estas empresas, o que inclui provedores de serviços de Internet e de segurança, assim como infraestruturas críticas, tais como software e hardware[124].

As estratégias dos países para a segurança cibernética deve levar em consideração os atores importantes nesta área, pois assim, poderá incorporar boa parte das capacidades que eles tem, tais como os estados, empresas e organizações internacionais. Butler e Lachow (2012) afirmam que um exemplo desta abordagem é realizado na Estratégia Cibernética Holandesa de 2011, que estabelece um plano bem construído que enquadra

[123] *Idem.*
[124] *Idem.*

tanto o setor público quanto o privado para assegurar a segurança cibernética[125]. Para isso segue em princípios básicos:

> "Vincular e reforçar iniciativas; Parcerias Público-Privadas; Responsabilidade individual; Divisão de responsabilidade entre departamentos; Cooperação internacional ativa; Medidas proporcionais (equilíbrio de segurança e direitos fundamentais); Auto regulação se possível, legislação e regulamentação se necessário." (MINISTRY OF SECURITY AND JUSTICE, 2011.)

Para o desenvolvimento de tais princípios, o governo holandês criou um Centro Nacional de Segurança Cibernética com o objetivo de compreender o desenvolvimento, ameaças e tendências, além de prover às partes um guia de como lidar com incidentes e decisões em momentos de crise. Em vista disto, o governo holandês considera essencial adotar uma abordagem colaborativa entre o setor público, o setor privado e as instituições de conhecimento[126].

Os Estado Unidos desenvolveram sua estratégia em 2011, nomeada de *International Strategy for Cybersecurity: Prosperity, Security, and Openness in a Networked World*. Primeiro documento que promove uma estratégia de âmbito internacional, este documento buscava prover uma rota para os departamentos estadunidenses e suas agências para definir e coordenar seus papéis na política da segurança cibernética internacional. Desenvolvido no governo Obama, a Estratégia buscava que a sociedade civil e o setor privado pudessem reforçar essa parceria através da consciência e ação. Por fim, encoraja aos outros Estados a terem essa visão de prosperidade, segurança e estrutura no mundo[127]. Logo, seu objetivo era:

> "...trabalhar internacionalmente para promover uma estrutura de informação e comunicação aberta, interoperacional, segura e confiável que de suporte aos acordos internacionais e o comercio, fortaleça a segurança internacional e a promoção da liberdade de expressão e inovação." (INTERNATIONAL STRATEGY FOR CYBERSPACE, 2011. Tradução livre)

O ponto central dessa Estratégia estava centrada no futuro da segurança cibernética, construindo uma política do espaço cibernético e identificando as prioridades políticas. Sendo assim, afirma que os Estados Unidos visam construir e sustentar um ambiente com "normas de comportamento para guiar as ações dos estados, aderir a parcerias e apoiar a instauração de leis no espaço cibernético." (HOLDORF, 2015)

[125] MINISTRY OF SECURITY AND JUSTICE, 2011.
[126] BUTLER, LACHOW. 2012.
[127] THE WHITE HOUSE, 2011.

4.1.2 Alianças Políticas e de Segurança

A princípio, as nações desenvolvem suas próprias estruturas para coordenar as autoridades sobre suas capacidades acerca do espaço cibernético, garantindo que sua organização governamental de assuntos cibernéticos trabalhe com homólogos em outros países para desenvolver um entendimento mútuo acerca das autoridades, capacidades e cooperação para ações coordenadas no espaço cibernético[128].

Dessa forma, os Estados podem trabalhar o seus próprios alinhamento de suas políticas e recursos valorizando seus interesses nacionais, assim a aderir ao ecossistema cibernético internacional. As alianças e parcerias de cooperação variam de acordo com as prioridades de cada país em relação ao interesse nacional e ao que se considera ameaça para tal. Por exemplo, a Alemanha tinha determinado que uma infestação de *botnet* (vários aparelhos conectados via Internet infectados e controlados por uma terceira pessoa) na sua infraestrutura privada era a prioridade de defesa nacional[129].

Inclusive o Reino Unido tinha estabelecido que violação de dados causada por crime e espionagem era a sua maior prioridade. Não obstante, a França e os Estados Unidos determinaram que a defesa das redes militares e governamentais eram suas maiores prioridades. A França então estabeleceu a Rede Francesa e Agência de Segurança de Informação (FNISA – sigla em inglês) para a implementação de mecanismos de defesa acerca de redes sensíveis do governo para evitar a espionagem. Já os Estados Unidos estavam focados em definir o papel governamental em proteger as redes e infraestruturas do setor privado, para prover um conjunto de objetivos e práticas da segurança cibernética[130].

Chega-se ao entendimento que em virtude das diferentes prioridades destes países, o foco na política e desenvolvimento de capacidades é obtido em diferentes áreas[131]. Dessa forma, as semelhanças entre as ameaças dos países tornam-se divergentes, seus propósitos comprometem o compartilhamento de informação ou cooperação em tempos de crise. É por esta razão que quando uma nação falha na segurança cibernética de um país, pode impactar uma aliança e, portanto, uma estrutura transnacional torna-se

[128] BUTLER, LACHOW. 2012.
[129] BUTLER, LACHOW. 2012.
[130] HATHAWAY, 2010.
[131] BUTLER, LACHOW. 2012.

necessária para que cada nação possa garantir suas leis, regulamentos e políticas internas e, com isso, não comprometer seus compromissos regionais e de segurança[132].

O desenvolvimento de tais bases para o entendimento e reunião de ameaças e capacidades comuns é necessária, e exemplos de alianças políticas e de segurança são a Organização do Tratado do Atlântico Norte (OTAN) e a Associação de Nações do Sudeste Asiático (ASEAN) para alcançar tais objetivos. A OTAN existe com o "propósito de dar suporte para a paz e segurança internacional, a OTAN como organização, está numa posição de desenvolver e aplicar medidas de segurança no caso de haver uma ameaças ou ataque cibernético relevante" (BUTLER, LACHOW. 2012). Uma destas medidas foi a criação da Política de Defesa Cibernética da OTAN, para uma reação de assistência aos países membros sob a ocorrência de um ataque cibernético[133].

Esta aliança coordena seus atos através do compartilhamento de informação e práticas favoráveis e exercícios de condutas. Para tanto, sua política confirmava que as leis internacionais aplicavam ao espaço cibernético. Em parte, a sua criação foi decorrente do pedido emergencial da Estônia após o ocorrido no país em 2008, porém as discussões após o ataque percorriam se constituía um ato de agressão no espaço cibernético, e muitos membros da OTAN consideraram que não fora um ataque sério para ativar o Artigo 5, em que qualquer membro sofresse um ataque, era considerado à todos os países membros[134].

Porém, como citado anteriormente, a dificuldade de grandes alianças de desenvolver políticas e capacidades operacionais coerentes com seus membros associados é muito complexo. A ASEAN, por exemplo, não vinha realizando tantas ações[135], apenas no final de 2016 durante a Semana Internacional Cibernética de Singapura que a Conferência Ministerial de Segurança Cibernética da ASEAN foi discutido sobre a importância das capacidades cibernéticas dos membros, além de assegurar um espaço cibernético mais seguro e a possibilidade de trocas em normas cibernéticas entre os 10 países membros[136].

---

[132] HATHAWAY, 2010.
[133] *Idem.*
[134] HATHAWAY, 2010.
[135] BUTLER, LACHOW. 2012.
[136] NATO CCDCOE, 2016.

4.1.3 Organizações e Conferências Internacionais

Ademais a variância das preocupações nacionais acerca do espaço cibernético e a sua segurança, o domínio cibernético pode ser utilizado com fins diversos, tais como legítimos e maliciosos. Estados, ONG's e outros atores estão procurando evoluir nas vulnerabilidades das TIC. A conectividade global, tecnologias vulneráveis e a anonimidade dificultam o controle e a segurança no campo cibernético, em que as organizações internacionais discutem junto com os outros atores acerca dos meios de reduzir os riscos e progredir na cooperação[137].

Apesar dos governos terem a liderança desenvolvendo e implementando medidas para a segurança cibernética, o GGE reitera que é importante que o setor privado e a sociedade civil participe das discussões[138]. Os membros da ONU adicionaram suas participações nas resoluções adotadas para uma lei internacional e cooperação para que os Estados possam aumentar suas capacidades de segurança acerca do ciberespaço em território nacional e, "através de um estudo do Instituto da ONU de Pesquisa para Desarmamento, mais de 40 países desenvolveram alguma capacidade militar cibernética e 12 deles para uma possível guerra cibernética." (WOLTER, 2013.)

Em adição, uma carta formal da Rússia, China Tajiquistão e Uzbequistão foi submetida à ONU em 2011 com a proposta de um Código Internacional de Conduta para a Segurança da Informação. Este código estabelecia que as nações não deveriam usar informação ou a tecnologia das telecomunicações para conduzir atores hostis ou agressivos que pudessem vir a ameaçar a paz internacional e a segurança[139]. Para isso tinha por visão:

> "1) Estabelecer um mecanismo de governança internacional multilateral, transparente e democrática; 2) Respeitar os direitos e liberdades de informação e do espaço cibernético enquanto leis futuras; 3) Ajudar países em desenvolvimento à desenvolverem tecnologias de informação e redes e 4) Cooperar no combate ao crime cibernético." (HOLDORF, 2015.)

Da mesma forma, o propósito do código estava em identificar os direitos e responsabilidades dos Estados, aumentar a cooperação com relação às ameaças e desafios e assegurar que as TIC's sejam usadas apenas para o desenvolvimento social e econômico. Porém, Jeffrey Carr, expert em segurança cibernética, identificou quatro

[137] WOLTER, 2013.
[138] *Idem.*
[139] HOLDORF, 2015.

passagens paradoxais que acabaram por rejeitar o Código de Conduta pela ONU. O primeiro é que o Código não encorajava o suporte internacional sobre a execução da lei entre os países. Segundo, a cooperação entre os membros só aconteceria se houvesse ameaça de extremistas políticos ou terroristas[140].

Terceiro, Carr alega que uma das passagens, permite que os Estados prossigam com políticas de censura, enquanto promove a liberdade de expressão. Por fim, o Código não menciona a espionagem cibernética. Em 2015 uma versão atualizada do Código de Conduta foi submetido à ONU para adesão, mas a versão não continha mudanças que fizesse com que os membros considerassem, por isso não se tornou em resolução[141].

Uma das primeiras Conferências a endereçar o crime cibernético e a problemas relacionados à internet foi a Convenção do Conselho Europeu em Crime Cibernético, sendo resultado de quatro anos de trabalho em sua preparação. Realizado em 2001 através do Conselho Europeu e Estados não-membros, como os Estados Unidos, sua estrutura tinha por objetivo analisar uma política comum criminal entre os países para proteger a sociedade do crime cibernético[142]. Desta forma, adota três princípios para a cooperação internacional:

> "1) Cooperação internacional será provida entre os Estados sem limites territoriais; 2) A obrigação de cooperar abrange não somente os crimes estabelecidos no tratado**,** mas também às evidencias de coleção eletrônica relacionadas à ofensa criminal; 3) As disposições sobre a cooperação internacional não precede acordos já existentes nestes assuntos." (WEBER, 2003.)

Estes princípios gerais são endossados através da assistência mútua entre os países, porém não obteve sucesso na participação universal dos membros. A natureza dos crimes cibernéticos cresce consideravelmente, sem mencionar a realização destes. Uma vez que ao tentar incorporar todos os crimes que os membros desejaram, ao invés de criminalizar as atividades, em que haveria um consenso, a Convenção não organizou uma legislação básica para o crime cibernético. Mesmo que houvesse, levaria anos para que todos os países ratificassem, e após isto, só funcionaria se houvesse a participação universal[143].

---

[140] *Idem.*
[141] *Idem.*
[142] WEBER, 2003.
[143] WEBER, 2003.

CONSIDERAÇÕES FINAIS

Ainda que esta seja uma temática internacional recente, a adesão do setor cibernético pelos atores internacionais toma mais destaque nas políticas, estratégias, tomadas de decisão, ações empresariais e da sociedade. Ao tanger a agenda de segurança, o tema parte para uma proposta securitizadora nos anos atuais, em que recursos são alocados para dar capacidade à área. Discursos são realizados, táticas e estratégias são adotadas representando a preocupação com as ameaças cibernéticas e as infraestruturas críticas; conferências e eventos são produzidos para discutir sobre as ramificações da segurança cibernética, desde crimes, jurisdição, governança, defesa e a proteção da sociedade, de forma inclusiva e participativa, tanto dos Estados quanto da sociedade.

No que tange à efetivação de um regime internacional da segurança cibernética ainda não há um consenso, porém códigos já foram propostos, normas sugeridas, aplicação da lei internacional vigorar no espaço cibernético; de forma a acrescentar e trabalhar o tema para um determinante comum. No entanto, a adesão de novos atores faz-se necessária para que o trabalho em conjunto seja realizado e se obtenha um consenso.

O estabelecimento de um regime internacional que regule a segurança cibernética se faz necessário para a manutenção da segurança internacional, seja estatal ou das organizações, como a segurança da sociedade civil. O processo desencadeia de regras internas e cooperação internacional através de compartilhamento de informação e capacidades para o mapeamento de um ambiente suscetível à ameaças. O problema para o estabelecimento destas normas é complicado, por isso se faz fundamental uma articulação entre aliados e parceiros através de uma coordenação global e cooperação.

Porém ações realizadas pelos Estados Unidos e outros países destaca que resta um "futuro online nebuloso" (HENRIQUE NETO, 2014), uma vez que não apenas um país possuía programas e planos de espionagem em outros países, porem que existe tipos de coalizões com outros países, das quais apenas o interesse prevalece quando se trata de invadir ou não informações confidenciais. Tais praticas, repudiadas pela comunidade internacional, constituem o lado obscuro da área cibernética, que por não haver uma legislação internacional ou limites fronteiriços, torna o sistema sensível e susceptível à ações maliciosas.

Entende-se também que apesar das dificuldades encontradas com a formação de normas para o espaço cibernético é provável que um regime seja formado no futuro. Tais regras e normas não se formam do dia para noite. O progresso pode ser a pequenos passos, porém a comunidade internacional pode vir a reconhecer a importância de tal medida e estima-se que encontre um acordo que propicie um regime internacional para a segurança cibernética.

Observa-se ainda que alianças políticas e de seguranças tomam grande visibilidade e aderência. Organizações especializadas em manutenção da paz e segurança internacional tomam o espaço cibernético e suas ameaças como pautas de reuniões, tomando políticas e resoluções plausíveis ao conhecimento sobre o tema, uma vez que este está em constante desenvolvimento, seja para a área militar, política, sustentável ou de governança. Nota-se também a preocupação de incluir as empresas privadas em tais medidas, uma vez que estas possuem grande capacidade de segurança e provem tais recursos para assegurar a estabilidade de indivíduos, empresas, organizações e Estados.

REFERÊNCIAS

Abc das Nações Unidas. UNIC Rio. 2011. Disponível em: < http://unicrio.org.br/img/2011/09/ABC_maio_2011.pdf>

BALZACQ, T. **The Three Faces of Securitization: Political Agency, Audience and Context.** European Journal of International Relations 2005; Vol. 11(2): 171–201

BUTLER, Bob and LACHOW, Irving**. Multilateral Approaches for Improving Global Security in Cyberspace**. Georgetown Journal of International Affairs, International Engagement on Cyber 2012: Establishing Norms and Improving Security (2012).

BUSH, George W. **Statement of Administration Policy: S. 1510 - Uniting and Strengthening America (USA) Act of 2001**. 2001c. Disponível em: <http://www.presidency.ucsb.edu/ws/index.php?pid=25629&st=&st1>

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. **Security: a new framework for analysis.** Lynne Rienner. 1998.

CAVELTY, Mirian Dunn. **Cyber-Security and Threat Politics: US efforts to secure the information age**. Routledge, 2008.

CAVELTY, Myriam Dunn and BRUNNER, Elgin M. **Introduction: Information, Power, and Security – An Outline of Debates and Implications** *in* Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. Ashgate Publishing Company Edited by Myriam Dunn, Victor Mauer, and Sai Felicia Krishna. 2007.

CANABARRO, Diego R. Governança Global da Internet: Tecnologia, Poder e Desenvolvimento. Tese (Doutorado) -- Universidade Federal do Rio Grande do Sul, Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Ciência Política. Porto Alegre-RS, 2014.

CANONGIA, C., MANDARINO JR., R. **Segurança cibernética: o desafio da nova Sociedade da Informação.** Parc. Estrat. Brasília-DF. vol. 14. n. 29. p. 21-46. 2009

CANONGIA, C.; MANDARINO JR., R; GONÇALVES JR., A. **Guia de Referência para a Segurança das Infraestruturas Críticas da Informação**. Gabinete de Segurança Institucional Secretaria Executiva Departamento de Segurança da Informação e Comunicações. Versão 01 – Nov./2010.

CARVALHO, Gustavo Seignemartin de. **Autonomia e Relevância dos Regimes**. Contexto Internacional. Rio de Janeiro, vol. 27, no 2, julho/dezembro 2005, p. 283-329

Challenges to building a safe and secure Information Society in World Information Society Report: Beyond WSIS. International Telecommunication Union, United Nations Conference on Trade and Development. Genebra, 2007

COUNCIL on FOREIGN RELATIONS**. Cyberspace Policy Review ("60 Day Cybersecurity Review").** 2009. Disponível em: <http://www.cfr.org/cybersecurity/cyberspace-policy-review-60-day-cybersecurity-review-may-2009/p19537>

CÚPULA MUNDIAL PARA A SOCIEDADE DA INFORMAÇÃO (2003b) Geneva Plan of Action. Documento n. WSIS-03/GENEVA/DOC/0005. Disponível em: <http://www.itu.int/wsis/docs/geneva/official/poa.html>.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Organização das Nações 1948. Disponível em: <http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf>

DUNN, Myriam; MAUER, Victor; KRISHNA-HENSEL, Sai Felicia. Power and Security in the information age : investigating the role of the state in cyberspace. Ashgate. 2007.

EUROPEAN COMMISSION. Internet Governance Principles. NETMundial. 2014. Disponível em: http://content.netmundial.br/contribution/internet-governance-principles/176

FORUM (IGF). **About the IGF**. 2015. Disponível em: <http://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf>.

Freedom Online Coalition. Cybersecurity and the United Nations. An Internet Free and Secure.
Disponível em: <https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/cybersecurity-and-united-nations/>. Acessado em: 19/01/2017.

G1.COM. **Estônia protagoniza primeira guerra virtual** *in* New York Times por Mark Landler e John Markoff, traduzido por Cláudia Freire. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL45961-6174,00.html>.

GENERAL ASSEMBLY OF THE UNITED NATIONS. First, Second and Third Commitee. Disponível em: <http://www.un.org/en/ga/>

Geneva Internet Platform. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Dispoível em: http://giplatform.org/actors/united-nations-group-governmental-experts-developments-field-information-and. Acessado em: 13/01/2017

GJELTEN, Tom. SHADOW WARS: Debating Cyber 'Disarmament'. World Affairs, Vol. 173, No. 4. 2010

GRIMES, Roger A. **Stop 80 percent of malicious attacks now.** InfoWorld. 2013. Disponível em: http://www.infoworld.com/article/2611443/security/stop-80-percent-of-malicious-attacks-now.html

GREENWALD, Glenn. **Sem lugar para se esconder**. 2014. Traduzido por Fernanda Abreu. Rio de Janeiro: Sextante, 2014

GREENWALD, Glenn, MACASKILL, Ewen. **NSA Prism program taps in to user data of Apple, Google and others**. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

HAFTENDORN, H. **The Security Puzzle: Theory-Building and Discipline-Building in International Security**. International Studies Quarterly, Vol. 35, No. 1 (Mar., 1991), p. 3-17

HANSEN, L; NISSENBAUM, H. **Digital Disaster, Cyber Security, and the Copenhagen School**. International Studies Quarterly, Vol. 53, No. 4, 2009, p. 1155-1175

HATHAWAY, Melissa E. **Toward a Closer Digital Alliance**. SAIS Review of International Affairs, Volume 30, Number 2, Summer-Fall 2010, pp. 21-31

HOLDORF, Polly M. **Prospects for an International Cybersecurity Regime.** US Air Force Institute for National Security Studies. 2015

HENRIQUE NETO, Sylvio. **A Resposta Brasileira à Espionagem Americana – O Conflito Entre Soberania, Segurança Nacional e Liberdades Civis**. 2º Seminário de Relações Internacionais: Graduação e Pós-graduação. 2014.

INTERNATIONAL TELECOMMUNICATION UNION. About ITU. 2017. Disponível em: <http://www.itu.int/en/about/Pages/overview.aspx>. Acesso em 30/06/2017

INTERNET GOVERNANCE FORUM. **Enhancing Cybersecurity and Building Digital Trust**. Main Meeting Hall. Transcriptions. 2015b. Disponível em: http://www.intgovforum.org/cms/187-igf-2015/transcripts-igf-2015/2884-2015-11-12-enhancing-cybersecurity-and-building-digital-trust-main-meeting-hall-finished.

_____. **Internet Governance Forum**. United Nations 2010-2016. Disponível em: < https://www.intgovforum.org/multilingual/>

_____. **IGF 2015**. United Nations. 2015. Disponível em: http://www.intgovforum.org/multilingual/content/igf-2015-4.

KEOHANE, Robert O. **The demand for international regimes**. International Organization. 1982. vol. 36, issue 02, pages 325-355

_____. (1993), **Instituciones Internacionales y Poder Estatal**. Buenos Aires, Grupo Editor Latinoamericano.

KRAMER, Franklin D. **Cyber Security: An Integrated Governmental Strategy For Progress**. Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity (2011), p. 136-150.

KRASNER, Stephen D. **Causas Estruturais e Consequências dos Regimes Internacionais: Regimes Como Variáveis Intervenientes**. Rev. Sociol. Polít., Curitiba, v. 20, n. 42, p. 93-110, jun. 2012

_____. **Communications and National Power: Life on the Pareto Frontier**. World Politics, Vol. 43, No. 3 (Apr, 1991), pp. 336-366, 1991

MARKS, Joseph. **U.N. body agrees to U.S. norms in cyberspace**. Politico. 2015. Disponível em: <http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900>. Acessado em 18/01/2017

MALCOLM, Jeremy. Multi-stakeholder governance and the Internet Governance. First Edition. Terminus Press. 2008

MAURER, T. **Cyber Norm Emergence at the United Nations – An Analysis of the UN‘s Activities Regarding Cyber-security?.** Discussion Paper 2011-11, Cambridge,

Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

MINISTRY OF SECURITY AND JUSTICE. **The National Cyber Security Strategy (NCSS) - Strength through cooperation**. 2011. Disponível em: <http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011/view>. Acesso em: 04/08/2017

Model United Nations. How Decisions are Made at the UN. http://outreach.un.org/mun/guidebook/introduction/how-decisions-are-made-at-the-un/

MUELLER, Milton L. Networks and states: the global politics of internet governance. Massachusetts Institute of Technology. 2010.

NATO CCDCOE. **ASEAN to Focus on Cybersecurity Capacity- and Confidence-Building in 2017**. 2016. Disponivel em: <https://ccdcoe.org/asean-focus-cybersecurity-capacity-and-confidence-building-2017.html>. Acesso em: 04/08/2017.

NISSENBAUM, H. **Where Computer Security Meets National Security**. Ethics and

Information Technology. 2005, Volume 7, Issue 2, p 61–73.

NEAL, Andrew W. **Exceptionalism and the politics of counter-terrorism: liberty, security, and the War on Terror.** Routledge. 1978.

NYE, J. S., JR. (1988) Problems of Security Studies. Paper presented at the XIV World Congress of the International Political Science Association, Washington, DC, August.

_____. **The Regime Complex for Managing Global Cyber Activities**. Centre for International Governance Innovation. Paper Series: N. 1 — may 2014

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **IGF Brochure**. About the IGF. 2014. Disponível em: < http://intgovforum.org/cms/2014/IGFBrochure.pdf>

_____. Report of the Working Group on Internet Governance. 2005. Disponível em: http://www.wgig.org/docs/WGIGREPORT.pdf.

_____. **THE INTERNET GOVERNANCE**

PYATI, Ajit K. WSIS: Whose vision of an information society? *First Monday*, Volume 10, Number 5. 2005. Disponível em: http://uncommonculture.org/ojs/index.php/fm/article/view/1241.

TAURECK, Rita. **Securitisation Theory and Securitisation Studies**. Journal of International Relations and Development, pp. 53-6. 2006.

THE WHITE HOUSE. **International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World**. 2011. Disponível em: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

THE WHITE HOUSE. **The Comprehensive National Cybersecurity Initiative**. 2008. Disponível em: <https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf>

THE WHITE HOUSE. **The National Strategy to Secure Cyberspace.** February 2003

THE WHITE HOUSE. **Remarks by the President on Securing Our Nation's Cyber Infrastructure.** 2009. Disponível em: <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. Developments in the Field of Information and Telecommunications in the Context of International Security. Fact Sheet. 2015.

United Nations Association of the United States of America. Sponsors and Signatories. Disponível em: <http://www.unausa.org/global-classrooms-model-un/how-to-participate/model-un-preparation/resolutions/sponsors-and-signatories>

United Nations. **NATO Cooperative Cyber Defence Centre of Excellence**. Organisations. Disponível em: https://ccdcoe.org/un.html. Acessado em :05/01/2016

United Nations General Assembly. A/RES/55/63. Combating the criminal misuse of information Technologies. Fifty-fifth session, Third Committee. 2000. Disponível em: https://ccdcoe.org/sites/default/files/documents/UN-001204-CriminalMisuseIT.pdf. Acessado em: 16/01/2017.

_____. A/RES/68/167. The right to privacy in the digital age. Sixty-eighth session, Third Committee. 2013. Disponível em: <https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf.> Acessado em: 16/01/2017.

_____. A/RES/56/121. Combating the criminal misuse of information technologies. Fifty-sixth session, Third Committee. 2001. Disponível em: https://ccdcoe.org/sites/default/files/documents/UN-011219-CriminalMisuseIT.pdf. Acessado em: 16/01/2017.

_____. A/HRC/RES/20/8. The promotion, protection and enjoyment of human rights on the Internet. Twentieth session, Human Rights Council. 2011. Disponível em: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/RES/20/8&Lang=E. Acessado em: 16/01/2017

_____. A/RES/54/49. Developments in the field of information and telecommunications in the context of international security. Fifty-fourth session. 1998. Disponível em: < https://ccdcoe.org/sites/default/files/documents/UN-991201-ITIS.pdf >. Acessado em: 05/01/2016

_____. A/RES/56/19. Developments in the field of information and telecommunications in the context of international security. Fifty-sixth session. 2001. Disponível em: < https://ccdcoe.org/sites/default/files/documents/UN-011129-ITIS.pdf >

_____. A/RES/57/239. Creation of a global culture of cybersecurity. Fifty-seventh session, Second Committee. 2002. Disponível em: https://ccdcoe.org/sites/default/files/documents/UN-021220-CultureOfCS.pdf. Acessado em: 16/01/2017.

_____. A/RES/58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures. Fifty-eighth session, Second Committee. 2003. Disponível em: https://ccdcoe.org/sites/default/files/documents/UN-031223-CultureOfCandCI.pdf. Acessado em: 16/01/2017.

_____. A/RES/64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. Sixty-fourth session, Second Committee. 2009. Disponível em: https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf. Acessado em: 16/01/2017.

_____. Continuation of the Internet Governance Forum – Note by the Secretary-General. Doc. N. A/65/78–E/2010/68. 2010. Disponível em: <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan039400.pdf>.

_____. **World Summit on the Information Society**. Fifty-sixth session. Doc. N. A/RES/56/183. 2002. Disponível em: http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf.

_____. **World Summit on the Information Society.** Sixtieth session. Doc. N. A/RES/60/252. 2006. Disponível em: <http://www.itu.int/en/wtisd/Pages/res60-252.aspx>

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. Developments in the Field of Information and Telecommunications in the Context of International Security. Fact Sheet. 2015.

WEBER, Amalie M. **The Council of Europe's Convention on Cybercrime**. Berkeley Technology Law Journal, Vol. 18, No. 1, Annual Review of Law andTechnology .2003. p. 425-446

WILLIAMS, Michael C. **Words, Images, Enemies: Securitization and International Politics.** International Studies Quarterly, pp. 511–531. 2003.

WOLTER, Detlev. **The UN Takes a Big Step Forward on Cybersecurity**. Arms Control Today, Vol. 43, No. 7. 2013. p. 25-29

ANEXO – ***Creation of a global culture of cybersecurity***

.....

General Assembly Resolution 57/239

Creation of a global culture of cybersecurity

The General Assembly, […] *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity […]

78th plenary meeting

20 December 2002

Annex

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks (―participants‖) must approach cybersecurity. A global culture of cybersecurity will require that al l participants address the following nine complementary elements:

(*a*) *Awareness.* Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(*b*) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(*c*) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implemente procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(*d*) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(*e*) *Democracy*. Security should be implemented in a manner consistente with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(*f*) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad - based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(*g*) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(*h*) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants‘ activities and all aspects of their operations;

(*i*) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

ANEXO – ***Self-assessment tool critical information infrastructure protection***

.....

General Assembly Resolution 64/211
Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

The General Assembly, […] *Invites* Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity, so as to highlight areas for further action, with the goal of increasing the global culture of cybersecurity […]

66th plenary meeting
21 December 2009

Annex

Voluntary self-assessment tool for national efforts to protect critical information infrastructures

Taking stock of cybersecurity needs and strategies

1. Assess the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.

3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present and the current management plan; note how changes in the economic environment, national security priorities and civil society needs affect these calculations.

4. Determine the goals of the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives and how such a strategy fits within regional and international initiatives.

Stakeholder roles and responsibilities

5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

• National Government ministries or agencies, noting primary points of contact and responsibilities of each;

• Other government (local and regional) participants;

• Non-governmental actors, including industry, civil society and academia;

• Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

Policy processes and participation

6. Identify formal and informal venues that currently exist for Government - industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

7. Identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

Public-private cooperation

8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information-sharing and incident management.

9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

Incident management and recovery

10. Identify the Government agency that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

11. Separately, identify national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident - management information.

12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

Legal frameworks

13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

Developing a global culture of cybersecurity

18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.