ELIANE SALDAN

OS DESAFIOS JURÍDICOS DA GUERRA NO ESPAÇO CIBERNÉTICO

Dissertação apresentada como requisito para a obtenção do título de Mestre em Direito Constitucional, no Curso de Pós-Graduação *Strictu Sensu* do Instituto Brasiliense de Direito Público – IDP.

Orientador: Prof. Dr. Marcio Pereira Pinto Garcia.

Brasília – DF

2012

ELIANE SALDAN

OS DESAFIOS JURÍDICOS DA GUERRA NO ESPAÇO CIBERNÉTICO

Dissertação apresentada como requisito para a obtenção do título de Mestre em Direito Constitucional, no Curso de Pós-Graduação Strictu Sensu do Instituto Brasiliense de Direito Público – IDP.

Aprovada pelos membros da banca examinadora em 16/10/2012.

Banca Examinadora:

_____

Presidente: Prof. Dr. Marcio Pereira Pinto Garcia

_____

Integrante: Prof. Dr. Paulo José Leite de Farias

_____

Integrante: Prof. Dr. Joanisval Brito Gonçalves

RESUMO

O assunto da dissertação é a regulamentação da guerra cibernética. O objetivo da pesquisa foi examinar se os ataques cibernéticos constituem armas de guerra, bem como verificar a adequação dos atuais paradigmas do *jus in bello* e do *jus ad bellum* para disciplinar os conflitos no espaço cibernético, o palco de batalha do Século XXI que abriga infraestruturas críticas. Foi possível constatar que a aplicação das atuais regras da Carta da ONU e do Direito Internacional Humanitário exige critérios técnicos seguros para determinar a autoria e a origem de um ataque, bem como a necessidade e a proporcionalidade da resposta. Também foi possível verificar que, a despeito da inexistência de uma regulamentação específica, o Direito de Genebra, da Haia e de Nova Iorque, bem como os princípios, usos e costumes do Direito Internacional, a Cláusula Martens, os tratados e as normas internas servem para disciplinar a guerra cibernética, em especial no que diz respeito à proteção de bens e pessoas civis. Os principais limites são o princípio da distinção, da precaução e da vedação de ataques indiscriminados. Além disso, a participação direta de civis em hostilidades no espaço cibernético, se não balizadas pelas regras dos conflitos armados, pode acarretar a prática de crimes de guerra, sujeitos às jurisdições nacionais e à jurisdição do Tribunal Penal Internacional (observado o princípio da subsidiariedade), cujo Estatuto poderá, futuramente, ser alterado para incluir expressamente as armas e hostilidades cibernéticas. Enquanto não for possível um consenso internacional a respeito da guerra cibernética, além do Conselho de Segurança da ONU, o Comitê Internacional da Cruz Vermelha e a Corte Internacional de Justiça (embora sua vocação seja outra) podem exercer suas atribuições de interpretação para elucidar dúvidas e minimizar as lacunas a respeito das normas para a guerra cibernética.

PALAVRAS-CHAVE: Guerra Cibernética. Armas Cibernéticas. Carta da ONU. Direito Internacional Humanitário. Princípios. Usos e Costumes da Guerra. Cláusula Martens. Tribunal Penal Internacional.

ABSTRACT

The theme of the approach is the regulation of cyberwar. The objective of this research was to determine whether the cyber attacks are weapons of war, and to verify the adequacy of current paradigms of *jus in bello* and *jus ad bellum* to regulate conflicts in cyberspace, the scene of the battle of the XXI Century which houses critical infrastructures. It was found that the application of current rules of the UN Charter and International Humanitarian Law requires insurance technical criteria to determine the authorship and source of an attack, as well as the necessity and proportionality of the response. It was also observed that, despite the absence of specific regulations, the Law of Genebra, The Hague and New York and the principles, practices and customs of international law, the Martens Clause, international treaties and national norms serve to regulate the cyberwar, in particular as regards the protection of property and civilians. The main limits are the principle of distinction, precaution and sealing of indiscrimate attacks. Furthermore, the direct participation of civilians in hostilities in cyberspace, if not buoyed by the rules of armed conflict, can lead to crimes of war, subject to national jurisdiction and the jurisdiction of the International Criminal Court (observing the principle of subsidiarity) whose Statue may eventually be changed to explicitly include weapons and cyber hostilities. While it is not possible an international consensus about the cyber war, the International Committee of the Red Cross, the International Court of Justice (although its institutional role is another) and UN Security Council may exercise their powers of interpretation to clarify doubts and to minimize the gaps concerning the standards for cyber warfare.

KEYWORDS: Cyber War. Cyber Weapons. The UN Charter. International Humanitarian Law. Principles. Habits and Customs of War. Martens Clause. International Criminal Court.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	- Associação Brasileira de Normas Técnicas.
AC Raiz	- Autoridade Certificadora Raiz.
ACS	- Alcântara Cyclone Space.
AfriNIC	- African Network Information Centre.
ANATEL	- Agência Nacional de Telecomunicações.
APNIC	- Asia-Pacific Network Information Centre.
ARIN	- American Registry for Internet Numbers.
ARP	- Advanced Research Projects
ARPA	- Advanced Research Projects Agency.
BGP	- Border Gateway Protocol.
B2B	- business-to-business.
B2C/C2B	- business-to-consumer / consumer-to-business.
B2G/G2B	- business-to-government / government-to-business.
CCOMGEX	- Centro de Comunicações e Guerra Eletrônica do Exército.
ccTLD	- country code top level domain.
CDCiber	- Centro de Defesa Cibernética.
CDCFA	- Comando de Defesa Cibernética das Forças Armadas.
CIGE	- Centro de Instrução de Guerra Eletrônica.
CLA	- Centro de Lançamento de Alcântara.
CMSI	- Cúpula Mundial sobre a Sociedade da Informação.
CGI.br	- Comitê Gestor da Internet no Brasil.
CGSI	- Comitê Gestor de Segurança da Informação.
CIA	- Central Intelligence Agency
C2C	- consumer-to-consumer.
COBIT	- Common Objectives For Information and Related Technology.
DARPA	- Defense Advanced Research Projects Agency.
DCTA	- Departamento de Ciência e Tecnologia Aeroespacial.
DNS	- Domain Name
DPN	- Top Level Domain

DSICGSI	- Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.
ENISA	- European Network and Information Security Agency.
EsNaDCiber	- Escola Nacional de Defesa Cibernética.
EU	- União Europeia
FBI	- Federal Bureau of Investigation
FISA	- Foreign Intelligence Surveillance Act.
FIX	- Ponto Federal de Interconexão de Redes.
FTP	- File Transfer Protocol
GSI / PR	- Gabinete de Segurança Institucional da Presidência da República.
G2C/C2G	- government-to-consumer / consumer-to-government.
GTGI	- Grupo de Trabalho sobre a Governança da Internet.
gTLD	- generic top level domain.
G2G	- government-to-government.
HTTP	- HyperText Transfer Protocol
IAB	- Internet Architecture Board.
IAE	- Instituto de Aeronáutica e Espaço.
IANA	- Internet Assigned Numbers Authority.
ICANN	- Internet Corporation for Assigned Names and Numbers.
ICCB	- Internet Configuration Control Board.
ICP Brasil	- Infraestrutura de Chaves Públicas Brasileira.
IEEE	- Institute of Electrical and Electronics Engineers.
IETF	- Internet Engineering Task Force.
IGF	- Fórum sobre Governança da Internet.
IP	- Internet Protocol
IPng	- Internet Protocol next generation.
IPSec	- Internet Protocol Security
IPv4	- Internet Protocol version 4
IPv6	- Internet Protocol version 6
IRTF	- Internet Research Task Force.
ISO	- International Standard Organization.
ISOC	- Internet Society.

ISPs	- Internet Service Providers.
ITA	- Instituto Tecnológico de Aeronáutica.
ITI	- Instituto Nacional de Tecnologia da Informação.
ITIL	- IT Infrastructure Library.
IW	- Information Warfare.
LACNIC	- Latin American and Caribbean Internet Addresses Registry.
LICC	- Lei de Introdução ao Código Civil.
MAG	- Multistakeholder Advisory Group (grupo de aconselhamento).
NASA	- National Aeronautics and Space Administration
NAT	- Network Address Translation.
NIST	- National Institute of Standards and Technology.
NSF	- National Science Foundation.
Nu CDCiber	- Núcleo do Centro de Defesa Cibernética.
OCDE	- Organização para a Cooperação e Desenvolvimento Econômico.
OEA	- Organização dos Estados Americanos.
ONU	- Organização das Nações Unidas.
OSI	- Open System Interconnection.
OTAN	- Organização do Tratado do Atlântico Norte.
PIPA	- Protect IP Act.
PNBL	- Programa Nacional de Banda Larga.
PNSIEC	- Política Nacional de Segurança das Infraestruturas Críticas.
PNUD	- Programa das Nações Unidas para o Desenvolvimento.
RARP	- Reverse Address Recognition Protocol
RENAF	- Rede Nacional de Fibras Óticas.
RFCs	- requests for coments.
RIP	- Remote Imaging Protocol
RIPE NCC	- Réseaux IP Européens Network Coordination Centre.
RIR	- Regional Internet Registry (Registro Regional de Internet).
RNP	- Rede Nacional de Ensino e Pesquisa.
SGB	- Satélite Geoestacionário Brasileiro.

SGTSIC - PEGANCOR	- Subgrupo Técnico de Segurança de Infraestruturas Críticas de Petróleo, Gás Natural e Combustíveis Renováveis.
SIVAM	- Sistema de Vigilância da Amazônia.
SIPAM	- Sistema de Proteção da Amazônia.
SISBIN	- Sistema Brasileiro de Inteligência.
SISDABRA	- Sistema de Defesa Aeroespacial Brasileiro.
SISFRON	- Sistema Integrado de Monitoramento de Fronteiras.
SISGAAZ	- Sistema de Gerenciamento da Amazônia Azul.
SOPA	- Stop Online Piracy Act.
STFC	- Serviço Telefônico Fixo Comutado
SVA	- Serviços de Valor Adicionado.
TCP	- Transmission Control Protocol
TCP/IP	- Transmission Control Protocol / Internet Protocol.
TI	- Tecnologia da Informação
TICs	- Tecnologias de Informação e Comunicação.
TLD	- Top Level Domain.
UDP	- User Datagram Protocol
UIT	- União Internacional de Telecomunicações.
USCYBERCOM	- United States Cyber Command.
VLS-1	- Veículo Lançador de Satélites 1.
WWW ou W3	- World Wide Web.
W3C	- World Wide Web Consortium.

SUMÁRIO

1 INTRODUÇÃO

A paz e a segurança internacionais são pilares do cenário de aprimoramento e exercício dos direitos humanos, das liberdades fundamentais, da autodeterminação e do desenvolvimento econômico, social e cultural dos povos. Todavia, não obstante os esforços para a preservação da paz e para a solução pacífica de controvérsias, a guerra sempre ocupou espaço nos diversos capítulos da evolução da humanidade, os quais continuam sendo escritos e impulsionados por outros protagonistas e objetivos, acompanhados de novas armas que desafiam a construção de novas estratégias e regras.

A Constituição da República Federativa do Brasil estabelece, desde o seu preâmbulo, o compromisso do Brasil de promover a solução pacífica das controvérsias na ordem interna e internacional, além de enumerar os princípios que regem as relações internacionais, como a autodeterminação dos povos, a não intervenção e a defesa da paz.

No plano ideal, a dinâmica das relações internacionais é regida por regras diplomáticas e jurídicas arquitetadas ao longo da marcha histórica com o objetivo de assegurar uma convivência amistosa entre os povos e entre as nações, bem como viabilizar fórmulas de solução pacífica para conflitos e controvérsias. Para as situações em que tais regras não são capazes de harmonizar interesses, também foram elaboradas normas para o uso da força nas situações autorizadas pela Carta da ONU.

A guerra, que sempre foi objeto de investigação doutrinária, pode ser definida por conceitos diversos, tais como o militar e o jurídico, os quais não esgotam o alcance da expressão, mas permitem concluir que se trata do uso da força, tolerado legalmente e limitado por regras que objetivam minimizar os nefastos efeitos da guerra, em especial para a população civil. Tais critérios estão previstos

em tratados, princípios, usos e costumes do Direito Internacional e também no Direito de Genebra, de Haia e de Nova Iorque, cujas violações podem configurar crimes de guerra tipificados no Estatuto de Roma.

Ocorre que o marco legal existente não foi pensado para os conflitos no espaço cibernético - o qual abriga infraestruturas críticas, sendo regido essencialmente por regras técnicas e não jurídicas - que além de se tornar estratégico para todos os países, também está se tornando o teatro de operações do Século XXI, palco de novas batalhas que desconhecem fronteiras e dificultam a identificação da autoria, trazendo intrincados desafios à segurança e à defesa do território e da soberania em razão do seu caráter transnacional e do entrelaçamento de diversos ordenamentos jurídicos pela dinâmica de funcionamento.

Além disso, por razões óbvias, a cooperação internacional que existe para a investigação e para o combate aos crimes e ao terrorismo no espaço cibernético tende a não funcionar quando os ataques cibernéticos forem protagonizados pelos próprios Estados.

Embora não existam definições e doutrinas consolidadas, muito menos normas jurídicas atualizadas na seara de guerra cibernética, os países já estão desenvolvendo estruturas de inteligência e de diplomacia cibernética, novas estratégias de segurança, defesa e ataque para o espaço cibernético, inclusive porque alguns episódios já foram suficientes para evidenciar não apenas as vulnerabilidades, mas o efetivo potencial das ameaças cibernéticas para desafiar a segurança dos países e estremecer as relações internacionais.

O que se verifica nos dias atuais é uma verdadeira corrida armamentista no espaço cibernético, pois a despeito da inexistência de uma regulamentação internacional, diversos países, inclusive o Brasil, estão se preparando para a guerra cibernética – o que é bastante preocupante quando se considera que a evolução jurídica não consegue acompanhar a rapidez das evoluções tecnológicas que podem ser utilizadas na guerra cibernética.

A despeito da importância do assunto para o futuro das relações internacionais, a complexidade que o envolve explica porque o tema está na pauta

da agenda mundial, porém, em estágio embrionário e longe da construção de um consenso entre os países. É fundamental e inadiável que a comunidade acadêmica e a sociedade internacional amadureçam os conceitos jurídicos e técnicos para a regulamentação da guerra cibernética.

Conforme Ramos (2009, p. 150)[1], "quando não há a compreensão da realidade de um objeto ou fenômeno, fica evidente que o caminho a perseguir é desvendá-lo." Para o mesmo autor, quando os conhecimentos sobre um assunto são insuficientes para explicar um fenômeno, então surge o problema – como se verifica com a guerra cibernética e suas implicações para o Direito Internacional.

Com o intuito de delimitar as lacunas normativas e contribuir para a sua superação, o trabalho objetiva analisar os novos paradigmas dos conflitos no espaço cibernético para verificar se os ataques cibernéticos podem ser considerados novas armas de guerra, bem como verificar em que medida as atuais normas podem ser aplicadas e se são suficientes para estabelecer limites e responsabilidades para a guerra cibernética, levando em conta o funcionamento e o caráter transnacional do espaço cibernético.

Para melhor estruturar as ideias e indagações que precisam ser feitas, o primeiro capítulo irá esclarecer a dinâmica do espaço cibernético, seu caráter transnacional e as principais estruturas de governança por atores estatais e não estatais, bem como as estruturas governamentais de defesa criadas no Brasil para a segurança de suas infraestruturas críticas e do seu espaço cibernético.

A partir da descrição do "campo" da guerra cibernética, ela será conceituada e diferenciada dos demais tipos de conflitos desencadeados no espaço cibernético, distinção que também pode ser extraída de diversos estudos realizados por empresas de segurança e estratégias de defesa divulgadas pelos países e órgãos internacionais; além disso, serão noticiados alguns dos muitos episódios verídicos que serviram de alerta para os países.

---

[1] RAMOS, Albenides. *Metodologia da pesquisa científica: como uma monografia pode abrir o horizonte do conhecimento.* p. 150.

Após a compreensão do espaço cibernético e dos conflitos que ele abriga, o trabalho será concluído com um capítulo dedicado a visitar as principais normas que regem os conflitos armados, verificando-se em que medida elas podem ser aplicadas ou devem ser repensadas para a guerra cibernética, verificando os desafios operacionais e jurídicos que ocupam o centro das atenções de estrategistas e juristas do mundo inteiro.

2 O ESPAÇO CIBERNÉTICO

A expressão espaço cibernético[2] comporta diversos sentidos e definições. Para os propósitos do trabalho, não serão objeto de investigação a sua evolução histórica e os conceitos técnicos, mas apenas os aspectos estruturais, funcionais e operacionais da arquitetura e do conteúdo na medida necessária para visualizar, além da ausência de fronteiras no espaço cibernético, como os diversos atores interagem em tal dinâmica.

Tais noções são relevantes para compreender como podem ser utilizadas as ferramentas de ataque e defesa no espaço cibernético, especificamente aquelas voltadas às infraestruturas críticas, por intermédio da rede mundial de computadores[3], celulares, *tablets* e demais *gadgets* e tecnologias que viabilizam a interação em tal ambiente, bem como para verificar se os conflitos cibernéticos podem ser regidos pelas atuais normas ou se elas devem ser repensadas para a nova realidade, o que será feito nos capítulos subsequentes.

Valendo-se de estruturas e sistemas de armazenamento, disponibilização e transmissão de dados (imagens, sons, vídeos e informações em diversos formatos), que podem circular por satélites, rádio, redes de telefonia e energia elétrica ou cabos de fibra ótica que interligam os mais diversos cantos do planeta, novas funcionalidades e novos modelos de negócios são desenhados diariamente para o

---

[2] A expressão *cyberspace* é atribuída a William Gibson e foi cunhada na obra de ficção *Neuromancer,* publicada em 1984, em Nova Iorque, pela Editora Ace Books. Compõe uma trilogia e explora a relação entre o homem e a máquina; recebeu os principais prêmios de produção literária de ficção científica e serviu de base para o filme Matrix, no qual o ator Keanu Reaves entra no ciberespaço e conecta seu sistema nervoso central a um computador.

[3] A palavra Internet (*Interconnected Networks / Internetwork System*), utilizada como nome próprio, se refere ao conjunto de todas as redes, à rede global e pública, o conglomerado de redes de computadores interligadas por protocolos de comunicação (TCP/IP), enquanto internet com letra minúscula é sinônimo de redes particulares de computadores interligando empresas, universidades, residências. A diferença ganhou relevância em 2006, na Conferência da União Internacional de Telecomunicações – UIT, da ONU, realizada na Turquia, quando a delegação norte-americana recusou a grafia com letra minúscula, a qual poderia representar que a Internet seria apenas mais um sistema de telecomunicações, como rádio ou telefone, que estaria no âmbito de regulação da UIT. Disponível em: <http://pt.wikipedia.org/wiki/Internet>. Acesso em: 24 fev. 2012.

espaço cibernético, definido como “um terreno onde está funcionando a humanidade hoje” (LÉVY, 1996)[4].

As relações econômicas, jurídicas e sociais (afetivas, educacionais, familiares, interpessoais e profissionais), bem como as funcionalidades do espaço cibernético estão em constante reconfiguração, orientada pela crescente cultura da conectividade, convergência, instantaneidade e interatividade de portais, *blogs* e redes sociais, que se multiplicam em progressão geométrica, enquanto as tentativas de regramento sequer estão em progressão aritmética.

Assim, ocorre a migração das atividades do governo eletrônico e do comércio eletrônico de produtos e serviços, com a facilidade de aproximar cidadãos, usuários, consumidores e fornecedores de qualquer ponto do planeta. A propósito, foi sugerida uma divisão do comércio eletrônico por Tadao Takahashi (2000, p.18)[5]. Em tal cenário, uma espécie de democracia digital e uma nova *e-lex mercatoria* estão impulsionando o comércio internacional virtual dos mais diversos produtos, serviços e conteúdos para entretenimento, publicidade, trocas, leilão ou oferta de informações, produtos e serviços de todas as espécies, com ou sem intuito lucrativo, como os *sites* colaborativos, de relacionamento e as redes sociais. Da mesma forma, a telefonia móvel, o comércio móvel ou sem fio (*m-commerce* ou *mobile commerce*, *w-commerce* ou *wireless commerce*) também fomentam a economia digital, que ainda será incrementada pela maior interatividade da TV digital ou conectada, com as *smart TVs*.

---

[4] LÉVY, Pierre. *O que é o virtual?*
O “profeta digital” é considerado antropólogo e filósofo do espaço cibernético, é autor de diversas outras obras sobre o tema: A Máquina Universo, A Árvore do Conhecimento, Cibercultura, Conexão Planetária, A Inteligência Coletiva, As tecnologias da inteligência: o futuro do pensamento na era da informática.

[5] TAKAHASHI, Tadao. *Sociedade da informação no Brasil.* p. 18.
Não obstante a variada gama de funcionalidades, formatadas e reinventadas diariamente, divide-se o comércio eletrônico (*e-commerce*) em algumas vertentes:
- B2B (*business-to-business*): transações entre empresas (exemplos: EDI, portais verticais de negócios);
- B2C/C2B (*business-to-consumer* / *consumer-to-business*): transações entre empresas e consumidores (exemplos: lojas e *shoppings* virtuais);
- **B2G/G2B** (*business-to-government* / *government-to-business*): transações envolvendo empresas e governo (exemplos: EDI, portais, compras);
- **C2C** (*consumer-to-consumer*): transações entre consumidores finais (exemplos: *sites* de leilões, classificados *on-line*);
- **G2C/C2G** (*government-to-consumer* / *consumer-to-government*): transações envolvendo governo e consumidores finais (exemplos: pagamento de impostos, serviços de comunicação);
- **G2G** (*government-to-government*): transações entre governo e governo.

Na leitura de Castells (2002, p. 41)[6] a respeito de tal cenário, “nossas sociedades estão cada vez mais estruturadas em uma oposição bipolar entre a Rede e o Ser”, caminhando para uma confusão estrutural entre função e significado. Tal pensamento resume o turbilhão de mudanças paradigmáticas em curso.

A célebre frase “o código é a lei” de Lessig (2006, p.1)[7], professor conhecido como arquiteto da rede, exprime o potencial da configuração da rede mundial de computadores para definir padrões de conduta, ao mesmo tempo em que evidencia que o ambiente cibernético é regido essencialmente por regras técnicas e não jurídicas.

Uma nova percepção do tempo, do espaço, dos valores e dos bens materiais parece delinear o cenário de uma aldeia global eletrônica sequer imaginada por McLuhan (1969)[8], com incontáveis desdobramentos jurídicos decorrentes da desconfiguração das tradicionais barreiras geográficas e da migração das atividades humanas para a chamada realidade virtual, suscitando temas desafiadores e motivadores da construção de novos raciocínios, particularmente quando a solução de controvérsias e conflitos não pode se valer das tradicionais fórmulas.

A integração de diferentes ordenamentos jurídicos em razão do caráter transnacional da rede mundial de computadores permite vislumbrar a dimensão das intrincadas questões jurídicas que podem surgir.

As bases da sociedade da informação[9] estão alicerçadas no espaço cibernético, que, por tal razão, se tornou estratégico para todos os países, algo que não era previsto na gestação da rede mundial de computadores, criada na década de 60 com propósitos militares pela ARPA – Advanced Research Projects Agency do

---

[6] CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura.* p. 41.

[7] LESSIG, Laurence. *Code.* p. 1. Disponível em: <http://codev2.cc/download+remix/Lessig-Code v2.pdf>. Acesso em: 24 fev. 2012.

[8] Herbert Marshall McLuhan, filósofo canadense considerado o profeta da globalização, cunhou a expressão “aldeia global” e escreveu o livro “O meio é a mensagem”, Rio de Janeiro: Record, 1969.

[9] O conceito de Sociedade da Informação também é plurívoco e a adjudicação de sentidos depende da perspectiva considerada, podendo passar pela leitura estrutural, sociológica, política, econômica, etc. De todas as perspectivas, pode ser extraído um denominador comum: a sociedade da informação está interligada em redes para as mais diversas finalidades, na qual a informação é recurso de poder.

Departamento de Defesa dos Estados Unidos para permitir a troca e compartilhamento de informações de forma descentralizada, em plena Guerra Fria, assim evitando possível colapso no caso de catástrofe ou de um ataque nuclear da então União Soviética, o qual jamais ocorreu.

Desde então, houve o aprimoramento e a ampliação da sua utilização para o meio acadêmico e depois comercial, porém sem qualquer plano inicial de gestão em escala mundial, muito menos com a abertura para outros governos ou setor privado, o qual se tornou protagonista fundamental para o desenvolvimento do espaço cibernético.

No Brasil, a Internet recebeu a primeira definição em 1995, quando o Ministério das Comunicações instituiu a utilização comercial, atribuindo-lhe o nome genérico que designa o conjunto de redes ou meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o *software* e os dados contidos nestes computadores.

De acordo com o Relatório do Fórum Econômico Mundial de 2010, que avalia o ambiente empresarial, o regulatório e de infraestrutura, o Brasil ocupa a 33ª posição no índice que mede o uso de ferramentas de TI (Tecnologias de Informação) por governos e a 56ª posição em relação à influência da tecnologia para o desenvolvimento e a competitividade. Dados estatísticos divulgados pelo Comitê Gestor da Internet apontam que 2,37 milhões de domínios foram registrados no primeiro semestre de 2011, o que coloca o Brasil na 7ª posição[10].

O Brasil deverá se tornar o quarto maior mercado do comércio eletrônico até 2015; estima-se que as vendas no *e-commerce* nacional devem chegar a R$18,7 bilhões em 2011[11]. Nos poderes Executivo, Legislativo e Judiciário são utilizadas ferramentas tecnológicas para a gestão e prestação de serviços públicos[12], assim como em todos os níveis de governo – federal, estadual, distrital e municipal – existem políticas públicas de inclusão digital, como os programas do Comitê Gestor

[10] Disponível em: <http://www.cgi.br/publicacoes/revista/edicao04/cgibr-revistabr-ed4.pdf >. Acesso em: 24 fev. 2012.
[11] Disponível em: <http://www.camara-e.net/2012/01/03/brasil-deve-ser-o-quarto-maior-mercado-de-e-commerce-em-quatro-anos/>. Acesso em: 24 fev. 2012.
[12] Disponível em: <www.governoeletronico.gov.br> e em < www.comprasnet.gov.br>. Acesso em: 24 fev. 2012.

de Inclusão Digital, dentre os quais se destaca o recente Programa Nacional de Banda Larga[13].

A infraestrutura e a rede Ipê da Rede Nacional de Ensino e Pesquisa (RNP), uma organização social mantida pelo Ministério da Ciência, Tecnologia e Inovação, interliga mais de 800 instituições de ensino e pesquisa com pontos de presença nas 27 unidades da Federação, compondo o *backbone* nacional; a RNP gerencia o Ponto Federal de Interconexão de Redes (FIX)[14], que é um ponto de troca de tráfego que viabiliza a interconexão entre redes e outros *backbones*, base da operação de transporte de informações da Internet Global, envolvendo diversos participantes[15]. Os demais *backbones* comerciais e governamentais, nacionais ou estaduais, conectam os milhares de usuários brasileiros por cabos submarinos de fibra ótica aos outros *backbones* espalhados pelo mundo.

Não há uma autoridade intergovernamental com mandato para centralizar a coordenação da rede mundial de computadores, mas todos os seus componentes físicos, lógicos e conteúdos têm proprietários e investidores, os quais, juntamente com os usuários, organizaram diversos arranjos e foros internacionais – intergovernamentais, privados ou mistos em torno da gestão dos inúmeros aspectos do espaço cibernético[16].

Isso explica a complexidade e a dificuldade para estabelecer consensos e marcos legais aceitos internacionalmente a respeito de qualquer tema em razão do caráter anárquico e descentralizado da rede. Com maior razão, a regulamentação dos possíveis conflitos entre diferentes países no espaço cibernético constitui grande desafio para estrategistas e juristas, não obstante sua indiscutível relevância, considerando que qualquer investida em tal ambiente pode propiciar vantagens consideráveis no combate, porém de consequências e efeitos secundários ainda bastante imprevisíveis.

---

[13] Disponível em: <http://www4.planalto.gov.br/brasilconectado/CGPID>. Acesso em: 24 fev. 2012.

[14] Foi implantado em Brasília com o objetivo de permitir a interconexão eficiente das redes governamentais de alcance nacional, de forma a evitar que cada uma destas redes precise buscar separadamente uma rede comercial com a qual possa fazer troca de dados (*peering*). A capital do país foi escolhida para abrigar o FIX devido ao fato de abrigar as sedes de vários órgãos federais. Disponível em: <http://www.rnp.br/ceo/>. Acesso em: 24 fev. 2012.

[15] Disponível em: <http://www.fix.org.br/participantes.html>. Acesso em: 24 fev. 2012.

[16] Tais como: www.iccan.org, www.ianna.org, www.w3.org, www.isoc.org, www.ietf.org, dentre outros.

É válida a advertência mencionada por Lucero (2011, p.12)[17], referente à importância que se deve dar para a compreensão do funcionamento do espaço cibernético:

> [...] o regime internacional para a Internet segue em construção e seu formato e modelo de gestão requerem dos atores interessados em nele influir, inclusive os governos, entendimento de como está estruturado e quais os processos que interferem no seu funcionamento.

Entender o funcionamento do espaço cibernético permite visualizar o entrelaçamento de distintos ordenamentos jurídicos, o que desafia os conceitos de fronteiras, território e soberania, com desdobramentos na aplicação de regras e, logicamente, na definição dos contornos da guerra cibernética.

A propósito, considerando-se a crescente dependência e relevância de todas as atividades de comércio e governo eletrônico, as quais também são alvos de investidas ilícitas de grande repercussão social[18], gerando esforços de cooperação internacional para investigação e combate aos crimes cibernéticos[19], o enfoque do estudo são os ataques cibernéticos hábeis a fragilizar um país, cujos alvos são suas infraestruturas críticas e infraestruturas críticas da informação, adiante definidas.

O risco efetivo da ocorrência de tais ataques, que já puderam ser constatados por vários países, constitui um dos grandes temas das relações internacionais no Século XXI, razão pela qual a defesa e a segurança cibernética se tornaram vitais para a sociedade internacional, que está vivenciando uma corrida armamentista cibernética.

E para melhor compreender o cenário de tais conflitos, convém verificar como os mecanismos e recursos do espaço cibernético estão estruturados no mundo.

---

[17] LUCERO, Everton. *Governança na internet: aspectos da formação de um regime global e oportunidades para a ação diplomática.* p. 12.

[18] Tais como os diversos ataques já notificados às redes e aos serviços de grandes empresas como G*oogle, Facebook, Sony*, dos quais resultam a interrupção de serviços, disseminação de vírus ou roubo de dados financeiros de milhares de usuários. Serão melhor abordados no desenvolver deste trabalho.

[19] Como a Convenção sobre Crimes Cibernéticos de 2001 ou Convenção de Budapeste (em vigor desde 2004), supervisionada pelo Conselho da Europa, a qual tipifica como crimes relacionados a dados e sistemas de informação, computadores, conteúdo e pornografia infantil e direitos autorais, além de estabelecer regras de competência e de cooperação internacional nas investigações e na coleta de provas.

2.1 A estrutura e o caráter transnacional do espaço cibernético

O funcionamento do espaço cibernético não segue a lógica de fronteiras, soberania e território desenhados no modelo de Estado Westphaliano[20], no qual o Estado Nação exerce sua soberania[21] e jurisdição[22] sobre os ocupantes de um território definido por fronteiras reconhecidas pelos demais países, com uma relação de supremacia no plano interno e igualdade no plano internacional[23]. Não obstante, existe uma profunda interdependência entre os países que explica as ações de cooperação internacional para investigações e combate aos crimes cibernéticos transfronteiriços que colocam diferentes países no mesmo polo de interesses e esforços, como se verifica na Convenção de Budapeste sobre Crimes Cibernéticos[24].

---

[20] O Tratado de Westphalia, de 1648, restabeleceu a paz na Europa após a Guerra dos Trinta Anos. Firmou o conceito de igualdade jurídica dos Estados, eliminando o poder da Igreja nas relações entre os mesmos. Tem valor histórico por representar os primeiros ensaios de uma regulamentação internacional positiva. Disponível em: <http://jus.com.br/revista/texto/4325/a-soberania-e-o-mundo-globalizado>. Acesso em: 24 fev. 2012.

[21] Poder de um Estado para criar e aplicar, nos limites do seu território, as leis que considerar adequadas, sem sofrer interferências externas de outros Estados ou de organismos internacionais. É um dos fundamentos da República Federativa do Brasil, nos termos do artigo 1º da Constituição Federal. O artigo 17 da Lei de Introdução às Normas do Direito Brasileiro (Lei 12.376/2010) dispõe sobre a ineficácia de atos e leis estrangeiras ofensivos à soberania, ordem pública e aos bons costumes no Brasil.

[22] A propósito de jurisdição na Internet e sob a perspectiva jurídico-internacional, o termo jurisdição compreende três categorias de poderes: (1) jurisdição legislativa, que se constitui na "jurisdição para prescrever" um princípio ou norma legal, seja por lei, decreto executivo, regulamentação administrativa ou por jurisprudência; (2) jurisdição judicial, que nada mais é do que a "jurisdição para adjudicar" demandas judiciais; e (3) jurisdição executiva, determinada pela "jurisdição para fazer cumprir" leis e regulamentos, bem como ordens e decisões judiciais, conforme obra de AUGUST, Ray. *International cyber-jurisdiction: a comparative analysis.* American Business Law Journal. p. 533. - Conceituação apresentada por OIKAWA, Alysson Hautsch, no artigo "*Conflito de leis e de jurisdição em casos envolvendo a internet: da necessidade de regulamentação internacional sobre a matéria*", no 2º CONGRESSO BRASILEIRO DE DIREITO INTERNACIONAL. Estudos de Direito Internacional, em Curitiba, 2004.

[23] O princípio da igualdade soberana, alicerce máximo de todo o corpo normativo, se materializa no Direito Internacional clássico através do entendimento de que todos os Estados soberanos são iguais para a ordem jurídica internacional, sem considerações de ordem social, econômica, cultural ou política. Disponível em: <http://dipundb.blogspot.com/2010/04/o-principio-da-igualdade-soberana.html>. Acesso em: 24 fev. 2012.

[24] Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 24 fev. 2012.

A Convenção de Budapeste, concebida pelo Conselho da Europa em 2001 e vigorando desde 2004, após a ratificação de cinco países, tipifica os principais crimes cometidos na *Internet*. Em seu preâmbulo, a Convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação

Mas como administrar eventual adversidade insuperável de interesses políticos e econômicos ou mesmo conflitos ideológicos entre diferentes governos e países que venham a se enfrentar com ferramentas e recursos do espaço cibernético? Tal questão ocupa lugar de destaque na agenda internacional contemporânea, pois o convívio internacional não pode mais ser discutido sem considerar os possíveis conflitos no espaço cibernético, cujo funcionamento não segue a lógica das relações internacionais.

A mitigação de fronteiras geográficas convencionais na rede mundial de computadores ocorre porque os recursos críticos de funcionamento do espaço cibernético são geridos e podem estar abrigados em jurisdições diversas, interagindo numa relação de interdependência de estruturas físicas e sistemas lógicos cuja dinâmica não segue uma relação entre o espaço físico e o espaço virtual ou cibernético.

Os ataques cibernéticos podem ser deflagrados a partir de países que não tenham qualquer responsabilidade, assim como os países estão sujeitos aos efeitos de ataques que podem ser camuflados e percorrer diversas jurisdições para afetar estruturas que dão suporte a um país, ainda que localizadas em outras jurisdições, o que permite verificar a possível complexidade das investigações para identificar a origem ou autoria. Tal complexidade é notada por Dyson (1997, p. 103)[25], na análise dos "níveis de espaço na rede virtual", principalmente no aspecto de fronteiras na jurisdição da internet.

---

entre os Estados e a iniciativa privada; ao versar sobre competência e cooperação internacional, no artigo 22, define quando e como uma infração é cometida e deixa a critério das Partes *a jurisdição mais apropriada para o procedimento legal.*

[25] DYSON, Esther. *Release 2.0 – A design for living in the digital age.* p. 103.
Existem três níveis a serem considerados na grande rede. O primeiro nível seria o espaço físico, onde as pessoas habitam e convivem, cada um governado por um único Estado-Nação. Dentro desse nível, as pessoas devem obedecer às leis de onde estão fisicamente localizadas. É o nível-base da jurisdição da *Internet*, vinculando a pessoa ao espaço físico que habita. O segundo nível é o dos provedores de acesso, na realidade o primeiro nível de jurisdição da *internet* em si. O provedor é a conexão entre o mundo físico e o virtual, e na maioria dos casos abriga em seu bojo um grande número de comunidades virtuais, sendo um verdadeiro 'país virtual'. O terceiro nível é o dos domínios e das comunidades que ultrapassam fronteiras nacionais por meio dos provedores. Dentro desse nível temos várias comunidades virtuais que operam sem respeitar fronteiras internacionais ou de outros provedores. O domínio seria o endereço e a forma pela qual determinada comunidade virtual se apresenta na rede.

A conexão entre computadores e outros equipamentos é feita por padrões ou protocolos desenvolvidos para viabilizar a transferência de dados nos variados formatos que circulam por estruturas físicas – *backbones*, servidores, roteadores, *switches*, etc. - interligados por satélites, rádio, redes de telefonia, energia, cabos de fibra ótica, TV por assinatura ou cabos submarinos que viabilizam a circulação da informação.

Uma das primeiras descrições da forma de conectar computadores foi feita pela ISO – *International Standard Organization*[26], no modelo de arquitetura OSI (*Open System Interconnection*), especificando sete camadas (física, enlace, rede, transporte, sessão, apresentação e aplicação) que podem ser agrupadas em cinco camadas (física, enlace, rede, transporte e aplicação) ou três grupos: camada física (computadores, redes, equipamentos, cabos), camada lógica (protocolos, sistemas e padrões técnicos para a circulação de informações) e camada de conteúdo e aplicações (informações).

Existem diversas outras definições e descrições, que podem variar conforme o modelo da arquitetura, da tecnologia e da estrutura de transmissão de dados envolvida, porém, todas elas contemplam a característica de que a informação percorre estruturas e sistemas situados em diversos territórios e jurisdições.

Os protocolos de comunicação entre computadores em rede TCP/IP[27] são os mais difundidos e utilizados na Internet, mas existem outros que, em síntese, também funcionam em camadas ou etapas que realizam diferentes funções atreladas à transmissão de dados em redes locais ou globais, abertas ou fechadas, públicas ou privadas. Os pacotes de dados trafegam a partir de sistemas lógicos e

---

[26] ISO - Organização Internacional para Padronização ou de Normalização representada no Brasil pela ABNT – Associação Brasileira de Normas Técnicas. A ISO é uma organização que congrega órgãos de padronização de mais de 170 (cento e setenta) países e tem diversas outras normas de boas práticas relacionadas à segurança da informação, como a NBR/ISO/IEC 17799:2005, atual ISO 27002, etc. Existem diversos outros modelos de certificação, controle, normas, práticas e padrões internacionais - COBIT (*Common Objectives For Information and Related Technology*), ITIL (IT *Infrastructure Librar*y), a série 800 das normas do NIST (*National Institute of Standards and Technology*). Disponível em: <www.iso.org >. Acesso em: 24 fev. 2012.

[27] *Transmission Control Protocol* (protocolo de controle de transmissão) e *Internet Protocol* (protocolo de interconexão), que inclui outros protocolos como TCP, UDP, DNS, ARP, RARP, DHCP, FTP, HTTP, RIP, BGP, entre outros. Substituíram o *Network* C*ontrol Protocol* que era utilizado pela ARPANET.

comandos que os fazem percorrer estruturas fisicamente situadas em diversos países, conforme a disponibilidade de tráfego.

A Internet se organiza em torno de nomes de domínio e de números de IP dos computadores que hospedam as informações (IP *addresses*)[28], ambos considerados recursos críticos atualmente gerenciados pela ICANN (*Internet Corporation for Assigned Names and Numbers*) e pela IANA[29] (Internet *Assigned Numbers Authority*), distribuídos dentro de um sistema concebido em 1983 (quando apenas cem computadores interligavam instituições acadêmicas), aprimorando o sistema inicial de RFCs (*requests for comments*) para uma hierarquia piramidal de distribuição a partir de servidores da zona raiz da internet (*root-servers*)[30] e parâmetros de concessão de nomes de domínios[31] (DNS - *Domain Name System* ou Sistema de Nomes de Domínios) e por uma política de concessão regional de registros da internet (RIR).

A ICANN aprovou regras que permitirão, a partir de 2012, a criação de novos domínios TLD – *Top Level Domain* de qualquer espécie, além do ".com", ".net" ".org", etc., ampliando as possibilidades de endereços personalizados com até sessenta e três caracteres, o que constitui uma revolução que poderá acarretar impactos ainda imprevisíveis. Grandes empresas e marcas notórias, prevendo o

[28] Os computadores eram identificados por uma sequência numérica semelhante aos números de telefone, o IP, cujo registro e correspondência ao computador eram feitos manualmente, através de arquivo "host.txt" e a manutenção da lista era feita pela *Network Information Center*, nos Estados Unidos. Com a expansão da rede, David Milles desenvolveu um sistema de conversão da sequência numérica do IP para letras, criando o nome de domínio. Jon Postel aperfeiçoou o sistema, criando o *Domain Name System* – DNS ou Sistema de Nomes de Domínios utilizado atualmente.
[29] Vide: <www.iccan.org> e < www.iana.org>.
[30] Vide: <www.root-servers.org>.
[31] Cada nome de domínio é composto de uma série de sequências de caracteres (*labels* ou rótulos) separados por pontos. Os domínios são organizados em diferentes níveis de um sistema que funciona de forma distribuída (servidores de nomes administrados de forma independente ligados à rede) e hierárquica. O domínio de primeiro nível, DPN ou *Top Level Domain* é o mais abrangente e dirigido a determinados conteúdos ou públicos-alvo (".com", ".gov", ".mil", ".edu", etc.) – *generic top level domain* ou gTLD ("gnso.icann.org") ao qual pode ser adicionado um código de País (".com.br", ".mil.br") – *country code top level domain* ou *ccTLD* – "ccnso.icann.org". Também existe o domínio de primeiro nível ".arpa", utilizado na infraestrutura da Internet. Ao DPN podem ser ligados inúmeros domínios de segundo nível (*brasil*.gov.br), aos quais são ligados domínios de terceiro nível (*www*.brasil.gov.br).

aumento nos casos de violação, sentir-se-ão compelidas a anteciparem a compra de novos domínios.[32]

Com a possibilidade de esgotamento do “estoque” de endereços IP da IANA do IPv4[33], atual versão dos protocolos, está sendo difundida e estimulada a adoção da nova geração de protocolos de Internet (IPng – *Internet Protocol next generation*), o IPv6[34], o qual, basicamente, comporta uma maior sequência numérica, o que amplia a quantidade de combinações possíveis para gerar novos endereços e também aumenta a qualidade, segurança e velocidade das comunicações.

Embora não sejam suficientes para eliminar as hipóteses de ataque cibernético, inclusive porque as vulnerabilidades de *softwares* continuarão a existir, algumas características do IPv6 são consideradas como inovações relevantes na perspectiva da segurança, como a possibilidade de agregar o IPSec para criptografar pacote de dados, reduzindo certas vulnerabilidades e dificultando ações ilícitas, conforme explicações de Geers (2011, p.87-94)[35] ao escrever a respeito da próxima geração de Internet e indagar se o IPv6 é a resposta inovadora. Além disso, cada dispositivo passa a ter um endereço efetivamente único e identificável, pois dispensa o uso do NAT - *Network Address Translation*, que permite o compartilhamento de um endereço por diversos dispositivos.

Diversos outros exemplos de adaptações ou inovações do espaço cibernético podem impactar o seu funcionamento e, consequentemente, as estratégias de defesa cibernética - pois as ameaças e vulnerabilidades costumam explorar o desconhecido ou novo – e também a identificação de jurisdições

---

[32] Disponível em: <http://www.nic.br/imprensa/clipping/2011/midia440.htm>. Acesso em: 24 fev. 2012.

[33] O endereço IPv4 é composto por quatro sequências numéricas, x.x.x.x, sendo x um número que pode ir de 0 a 255, como 192.168.1.10. O IPv4 tem 32 bits (4 conjuntos de 8 bits), o que permite, teoricamente, a criação de 4.294.967.296 endereços. O IPv6 é composto por 128 bits, o que significa a possibilidade de 340.282.366.920.938.463.463.374.607.431.768.211.456 ou 340 undecilhões de IPs. O IPv6 utiliza oito sequências de até quatro caracteres separados por ':' considerando o sistema hexadecimal. Exemplo: FECC:2DBD:D228:7153:3211:FF57:D3C9:10F1. O cabeçalho do IPv6 tem 40 bits, o dobro do IPv4.

[34] Disponível em: <http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4>. Acesso em: 24 fev. 2012.

[35] GEERS, Kenneth. Stra*tegic Cyber Security..* p. 87-94.
Disponível em: <http://pt.scribd.com/doc/62478319/Strategic-Cyber-Security-K-Geers >. Acesso em: 24 fev. 2012.

envolvidas em eventuais ataques, como ocorre na computação em nuvem ou *cloud computing*[36].

A computação em nuvem consiste, em síntese, na disponibilização de ambientes para armazenamento de dados acessíveis pela Internet, reduzindo a demanda de infraestruturas físicas locais e de instalação de *softwares* em computadores corporativos, ou seja, os dados ficam na Internet (nuvem), o que dificulta a definição de leis e jurisdições aplicáveis em caso de crimes e investigações, razão pela qual sua popularização também é apontada como um desafio à segurança cibernética. Esta mesma conclusão foi apresentada pela European Network and Information Security Agency (ENISA) em seu Relatório "Cloud Computing – Benefits, Risks and Recommendations for Information Security", em novembro de 2009[37].

Em outras palavras, o espaço cibernético alberga diferentes infraestruturas físicas e estruturas ou sistemas lógicos para armazenamento e transmissão de conteúdo, os quais estão em constante construção e formatação, a exemplo do Projeto Internet 2, da *University Corporation for Advanced Internet Development*, com a qual a Rede Nacional de Pesquisa firmou Memorando de Entendimento[38].

São, portanto, diversos atores interagindo ou compartilhando estruturas e ambientes complexos e em constante configuração, a partir de interesses diversos, o que permite compreender porque nenhum Estado detém o monopólio do poder ou a titularidade da jurisdição e da soberania sobre o espaço cibernético, bem como a dificuldade de perfilar limites territoriais ou fronteiras em tal ambiente.

As infinitas funcionalidades do espaço cibernético são engendradas, portanto, a partir de conteúdos, tecnologias, sistemas e estruturas físicas que

---

[36] Em telecomunicações, uma nuvem é a parte imprevisível de qualquer rede através da qual os dados trafegam entre dois pontos; entre quaisquer dois pontos de uma rede de comutação de pacotes (*packet-switched*), o caminho físico percorrido pelo pacote pode variar de um pacote para outro; em uma rede de comutação de circuitos (c*ircuit-switched*), o circuito específico determinado pode variar de uma conexão para outra. THING, Lowell, tradução Bazán Tecnologia e Linguística e Texto Digital. Dicionário de Tecnologia, São Paulo: Futura, 2003, pág. 161.

[37] Disponível em: <http://www.enisa.europe.eu/media/news-items/final-world-economic-forum-report-on-cloud-computing-with-agency-imput-launched>. Acesso em: 22 fev. 2012.

[38] Disponível em: <http://www.internet2.edu/international/index.cfm> e em <http://www.rnp.br/redes/internet2.html>. Acesso em: 22 fev. 2012.

pertencem ou são compartilhados por governos e particulares, estando espalhados pelos cinco continentes, submersos ou no espaço sideral, em áreas de domínio público internacional[39], quando não estão em plataformas flutuantes, que podem ser utilizados para as mais diversas finalidades, inclusive ataques cibernéticos, o que dificulta a identificação da jurisdição. Conforme Rezek (2000, p. 291)[40]:

> [...] é da tradição doutrinária que a expressão domínio público internacional designe aqueles espaços cuja utilização suscita o interesse de mais de um Estado soberano – às vezes de toda a comunidade internacional – ainda quando sujeitos à incidência de determinada soberania.

A propósito, nos debates acerca da natureza jurídica da Internet, uma das teses em discussão, também ainda incipiente, a considera de domínio público internacional ou espécie de bem público global, no conceito do Programa das Nações Unidas para o Desenvolvimento - PNUD[41], por se tratar de um espaço de interesse comum, que extrapola o âmbito da soberania e das fronteiras territoriais dos Estados, razão pela qual estaria sujeito a uma soberania compartilhada por todos os países – nos moldes da Convenção de Montego Bay sobre Direito do Mar[42]

---

[39] Espaços cuja utilização é do interesse de mais de um Estado e da sociedade internacional, mesmo quando sujeitos à soberania de determinado país, como o mar, os rios internacionais, o espaço aéreo, o espaço sideral, o continente antártico, regidos por convenções e tratados específicos.

[40] REZEK, Francisco. *Direito internacional público: curso elementar*. p. 291.

[41] Trata-se de um bem essencial para todo ser humano e para todos os povos. O conceito pode ser ético-substancial (inerente à qualidade de ser humano) ou ético-instrumental (de natureza normativa, institucional, científica, tecnológica, etc., necessários para tutelar os bens públicos globais ético-substanciais. Trata-se de conceito recente, introduzido em 1999 na publicação do PNUD, organizada por Inge Kaul, Isabelle Grunberg e Marc Stern "*Global Public Goods: International Cooperation in the 21st Century*" (New York: Oxford University Press), na qual Débora L. Spar escreveu o tópico "*The Public Face of Cyber*space". Disponível em <http://www.undp.org/globalpublicgoods/TheBook/thebook.html>. Acesso em: 25 fev. 2012.

[42] Disponível em: <http://www2.mre.gov.br/dai/m_1530_1995.htm>. Acesso em: 24 fev. 2012.

ARTIGO 136 - Patrimônio comum da humanidade

A Área e seus recursos são patrimônio comum da humanidade.

ARTIGO 137 - Regime jurídico da Área e dos seus recursos

1. Nenhum estado pode reivindicar ou exercer soberania ou direitos de soberania sobre qualquer parte da Área ou seus recursos; nenhum Estado ou pessoa física ou jurídica pode apropriar-se de qualquer parte da Área ou dos seus recursos. Não serão reconhecidos tal reivindicação ou exercício de soberania ou direitos de soberania nem tal apropriação.

2. Todos os direitos sobre os recursos da Área pertencem à humanidade em geral, em cujo nome, atuará a Autoridade. Esses recursos são inalienáveis. No entanto, os minerais extraídos da Área só poderão ser alienados de conformidade com a presente Parte e com as normas, regulamentos e procedimentos da Autoridade.

3. Nenhum Estado ou pessoa física ou jurídica poderá reivindicar, adquirir ou exercer direitos relativos aos minerais extraídos da Área, a não ser de conformidade com a presente Parte. De outro modo, não serão reconhecidos tal reivindicação, aquisição ou exercício de direitos.

ARTIGO 138 - Comportamento geral dos Estados em relação à Área

O comportamento geral dos Estados em relação à Área deve conformar-se com as disposições da presente Parte, com os princípios enunciados na Carta das Nações Unidas e com outras normas de

em seus artigos 136 a 138 e outras que disciplinam outros bens e territórios considerados Patrimônio da Humanidade, entre os quais se destacam: Tratados da Antártida, da Lua e do Espaço (Tratado sobre Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico, Inclusive a Lua e Demais Corpos Celestes).

A delimitação ou divisão de poderes está ligada intrinsecamente à manipulação e à titularidade dos recursos críticos, das estruturas e das tecnologias envolvidas, bem como às decisões relacionadas à sua arquitetura de funcionamento, pois tais escolhas e regras técnicas definem os modos de interação no espaço cibernético. Ocorre que tanto a localização quanto a titularidade e o poder de decisão afeto às estruturas físicas, lógicas e de conteúdo do espaço cibernético, assim como o poder de decisão envolvendo tais estruturas, estão dispersas em diversos locais e nas mãos de diversos atores estatais e não estatais. Portanto, o Estado não ostenta mais o monopólio do poder regulador, que não desaparece, mas se desloca para novas mãos, inclusive dos detentores da capacidade de explorar as vulnerabilidades do espaço cibernético que acabam impulsionando a adoção de padrões comportamentais e medidas de segurança.

Com a finalidade de melhor compreender a gestão do espaço cibernético, o tópico subsequente descreverá os principais protagonistas e fóruns de governança.

2.2 Atores e Gestão ou Governança do Espaço Cibernético

Considerando que as estruturas e os padrões tecnológicos determinam o funcionamento e o modo de interação no espaço cibernético, é decorrência lógica que o poder decisório seja disputado pelos fabricantes, fornecedores e proprietários das estruturas e tecnologias, da mesma forma que é natural que os usuários –

---

direito internacional, no interesse da manutenção da paz e da segurança e da promoção da cooperação internacional e da compreensão mútua.

cidadãos, governos e organizações – também busquem interferir nos processos decisórios para defender seus interesses. A circulação mundial de informações atrai a atenção de governos e organismos internacionais que têm dificuldades para definir a legislação aplicável, investigar e punir crimes cibernéticos e outros conflitos de interesses[43].

Dois casos clássicos servem para ilustrar a dificuldade de definir a legislação aplicável e a jurisdição na Internet. O primeiro ocorreu em 2000, quando um juiz francês determinou a uma equipe de especialistas em tecnologia que encontrasse maneiras de bloquear o acesso de usuários franceses a um site de leilões da *Yahoo,* o Santa Clara, com sede na Califórnia, por oferecer material de conteúdo nazista e racista, o que é proibido na França - o objetivo era evitar o direcionamento do leilão de peças nazistas para a França e o aceite de lances feitos por franceses. Além de contestar a decisão francesa, o portal recorreu à justiça americana, requerendo a declaração de que as ordens francesas fossem declaradas inexequíveis, partindo das premissas de que a França não teria jurisdição sobre a matéria e de que a lei americana não proibia as atividades. Na ação proposta perante o Judiciário americano, alegou-se a impossibilidade de a Corte da Califórnia julgar os franceses, o que não foi aceito, considerando o envio da carta-notificação em abril de 2000, a obtenção da ordem judicial ordenando à *Yahoo* que filtrasse o acesso a seus sites e a utilização de oficiais de justiça norte-americanos para notificar a *Yahoo*, na Califórnia, da decisão francesa. Além disso, concluiu-se que não havia desrespeito à soberania francesa, e sim à americana, diante de uma ordem de censura estrangeira, em afronta à liberdade de expressão, protegida pela Constituição americana.

No segundo caso, as atividades do portal "www.wikileaks.org" revelaram intricados conflitos de jurisdição. A divulgação de documentos confidenciais de empresas, pessoas e governos de todos os recantos do mundo, armazenados em banco de dados constituído de informações enviadas por supostos colaboradores

[43] Como os recentes debates a respeito dos projetos de lei norte-americanos *Stop Online Piracy Act* (SOPA) e *Protect IP Ac*t (PIPA), que tutelam direitos autorais sobre filmes, livros e músicas na Internet. Se aprovados, o poder judiciário dos Estados Unidos poderá determinar o bloqueio de sites de busca, redes sociais e qualquer outro portal nacional ou estrangeiro que conduza o usuário norte-americano a conteúdo que viole direitos autorais. Críticos afirmam que há ofensa à soberania de outros países e risco de censura e violação da privacidade.

anônimos de diversas nacionalidades, com mecanismos de criptografia que objetivam preservar o anonimato, como a rede TOR, que serve para dificultar o rastreamento da origem das informações. Apenas para fins ilustrativos, supondo-se a possibilidade de definir e individualizar eventuais responsabilidades, o que constitui um problema de extrema complexidade para o levantamento confiável de evidências digitais, o segundo desafio seria a definição da jurisdição competente e da lei aplicável. A situação é inusitada não apenas em função das repercussões envolvidas, mas pela facilidade de disseminação das informações e da dificuldade do seu rastreamento, atividades que perpassam não apenas os mais variados interesses, mas também territórios e jurisdições.

A relevância da compreensão a respeito dos atores envolvidos na gestão e na governança da Internet, para o propósito do trabalho, decorre das inúmeras possíveis implicações para as estratégias de defesa e segurança no espaço cibernético[44].

A história e a pauta da governança da Internet que vêm sendo desenhadas desde a sua ampliação para o meio acadêmico e comercial sempre foram permeadas por batalhas políticas e comerciais relacionadas aos modelos de arquitetura, discussão da neutralidade e à disputa pela adoção de padrões abertos ou proprietários de protocolos e tecnologias. Da mesma forma, discute-se a gestão compartilhada e alocação de recursos críticos, relacionados à infraestrutura e gerenciamento de recursos essenciais da Internet, tais como: a administração do sistema de nomes de domínio e endereços de protocolos da Internet (endereços IP), a administração do sistema de servidores-raiz, padrões técnicos, *peering* e interconexão, infraestrutura de telecomunicações (inclui tecnologias inovadoras e convergentes) e a multilingualização[45].

---

[44] A empresa chinesa China Telecom, controlada pelo governo chinês, já foi acusada de ter "sequestrado" ou desviado o tráfego da Internet para a China, incluindo sites empresariais e governamentais dos Estados Unidos (NASA, Senado e Departamentos de Defesa e Comércio) e de seus aliados, enviando a roteadores uma mensagem segundo a qual o roteamento do tráfego através da China seria mais rápido; isso permitiria que todos os dados desviados fossem armazenados para posterior decodificação e análise.

[45] Disponível em: <http://governanca.cgi.br/recursos-criticos/> e em <http://www.wgig.org/docs/WGIGREPORT.pdf>. Acesso em 25 fev. 2012.

A gestão dos nomes de domínios, dos endereços IP e dos servidores raiz da Internet, atualmente concentrada em empresas americanas ou em instituições ligadas ao governo norte-americano - por razões históricas e comerciais - são os temas que mais despertam o interesse mundial.

Com a extinção da ARPANET em 1990, a gestão da Internet, até então restrita ao meio acadêmico, passou a ser realizada pela *National Science Foundation*[46] - NSF -, a qual reduziu as restrições da sua utilização para fins comerciais e, gradativamente, delegou a gestão dos domínios à iniciativa privada. Após uma abrupta expansão de provedores de redes comerciais, a gestão passou a ser feita pela IANA – *Internet Assigned Numbers Authority*, ligada ao governo norte-americano, até 1998, quando foi criada a ICANN – *Internet Corporation for Assigned Names and Numbers*, organização internacional sem fins lucrativos criada para assumir algumas funções da IANA (mediante contrato).

Coube à IANA a responsabilidade pela concessão do código de domínio de alto nível dos países – os *country code top-level domain (ccTLD)*, representados por duas letras (br. es, ar, etc.), identificadores oficiais dos topônimos de países criados com base em normas geográficas de 1974, as quais estabeleceram códigos para nomes de países e dependências, o ISO 3166-1[47]. A ICANN é responsável pela alocação do espaço de endereços de protocolos da Internet (IP), pela atribuição de identificadores de protocolos, pela administração de domínios de primeiro nível (.com, .info, etc.) e pelo gerenciamento do sistema de servidores-raiz.

A IANA controla e delega regionalmente os IPs para os RIRs (*Regional Internet Registry*) que, por sua vez, delegam aos ISPs (*Internet Service Providers*), por intermédio de gestores locais; estes, por sua vez, fazem o controle e a administração dos provedores e das organizações vinculadas a usuários finais.

Conforme disponibilizado pela *The Number Resource Organization* (NRO) em seu portal na Internet, atualmente, existem cinco RIRs em operação: *American Registry for Internet Numbers* (ARIN) na América do Norte e partes do Caribe; *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) na Europa,

[46] Vide: <www.nsf.gov>.
[47] Vide: <http://www.iso.org/iso/iso-3166-1_decoding_table>

Oriente Médio e Ásia Central; *Asia-Pacific Network Information Centre* (APNIC), na Ásia e Pacífico; *Latin American and Caribbean Internet Addresses Registry* (LACNIC), na América Latina e partes do Caribe e o *African Network Information Centre* (AfriNIC), na África[48].

No *Statement of Policy, Management of Internet Names and Addresses* (Especificação de políticas, administração de nomes e endereços na Internet), documento de 5 de junho de 1998 conhecido como *White Paper*[49], o governo dos Estados Unidos, então responsável, declarou reconhecer uma nova corporação sem fins lucrativos, formada por interessados na Internet provenientes do setor privado, destinada a administrar políticas para o sistema de nomes e endereços na Internet. No processo de transição, a corporação sem fins lucrativos firmaria contratos para que o governo americano encerrasse sua função no sistema de endereços de nomes e números na Internet, sem comprometer a estabilidade da Internet.

Ainda é bastante forte a influência dos Estados Unidos sobre recursos críticos da Internet - nomes de domínios, endereços IP e servidores-raiz - porque vinculados a empresas ou instituições americanas. A ICANN tem um contrato com o Departamento de Comércio dos Estados Unidos, que também tem poder sobre a gestão dos servidores-raiz que controlam a Internet. Tal questão é objeto de questionamento dos demais países, incluindo do governo brasileiro[50]; ganhou força nos debates iniciados em 2003, na Cúpula Mundial sobre a Sociedade da Informação, convocada pela Organização das Nações Unidas (através da Resolução N^{o} 56/183-ONU, de 21 de dezembro de 2001)[51], a pedido da União Internacional de Telecomunicações[52].

A Cúpula Mundial sobre a Sociedade da Informação – CMSI - é um fórum de debates no qual participam representantes de governos, da sociedade civil, da iniciativa privada, de organizações não governamentais e de organismos internacionais. Além das diversas reuniões preparatórias, foram realizados

[48] Disponível em: <http://www.nro.net/about-the-nro/regional-internet-registries>
[49] Disponível em:<http://www.icann.org.br/general/agreements.htm>. Acesso em: 25 fev. 2012.
[50] Disponível em: <http://www.estadao.com.br/noticias/impresso,brasil-quer-discutir-novo-modelo-de-gestao-para-internet-,826101,0.htm>. Acesso em: 25 fev. 2012.
[51] Resolução N^{o} 56/183-ONU. Disponível em: <http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf>. Acesso em: 25 fev. 2012
[52] Vide: <www.itu.int>.

encontros em Genebra, na Suíça, em 2003, do qual resultou a Declaração de Princípios[53] e o Plano de Ação[54], em Túnis, na Tunísia, em 2005 - do qual resultou a Agenda de Túnis[55]. No Relatório do Grupo de Trabalho sobre a Governança da Internet (GTGI) surgiu a definição de que:

> [...] governança da Internet é o desenvolvimento e a execução pelos Governos, sociedade civil e iniciativa privada, em seus respectivos papéis, de princípios, normas, regras, procedimentos decisórios e programas compartilhados que delineiam a evolução e o uso da Internet[56].

Desdobramentos da CMSI, o GTGI[57], o Fórum sobre Governança da Internet (IGF)[58], o Grupo de Aconselhamento (*Multistakeholder Advisory Group* - MAG) e respectivo Secretariado, são fóruns multilaterais e multissetoriais que reúnem usuários, governos e representantes da sociedade civil, setor privado e comunidade técnica (*multistakeholder*) para debater políticas de governança e tecnologias.

A Agenda de Túnis de 2005 incumbiu o IGF de promover reuniões nos cincos anos sucessivos[59], período após o qual sua continuidade seria objeto de avaliação pela Assembléia Geral das Nações Unidas. No decorrer de 2011, o Grupo de Trabalho da Comissão de Ciência e Tecnologia para o Desenvolvimento da ONU não conseguiu formalizar um relatório final, mas chegou a um acordo geral provisório sobre os resultados e as propostas de adaptações do IGF, do MAG e do Secretariado.[60]

Um dos diversos temas discutidos pela Cúpula Mundial da Sociedade da Informação é a proposta de internacionalização da administração dos arquivos da zona-raiz do sistema que, atualmente, por intermédio da ICANN, é controlada pelos EUA, cuja comitiva, porém, apesar de reconhecer que outros governos têm interesses legítimos na gestão dos domínios nacionais (ccTLD), defende que o atual sistema é eficiente e que a gestão deve continuar sendo feita pelo setor privado,

---

[53] Disponível em: <http://www.itu.int/wsis/docs/geneva/official/dop.html>. Acesso em: 25 fev. 2012.
[54] Disponível em: <http://www.itu.int/wsis/docs/geneva/official/poa.html>. Acesso em: 25 fev. 2012.
[55] Disponível em: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. Acesso em: 25 fev. 2012.
[56] Disponível em: <http://www.wgig.org/docs/WGIGREPORT.pdf>. Acesso em: 25 fev. 2012.
[57] Disponível em: <www.wgig.org>. Acesso em: 25 fev. 2012.
[58] Disponível em: <www.intgovforum.org>. Acesso em: 25 fev. 2012.
[59] Que ocorreram na Grécia (2006), Brasil (2007), Índia (2008), Egito (2009) e Lituânia (2010). Em setembro de 2011, o encontro foi realizado no Quênia e em 2012 será em Baku, no Azerbaijão.
[60] Disponível em: <http://observatoriodainternet.br/avanco-nas-discussoes-sobre-aprimoramento-do-igf>. Acesso em: 25 fev. 2012.

evitando que governos autoritários manipulem o fluxo de informações e a liberdade de expressão, conforme comentado na obra de Lucero (2011, p. 110-111)[61].

No Plano Estratégico da ICANN para o período de junho de 2011 a junho de 2014, a manutenção de uma única raiz oficial é um dos objetivos estratégicos defendidos em prol de uma Internet global, única e interoperável[62].

Persiste uma grande disparidade a respeito das competências e composições necessárias para estabelecer uma cooperação na governança da Internet, bem como sobre a participação ou não de governos na gestão da Internet. Na 66ª reunião que ocorreu entre setembro e dezembro de 2011, a Assembleia Geral da ONU discutiu o papel das Tecnologias de Informação e Comunicação (TICs) para o Desenvolvimento, suscitando à governança da Internet inúmeras polêmicas. Os Estados-membros aprovaram uma resolução para a realização de uma reunião com o objetivo de promover um entendimento comum sobre a cooperação aprimorada ou reforçada - *enhanced cooperation* - nos termos dos parágrafos 34 e 35 da Agenda de Tunis.[63]

No Plano de Ação de Genebra, a Cúpula Mundial sobre a Sociedade da Informação atribuiu à União Internacional de Telecomunicações a incumbência de capitanear as ações relacionadas à infraestrutura da informação e comunicação e à criação de confiança e segurança no uso das TICs, o que levou o Secretário-Geral Hamadaoun Tomé a defender, em 2010, a necessidade de um diploma internacional de segurança cibernética ou de não proliferação de armas cibernéticas, durante o Fórum Econômico Mundial de Davos, na Suíça[64].

É inegável que ainda existem divergências a respeito da extensão do mandato da UIT para tratar da segurança cibernética enquanto matéria de segurança e defesa nacional, crimes cibernéticos e conteúdo das informações,

---

[61] LUCERO, Everton. *Governança na internet: aspectos da formação de um regime global e oportunidades para a ação diplomática.* p. 110-111.

[62] Disponível em: <http://www.icann.org.br/strategic-plan/strategic-plan-2011-2014-28mar11.pdf>. Acesso em: 25 fev. 2012.

[63] Disponível em: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. Acesso em: 25 fev. 2012.

[64] Disponível em: <http://www.zdnet.co.uk/news/security-threats/2010/09/03/itu-head-cyberwar-could-be-worse-than-tsunami-40089995/>. Acesso em: 25 fev. 2012.

sendo difícil definir a barreira das soluções técnicas para as vulnerabilidades da infraestrutura.

Diversas outras organizações dedicadas à Internet são responsáveis pelas discussões de normas, padrões e protocolos técnicos, arquitetura e infraestrutura, destacando-se a *Internet Engineering Task Force* - IETF[65], a *Internet Research Task Force* - IRTF[66], a *Internet Society* - ISOC[67], o *Internet Architecture Board* - IAB[68], o *World Wide Web Consortium* – W3C[69], o *Institute of Electrical and Electronics Engineers* - IEEE[70], entre outros. As discussões técnicas, pesquisas e sugestões feitas por tais organizações são conduzidas por seus integrantes, representantes de empresas e governos, e por tal razão não estão imunes a influências proporcionais à representatividade de cada setor.

No Brasil, a primeira definição de Internet foi escrita pelo Ministério das Comunicações em 1995[71]. Atualmente, a governança da Internet é conduzida pelo Comitê Gestor da Internet, composto por membros do governo, setor empresarial, do terceiro setor e da comunidade acadêmica, com a atribuição de coordenar e integrar todas as iniciativas de serviços de Internet no país, como o registro de domínios, segurança, estudos sobre as tecnologias, pontos de troca de tráfego, padronizações,

---

[65] Em conjunto com W3C e ISO/IEC, desenvolve os padrões de comunicação da Internet, como o TCP/IP. Sua função é garantir a evolução da arquitetura da internet e seu bom funcionamento. Disponível em: <www.ietf.org>. Acesso em: 25 fev. 2012.

[66] É um grupo irmão do IETF. Seu objetivo declarado é "promover pesquisa de importância para a evolução do futuro da Internet através da criação de pequenos grupos de pesquisas focados, a longo prazo trabalhando em tópicos relacionados aos protocolos, aplicações, arquitetura e tecnologia da Internet." É composto por Grupos de Pesquisas que estudam questões de longo-prazo relacionadas com a Internet e suas tecnologias. Disponível em: <www.irtf.org>. Acesso em: 25 fev. 2012.

[67] Organização sem fins lucrativos cuja missão é assegurar o livre desenvolvimento, a evolução e o uso da internet em favor de todas as pessoas ao redor do mundo. Disponível em: <www.internetsociety.org>. Acesso em: 25 fev. 2012.

[68] É o comitê encarregado de supervisionar o desenvolvimento técnico e de engenharia da Internet pela ISOC. Supervisiona forças tarefas, como a IETF e a IRT. Denominava-se *Internet Activities Board*, criado em 1984 para suceder o *Internet Configuration Control Board* – ICCB, criado em 1979 pela DARPA e integrado pelos pioneiros do projeto ARPANET para acompanhar as atividades de definição de protocolos e padrões técnicos. Disponível em: <www.iab.org>. Acesso em: 25 fev. 2012.

[69] É a principal organização de normas internacionais para a World Wide Web (WWW ou W3 abreviada); tem escritório no Brasil desde 2007. Disponível em: <www.w3.org>. Acesso em: 25 fev. 2012.

[70] Reúne engenheiros, cientistas e pesquisadores e se dedica ao avanço da teoria e da prática da engenharia eletrônica, elétrica e da computação. Disponível em: <www.ieee.org>. Acesso em: 25 fev. 2012.

[71] Norma 004, de 1995, item 3, alínea a.

etc[72]. Na Resolução CGI.br/RES/2011/004/P[73], o Comitê Gestor reafirmou o entendimento a respeito da diferença entre a Internet (serviço de valor adicionado) e os serviços de telecomunicações, definidos nos artigos 60 e 61 da Lei Geral de Telecomunicações[74]. Demi Getschko, representante do CGIbr, em entrevista à CDTV do portal Convergência Digital, ratificou o entendimento que afasta a competência da ANATEL para dispor sobre a matéria relativa à prestação de serviços dos provedores de acesso à Internet[75].

Além disso, diversos tratados, normas internas, políticas públicas e órgãos reguladores nacionais e internacionais direta ou indiretamente ligados às estruturas físicas, lógicas ou à gestão do conteúdo compartilham, de certa forma, a governança do espaço cibernético, pois qualquer regra pode impactar ou resultar de outras regras. Tal interdependência está sendo objeto de discussão nos debates relacionados aos projetos de marco civil e penal e da revisão da Lei de Direitos Autorais no Brasil.

---

[72] Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm>. Acesso em: 25 fev. 2012. Ressalta-se ainda que a Resolução do CGI.br/Res/2009/03/9 estabelece os seguintes princípios para a governança da Internet: 1) Liberdade, Privacidade e Direitos Humanos, 2) Governança Democrática e Colaborativa, 3) Universalidade, 4) Diversidade, 5) Inovação, 6) Neutralidade da Rede, 7) Inimputabilidade da Rede, 8) Funcionalidade, Segurança e Estabilidade, 9) Padronização e Interoperabilidade e 10) Ambiente Legal e Regulatório. Vide: < http://www.cgi.br/regulamentacao/resolucao2009-003.htm>.

[73] Disponivel em: < http://www.cgi.br/regulamentacao/resolucao2011-004.htm >, acesso em 25 fev 2012.

[74] Art. 60. Serviço de telecomunicações é o conjunto de atividades que possibilita a oferta de telecomunicação.

§ 1° Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza.

§ 2° Estação de telecomunicações é o conjunto de equipamentos ou aparelhos, dispositivos e demais meios necessários à realização de telecomunicação, seus acessórios e periféricos, e, quando for o caso, as instalações que os abrigam e complementam, inclusive terminais portáteis.

Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.

§ 1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.

§ 2° É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações.

[75] Entrevista disponível em: <http://www.youtube.com/watch?v=mwzBppuLaJE>. Acesso em: 25 fev. 2012.

2.3 Proteção do Espaço Cibernético e das Infraestruturas Críticas no Brasil

Com a crescente dependência tecnológica é possível observar que a defesa e a segurança do espaço cibernético são questões cada vez mais estratégicas, sendo certo que nenhum país pode prescindir da capacidade de dissuasão, enfrentamento e neutralização das ameaças cibernéticas para defender sua soberania e autodeterminação. Tais missões são desafiadoras porque passam pela gestão do espaço cibernético, que supõe ações conjuntas entre diversos atores e Estados - cujos interesses podem conflitar – ao mesmo tempo em que a atribuição de mandato para definição de regras jurídicas ou técnicas ainda é objeto de cobiça e disputas entre mercados e governos.

O Brasil, reconhecido mundialmente como uma potência econômica em expansão, está galgando importantes progressos científicos e tecnológicos – como as descobertas do pré-sal e projetos de construção de submarino nuclear - além de ser sede de importantes eventos internacionais nos próximos anos, razão pela qual é indiscutível a relevância da segurança de seu espaço cibernético e de suas infraestruturas críticas.

As estratégias de defesa e segurança cibernética são formuladas e compartilhadas pelo Gabinete de Segurança Institucional da Presidência da República e pelas Forças Armadas, com a liderança do Exército. Além disso, desempenhando os respectivos papéis, também interagem nos temas relacionados ao espaço cibernético os órgãos de inteligência e investigação de crimes cibernéticos, diplomacia e regulação da Internet e das telecomunicações.

Também existem equipes de resposta e tratamento de incidentes em redes, como o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal[76], o Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa[77], o Centro de Estudos,

[76] Vide: <http://www.ctir.gov.br/>.
[77] Vide: <http://www.rnp.br/cais/>.

Resposta e Tratamento de Incidentes de Segurança no Brasil[78], mantido pelo Comitê Gestor da Internet no Brasil, além de diversos outros Grupos de Segurança e Resposta a Incidentes espalhados pelo território nacional, de empresas ou órgãos governamentais, como o Centro de Coordenação para Tratamento de Incidentes de Rede do Exército[79].

As infraestruturas críticas são as instalações, serviços, bens e sistemas que, interrompidos ou destruídos, acarretam sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade[80]. As infraestruturas críticas da informação são o subconjunto de ativos da informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade[81] - às quais está vinculada a segurança da informação e das comunicações; contempla *hardwares*, *softwares* e equipamentos interconectados por fibras óticas ou pelo espectro eletromagnético, locais de armazenagem, processamento e transmissão de toda a informação, além da própria informação, ou seja, o conjunto de partes físicas e virtuais que compõem o espaço cibernético – como ensinado por Mandarino Júnior (2010, p. 64)[82], o qual também esclarece que:

> a proteção da infraestrutura crítica da informação e a proteção da infraestrutura da informação crítica são complementares: enquanto a primeira identifica e protege *hardware*, *software*, dados e serviços que suportam infraestruturas críticas, a segunda busca identifica e protege informações consideradas críticas, como planos e relação de vulnerabilidades de uma infraestrutura crítica[83].

Há, portanto, uma profunda interdependência entre o espaço cibernético e as infraestruturas críticas, bem como as infraestruturas críticas da informação, na

---

[78] Vide: <http://www.cert.br/>.
[79] Vide: < http://stir.citex.eb.mil.br/>.
[80] Nos termos da Portaria nº 45, de 8 de setembro de 2009, do GSI/PR:
Artigo 2º.
Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas.
§ 1º São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. Disponível em: < http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009>. Acesso em: 25 fev. 2012
[81] De acordo com a Portaria nº 34, de 6 de agosto de 2009, do GSI/PR:
Disponível em: < http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=4&data=06/08/2009>. Acesso em: 25 fev. 2012.
[82] MANDARINO JÚNIOR, Raphael. *Segurança e defesa do espaço cibernético brasileiro*. p. 64.
[83] Idem ibidem, p. 38-39.

medida em que são estruturadas nas tecnologias da informação e comunicação e dependentes, portanto, da segurança da informação, a qual pressupõe a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Tais propriedades estão definidas na Instrução Normativa nº 1/2008-GSI/PR[84], que disciplina a gestão da segurança da informação e comunicações na Administração Pública Federal, a qual será objeto de revisão a ser feita por grupos de trabalho criados pela Portaria nº 52, de 13 de dezembro de 2011[85], aos quais incumbirá o levantamento de informações técnicas e legais que possam afetar a segurança da informação e comunicações, conforme eixos temáticos considerados relevantes: tratamento da informação, gestão de mudanças, verificação de conformidade e melhoria contínua, computação em nuvem, inventário e monitoramento de ativos de informação, redes sociais, mobilidade e aplicações seguras.

A Política Nacional de Segurança da Informação[86] nos órgãos e nas entidades da Administração Pública Federal tem pressupostos, objetivos e diretrizes atribuídas à Secretaria Executiva do Conselho de Defesa Nacional, órgão de

---

[84] De acordo com a IN nº 1/2008, do GSI/PR, **autenticidade** é a propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade; **confidencialidade** é a propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado; **disponibilidade** é a propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade; **integridade** é a propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: 25 fev. 2012.

[85] Convém destacar os considerandos da referida norma: [...] considerando: os avanços acelerados das tecnologias de informação e comunicação (TIC) e seus impactos nas redes, sistemas e bancos de dados do Governo Federal; o aumento crescente de ameaças cibernéticas e de ataques que exploram vulnerabilidades de redes, sistemas e bancos de dados, bem como brechas de segurança da informação e comunicações, que podem afetar as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade; a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação como fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações no âmbito da Administração Pública Federal, direta e indireta; Resolve:
Art. 1° Instituir, no âmbito do Comitê Gestor de Segurança da Informação - CGSI, 8 (oito) Grupos de Trabalho para estudo, análise e proposição de normas complementares à Instrução Normativa GSI nº 1, de 13 de junho de 2008, acerca de temas relevantes relacionados à Segurança da Informação e Comunicações para a Administração Pública Federal, direta e indireta. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=10&data=14/12/2011>. Acesso em: 25 fev.2012.

[86] Instituída pelo Decreto n° 3.505, de 2000, disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 31 jul. 2011.

consulta da Presidência da República nos assuntos relacionados com a soberania nacional e a defesa do Estado democrático.[87] Tal Secretaria Executiva é assessorada pelo Comitê Gestor da Segurança da Informação, que é coordenado pelo Gabinete de Segurança Institucional da Presidência da República. A Política Nacional de Segurança da Informação atribui à Agência Brasileira de Inteligência a competência para apoiar o Conselho de Defesa Nacional, integrar comitês, câmaras técnicas, equipes e grupos de estudo.

A Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, presidida pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, tem a incumbência de formular políticas públicas e diretrizes de matérias relacionadas às relações exteriores e à defesa nacional no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério, incluindo cooperação internacional em assuntos de segurança e defesa, atividades de inteligência, segurança para as infraestruturas críticas, como também serviços, segurança da informação e segurança cibernética[88].

O Grupo Técnico de Segurança Cibernética, criado no âmbito da Câmara de Relações Exteriores e Defesa Nacional e composto por representantes dos Ministérios da Justiça, da Defesa, das Relações Exteriores e dos Comandos do Exército, da Marinha e da Força Aérea, tem a função de propor diretrizes e estratégias para a Segurança Cibernética da Administração Pública Federal[89].

---

[87] Nos termos da Constituição Federal de 1988:
Art. 91. O Conselho de Defesa Nacional é órgão de consulta do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do Estado democrático, e dele participam como membros natos: [...]
§ 1º - Compete ao Conselho de Defesa Nacional:
I - opinar nas hipóteses de declaração de guerra e de celebração da paz, nos termos desta Constituição;
II - opinar sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal;
III - propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo;
IV - estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.

[88] Decreto n° 4.801, de 2003, com as alterações do Decreto n° 7.009, de 2009. Disponível em: <http: //www.planalto.gov.br/ccivil_03/decreto/2003/D4801.htm>. Acesso em: 25 fev. 2012.

[89] Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009>. Acesso em: 25 fev. 2012.

O Livro Verde sobre Segurança Cibernética no Brasil[90], elaborado em 2010 pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSICGSI descreve o cenário atual e estabelece as diretrizes para a futura elaboração do Livro Branco da Política Nacional de Segurança Cibernética, sendo interessante destacar a proposta de fomentar articulação de acordos internacionais para potencializar a segurança cibernética no País e a capacidade de defesa e dissuasão, bem como a de elaborar a Política Nacional de Segurança das Infraestruturas Críticas. O Livro Verde aponta as seguintes possíveis diretrizes para a Política Nacional de Segurança das Infraestruturas Críticas – PNSIEC:

> CONHECER E MAPEAR o grau de vulnerabilidade do país em relação aos seus sistemas de informação e as suas infraestruturas críticas de informação por meio de programa específico, no médio e longo prazo, que compreenda:
>
> a) a macro-coordenação do mapeamento dos ativos de informação das infraestruturas críticas;
>
> b) o apoio ao processo de auditoria de segurança das infraestruturas críticas da informação, definindo requisitos mínimos de segurança; e
>
> c) a macro-coordenação e o desenvolvimento de sistema de monitoramento de ameaças cibernéticas e divulgação de alertas de suporte às infraestruturas críticas;
>
> ELABORAR E/OU ADAPTAR metodologia, no médio e longo prazo, para avaliações de risco e de continuidade de negócio em segurança cibernética, o que inclui dentre outras ações:
>
> a) identificar o grau de interdependência dos serviços das infraestruturas críticas do país;
>
> b) desenvolver e/ou adaptar metodologia comum para avaliar as vulnerabilidades das infraestruturas críticas de informação, dos seus sistemas e de seus serviços;
>
> c) conceber um sistema dinâmico de medidas preventivas, próativas, e reativas contra ameaças e ataques cibernéticos;
>
> DESENVOLVER PROGRAMA de capacitação de gestores atuantes nas infraestruturas críticas que contemple dentre outras competências: análise e gestão de riscos, segurança das infraestruturas críticas da informação, resiliência operacional e organizacional, monitoramento e resposta a ataques cibernéticos[91].

Existem Grupos Técnicos específicos para as Infraestruturas Críticas dos setores de Energia (energia elétrica, petróleo, gás natural e combustíveis

---

[90] Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 25 fev. 2012.

[91] Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/3_Livro_GSIC_UNB.pdf>. Acesso em: 25 fev. 2012.

renováveis)[92], Transporte (aquaviário, aéreo e terrestre)[93], Comunicações (telecomunicações, serviços postais e radiodifusão)[94], Água (abastecimento urbano e barragens)[95] e Finanças (bancário e financeiro)[96], além de um Núcleo de Segurança de Infraestruturas Críticas[97] e grupos de trabalho de Certificação Digital[98] e Criptografia[99] no DSICGSI.

Diversos sistemas e infraestruturas podem ser considerados críticos e estratégicos, podendo ser citados o Sistema de Vigilância da Amazônia (SIVAM), o Sistema de Proteção da Amazônia (SIPAM), o Sistema Integrado de Monitoramento de Fronteiras (SISFRON), o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), o Sistema de Gerenciamento da Amazônia Azul (SISGAAZ), a Infraestrutura de Chaves Públicas Brasileira (ICP Brasil), instituída pela Medida Provisória nº 2.200 - 2, de 24 de agosto de 2001, a Autoridade Certificadora Raiz (AC Raiz) gerida pelo ITI[100] ou mesmo as demais autoridades certificadoras e registradoras, integrantes da cadeia de certificados digitais.

Ao Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, criado em 2009 no âmbito do DSICGSI, incumbe: levantar e avaliar as potenciais vulnerabilidades e riscos à Segurança de Infraestruturas Críticas da Informação, identificada a sua interdependência; propor, articular e acompanhar medidas necessárias à segurança; estudar, propor e acompanhar a implementação

---

[92] A Portaria nº 11 - GSIPR/CH, de 16 de junho de 2008, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Petróleo, Gás Natural e Combustíveis Renováveis (SGTSIC - PEGANCOR) e a Portaria nº 12 - GSIPR/CH, de 16 de junho de 2008, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Energia Elétrica (SGTSIC - Energia Elétrica).

[93] A Portaria nº 25, de 27 de abril de 2010, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Terrestres (SGTSIC-Transportes Terrestres), a Portaria nº 27, de 27 de abril de 2010, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aquaviários (SGTSIC - Transportes Aquaviários) e a Portaria nº 28, de 27 de abril de 2010, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aéreos (SGTSIC - Transportes Aéreos).

[94] A Portaria 4/2009-SGTSIC radiodifusão. A Portaria 5/2009-SGTSIC telecomunicações. A Portaria 6/2009-SGTSIC postais.

[95] A Portaria nº 29, de 27 de abril de 2010, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Barragens (SGTSIC - Barragens) e a Portaria nº 30, de 27 de abril de 2010, institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Abastecimento Urbano de Águas (SGTSIC - Abastecimento Urbano de Águas).

[96] A Portaria nº 26, de 27 de abril de 2010, institui o Grupo Técnico de Segurança de Infraestruturas Críticas de Finanças (GTSIC - Finanças).

[97] A Portaria nº 31, de 27 de abril de 2010, cria, no âmbito do Gabinete de Segurança Institucional da Presidência da República -GSIPR, o Núcleo de Segurança de Infraestruturas Críticas.

[98] Vide: <http://dsic.planalto.gov.br/documentos/portaria_11_ago_2007.htm>.

[99] Vide: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=13&data=07/08/2009>.

[100] Vide: <http://www.iti.gov.br/twiki/bin/view/Certificacao/CertificadoConceitos>.

de um sistema de informações que conterá dados atualizados de Infraestruturas Críticas da Informação, para apoio a decisões; pesquisar e propor um método de identificação de alertas e ameaças da Segurança de Infraestruturas Críticas da Informação[101] para as quais foi criado um Guia de Referência[102].

A Estratégia Nacional de Defesa[103] estabelece que todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, dando ênfase às medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, ao transporte, à água e às telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, coordenados pelo Gabinete de Segurança Institucional.

O setor cibernético é definido como estratégico e essencial na Estratégia Nacional de Defesa, a qual estabelece que as capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares e que incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. Além de enfatizar que, como decorrência de sua natureza, o setor cibernético transcende a divisão entre defesa e desenvolvimento, civil e militar, também prevê a Estratégia Nacional de Defesa a necessidade de aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos – bem como, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do Gabinete de Segurança Institucional da Presidência da República[104].

---

[101] Além de outras julgadas relevantes, nos termos do Artigo 6º da Portaria nº 34, de 2009. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=4&data=06/08/2009>. Acesso em 25 fev. 2012.

[102] Vide: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>.

[103] Instituída pelo Decreto nº 6.703, de 18 de dezembro de 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em 25 fev. 2012.

[104] Conforme o documento denominado Estratégia Nacional de Defesa (END). Disponível em : <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 25 fev.2012.

As capacitações cibernéticas devem contemplar o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. Está prevista a constituição de uma organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar.

A força naval submarina a ser desenvolvida no Brasil deverá ganhar autonomia nas tecnologias cibernéticas que guiem os submarinos e seus sistemas de armas e que lhes possibilitem atuar em rede com as outras forças navais, terrestres e aéreas.

O encargo de coordenar e integrar as ações de defesa cibernética nas Forças Armadas foi atribuído ao Exército[105] e, em agosto de 2010, foi ativado o Núcleo do Centro de Defesa Cibernética (Nu CDCiber), atual Centro de Defesa Cibernética (CDCiber)[106], responsável por coordenar as atividades do setor cibernético.

Das diversas ações, destaca-se a capacitação de recursos humanos, a implantação da Escola Nacional de Defesa Cibernética (EsNaDCiber) e o fomento da pesquisa e da indústria nacional de defesa – o que está alinhado com a proposta do Livro Branco de Defesa Nacional[107].

A Secretaria de Assuntos Estratégicos da Presidência da República, na incumbência de promover o planejamento governamental de longo prazo e a implementação da Estratégia Nacional de Defesa no setor cibernético, promoveu reunião técnica, em dezembro de 2010[108], da qual resultaram metas e a criação do comitê gestor de atividades de cibernética e de tecnologia da informação, bem como a proposta de criação do Comando de Defesa Cibernética das Forças Armadas (CDCFA), a ser composto por civis e militares, para realizar o planejamento, o emprego, a coordenação e a orientação técnica e normativa das atividades do sistema brasileiro de defesa cibernética.

---

[105] Diretriz Ministerial n° 14, de 2009.
[106] A Portaria nº 666, de 4 de agosto de 2010, criou o Centro de Defesa Cibernética do Exército e a Portaria nº 667, de 4 de agosto de 2010, ativou o Núcleo do Centro de Defesa Cibernética.
[107] Disponível em: <http://www.defesa.gov.br/projetosweb/livrobranco/end.php>. Acesso em 25 fev. 2012.
[108] Disponível em: <http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em 25 fev. 2012.

Outros órgãos governamentais também interagem nas questões relacionadas à defesa e à segurança cibernética, com atribuições de regulação, investigação como o Departamento da Polícia Federal nos crimes federais[109] e atividades de inteligência, a cargo da Agência Brasileira de Inteligência[110], órgão central do Sistema Brasileiro de Inteligência – SISBIN, cujas atividades se destinam à defesa do Estado, da sociedade e da soberania nacional, avaliando ameaças internas e externas à ordem constitucional, inclusive as ameaças cibernéticas.

A propósito, as atividades de inteligência no espaço cibernético já têm um rol bastante diversificado de exemplos - alguns inclusive reconhecidos no âmbito das relações internacionais[111] - o qual tende a ampliar exponencialmente, também em função do combate ao terrorismo[112].

O Comitê Gestor da Internet no Brasil, enquanto órgão orientador[113], exerce diversas atribuições que têm efeitos sobre a segurança das infraestruturas críticas e dos usuários da Internet. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil trata incidentes de segurança e presta apoio a administradores de redes e usuários de Internet no país, além de estudar as tendências de ataques, divulgar estudos sobre segurança de redes e desenvolver mecanismos de alerta antecipado para redes possivelmente em risco[114].

Em 2008, a Agência Nacional de Telecomunicações desenvolveu o Plano Geral de Atualização de Regulamentação das Telecomunicações[115], o qual contempla a previsão de estudos e adoção de medidas para a proteção da infraestrutura nacional de telecomunicações contra falhas e ataques de guerra

---

[109] Vide: <www.dpf.gov.br>, que conta com uma Divisão de Repressão a Crimes Cibernéticos da competência federal. Diversos Estados da Federação também possuem delegacias especializadas.

[110] Vide: <www.abin.gov.br>. Na ABIN existe um Sistema de Inteligência de Defesa. Disponível em: <https://www.defesa.gov.br/arquivos/File/doutrinamilitar/Portarias/295_2002.pdf>. Acesso em 25 fev. 2012.

[111] Tais como o ECHELON, sistema global de interceptação de comunicações privadas e econômicas, o *Carnivore Diagnostic Tool*.

[112] Como já ocorreu, por exemplo, com a aprovação do *USA Patriot Act* pelo Congresso Americano em resposta aos atentados de 11 de setembro de 2001, ampliando o alcance das ações de inteligência no espaço cibernético.

[113] Vide: <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm>.

[114] Vide: <www.cert.br>.

[115] Resolução ANATEL Nr 516, de 30 de outubro de 2008. Plano Geral de Atualização da Regulamentação das Telecomunicações no Brasil. Disponível em: <http://www.anatel.gov.br>. Acesso em: 24 fev. 2012.

cibernética. Foram previstas três etapas de trabalho: proteção de infraestrutura crítica de telecomunicações, regulamento de interrupções sistêmicas do STFC[116] e segurança e proteção da infraestrutura nacional de telecomunicações do Sistema Rede Nacional de Fibras Óticas (RENAF)[117]. A ANATEL também integra o acima referido Subgrupo Técnico de Infraestruturas Críticas de Telecomunicações do GSI, que objetiva a implementação de medidas e ações relacionadas com a segurança de tais estruturas.

Alguns eventos internacionais acarretarão aumento de demanda e mudanças no setor de telecomunicações e no espaço cibernético brasileiro. A ANATEL implementará a rede de telefonia da 4ª geração (4G) até maio de 2013, para evitar o risco de congestionamento; já promoveu a licitação de direitos de exploração de satélites para aumentar a capacidade das telecomunicações[118].

O Plano Nacional de Desenvolvimento das Atividades Espaciais[119] tem diversos projetos estratégicos relacionados aos satélites, essenciais para a segurança e para a soberania nacional. O Satélite Geoestacionário Brasileiro (SGB), retomado para viabilizar o Programa Nacional de Banda Larga[120], e o Centro de

---

[116] Anexo à Resolução n.º 426, de 9 de dezembro de 2005 – Regulamento do Serviço telefônico fixo Comutado
Art. 4º O STFC é classificado, quanto a sua abrangência, como serviço de telecomunicações de interesse coletivo.
Art. 5º O STFC é prestado em regime público e em regime privado, e objeto de, respectivamente, concessão ou permissão e autorização, conforme disposto no Plano Geral de Outorgas (PGO).
Art. 6º São modalidades do STFC:
I - local: destinada à comunicação entre pontos fixos determinados situados em uma mesma área local ou em localidades distintas que possuam tratamento local;
II - longa distância nacional: destinada à comunicação entre pontos fixos determinados, situados em áreas locais distintas no território nacional e que não pertençam a localidades que possuam tratamento local; e
III - longa distância internacional: destinada à comunicação entre um ponto fixo situado no território nacional e outro ponto no exterior.
Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=116032&assuntoPublicacao=Regulamento%20do%20Servico%20Telefonico%20Fixo%20Comutado&caminhoRel=null&filtro=1&documentoPath=biblioteca/resolucao/2005/anexo_res_426_2005.pdf>. Acesso em: 24 fev. 2012.

[117] Disponível em: <hhttp://www.teletime.com.br/4/2011/guerra-cibernetica/tt/226285/revista.aspx>. Acesso em: 24 fev. 2012.

[118] Disponível em: <http://www.copa2014.gov.br/pt-br/noticia/proposta-de-edital-da-anatel-preve-4g-nas-cidades-sede-ate-maio-de-2013>. Acesso em: 24 fev. 2012.

[119] Disponível em: <hhttp://www.aeb.gov.br/download/PDF/pnae_web.pdf>. Acesso em: 24 fev. 2012.

[120] Disponível em: <hhttp://www4.planalto.gov.br/brasilconectado/pnbl>. Acesso em: 24 fev. 2012.

Lançamento de Satélites em Alcântara, no Maranhão[121] afetarão a gestão do espaço cibernético.

No âmbito da diplomacia cibernética ou da política externa digital, o Brasil integra diversos fóruns internacionais correlatos à sociedade da informação, incluindo crimes cibernéticos e temas relativos à segurança e defesa cibernética, além dos grupos temáticos da Cúpula Mundial da Sociedade da Informação, por intermédio da Divisão da Sociedade da Informação do Ministério das Relações Exteriores.

Recentemente, o Ministro da Defesa discutiu a possibilidade de ampliar a cooperação em projetos de defesa cibernética com a Argentina[122] e com a Bolívia[123], com quem criou uma comissão conjunta de técnicos das Forças Armadas.

O Brasil não tem, nas suas relações internacionais, tradição de atacar ou invadir outros países, o que reflete diretrizes constitucionais que estabelecem a solução pacífica de controvérsias. Todavia, tal cultura pacifista pressupõe a capacidade de dissuasão, ou seja, de não permitir que a paz seja rompida. Daí a relevância das Estratégias de Defesa Cibernética e da capacitação tecnológica, direção na qual outros países também estão seguindo, conforme será possível verificar nas próximas linhas.

[121] Vide: <hhttp://www.cla.aer.mil.br/>.
[122] Disponível em: <https://www.defesa.gov.br/index.php/noticias-do-md/2454578-06092011-defesa-celso-amorim-defende-ampliacao-da-cooperacao-entre-paises-sul-americanos-na-area-de-defesa.html>. Acesso em: 24 fev. 2012.
[123] Disponível em: <https://www.defesa.gov.br/index.php/noticias-do-md/2454798-17012012-defesa-brasil-e-colombia-ampliam-cooperacao-na-area-de-defesa.html>. Acesso em: 24 fev. 2012.

3 OS CONFLITOS NO ESPAÇO CIBERNÉTICO

Acompanhando a irreversível migração das atividades humanas para o espaço cibernético e explorando a profunda interdependência das infraestruturas críticas, os ataques cibernéticos, com seu potencial para desestabilizar setores relevantes da sociedade ou até mesmo um País, comprometendo a segurança, passaram a figurar na agenda das relações diplomáticas e no centro das atenções de governos e estrategistas militares que estão se preparando para atuar no teatro de operações do Século XXI. Além disso, diversos relatórios e pesquisas são realizados constantemente por empresas do ramo, com finalidades, critérios e abrangências variáveis.

Estudo divulgado em janeiro de 2012 pela revista *The Economist* contempla um *ranking* de maturidade em segurança cibernética com países do G20, exceto integrantes da União Europeia, materializado no Índice de Poder Cibernético (*Cyber Power Index*)[124], realizado com indicadores da vulnerabilidade a ataques cibernéticos e da capacidade de implantação de uma infraestrutura crítica necessária para uma economia segura: quadro jurídico-institucional do espaço cibernético, contexto econômico e social, infraestrutura tecnológica e aplicação em setores estratégicos. O *ranking* é liderado pelo Reino Unido e o Brasil, único país emergente, ocupa o décimo lugar no *ranking* mundial.

O relatório "*Cyber-security: The vexed question for global rules*", elaborado pela *Security and Defence Agenda* a pedido da *McAfee*, divulgado em janeiro de 2012[125], considerou entrevistas com 80 (oitenta) especialistas em segurança digital e pesquisas com outros 250 (duzentos e cinquenta) de 35 (trinta e cinco) países. Quase 60% revelaram o entendimento de que existe uma corrida armamentista cibernética em curso, 36% acreditam que segurança cibernética é mais importante do que defesa antimísseis e para 45% o assunto é tão importante quanto a defesa de fronteiras.

---

[124] Disponível em: <http://cyberhub.com/CyberPowerIndex>. Acesso em 24 fev. 2012.

[125] Relatório disponível em: <http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_ FINAL.pdf>. Acesso em 24 fev. 2012.

Na pesquisa realizada em 2010 pelo *Center For Strategic and International Studies*[126], foram ouvidos 600 executivos da área de segurança de empresas de infraestruturas críticas de 14 países, os quais revelaram que mais de 50% das empresas já sofreram ataques de grande escala ou invasões de governos, grupos criminosos ou terroristas; 55% acreditam que as leis ou as autoridades locais são insuficientes para conter ou reprimir os ataques cibernéticos. Na pesquisa, os Estados Unidos e a China foram considerados os potenciais agressores cibernéticos mais preocupantes.

Na obra do jornalista inglês Glenny (2011, p. 242)[127], baseada em fatos verídicos e entrevistas, são relatados alguns dos principais episódios e desafios relacionados ao espaço cibernético, incluindo a atuação de protagonistas que se infiltram no mercado de segurança cibernética que, por tal razão, pode fornecer tanto as soluções como as ameaças relacionadas aos crimes cibernéticos, à espionagem industrial e à própria guerra cibernética. O autor reconhece que as armas cibernéticas têm o potencial de paralisar a infraestrutura nacional vital de um país e arruinar a vida das pessoas, justificando-se, em tais casos, a intervenção militar, embora não aponte qual medida.

Não obstante as eventuais especulações comerciais ou jornalísticas que exploram o tema, episódios verídicos de maior ou menor gravidade são cada vez mais divulgados – quando chegam ao conhecimento público – ou tratados de forma reservada como uma ameaça à segurança e à soberania dos países, quando não estão sendo estudados por estrategistas militares e políticos para eventual emprego bélico.

Em 2011, os Estados Unidos cogitaram realizar um ataque cibernético utilizando um sistema chamado *Blinder* contra a Força Aérea da Líbia, que seria o primeiro país a se tornar, oficialmente, alvo de uma ofensiva cibernética contra seu sistema de defesa aérea, evitando que os radares detectassem informações que seriam utilizadas para direcionar mísseis contra aviões de guerra da OTAN[128]. A

---

[126] Relatório disponível em: <http://img.en25.com/Web/McAfee/CIP_report_final_pt-br_fnl_lores.pdf>. Acesso em 24 fev. 2012.
[127] GLENNY, Misha. *Mercado sombrio: o cibercrime e você*., p. 242.
[128] Disponível em: <http://video.globo.com/Videos/Player/Noticias/0,,GIM1667315-7823-EUA+PREPARAM+GUERRA+CIBERNETICA+CONTRA+LIBIA,00.html> e em:<http://www.washingtonpost

medida não foi adotada para evitar o precedente e porque não havia tempo suficiente e certeza de que esse tipo de ataque poderia ser autorizado pelo Presidente sem comunicar o Congresso. Além disso, eram imprevisíveis os danos colaterais de uma possível interrupção de geradores de energia, elevando o risco de atingir estruturas civis, como hospitais.

Em tal universo, ainda não há uma clara definição das diferenças e correlações das ações – protagonizadas por atores estatais ou não estatais – que podem ser vinculadas à guerra e à espionagem cibernética, aos crimes e ao terrorismo cibernético ou apenas ao ativismo no espaço cibernético. Mas todas as hipóteses guardam uma semelhança: a utilização de armas ou ferramentas cibernéticas para realizar ataques cibernéticos, desestabilizar oponentes ou defender interesses por intermédio deles.

Por tais razões, assim como o Brasil, diversos países e organismos internacionais estão se mobilizando para enfrentar as ameaças cibernéticas, criando estruturas e desenvolvendo doutrinas militares, diplomacia[129] e inteligência cibernética[130] para defender sua soberania no espaço cibernético, quando já não estão desenvolvendo armas virtuais, realizando exercícios simulados e espionagem cibernética.

Depois dos atentados de 11 de setembro de 2001, uma profunda alteração nas relações internacionais foi marcada pelas medidas de combate ao terrorismo adotadas pelos Estados Unidos, destacando-se a aprovação do *USA Patriot Act* pelo Congresso Americano, o qual ampliou o alcance das ações de inteligência e outras formas de investigação no espaço cibernético, com a interceptação de comunicações[131].

.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html>. Acesso em: 11 dez. 2011.

[129] A respeito da diplomacia cibernética. Disponível em: <http://portuguese.brazil.usembassy.gov/ciberneticapt.html> e em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/view/43>. Acesso em: 11 dez. 2011.

[130] A respeito das ações de inteligência cibernética. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf> e em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4e3ae31e2c097.pdf>. Acesso em: 11 dez. 2011.

[131] Práticas que remontam ao projeto ECHELON, sistema global de interceptação de comunicações privadas e econômicas, que teria sido estabelecido a partir do acordo ultrassecreto *UK-USA Security Agreement*, conhecido como AUSCANNZUKUS ou *Five Eyes*, firmado em 1948 entre os Estados

O *USA Patriot Act* estabelece uma colaboração estreita entre investigadores e serviços secretos, em particular no que diz respeito ao terrorismo internacional, com a troca de informações sem os limites impostos pela Lei de Vigilância de Inteligência Estrangeira (FISA – *Foreign Intelligence Surveillance Act*). Deixa de ser exigido o requisito do fim a que se destina a coleta de informações, alarga a competência jurisdicional para instalar dispositivos de intercepção de comunicações e seguir o alvo da investigação onde quer que se encontre (mandados ou ordens judiciais em branco para aplicação em várias jurisdições). A seção 220 abrevia os requisitos necessários para obter um mandado, prescindindo da autorização dos juízes onde o *Internet Service Provider* (ISP) está colocado, ultrapassando a barreira da mudança de jurisdição. O Tribunal com jurisdição sobre a investigação pode emitir um mandado sem a intervenção da jurisdição onde o ISP está localizado, seguindo informação nos moldes da natureza transjurisdicional da Internet. A seção 217 permite que as autoridades judiciais interceptem as comunicações do invasor de um sistema de computador protegido, definido como um sistema usado pelo Governo Federal, por uma instituição financeira, ou usado para comunicações interestaduais ou para comércio internacional; invasor é a pessoa que acede a um computador protegido sem autorização e que, portanto, não tem uma expectativa razoável de privacidade em qualquer comunicação transmitida através ou de um computador protegido (KERR, 2003)[132].

Em fevereiro de 2003, os Estados Unidos divulgaram a Estratégia Nacional para a Segurança do Espaço Cibernético voltada à proteção de infraestruturas críticas da informação[133]. Em 2009, foi criado o *United States Cyber Command* (USCYBERCOM) e, em maio de 2011, foi anunciada a Estratégia Internacional para o Espaço Cibernético, na qual é proposta a criação de normas internacionais de segurança. Trata-se da primeira estratégia formal de defesa cibernética segundo a

---

Unidos e o Reino Unido, Nova Zelândia, Canadá e Austrália e também contaria com a colaboração de empresas de *hardware, software* e telecomunicações. É objeto do Relatório A5-0264/2001 do Parlamento Europeu. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//PT>. Já a respeito do *Carnivore Diagnostic Tool,* disponível em: <http://web.archive.org/web/20021120212738/http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm>. Acesso em: 11 dez. 2011.

[132] KERR, Orin S. *Internet surveillance law after the USA Patriot Act: the big brother that isn´t.* Northwestern University Law Review, v. 97. 2003. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501>. Acesso em: 25 fev. 2012.

[133] Disponível em: <http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberspace_strategy[1].pdf>. Acesso em: 25 fev. 2012.

qual um ataque cibernético oriundo de outro país, que comprometa estruturas críticas, cause mortes, prejuízos, destruição ou transtornos de alto nível, poderá ser interpretado como ato de guerra que poderia motivar a resposta com a utilização de força militar convencional pelo conceito de equivalência[134].

O Escritório Nacional de Contraespionagem americano divulgou, em outubro de 2011, o relatório "*Foreigh Spies Stealing US Economic Secrets in Cyberspace*", no qual acusa formalmente a China e a Rússia de utilizarem serviços de inteligência para espionagem econômica, invadindo sistemas com o intuito de colher dados sobre tecnologias militares e recursos minerais[135].

A estratégia americana de defesa, divulgada em janeiro de 2012, dá ênfase à capacidade cibernética e aos investimentos em segurança cibernética contra ataques, à expansão de plataformas de inteligência baseadas no espaço e ao desenvolvimento de bombardeiro invisível a radares[136].

O Reino Unido criou, em 2009, o *Cyber Security Operations Center* e lançou a *Cyber Security Strategy of the United Kingdom*[137], recentemente atualizada. Em dezembro de 2011, a agência de inteligência britânica *Government Communications Headquartes* lançou um desafio para recrutar decifradores de códigos[138]. Diversos

---

[134] Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 25 fev. 2012.

[135] Disponível em: <http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf>. Acesso em: 25 fev. 2012.

[136] Disponível em: <http://www.valor.com.br/internacional/1170402/obama-apresenta-nova-estrategia-de-defesa-dos-estados-unidos>. Acesso em: 25 fev. 2012.

No sítio do Governo Americano, disponível em: < http://www.defense.gov/news/Defense_Strategic_Guidance.pdf>. Acesso em: 25 fev. 2012.

Sustaining US Global Leadership: Priorities for 21st Century Defense:

Our planning envisages forces that are able to fully deny a capable state's aggressive objectives in one region by conducting a combined arms campaign across all domains – land, air, maritime, space, and cyberspace.

EUA mantém liderança global: Prioridades para a defesa no Século 21:

Nosso planejamento prevê as forças que são capazes de eliminar totalmente objetivos agressivos em uma região de um Estado capacitado, através da realização de uma campanha combinada de armas em todos os domínios - terra, aéreo, espaço e ciberespaço. (Tradução livre).

[137] Disponível em: <http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf>. Acesso em 30 jan. 2012.

[138] Disponível em: <http://www.canyoucrackit.co.uk/>. Acesso em 30 jan. 2012.

outros países também já divulgaram a criação de órgãos e políticas de defesa cibernética[139].

Em 2005, a União Europeia criou a Agência de Segurança Cibernética, a *European Network and Information Security Agency* – ENISA, que divulgou, em dezembro de 2011, o primeiro relatório de segurança cibernética no setor marítimo[140]; estudos sobre computação em nuvem também foram publicados em 2009 e 2011[141].

Em março de 2009, a Comissão Europeia publicou um plano de ação destinado a reforçar a segurança e a resiliência das infraestruturas críticas da informação[142]. A Agenda Digital para a Europa[143], adotada em maio de 2010, destaca a necessidade de um esforço geral para garantir a segurança e a resiliência das infraestruturas críticas da informação e responder às formas cada vez mais sofisticadas de ataques cibernéticos.

Em setembro de 2010, foi proposta uma diretiva para os ataques contra os sistemas de informação para reforçar a cooperação e responder às novas formas de ataques, incluindo *bootnets*, além da criação de centros de resposta a incidentes e

---

[139] A propósito, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. United Nations, Center for Strategic and International Studies*.
Disponível em: <http://unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf>, e em: <http://www.secupedia.info/wiki/Hauptseite>. Acesso em 30 jan. 2012.

[140] Disponível em: <http://www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector/cyber -security-aspects-in-the-maritime-sector-1>. Acesso em 30 jan. 2012.

[141] *Cloud Computing Information Assurance Framework* (2009), disponível em: <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport> e *Security and resilience in governmental clouds* (2011), disponível em: <http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/>. Acesso em 25 fev. 2012.

[142] "*Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência*" é o que dita o Comunicado n.º 149/2009 da Comissão Europeia. Disponível em: <http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=pt&DosId=198140>. Acesso em 26 fev. 2012. Também a Resolução do Conselho de 18 de Dezembro de 2009 sobre uma abordagem de colaboração europeia no domínio da segurança das redes e da informação (2009/C 321/01).
Já o processo *Meridian visa* dotar os governos de todo o mundo de um meio através do qual possam discutir o modo de cooperar em nível de políticas no que respeita à proteção das infraestruturas críticas da informação. Disponível em: <http://meridianprocess.org/Default.aspx>. Acesso em 26 fev. 2012.

[143] Disponível em: <http://europa.eu/legislation_summaries/information_society/strategies/si0016_pt.htm>. Acesso em 26 fev. 2012.

realização de exercícios simulados[144]. Na cimeira UE-EUA realizada em Lisboa em 2010, foi criado o Grupo de Trabalho UE-EUA para a cibersegurança e a cibercriminalidade com o objetivo de combater novas ameaças às redes globais[145].

A Organização do Tratado do Atlântico Norte (OTAN) considera que os conflitos cibernéticos estão entre as mais prováveis ameaças não convencionais da próxima década e já divulgou o entendimento de que um ataque cibernético contra uma infraestrutura crítica de um país membro pode ser equiparado a um ataque armado e justificar uma resposta militar, inclusive com medidas de defesa coletiva[146].

Após os ataques à Estonia, em 2007, os quais serão relatados adiante, a OTAN inaugurou o *Cooperative Cyber Defense Center of Excellence*[147] em maio de 2008. Na cimeira de Lisboa de 2010, a OTAN adotou o novo conceito estratégico segundo o qual pode atuar em qualquer lugar do mundo. Na seção "O Ambiente de Segurança", o ponto 12 destaca que os ciberataques estão a tornar-se mais frequentes, mais organizados e infligem danos mais custosos às administrações governamentais, empresas, economias e potencialmente às redes de transporte e logísticas e outras infraestruturas críticas; podem atingir um ponto em que ameaçam a prosperidade, segurança e estabilidade nacionais e euro-atlântica. Forças militares estrangeiras e serviços de inteligência, organizações criminosas, terroristas ou grupos extremistas podem, cada um, ser a fonte destes ataques. Para responder a esta ameaça, o ponto 19 estabelece que a OTAN terá as "capacidades necessárias para dissuadir e defender-se contra qualquer ameaça à Segurança das nossas populações (…), nomeadamente (…), levar a efeito a formação, exercícios, planos de contingência e troca de informações necessárias a assegurar a nossa defesa contra toda a gama de desafios de segurança convencionais e emergentes e proporcionar garantias visíveis e de reforço a todos os Aliados." Mais à frente, "(…) desenvolver a nossa capacidade de prevenir, detectar, defender e recuperar de ataques cibernéticos, inclusive usando o processo de planeamento da OTAN para

---

[144] Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:PT:HTML>. Acesso em 26 fev. 2012.
[145] Disponível em: <http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/10/315&format=HTML&aged=1& language=EN&guiLanguage=en>. Acesso em 26 fev. 2012.
[146] Disponível em: <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm> e em: <http://www.nato.int/cps/en/natolive /index.htm>. Acesso em 26 fev. 2012.
[147] Disponível em: <http://www.ccdcoe.org/>. Acesso em 26 fev. 2012.

reforçar e coordenar as capacidades nacionais de defesa cibernética, colocando todos os organismos da OTAN sob ciberproteção centralizada e melhor integrar a ciberconsciencialização (*cyber awareness*), alerta e resposta com os países membros"[148].

A Organização dos Estados Americanos (OEA) aprovou, em 2004, a adoção de uma Estratégia Interamericana Integral para combater as Ameaças à Segurança Cibernética, sendo um dos objetivos a criação de uma rede hemisférica, que funcione 24 horas por dia, sete dias por semana, de pontos nacionais de contato entre as Equipes de Resposta a Incidentes de Segurança em Computadores com mandato e capacidade de atuar em crises, incidentes e ameaças relacionadas à segurança em computadores[149].

Em janeiro de 2011, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) divulgou o relatório "*Reducing Systemic Cybersecurity Risk*"[150], elaborado por dois especialistas ingleses que avaliaram os riscos e as ameaças relacionados à guerra cibernética, chegando à conclusão de que o termo indevidamente utilizado representa uma remota possibilidade que não se confunde com espionagem e atividades ilícitas. Também acreditam os autores do relatório, que as futuras armas cibernéticas serão projetadas para explorar vulnerabilidades e para serem utilizadas em conjunto com outras armas.

A Organização das Nações Unidas debate a não proliferação de armas da informação no "*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*" e tem diversas resoluções[151] e iniciativas relacionadas à segurança cibernética no âmbito da União Internacional de Telecomunicações.

---

[148] Disponível em: <http://natolibguides.info/nsc>. Acesso em: 26 fev. 2012.
[149] Disponível em: <http://www.oas.org/xxxivga/portug/docs/doc_aprovados/adocao_estrategia_combater_seguranca_cibernetica.htm>. Acesso em 26 fev. 2012.
[150] Disponível em: <http://www.oecd.org/dataoecd/3/42/46894657.pdf>. Acesso em 26 fev. 2012.
[151] As Resoluções 55/63 e 56/121 da Assembleia Geral das Nações Unidas: sobre o combate ao uso doloso das tecnologias da informação. A Resolução 57/239 relativa à criação de uma cultura global de segurança cibernética. A Resolução 58/199 sobre a criação de uma cultura global de segurança cibernética e a proteção de sistemas críticos de informação.

Os Estados Unidos e países da União Europeia já realizaram, conjuntamente, exercícios de simulação de guerra cibernética durante eventos como o *Cyber Atlantic* 2011[152] e *Cyber Europe* 2010, promovido pela Agência de Segurança Cibernética da União Europeia, a *European Network and Information Security Agency* – ENISA, envolvendo mais de setenta especialistas de organizações públicas que enfrentaram mais de trezentos ataques simulados para paralisar a Internet e serviços críticos da Europa[153].

No Brasil, o Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEX) e o Centro de Instrução de Guerra Eletrônica (CIGE) realizaram o 1º Exercício de Guerra Cibernética das Forças Armadas nos dias 31 de outubro e 1º de novembro de 2011, com o objetivo de habilitar militares para empregar ferramentas e técnicas de guerra cibernética. No exercício, foi simulada uma situação de conflito na qual eram utilizadas armas cibernéticas e exploradas as possíveis vulnerabilidades de infraestruturas críticas nacionais a serem defendidas pelos participantes[154].

Tais movimentos confirmam que as ameaças do Século XXI não têm fronteiras e que os conflitos cibernéticos são tratados como assunto estratégico, além de confirmar que qualquer medida de ataque ou de defesa é preparada com antecedência, conforme comentários no decorrer da entrevista de Clarke[155], segundo o qual os países já estão se infiltrando nas redes uns dos outros, e instalando portas dos fundos, para terem acesso rápido a essas redes quando precisarem, pois para realizar um ataque cibernético é preciso fazer com que os

---

Comentários no sítio da Organização dos Estado Americanos – OEA, conforme disponível em: <http://www.oas.org/xxxivga/portug/docs/doc_aprovados/adocao_estrategia_combater_seguranca_cibernetica.htm> Acesso em: 26 fev. 2012.

[152] Disponível em: <http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011>. Acesso em: 26 fev. 2012.

[153] Disponível em: <http://www.enisa.europa.eu/media/press-releases/eu-agency-enisa-issues-final-report-video-clip-on-cybereurope-2010-the-1st-pan-european-cyber-security-exercise-for-public-bodies>. Acesso em: 26 fev. 2012.

[154] Disponível em: <http://www.ccomgex.eb.mil.br/noticias/est_guerra_ciber.pdf>. Acesso em: 26 fev. 2012. A Rede Nacional de Pesquisa também realizou, durante o Seminário de Capacitação e Inovação de 2011, exercícios simulados de ações de apoio ao ETIR Central – Equipe Central de Tratamento e Resposta a Incidentes de um país fictício ameaçado por ataques cibernéticos.

[155] Entrevista com Richard Clarke disponível em: <http://www.youtube.com/watch?v=9JnXrtLIp1k>. Acesso em 26 fev. 2012. Clarke foi o responsável pela estratégia de combate ao terrorismo cibernético no Governo Bush e pelo estudo que levou Barack Obama a criar o comando de defesa cibernética.

trens parem, que a água deixe de ser bombeada, que oleodutos explodam, que a energia seja cortada e “se o presidente disser a você que quer fazer tal coisa, não é possível começar naquele dia e tentar invadir as redes”.

3.1 Os Ataques Cibernéticos

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil define ataque como a tentativa, bem ou malsucedida, de acesso ou uso não autorizado a um programa de computador, além das tentativas de negação de serviço; também define invasão como um ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador[156].

Qualquer sistema que permita a entrada de dados, por meios físicos ou redes sem fio, pode ser alvo de espionagem ou ataques cibernéticos, os quais desafiam medidas de prevenção, detecção e resposta, mitigação e recuperação, além de preservação de evidências digitais relevantes para uma investigação.

Em audiência realizada no início de fevereiro de 2012 pelo Senado americano com representantes da CIA e do FBI, ao lado da proliferação das armas, da espionagem e do terrorismo, os ataques cibernéticos patrocinados por atores estatais ou não estatais foram colocados como uma das principais ameaças do futuro[157].

De acordo com dados divulgados em janeiro de 2012 pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil[158], o país registrou seu maior índice de ataques em 2011: aproximadamente quatrocentos mil

[156] Disponível em: <http://cartilha.cert.br/glossario/>. Acesso em: 26 fev. 2012.
[157] Disponível em: <http://informationweek.itweb.com.br/6866/ataques-ciberneticos-se-tornam-principal-ameaca-terrorista-diz-fbi/>. Acesso em: 26 fev. 2012.
[158] Disponível em: <http://www.cert.br/stats/incidentes/2011-jan-dec/analise.html>. Acesso em: 26 fev. 2012.

incidentes agrupados em tentativas de fraude (páginas falsas de bancos e de comércio eletrônico, cavalos de troia utilizados para roubo de informações e credenciais), ataques a servidores *web* (para hospedar páginas falsas, cavalos de troia, *scripts* para *spam* ou *scam* e ferramentas de ataque), varreduras e propagação de códigos maliciosos e outros incidentes. As 320 grandes redes governamentais contabilizadas e controladas pelo Departamento de Segurança da Informação e Comunicações da Presidência da República sofrem, em média, 4 milhões de ataques por ano e 2.100 ataques por hora[159].

Em 2011, a empresa *McAfee* divulgou um relatório do que pode ser a maior série de invasões ou ataques cibernéticos da história[160], envolvendo espionagem em redes de mais de setenta organizações, governos e empresas - inclusive fabricantes de material bélico ou de alta tecnologia - que poderia ter a China como protagonista estatal.

Os ataques cibernéticos têm diferentes níveis de gravidade que diferem conforme os objetivos ou atores envolvidos, que podem variar entre amadores, *hackers*[161], *crackers*[162], grupos ativistas, crime organizado, grupos terroristas ou Estados. Conforme será elucidado adiante, dependendo da sofisticação e das finalidades dos ataques cibernéticos, eles podem ser associados à prática de ativismo, crimes, espionagem, terrorismo ou guerra cibernética - o objeto deste estudo.

Ocorre que a identificação da origem e da autoria de um ataque hostil pode ser um grande desafio em razão da utilização de técnicas que dificultam as investigações, o que tende a se agravar quando ocorre em contexto de conflitos, no

---

[159] De acordo com Raphael Mandarino Júnior, em entrevista concedida em setembro de 2011, Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=28035&sid=18>. Acesso em: 26 fev. 2012.

[160] Disponível em: <http://www.nytimes.com/2011/08/04/technology/security-firm-identifies-global-cyber-spying.html>. Acesso em: 26 fev. 2012.

[161] *Hackers* são indivíduos que elaboram e modificam *software* e *hardware* de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas, além de terem muito conhecimento em informática. Os *hackers* utilizam todo o seu conhecimento para melhorar *softwares* de forma legal. Disponível em: <http://pt.wikipedia.org/wiki/Hacker>. Acesso em: 26 Fev 2012.

[162] *Crackers* é o termo usado para designar quem pratica a quebra (*cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por *hackers* em defesa contra o uso jornalístico do termo *hacker*. Podem ser classificados em *crackers* de criptografia, *crackers* de *softwares* e desenvolvedores de vírus, *worms*, *trojans* e outros *malwares*. Disponível em: <http://pt.wikipedia.org/wiki/Cracker>. Acesso em: 26 Fev 2012.

qual a cooperação internacional pode ser completamente inviável. Além disso, as ferramentas e tecnologias utilizadas estão em constante modificação, surgindo, diariamente, novas técnicas que exploram outras vulnerabilidades, citando-se, como exemplo, a tendência de aumento de aplicações maliciosas para explorar dispositivos móveis[163].

3.1.1 Ferramentas e Técnicas de Ataques Cibernéticos

O rol das ferramentas de ataques cibernéticos é bastante diversificado e algumas delas se aproximam de métodos de espionagem ou de inteligência cibernética, os quais podem variar desde programas governamentais secretos até besouros espiões[164].

As investidas cibernéticas podem utilizar desde técnicas menos sofistificadas e amplamente divulgadas na própria Internet - que podem afetar infraestruturas críticas da informação dependendo da proporção - até técnicas novas e complexas, especialmente desenvolvidas para atingir determinado alvo.

Das inúmeras ferramentas e ténicas de ataque, constantemente reinventadas[165], algumas se destacam em razão da sofisticação ou da gravidade da sua repercussão, características que as elevam ao patamar de ameaças à segurança nacional, equiparáveis a armas de guerra, que podem envolver desde as redes governamentais e a cadeia de fornecedores das infraestruturas críticas até

[163] Disponível em: <http://computerworld.uol.com.br/seguranca/2011/12/02/malwares-em-dispositivos-moveis-vao-dobrar-em-2012/>. Acesso em 26 fev.2012.
[164] Disponível em: <http://noticias.r7.com/tecnologia-e-ciencia/noticias/cientistas-criam-besouros-controlados-por-controle-remoto-para-gravar-conversas-20091019.html>. Acesso em 26 fev.2012.
[165] No Brasil, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança desenvolve projetos de análise de tendências de ataques, mantendo uma rede distribuída de *honeypots* para aumentar a capacidade de detecção de incidentes e correlação de eventos, além de *spampots* para colher dados de utilização da infraestrutura da Internet para o envio de *spam*. Disponível em: <http://www.cert.br/projetos/>. Acesso em 26 fev. 2012.

redes privadas ou usuários de redes sociais, os quais podem ser involuntários participantes de ataques cibernéticos.

Além disso, como já foi apontado em relatórios anteriormente referidos, a porta de entrada de alguns ataques cibernéticos que podem comprometer infraestruturas pode estar na cadeia de fornecedores de produtos ou serviços.

Em março de 2011, a empresa de segurança RSA, fornecedora de *tokens* de identificação ao Pentágono, à fabricante de armas *Lockheed Martin*, a grandes bancos, etc., sofreu um ataque deflagrado a partir de um *e-mail* enviado ao departamento de recursos humanos, do qual resultou o vazamento de informações sobre um dos mais valiosos códigos, segredo de geração de chaves dos *tokens*; posteriormente, a empresa *Lockheed Martin* também sofreu ataques. O ataque foi realizado por dois grupos de *hackers* e foi considerado sofisticado a ponto de ser atribuído a outro Estado.[166]

Em fevereiro de 2012, a empresa *Symantec*, uma das maiores desenvolvedoras de *sofwares* de segurança, sofreu extorsão de um grupo que cobrou US$50 mil para abster-se de publicar na Internet um código fonte da programação de vários produtos supostamente roubado[167].

Sem a pretensão de esgotar as hipóteses ou aprofundar tecnicamente a descrição, as técnicas de ataque cibernético mais divulgadas serão descritas a seguir, com a ressalva de que, diariamente, novas técnicas são desenvolvidas, especialmente as voltadas para as redes sociais e para os dispositivos móveis.

Os conceitos, a seguir reproduzidos, foram extraídos da Cartilha de Segurança do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil:[168]

---

[166] Disponível em: <http://www.zdnet.co.uk/news/security-threats/2011/10/11/rsa-nation-state-double-teamed-on-securid-attack-40094162/>. Acesso em 26 fev. 2012.
[167] Disponível em: <http://www.valor.com.br/impresso/empresas/symantec-diz-ter-sido-alvo-de-tentativa-de-extorsao>. Acesso em: 26 fev. 2012.
[168] Disponível em: <http://cartilha.cert.br/glossario/> Acesso em: 26 fev. 2012.
A descrição de outras ameaças pode ser encontrada no relatório denominado “Os maiores riscos de segurança cibernética” do *Sans Institute*, disponível em: <http://www.sans.org/top-cyber-security-

Backdoor: Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Bot: Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc.

Botnets: Redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc.

Cavalo de troia: Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Código malicioso: Termo genérico que se refere a todos os tipos de programas que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de troia, *rootkits*, etc.

DDoS: Do inglês ***D****istributed* ***D****enial* ***o****f* ***S****ervice*. Ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

DoS: Do inglês ***D****enial* ***o****f* ***S****ervice*.

Engenharia social: Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Exploit: Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador.

Keylogger: Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

Malware: Do Inglês ***Mal****icious soft****ware*** (*software* malicioso). Veja Código malicioso.

Negação de serviço: Atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

Phishing: Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir

---

risks/> e em: <http://www.sans.org/top-cyber-security-risks/pdfs/portuguese.pdf> >. Acesso em: 26 fev. 2012.

O *Center for Strategic and International Studies* divulgou estudo sobre vinte controles críticos necessários para a segurança cibernética, no qual são apontadas as principais ameaças cibernéticas: Disponível em: <http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf>. Acesso em: 26 fev. 2012.

> usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros
>
> ***Rootkit:*** Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.
>
> ***Scam:*** Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.
>
> ***Scanner:*** Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
>
> ***Screenlogger:*** Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazenar a região que circunda a posição onde o *mouse* é clicado. Veja também *Keylogger*.
>
> ***Sniffer:*** Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.
>
> ***Spyware:*** Termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.
>
> ***Worm:*** Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

Outra técnica relevante, quando se fala em guerra cibernética, é conhecida como *zero-day exploit*[169] ou “dia zero”, que consiste na exploração de vulnerabilidades ou falhas em *softwares* que ainda não receberam correções. A esteganografia, ferramenta de segurança – que não se confunde com criptografia - utilizada para ocultar informações dentro de outros dados (imagens, por exemplo), também pode ser empregada na guerra cibernética.

---

[169] Foi a técnica utilizada no ataque à usina nuclear do Irã pelo Stuxnet, que explorou as vulnerabilidades do sistema SCADA da Siemens.
Disponível em: <http://www.zerodayinitiative.com/advisories/upcoming/>. Acesso em: 26 fev. 2012.

Além disso, existem diversas técnicas para dificultar a investigação da origem e da verdadeira autoria de um ataque e outras para deflagrar ataques a partir de países que tenham um sistema jurídico e policial frágil, o que minimiza os riscos dos atacantes.

3.2 A Guerra Cibernética

A história da humanidade sempre foi permeada pela existência de conflitos, mudando apenas os protagonistas, os objetivos, as estratégias e as armas utilizadas. A guerra pode ser descrita por conceitos jurídicos, militares, técnicos, dentre outros e os quais se diversificam no tempo.

Os conflitos armados são regidos por regras do direito internacional, as quais foram elaboradas quando sequer eram cogitados os conflitos cibernéticos, que ainda estão mais próximos do conceito da guerra irregular, na qual forças não regulares são empregadas ou forças regulares são empregadas fora dos padrões de normas da guerra convencional[170].

Decorrência de interesses conflitantes não conciliados pela via diplomática, a guerra acontece quando a solução pacífica de conflitos não pode ser atingida, pois, conforme Clausewitz (1832), a guerra é a continuação da política por outros meios[171].

Todavia, não obstante a indiscutível relevância da clássica doutrina clausewitziana, é importante considerar que o momento histórico de sua concepção,

---

[170] Glossário das Forças Armadas, Ministério da Defesa, Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007 (MD35-G-01, 4ª Edição/2007). Disponível em: <https://www.defesa.gov.br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/MD35_G_01_GlossarioFA_4aEd2007.pdf>. Acesso em 26 fev. 2012.

[171] CLAUSEWITZ, Carl Von. *On war.*
A sua obra póstuma "Da Guerra", publicada em 1832, rechaçava a "guerra pela guerra". Disponível em: <http://www.gutenberg.org/files/1946/1946-h/1946-h.htm>. Acesso em: 26 fev. 2012.

no início do Século XIX, contava com um sistema internacional que espelhava uma "simetria equipolar" formal em relação ao poderio militar dos Estados-Nações, no qual não existiam as armas de destruição em massa, hábeis a promover a guerra total, na qual os beligerantes empregam todo o seu Poder Nacional, sem restrições quanto aos métodos e engenhos e mesmo quanto às leis convencionais de guerra[172].

Da mesma forma, o desenvolvimento de armas cibernéticas por atores estatais e não estatais, bem como as graves consequências possíveis das investidas cibernéticas sugerem a necessidade de uma releitura não apenas das regras jurídicas, mas também das doutrinas diplomáticas e militares, pois além do desequilíbrio de capacidades cibernéticas, as novas táticas organizacionais, doutrinárias e tecnológicas da guerra cibernética podem configurar uma Revolução em Assuntos Militares (HALPIN, 2006)[173].

Até mesmo as milenares e eternas recomendações deixadas por Sun Tzu, na obra Arte da Guerra[174], continuam válidas, porém precisam de adaptações para a realidade cibernética. Alguns fatores precisam ser somados às táticas de Sun Tzu, conforme descrito por Geers (2011, p. 20-21)[175] na obra *Sun Tzu and Cybe War:*

> 1. A Internet é um ambiente artificial que pode ser moldado em parte de acordo com os requisitos de segurança nacional.
>
> 2. A proliferação de tecnologias e ferramentas de *hacker* faz com que seja impossível estar familiarizado com todos eles.
>
> 3. A proximidade dos adversários é determinada pela conectividade e largura de banda e não pela geografia terrestre.
>
> 4. As atualizações de *software* e reconfigurações de rede mudam o espaço da batalha cibernética de forma imprevisível e sem aviso prévio.
>
> 5. Ao contrário de nossa compreensão histórica da guerra, o conflito cibernético favorece ao atacante.
>
> 6. Ciberataques são flexíveis o suficiente para serem eficazes para propaganda, espionagem e para a destruição de infraestrutura crítica.

---

[172] Glossário das Forças Armadas, Ministério da Defesa, Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007 (MD35-G-01, 4ª Edição/2007). Disponível em: <https://www.defesa.gov.br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/MD35_G_01_GlossarioFA_4aEd2007.pdf>. Acesso em 26 fev. 2012.

[173] HALPIN, Edward et al. *Cyberwar, Netwar and the Revolution in Military Affairs*.

[174] Disponível em: <http://www.gutenberg.org/catalog/world/readfile?fk_files=2351771&pageno=1>. Acesso em: 26 fev. 2012.

[175] GEERS, Kenneth. *Sun Tzu and cyber war*, p. 20-21.
Disponível em: <http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf>. Acesso em: 26 fev. 2012. Tradução Livre.

> 7. A dificuldade de obter-se a identificação confiável de responsáveis por ciberataque diminui a credibilidade da dissuasão, a retaliação e a acusação.
>
> 8. A natureza "calma" do ciberconflito denota que uma batalha significativa poderia ocorrer com o conhecimento apenas dos participantes diretos.
>
> 9. A falta de experiência e provas podem fazer da vitória, da derrota e dos danos de batalha um empreendimento altamente subjetivo.
>
> 10. Há poucas inibições morais a ataques cibernéticos, pois se referem principalmente ao uso e abuso de dados e código de computador. Até agora, pouco percebido como sofrimento humano.

A revista *The Economist*, de julho de 2010, categoriza o espaço cibernético como o quinto domínio da guerra, no qual a linha divisória entre a criminalidade e a guerra é bastante tênue, além de destacar que o custo relativamente baixo de apropriação das ferramentas cibernéticas pode ser explorado por grupos terroristas para comunicação e propaganda[176].

Embora a teoria do poder cibernético ainda não esteja suficientemente madura para extrair qualquer conclusão segura a respeito dos seus impactos nas relações internacionais, Nye (2010) prevê que a habilidade de usar o espaço cibernético para influenciar e trazer vantagens em outros ambientes poderá ser explorada tanto por mecanismos de *hard power* (poder de coerção) quanto de *soft power* (poder de cooptação e persuasão)[177].

O glossário das Forças Armadas define guerra cibernética como:

> "o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil."

É diferente da guerra eletrônica, cujo conceito, no mesmo glossário, é:

---

[176] *Ciberwar: The threat from the internet*. The Economist, julho de 2010, EUA, New York, p. 11-12. Disponível em: <http://www.economist.com/node/16481504>. Acesso em: 20 dez. 2011.

[177] NYE, Joseph. *Cyber Power***.** Belfer Center For Science and Internacional Affairs. Harvard Kennedy School. Cambridge. 2010. Disponível em: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. Acesso em: 11 nov. 2011. Além disso, na obra *The Future of Power* (New York: PublicAffairs, 2011), Nye destaca que o mundo está assistindo duas formas relevantes de redistribuição do poder entre Estados e dos Estados para atores não estatais; também discorre sobre o *cyber power* e trabalha com o conceito de *Smart Power*, o qual representa a capacidade de desenvolver uma estratégia que combine *Hard e Soft Power*, essencialmente a partir da força militar e das capacidades diplomáticas.

> "o conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas".

Segundo a clássica definição de Martin C. Libicki (1995) [178], a guerra cibernética é um dos vetores ou ramificações da guerra da informação, que pressupõe a combinação de técnicas da guerra de comando e controle[179], da guerra baseada na inteligência, da guerra eletrônica, de operações psicológicas, guerra de *hackers*, guerra de informações econômicas, além das técnicas da guerra cibernética. Na definição de Cepik (2003, p. 69) [180] :

> "O conceito de *information warfare* (IW) resulta da tentativa de integração e expansão das operações de guerra eletrônica, guerra de comando e controle (C2 *warfare*) e disciplinas defensivas em inteligência. Por analogia com a guerra terrestre ou marítima, a guerra informacional compreende o conjunto de ações ofensivas e defensivas conduzidas no ambiente informacional para controlar o *cyberspace*. Ciberespaço é aqui entendido como o 'lugar' onde interagem computadores, programas, sistemas de comunicação e equipamentos que operam via irradiação de energia no espectro eletromagnético. Porém, menos por um 'lugar' ou um conjunto classificável de ações, a guerra informacional define-se melhor por seus objetivos: obter e manter superioridade informacional na batalha ou na guerra. Ações tão diferentes entre si como um ataque aéreo a uma central de telecomunicações, operações de *sigint*, missões aéreas para reconhecimento do campo de batalha ou a implantação clandestina de códigos de computador com 'bombas lógicas' poderiam ser parte de uma campanha de guerra informacional. Destaque-se que essas operações de IW não devem ser tomadas como configurando uma 'guerra' à parte. A guerra permanece una e indivisível enquanto realidade; o que está em jogo é a perspectiva – ainda não consolidada ou atestada como mais útil do que a preocupação com esse tema por organizações combatentes já consolidada – de criação de uma 'arma' ou especialidade combatente de informações."

Parks e Duggan (2001)[181] também definem a guerra cibernética como um conjunto da guerra da informação que envolve ações no mundo cibernético, ou seja,

---

[178] LIBICKI, Martin C. *What is information warfare*?", 1995 Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA367662>. Acesso em 24 fev. 2012.
Além disso, vale destacar a classificação proposta por Alvin e Heidi Toffler, segundo a qual a onda da guerra da informação sucedeu à onda das guerras industriais e à onda das guerras agrícolas. *War and anti-War: Survival at the Dawn of the 21st Century* (New York: Warner Books, 1995)

[179] Uso coordenado de ações de segurança, despistamento, operações psicológicas, guerra eletrônica e destruição física, apoiadas por um sistema de inteligência, destinadas a negar informações, influenciar, degradar ou neutralizar capacidades de comando e controle do oponente, protegendo, ao mesmo tempo, a estrutura de comando e controle amiga. Glossário FFAA.

[180] CEPIK, Marco A.C. *Espionagem e democracia*, p. 69. Disponível em: <http://www.editora.fgv.br/?sub=produto&id=104>. Acesso em 2. jan. 2012.

[181] PARKS, Raymond C., DUGGAN, David P. *Principles of cyber-warfare.* Disponível em: <http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf>. Acesso em 20 jan. 2012. Tradução livre.

qualquer rede de computadores, das quais a Internet e as redes a ela relacionadas são as mais relevantes. Para os autores, a definição militar mais próxima de tal conceito é a combinação de ataque e defesa de redes de computadores, incluindo operações especiais de informação. Além disso, propuseram alguns princípios para a guerra cibernética:

- Princípio do Efeito Cinético;
- Princípio da Dissimulação e Visibilidade;
- Princípio da Mutabilidade;
- Princípio do Disfarce;
- Princípio da Dualidade do Armamento;
- Princípio da Compartimentação e da Usurpação;
- Princípio da Incerteza;
- Princípio da Proximidade.

Costuma-se atribuir à guerra cibernética a assimetria, característica das guerras de quarta geração ou guerras do futuro, cujos teóricos a caracterizam pelas mudanças de protagonistas, objetivos e ferramentas de combate, com um possível retorno às táticas que antecederam a Paz de Westphalia, nas quais era significativa a participação de atores não estatais e utilização de meios diversos das forças militares. Além disso, os níveis tático e físico tendem a não ser tão decisivos quanto os níveis operacional, estratégico e moral (LIND, 2005, p. 13)[182]. Em outras palavras, o conceito de guerra de quarta geração rompe com o estereótipo da guerra como a mera confrontação formal e direta entre duas Forças regulares de Estados nacionais antagônicos (VISACRO, 2011, p. 53) [183].

Um pequeno grupo de pessoas, ou mesmo um único indivíduo detentor de informações e conhecimentos específicos, com poucos recursos, pode representar uma grande ameaça a uma organização ou a um Estado, elos mais fortes, porém mais vulneráveis na medida em que seu gigantismo e complexidade podem dificultar um controle constante e efetivo de seus sistemas e ativos de informação.

Em tal contexto, pode ser difícil identificar o inimigo, pois as distâncias são relativizadas. O caminho percorrido pela informação nem sempre corresponde a pequenas distâncias em termos geográficos, pois segue uma lógica de roteamento e

---

Também a respeito: FARMER, David B., *Do the principles of war apply to cyber war?.* Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA522972>. Acesso em: 20 jan 2012.

[182] LIND, William S. *Compreendendo a guerra de quarta geração*. p. 13.

[183] VISACRO, Alessandro. *Os desafios da transformação,* p. 53.
O autor faz um quadro comparativo com as características das guerras de cada geração.

configurações que independe das tradicionais fronteiras. Em outras palavras, a lógica do espaço cibernético está vinculada a aspectos técnicos e não geográficos. Por isso os comandos de ataque podem percorrer grandes distâncias, passando por diversos territórios, em pouco tempo, dificultado o rastreamento e a identificação da origem e autoria de um ataque cibernético.

O ambiente cibernético pode ser considerado, portanto, um novo domínio ou palco de batalha, depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético. Os contornos da guerra cibernética, todavia, contemplam fatores e variáveis diversos que exigem novos raciocínios de defesa, pois as hostilidades no ambiente cibernético podem se desenrolar de formas distintas, que nem sempre permitem identificar o oponente e seus objetivos, a real origem, muito menos o momento e o impacto do ataque. Por isso, embora alguns conceitos da guerra cinética possam ser aplicados à guerra cibernética, outros chegam a ser antagônicos, embora seja certo que os efeitos de um ataque cibernético possam ser tão ou até mais nefastos quanto os de uma guerra convencional se afetarem infraestruturas críticas.

Os possíveis alvos na guerra cibernética não são, portanto, apenas sistemas governamentais ou de defesa, mas também podem ser sistemas e redes correlatos a serviços cuja indisponibilidade pode comprometer a segurança ou causar colapso, econômico ou não, tais como o setor energético, usinas elétricas, hidrelétricas, petrolíferas e nucleares, telecomunicações, logística e transporte, segurança e emergência, redes hospitalares, instituições financeiras e polos tecnológicos.

Em tal contexto, a definição do campo de batalha e dos alvos está cada vez mais difícil, pois os ataques cibernéticos podem afetar sistemas, lideranças e cidadãos em qualquer parte do mundo, em tempo de paz ou em tempo de guerra, com um relativo anonimato assegurado ao agressor, dificultando a retaliação.

Existe uma corrente que não reconhece a existência da guerra cibernética, mas a necessidade das medidas de segurança para combater crimes e espionagem. Em março de 2010, o então coordenador de segurança cibernética da Casa Branca, Howard Schmidt, afirmou que não há guerra cibernética, porque, em termos legais,

o estado de guerra pressupõe uma declaração formal[184]. Tal entendimento contradiz Michael McConnell, ex-diretor de inteligência dos EUA que, dias antes, havia afirmado que o país estava em guerra cibernética e estava perdendo[185].

Na opinião de Richard Clarke [186], se um país declarar guerra contra o outro, os ataques cibernéticos ocorrerão com a frequência de uma guerra comum e serão utilizados, por exemplo, para derrubar redes elétricas. Na sua definição:

> "Guerra Cibernética é o acesso não autorizado - por, em nome de ou em apoio a um Estado - a um computador ou rede de computadores de outro Estado, ou qualquer outra atividade que afete um sistema de computador, em que a finalidade seja adicionar, alterar ou falsificar dados ou causar a interrupção ou danos em um computador, dispositivo de rede ou nos objetos controlados por um sistema computadorizado." (CLARKE, 2010)[187]

A guerra cibernética objeto desta abordagem, portanto, diz respeito aos conflitos que podem envolver diferentes países, situação que não se confunde com o terrorismo ou com os crimes cibernéticos, adiante conceituados - não obstante tais situações também possam afetar Estados, quando praticados por indivíduos ou organizações que atuam por motivos ideológicos ou financeiros contra governos ou redes, sistemas, estruturas, instalações e serviços estratégicos.

Na realidade, especialmente enquanto a comunidade internacional não definir regras a respeito da guerra cibernética, é bastante provável que qualquer país que pretenda realizar uma ofensiva contra outro busque camuflar suas ações como atos criminosos ou terroristas do ambiente cibernético, razão pela qual os temas podem estar conectados, embora sejam distintos.

Ainda não existem definições e doutrina consolidadas, muito menos normas jurídicas a respeito da guerra cibernética. Não obstante, o fato é que os países estão se mobilizando para desenvolver novas estratégias de defesa e segurança, porque

---

[184] Disponível em: <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>. Acesso em: 28 jul. 2011.
[185] Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html>. Acesso em: 28 jul. 2011.
[186] Disponível em: <http://www.conjur.com.br/2011-mar-11/ideias-milenio-ataques-ciberneticos-tornaram-armas-guerra>. Acesso em: 25 jul. 2011.
[187] CLARKE, Richard. *Cyber war: the next threat to national security and what to do about it*. Disponível em: <http://www.richardaclarke.net/cyber_war.php?ch=7#excerpts>. Acesso em: 28 jul. 2011. Tradução livre.

alguns eventos envolvendo o espaço cibernético já foram suficientes para evidenciar não apenas as vulnerabilidades, mas também o grande e efetivo potencial das ameaças cibernéticas para colocar a segurança dos países em risco e estremecer as relações internacionais. Por tais razões, expressões como corrida armamentista ou guerra fria no ciberespaço, “*pearl harbor* eletrônico”, “11 de setembro digital” e “*cibergedom*” deixam de parecer especulações para ocupar espaço entre as questões relevantes para todos os países.

3.2.1 Possíveis precedentes de guerra cibernética

Dos incontáveis conflitos no espaço cibernético que já foram noticiados, alguns se diferenciam dos corriqueiros ataques porque envolvem diferentes países como possíveis protagonistas em polos adversos ou apenas como alvos de ataques, algumas vezes também figurando empresas privadas no meio do campo de batalha.

Não obstante, até a presente data, nenhum governo admitiu oficialmente a utilização de ofensivas cibernéticas, assim como não foram divulgadas provas cabais que permitam definir a origem e atribuir a autoria a qualquer Estado.

Embora os inúmeros relatos de ataques cibernéticos contra governos sejam contemporâneos à própria criação e desenvolvimento do espaço cibernético, os casos a seguir relatados - escolhidos por razões exclusivamente didáticas, sem juízo de valor sobre os fatos tais como noticiados mundialmente - emprestam utilidade ao propósito do trabalho para demonstrar que as crises entre diferentes Estados podem ser migradas e fomentadas no ciberespaço, o que explica a atenção dedicada ao tema por estrategistas.

Os ataques sofridos pela Estônia[188], país amplamente informatizado, em 2007, deflagrado pela remoção de um memorial de guerra da era soviética de uma praça da capital Tallinn, culminou com uma série de ataques cibernéticos dirigidos contra portais do governo, da imprensa e de empresas privadas, causando um "*blackout*" na internet estoniana por várias semanas, o qual levou meses para ser totalmente superado. Os ataques foram atribuídos à Rússia - que oficialmente negou a acusação – e tiveram origem em diversos locais, incluindo supostos provedores do governo russo, razão pela qual o episódio é considerado a primeira guerra cibernética, embora não declarada. O episódio, sem precedentes, levou a OTAN – Organização do Tratado do Atlântico Norte a enviar especialistas em terrorismo virtual à Estônia para auxiliar nas investigações e a criar o Centro de Excelência para a Cooperação em Defesa Cibernética, em maio de 2008, na Estônia[189]. Ataques similares à Geórgia, em 2008[190], também atribuídos e não reconhecidos pela Rússia, ocorreram poucas semanas antes e durante um conflito entre os dois países, também causaram um apagão cibernético, afetando agências governamentais e infraestruturas tecnológicas pouco antes da chegada dos russos.

Em setembro de 2007, Israel realizou ataque aéreo à Síria[191] para bombardear uma suposta usina nuclear que seria construída com a Coreia do Norte; o governo israelense teria se infiltrado no sistema de defesa aérea da Síria, porque os aviões israelenses não foram detectados por radares, o que possivelmente ocorreu em razão da utilização de programas específicos para burlar os sistemas sírios de controle de tráfego, que transmitiram sinais falsos.

Também em 2007, a China[192] foi acusada de atacar redes governamentais, instalando programas (*trojan horses*) no sistema de e-mails do Departamento de Defesa americano, no Pentágono, nos computadores do governo da Inglaterra, nos computadores dos ministros e da chanceler alemã Angela Merkel. A China negou as acusações, mas admitiu que seus programas contemplam a utilização de

---

[188] Disponível em: <http://www.guardian.co.uk/russia/article/0,,2081438,00.html> Acesso em: 30 jul. 2011.
[189] Disponível em: <http://www.ccdcoe.org/> Acesso em: 30 jul. 2011.
[190] Disponível em: <http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf> Acesso em: 30 jul. 2011.
[191] Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,ERT198270-17773,00.html> Acesso em: 30 jul. 2011.
[192] Disponível em: <http://veja.abril.com.br/120907/p_078.shtml> Acesso em: 30 jul. 2011.

computadores em eventuais ações militares. Recentemente, em maio de 2011, hackers chineses afirmam ter invadido o sistema da rede elétrica da Letônia[193].

A Coreia do Norte é apontada como responsável pelos ataques realizados, em julho de 2009, contra sites governamentais, de instituições financeiras e de imprensa nos Estados Unidos e na Coreia do Sul, manipulando aproximadamente 40 (quarenta) mil computadores "zumbis"[194]. O episódio teria se repetido recentemente, em maio de 2011[195], quando um dos maiores bancos da Coreia do Sul foi paralisado por causa de ataques cibernéticos também atribuídos à Coreia do Norte.

Em outubro de 2010, o vírus "*stuxnet*", supostamente desenvolvido pelos governos israelense e americano[196], foi infiltrado, possivelmente por um *pen drive*, nos sistemas do reator nuclear de Bushehr, no Irã, construído pela Rússia, com a finalidade de inutilizar centrífugas aumentando sua rotação, enquanto sinais de normalidade eram enviados para o controle. O episódio afetou o projeto nuclear iraniano e por isso é amplamente noticiado como espécie de ataque de guerra cibernética. A empresa russa de segurança da computação *Kaspersky Labs* afirmou, em dezembro de 2011, que o *Stuxnet* pode ser o primeiro de um conjunto de armas cibernéticas[197].

Em junho de 2011[198], diversos portais governamentais brasileiros, como da Presidência da República, da Receita Federal e da Petrobrás, foram alvos de ataques cibernéticos assumidos pelo grupo *Lulz Security Brazil*, um braço do grupo internacional que também já teria invadido servidores da agência de inteligência e da polícia federal americanas, a CIA e o FBI; o grupo afirmou, no *Twitter*, que o ataque seria um protesto contra a corrupção e o aumento dos combustíveis. No mesmo

---

[193] Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/05/hackers-chineses-dizem-ter-invadido-rede-eletrica-da-letonia.html> Acesso em: 30 jul. 2011.
[194] Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,ERT198270-17773,00.html> Acesso em: 30 jul. 2011.
[195] Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2011/05/110503_coreias_banco_ataque_cc.shtml> Acesso em: 30 jul. 2011.
[196] Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all> Acesso em: 30 jul. 2011.
[197] Disponível em: <http://blogs.estadao.com.br/link/tag/stuxnet/> Acesso em: 30 jul. 2011.
[198] Disponível em: <http://www.teletime.com.br/22/06/2011/hackers-declaram-guerra-virtual-as-paginas-do-governo/tt/ 229147/news.aspx> Acesso em: 30 jul. 2011.

período, o grupo *Fatal Error Crew*[199], que já havia atacado o portal da Presidência em janeiro de 2011, divulgou o endereço de 500 (quinhentos) portais de Prefeituras e Câmaras Municipais atacadas. Em audiência pública realizada em julho de 2009 pela Câmara dos Deputados[200], Raphael Mandarino Júnior, diretor de segurança da informação do Gabinete de Segurança Institucional da Presidência da República, relatou que uma quadrilha do Leste Europeu invadiu um servidor de computadores de um órgão público, trocou a senha e pediu um resgate de US$ 350 mil (trezentos e cinquenta mil dólares) para devolver a senha antiga, o que não ocorreu porque o controle foi recuperado.

Durante o mês de janeiro de 2012, Israel sofreu uma série de ataques cibernéticos realizados por supostos *hackers* palestinos que afetaram portais da bolsa de valores, jornais e hospitais, além de expor dados de cartões de crédito de israelenses. Os ataques levaram o Vice-Ministro de Relações Exteriores a declarar que seriam ataques terroristas, os quais seriam respondidos com força por causa da violação da soberania cibernética do país. No período, o porta-voz do Hamas na Faixa de Gaza cumprimentou os *hackers* árabes, pediu uma guerra eletrônica contra a ocupação israelense e chegou a convocar *hackers* pró-palestinos para intensificar a guerra cibernética contra Israel[201].

Em fevereiro de 2012, o grupo ativista *Anonymous* divulgou vídeo no qual declara guerra cibernética a Israel e promete remover o país da Internet a partir do de ataques programados para o dia 14 daquele mês[202].

Trata-se, possivelmente, da primeira declaração ostensiva de tal espécie de ataque realizada por um grupo “anônimo” contra um Estado, que evidencia o protagonismo de atores não estatais.

---

[199] Disponível em: <http://www.istoe.com.br/reportagens/143548_BRASIL+SOB+ATAQUE+DE+HACKERS> Acesso em: 30 jul. 2011.
[200] Disponível em: <http://www.conjur.com.br/2009-ago-23/redes-computadores-governo-sofrem-mil-ataques-hora> Acesso em: 30 jul. 2011.
[201] Disponível em: <http://blogs.estadao.com.br/jt-radar/israel-enfrenta-guerra-cibernetica/> Acesso em: 30 jul. 2011.
[202] Disponível em: <http://www.youtube.com/watch?v=QNxi2lV0UM0> Acesso em: 30 jul. 2011.

3.3 Ativismo, crimes e terrorismo cibernético

Não obstante tais práticas recebam uma regulamentação jurídica distinta daquela que delimita o tema escolhido para o presente trabalho (conflitos armados regidos pelo direito internacional), convém delinear os traços distintivos do ativismo, dos crimes e do terrorismo cibernético com a finalidade de evidenciar a linha divisória da guerra cibernética, que, todavia, pode ser bastante tênue em situações nas quais todas as atividades podem estar relacionadas entre si e ao mesmo propósito.

O ativismo cibernético, quando voltado para atividades e propósitos lícitos e quando não ingressa no abuso ou agressão a direitos alheios, encontra a guarida que tutela o exercício da liberdade de expressão. Pode ocorrer em blogs, portais ou redes sociais, nas quais a força de expressão de atores não estatais pode adquirir relevância, inclusive para desencadear importantes movimentos sociais, como ocorreu no Egito, culminando com a renúncia do Presidente no início de 2011[203].

Em fevereiro de 2012, a China, que é o país que mais exerce o controle sobre os usuários da Internet em seu território, decretou o fim do anonimato nas redes sociais[204]. Também no início de 2012, o FBI divulgou seu interesse em monitorar o *Facebook* e o *Twitter* com o alegado intuito de se antecipar a atos terroristas e crimes[205].

Além das redes sociais, o ativismo também pode tomar a forma de protestos contra a corrupção e limitação da liberdade na rede, por exemplo, realizados com

---

[203] O governo egípcio chegou a determinar o "desligamento" da rede egípcia da Internet (rotas de BGP – *Border Gateway Protoco*l do país) para inibir os protestos pelo *Facebook* e pelo *Twitter*, todavia, a *Google* disponibilizou um serviço para permitir o envio de mensagens ao *Twitter* por ligação telefônica. Disponível em: <http://oglobo.globo.com/mundo/redes-sociais-desempenharam-papel-fundamental-na-queda-de-mubarak-afirmam-especialistas-2823615>. Acesso em: 25 jan. 2012.

[204] Disponível em: <http://www1.folha.uol.com.br/tec/1046017-china-decreta-fim-do-anonimato-dos-usuarios-de-redes-sociais.shtml>. Acesso em: 25 jan. 2012.

[205] Disponível em: <http://blogs.estadao.com.br/link/fbi-quer-monitorar-facebook-e-twitter/>. Acesso em: 25 jan. 2012.

ataques cibernéticos conduzidos por atores independentes, cujas atividades geram simpatia ou controvérsias a respeito da legalidade, particularmente quando suas atividades afetam a segurança nacional, como a divulgação de alguns documentos secretos pelo *Wikileaks*, ou a normalidade de atividades – tal como ocorreu com os ataques aos bancos brasileiros pelo *Anonymous* em janeiro de 2012[206].

Os ataques realizados em janeiro de 2012 pelo *Anonymous* em protesto contra a paralisação do portal de compartilhamento de arquivos *Megaupload* e também contra os projetos SOPA e PIPA, envolvendo discussão a respeito de direitos autorais na Internet nos EUA, podem ter envolvido, inadvertidamente, usuários de redes sociais[207].

Além disso, o mesmo canal de manifestações legítimas pode se tornar um ambiente propício para a disseminação de vírus e a prática de crimes[208] ou atividades duvidosas, como aluguel de *hackers*[209] ou de redes "zumbis" para ataques[210].

No tocante aos crimes cibernéticos[211], além das normas internas dos países[212], a Convenção de Budapeste[213], primeira tentativa de regulamentação

---

[206] link ataque a bancos

[207] Disponível em: <http://idgnow.uol.com.br/seguranca/2012/01/20/usuarios-podem-ter-participado-de-ataques-do- anonymous-mesmo-sem-saber/>. Acesso em: 25 jan. 2012.

[208] Disponível em: <http://olhardigital.uol.com.br/produtos/central_de_videos/nova_onda_de_cyber_ataques_assusta_ usuarios_de_redes_sociais>. Acesso em: 25 jan. 2012.

[209] Disponível em: <http://online.wsj.com/article/SB10001424052970203806504577181283810631766.html>. Acesso em: 25 jan. 2012.

[210] Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u16928.shtml>. Acesso em: 25 jan. 2012.

[211] Os sistemas de processamento de dados podem ser meio ou alvo; os crimes podem ser impróprios (praticados por intermédio de computadores), próprios (só podem ser cometidos no ambiente cibernético) ou propriamente ditos (o computador ou o sistema são alvos).

[212] No Brasil, além das propostas legislativas para o marco civil e marco penal, já existem diversas normas, específicas ou não, que tipificam condutas ilícitas no espaço cibernético.

[213] Disponível em: <http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf>. Acesso em: 25 fev. 2012.

A Convenção de Budapeste, concebida pelo Conselho da Europa em 2001 e vigorando desde 2004, após a ratificação de cinco países, tipifica os principais crimes cometidos na *Internet*. Em seu preâmbulo, a Convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação entre os Estados e a iniciativa privada; ao versar sobre competência e cooperação internacional, no artigo 22, define quando e como uma infração é cometida e deixa a critério das Partes *a jurisdição mais apropriada para o procedimento legal.*

global, está sendo rediscutida por um grupo de trabalho da ONU[214], integrado pelo Brasil, que está avaliando se a melhor forma de disciplinar a matéria é uma convenção – que exige um difícil consenso internacional - ou normas *Soft Law* – regras meramente recomendatórias, flexíveis para adaptações e relativo poder de coerção.

O terrorismo cibernético[215] igualmente carece de conceituação e normatização de abrangência global. A Convenção Interamericana contra o Terrorismo e a Estratégia Global das Nações Unidas de Contraterrorismo objetivam impedir a uso da internet com finalidades terroristas.

Além das ferramentas de ataques cibernéticos, a Internet é um recurso barato e valioso para fazer propaganda, técnica essencial para os grupos terroristas. Por tal razão, foram adicionados à Convenção de Budapeste três novos delitos: propaganda, recrutamento e treinamento de terroristas[216].

[214] http://www.youtube.com/watch?v=F79IaZHUUaI
[215] LIBICKI, Martin C. *Cyberdeterrence and Cyberwar*, 2009. Disponivel em: < http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>. Acesso em: 25 fev. 2012.
[216] http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf, pág. 27.

4 A REGULAMENTAÇÃO DA GUERRA CIBERNÉTICA

Considerando que os ataques cibernéticos podem ser empregados como armas, ultrapassando a fronteira da ilicitude ou do terrorismo para ingressar na esfera de conflitos entre países, o presente capítulo objetiva verificar a aplicabilidade das regras que atualmente disciplinam o uso da força à guerra cibernética, as adaptações necessárias e os desafios técnicos e jurídicos para sua implementação, assim como para a aplicação das normas atualmente existentes, conforme Gervais (2011)[217].

A despeito da indisposição de muitos países para discutir um assunto tão delicado de forma aberta e coletiva, os capítulos anteriores demonstram que as ameaças cibernéticas são efetivas, razão pela qual estão na pauta da diplomacia e da inteligência cibernética e nas mentes de estrategistas militares e juristas do mundo inteiro - como bem ressalta Hayden (2011)[218] – que estão buscando respostas para elementares indagações. Episódios ocorridos na Estônia, na Geórgia - discutido por Swanson (2009) [219] - e no Irã – examinados por Richardson (2011)[220] - estão gerando debates a respeito das possíveis violações ao direito humanitário internacional.

É possível prever as consequências dos ataques cibernéticos para a população civil? Pode um país se valer de sua força militar convencional ou de armas cibernéticas para defender sua soberania ou para revidar outros ataques cibernéticos? Qual será a medida da proporcionalidade, da necessidade e da urgência? Quem terá mandato e quais critérios técnicos e jurídicos devem ser utilizados para atribuição de origem e autoria de ataques, considerando a ausência

---

[217] GERVAIS, Michael. *Cyber attacks and the laws of war.* 2011 Disponível em: < http://ssrn.com/abstract=1939615 or http://dx.doi.org/10.2139/ssrn.1939615>. Acesso em 25 fev. 2012.

[218] HAYDEN, Michael. *The battlefield of cyberspace: the inevitable new military branch – the cyber force,* p. 295-32.

[219] SWANSON, Lesley. *The era of cyber warfare: applying international humanitarian law to the 2008 Russian – Georgian cyber conflict*. p. 302-333.

[220] RICHARDSON, John C. *Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield*. 2011. Disponível em: <http://ssrn.com/abstract=1892888> ou em: <http://dx.doi.org/10.2139/ssrn.1892888>. Acesso em: 25 fev. 2012.

de fronteiras no espaço cibernético? Os ataques cibernéticos podem acarretar a prática de crimes de guerra, inclusive por civis?

Tais indagações podem trazer inúmeras implicações para os Direitos Humanos e para o Direito Humanitário Internacional, algumas das quais serão verificadas na sequência, sem a pretensão de trazer todas as respostas. É indiscutível a relevância da construção de um marco legal mínimo para a guerra cibernética, conforme Graham (2010)[221], sem olvidar que o funcionamento do espaço cibernético é essencialmente regido por regras técnicas - que estão em constante mutação - e não apenas jurídicas.

Preocupações com as questões do *jus ad bellum*, incluindo se os ataques cibernéticos constituem um ato de agressão ou se justificariam recorrer à força armada em resposta, devem ser somadas às questões do *jus in bello*, ou seja, como as normas da guerra vão disciplinar o uso da força de ataques cibernéticos durante um conflito armado, restando ainda muitas indagações, recorda Benatar (2009)[222].

Os países estão migrando suas estratégias militares para o espaço cibernético, conforme Walker (2010)[223], todavia, eles têm diferentes capacidades e diferentes vulnerabilidades. Assim como nem todos têm poder financeiro e comercial para fins de coerção econômica, o mesmo ocorre com as capacidades de defesa e de ataque no espaço cibernético.

A construção de marco legal a respeito do uso da força e os modos de conflito têm variados efeitos no poder e nas relações de poder. Conjugar interpretação legal com interesses estratégicos é excepcionalmente difícil porque os futuros efeitos da tecnologia da informação sobre o poder e sobre os conflitos continuam incertos. Os significados com os quais os Estados e os atores internacionais normatizaram os conflitos mudaram.

Mais do que discutir como o direito internacional deve ser interpretado para contemplar os novos desafios, é importante saber qual a relação entre o direito e a

---

[221] GRAHAM, David E. *Cyber threats and the law of war*. 2010.
[222] BENATAR, Marco. *The use of cyber force: need for legal justification?* Obtido em: DHeinOnline, 1 Goettingen J. Int´l L 375, 2009.
[223] WALKER, Paul A. *Traditional military activities in cyberspace: preparing for netwar*. p. 337-359.

tecnologia. Os estrategistas devem se preparar para atuar com arcabouço normativo altamente incerto e ambiente tecnológico em constante mutação, sem olvidar que os esforços multilaterais para regular o espaço cibernético podem ter efeitos limitados ou provisórios.

Será difícil construir um marco legal internacional para a guerra cibernética, pois os diferentes interesses estratégicos e capacidades levarão os países a diferentes direções, dificultando um consenso. Não obstante, ainda que as regras jurídicas possam não atingir um grau de efetividade absoluta em tal contexto, sua inexistência tende a estimular ações indevidas, pois os proveitos e os riscos são atrativos, razão pela qual Hollis (2007) reforça a necessidade de tal evolução[224].

Todavia, enquanto a complexa formulação de um consenso sobre o tema não for possível[225], incumbe aos estrategistas e juristas construir soluções com base na doutrina e nas regras atualmente existentes, muitas das quais podem ser aplicadas à guerra cibernética, a despeito da necessidade de revisitar alguns conceitos.

A propósito, é importante recordar que a Convenção de Viena sobre o Direito dos Tratados de 1969[226] contempla regras de interpretação dos acordos internacionais, a qual deve ser feita sempre de boa-fé, à luz dos objetivos, finalidades, contexto e motivação da sua elaboração. Por isso, a interpretação de um tratado que foi elaborado para proteger bens e pessoas, por exemplo, como é o caso das Convenções de Genebra, jamais pode ser feita de forma que limite ou impeça tal proteção. Aliás, as próprias Convenções reforçam o princípio de que nem mesmo as suas disposições não podem ser invocadas para limitar ações

---

[224] HOLLIS, Duncan B., Why States Need an International Law for Information Operations. Lewis & Clark Law Review, Vol. 11, p. 1023, 2007; Temple University Legal Studies Research Paper No. 2008-43. Disponível em: <http://ssrn.com/abstract=1083889>. Acesso em: 24 fev. 2012.

[225] HOLLIS, Duncan B. *New tools, new rules: international law and information operations. The message of war: information, influence and perception in armed conflict.* G. David and T. McKeldin, eds., 2008; Temple University Legal Studies Research Paper No. 2007-15. Disponível em: <http://ssrn.com/abstract=1009224>. Acesso em: 24 fev. 2012.

[226] Incorporado ao direito brasileiro, com reserva aos artigos 25 e 26, pelo Decreto nº 7.030, de 14 de dezembro de 2009. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D7030.htm

humanitárias[227]. Tais critérios são extremamente relevantes inclusive para que atores não estatais possam discutir ações e interpretações estatais.

Aliás, as Convenções de Genebra confiam a função de interpretação à Comissão Internacional da Cruz Vermelha em caso de desacordo entre países conflitantes a respeito de suas disposições, atuando para encontrar uma solução no interesse das pessoas protegidas pelas Convenções[228]. Vale lembrar, ainda, que os Estados, de comum acordo, podem submeter critérios díspares de interpretação de tratados internacionais ao Tribunal Internacional de Justiça, órgão judiciário da Organização das Nações Unidas (embora sua vocação natural seja outra)[229].

4.1 Regras Aplicáveis à Guerra Cibernética

Não há uma definição para a guerra estabelecida em convenção internacional, mas o direito internacional faz distinção entre conflitos internacionais e internos - dentro de um único Estado. É definida pela doutrina como a contenda entre dois ou mais Estados por meio de suas forças armadas, com o propósito de sobrepor um ao outro as condições de paz do interesse do vitorioso[230].

Admite-se que o “estado de guerra” pode existir sem uma hostilidade ativa da mesma forma que as hostilidades podem ocorrer independentemente do estado de guerra, além de ser debatida a existência de um “status mixtus” entre a paz e a guerra, caracterizado pela utilização simultânea das leis de guerra para determinados fins e das leis de paz para outros[231].

---

[227] Artigo 9º das Convenções de Genebra I, II e III, artigo 10 da Convenção de Genebra IV, artigo 75, item 8, do Protocolo Adicional I.
[228] Artigo 11 das Convenções de Genebra I, II e III, artigo 12 da Convenção de Genebra IV.
[229] Artigo 36 do Estatuto do Tribunal Internacional de Justiça, disponível em: http://www.icj-cij.org/homepage/sp/icjstatute.php
[230] OPPENHEIM, L. *International Law*. 7ª ed., v II, Lauterpacht, 1952, p. 202.
[231] DINSTEIN, Yoram. *Guerra, agressão e legítima defesa*. 3. ed. p. 13 e 22.

Em excepcionalíssimas situações, o uso da força é legitimado pela Carta da Organização das Nações Unidas de 1945, a qual autoriza o emprego de forças armadas em operações de imposição da paz, guerras de libertação nacional e legítima defesa – trata-se do *jus ad bellum*[232] ou direito à guerra.

Mesmo em tais situações, o uso da força não é ilimitado, pois existem regras para o combate – *jus in bello*[233] – materializadas nas Convenções de Genebra (proteção de vítimas e bens), na Convenção de Haia (métodos e regras de combate) e Convenção de Nova Iorque (salvaguarda de Direitos Humanos e limitação do uso de armas), em resoluções da ONU, princípios gerais, usos e costumes do direito internacional. Além de tais normas, diversas outras regras internacionais disciplinam questões afetas aos conflitos armados, especialmente a utilização de armas e a proteção de bens e pessoas.

As transgressões aos limites impostos ao uso da força podem configurar violações aos Direitos Humanos e crimes de guerra, definidos no Estatuto de Roma, que instituiu o Tribunal Penal Internacional (*jus post bellum*).

A história e a evolução do Direito Humanitário Internacional se confunde com a história da Cruz Vermelha[234], que já manifestou sua preocupação com o fato de que "advogados e técnicos especialistas concordam que o risco de possíveis ataques a redes de informática é considerável, levantando questões sobre a aplicação do Direito Internacional Humanitário (DIH) e até a própria definição de conflitos armados"[235]. A despeito de todas as controvérsias e das reformulações que a nova realidade exige, a Cruz Vermelha defende a aplicabilidade das normas atualmente existentes:

---

[232] REMUS, Titiriga. *Cyber warfare and law of the nations.* (Jus Ad Bellum) (October 19, 2011). Disponível em: <http://ssrn.com/abstract=1946470 or http://dx.doi.org/10.2139/ssrn.1946470>. Acesso em: 25 fev. 2012.

[233] CHAINOGLOU, Kalliopi. *An assessment of jus in bello issues concerning computer network attacks: a threat reflected in national security agendas* (April 13, 2011). Romanian Journal of International Law, v. 12. p. 25-63. 2010. Disponível em: <Available at SSRN: http://ssrn.com/abstract=1809127>. Acesso em: 25 fev. 2012.

[234] A respeito da história do Direito Humanitário Internacional. Disponível em: <http://www.icrc.org/por/war-and-law/index.jsp>. Acesso em: 25 fev. 2012.
SWINARSKI, Christophe. *A norma e a guerra: palestras sobre direito internacional humanitário. Competências e funções do comitê internacional da cruz vermelha - órgão da ação internacional humanitária.* p. 65-82.

[235] Disponível em: <http://www.icrc.org/por/war-and-law/conduct-hostilities/information-warfare/index.jsp>. Acesso em: 25 fev. 2012.

> "Para fins desta discussão, a guerra cibernética se refere aos meios e métodos de guerra que contam com informações tecnológicas e são usados no contexto de um conflito armado segundo a definição contida no Direito Internacional Humanitário – em oposição às operações cinéticas militares tradicionais. Da mesma maneira, termos como 'ataques cibernéticos', 'operações cibernéticas' ou 'ataques de redes de computadores' não têm um significado legal acordado internacionalmente e são usados em diferentes conceitos (nem sempre limitados aos conflitos armados) e com diferentes significados. [...] O Direito Internacional Humanitário (DIH) só se aplica se as operações cibernéticas forem cometidas em um contexto de conflito armado – seja ele entre Estados, entre Estados e grupos armados organizados ou entre grupos armados organizados. Portanto, precisamos distinguir a questão geral da segurança cibernética da questão específica das operações cibernéticas em conflitos armados. Termos como 'ataques cibernéticos' ou mesmo 'terrorismo cibernético' podem evocar métodos de guerra, mas as operações às quais se referem não são necessariamente conduzidas em um conflito armado. [...] O DIH não menciona especificamente as operações cibernéticas. Devido a isso, e devido a que a exploração da tecnologia cibernética é relativamente nova e às vezes parece introduzir uma mudança qualitativa completa nos meios e nos métodos de guerra, ocasionalmente se argumentou que o DIH está mal-adaptado ao campo cibernético e não pode ser aplicado à guerra cibernética. No entanto, a ausência de referências específicas no DIH às operações cibernéticas não significa que tais operações não estejam sujeitas às regras do DIH. Se os meios e os métodos da guerra cibernética produzirem os mesmos efeitos no mundo real que as armas convencionais (como destruição, interrupção de serviços, estragos, ferimentos ou mortes), são regidos pelas mesmas regras que as armas convencionais."[236]

Na sequência, serão destacadas algumas disposições do direito internacional público - normas dos conflitos armados e do direito humanitário internacional - que são aplicáveis à guerra cibernética[237], demonstrado-se que elas precisam de uma releitura e adequação para as peculiaridades do espaço cibernético.

4.1.1 A Carta da ONU

A Carta das Nações Unidas ou Carta de São Francisco criou a Organização das Nações Unidas logo após a II Guerra Mundial com o objetivo de manter a paz e

---

[236] DROEGE, Cordula. *Não há brechas jurídicas no ciberespaço.* Disponível em: <http://www.icrc .org/por/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>. Acesso em: 25 fev. 2012.

[237] PAPANASTASIOU, Afroditi. *Application of international law in cyber warfare operations* (September 8, 2010). Disponível em: <http://ssrn.com/abstract=1673785> ou em: <http://dx.doi.org/10.2139/ssrn.1673785>. Acesso em: 25 fev. 2012.

segurança internacionais, além de centralizar o monopólio[238] do uso legítimo da força quando necessário para evitar ameaças ou ruptura da paz e reprimir atos de agressão.

Seu artigo 2º (4) estabelece que "todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas."

De acordo com o artigo 39, cabe ao Conselho de Segurança determinar a existência de ameaça ou ruptura da paz ou ato de agressão, decidindo quais medidas coercitivas ou preventivas devem ser adotadas à luz dos artigos 41 e 42, para a manutenção ou restabelecimento da paz e da segurança internacional.

As medidas previstas no artigo 41 incluem a adoção, pelos Membros, da interrupção completa ou parcial das relações econômicas, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radiofônicos ou de qualquer outra espécie, além do rompimento das relações diplomáticas. Se tais medidas não forem suficientes, o artigo 42 prevê que o Conselho de Segurança poderá adotar ações que julgar necessárias para manter ou restabelecer a paz e a segurança internacional, com o emprego de forças aéreas, navais ou terrestres.

O artigo 51 assegura o direito de legítima defesa[239] individual ou coletiva na ocorrência ou na iminência de ataque armado contra qualquer Membro das Nações Unidas até que o Conselho de Segurança adote medidas de sua competência. As ações adotadas no exercício da legítima defesa devem ser imediatamente comunicadas ao Conselho, não se sobrepondo à sua autoridade e às suas

---

[238] Além do Conselho de Segurança da Organização das Nações Unidas, o artigo 52 admite acordos regionais estabelecendo que "nada na presente Carta impede a existência de acordos ou de entidades regionais, destinadas a tratar dos assuntos relativos à manutenção da paz e da segurança internacionais que forem suscetíveis de uma ação regional, desde que tais acordos ou entidades regionais e suas atividades sejam compatíveis com os Propósitos e Princípios das Nações Unidas." A OEA – Organização dos Estados Americanos – www.oas.org - e a OTAN – Organização do Tratado do Atlântico Norte – www.nato.int - são exemplos de acordos regionais.

[239] KESAN, Jay P.; HAYES, Carol M. *Mitigative counterstriking: self-defense and deterrence in cyberspace.* (April 7, 2011). Illinois Public Law Research Paper No. 10-35; Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Harvard Journal of Law and Technology, Forthcoming. Disponível em: <http://ssrn.com/abstract=1805163>. Acesso em: 25 fev. 2012.

competências. A legítima defesa[240], portanto, é um direito assegurado pela Carta das Nações Unidas que pressupõe, todavia, a identificação segura da autoria da ameaça ou do ataque sofrido.

Para ser qualificada como legítima defesa, a resposta deve ser guiada pelos princípios da necessidade e da proporcionalidade, observado o critério de urgência para não permitir resposta depois de decorrido muito tempo. A necessidade depende da atribuição do ataque a uma fonte específica e da caracterização da intenção correlata para então ser permitido o uso da força na resposta. A proporcionalidade autoriza que a força usada na resposta seja equivalente ao ataque sofrido; objetiva limitar os danos decorrentes das guerras, impondo que os métodos e meios de guerra utilizados sejam proporcionais ao objetivo militar e que a resposta seja proporcional ao ataque sofrido.

Se a definição de tais critérios já é difícil nos conflitos armados convencionais, ela se torna muito mais complexa com os ataques cibernéticos, pois as tradicionais definições de uso da força[241] são insuficientes para esclarecer quais ataques cibernéticos são toleráveis, bem como a medida da necessidade e da proporcionalidade da resposta.

A Carta da ONU foi escrita antes do advento da Internet, razão pela qual a guerra cibernética desafia as tradicionais definições sobre uso da força. Em outras palavras, o paradigma do *jus ad bellum* precisa ser revisitado para estabelecer condições de proteção aos Estados, particularmente no caso de ataques contra infraestruturas críticas nacionais.

Ataques cibernéticos dirigidos a causar danos físicos a bens tangíveis ou intangíveis, ferimento ou morte de seres humanos podem ser caracterizados como agressão. Mas e as perturbações de ordem econômica, que também ameaçam a paz?

---

[240] DELIBASIS, Dimitrios. *Cyberspace warfare and self-defence* (October 10, 2011). Disponível em: <http://ssrn.com/abstract=1942279>. Acesso em: 25 fev. 2012.

[241] SCHMITT, Michael N. *Computer network attack and the use of force in international law: thoughts on a normative framework*. Columbia Journal of Transnational Law. v. 37. 1998-99. Disponível em: <http://ssrn.com/abstract=1603800>. Acesso em: 25 fev. 2012.

É preciso definir o que configura o uso da força no espaço cibernético[242], ou seja, se os ataques cibernéticos podem ser enquadrados no conceito de uso da força do artigo 2(4) da Carta da ONU para efeito de avaliar a possibilidade de se invocar o direito à legítima defesa ou a adoção de medidas pelo Conselho de Segurança da ONU. Além disso, também existem controvérsias a respeito do exercício do direito à legítima defesa, particularmente no tocante à possibilidade ou não de um país se antecipar a um ataque. As interpretações oscilam entre visões restritivas e expansionistas.

Apesar das tentativas de Estados desenvolvidos de incluir a coerção econômica no artigo 2º, durante a elaboração da Carta, tal prática restou expressamente excluída. As dificuldades de interpretação residem nas distinções entre força e coerção. Incluir todas as ações de guerra cibernética dentro da definição de uso da força requer uma maior expansão do artigo 2º, porém, uma interpretação extensiva do uso da força pode dificultar a exclusão dos atos de coerção. É necessário distinguir os ataques cibernéticos que não causam danos físicos, como incursões e bloqueios eletrônicos, dos atos de coerção política e econômica, tradicionalmente excluídas do artigo 2º, mas que podem ter os mesmos efeitos.

O dilema consiste em classificar ataques cibernéticos que não causam danos físicos ou somente causam indiretamente, à luz da proibição do uso da força. Definir ataques cibernéticos em centros de gravidade econômicos como uso da força à luz do atual regime internacional pode trazer consequências legais indesejáveis; incorporar os ataques cibernéticos a infraestruturas críticas da economia na definição do uso da força não pode ser feito com precisão suficiente para excluir outras políticas econômicas que também são ferramentas necessárias à política internacional e foram deliberadamente excluídas da definição internacional do uso da força, particularmente pelas democracias baseadas em mercados[243].

---

[242] ROSCINI, Marco. *World wide warfare - 'jus ad bellum' and the use of cyber force* (June 30, 2010). Max Planck Yearbook of United Nations Law. v. 14. p. 85-130. 2010. Disponível em: <http://ssrn.com/abstract=1683370>. Acesso em: 25 fev. 2012.

[243] HOISINGTON, Matthew. *Cyberwarfare and the use of force giving rise to the right of self-defence*. Boston College International & Comparative Law Review. v. 32. p. 439-454.
Citation: 32 B. C. Int'l & Comp. L. Rev. 439 2009

Padrões inequívocos de conduta que sejam universalmente reconhecidos e aceitos precisam ser fixados. A evolução normativa da comunidade internacional deve verificar se os ataques cibernéticos, ofensivos ou defensivos, constituem um ilegal uso da força e se a ameaça viola o direito internacional.

Por exemplo[244], na situação hipotética de um país alegar suspeita de que outro país está desenvolvendo arsenal de armas nucleares e decidir que paralisar seu sistema financeiro seria a medida mais eficaz para dissuadir posteriormente o programa nuclear, o mesmo objetivo poderia ser atingido com ataques aéreos, retaliação do sistema financeiro, infiltração de moeda falsa ou invasão e destruição de informações bancárias e redes computacionais do sistema financeiro do país suspeito. Tais opções configuram uso da força à luz das vedações e disposições da Carta da ONU? Em situações extremas, a proteção do País pode depender de uma resposta imediata, robusta e agressiva. Para delinear a exceção à regra que proíbe o uso da força, a comunidade internacional deveria aprovar uma lista de infraestruturas críticas que um Estado pode proteger com medidas ativas de defesa. Se uma infraestrutura crítica identificada na lista sofrer um ataque cibernético, poderia o país responder com uma presumida legítima defesa de boa-fé, sem antes atribuir ou caracterizar o ataque no nível de especificidade exigido pela tradicional fórmula?

Outra questão delicada é a atribuição de autoria, a identificação da origem de um ataque e a caracterização da intenção hostil, especialmente importantes e complexas levando em conta os ataques remotos e anônimos, a constante invenção de novas técnicas e a possibilidade de utilizar estruturas e atores inocentes, pois a regra da legítima defesa não autoriza atos de defesa ativa além das fronteiras se a provocação não puder ser atribuída a outro país, assim como protege pessoas e bens civis.

Um sistema normativo que exige a determinação da autoria e a caracterização da intenção hostil do ataque cibernético – requisitos passíveis de manipulação quando não se tornam inviáveis - para então autorizar o exercício da

[244] WAXMAN, Matthew C. *Cyber-attacks and the use of force: back to the future of article 2.* (March 16, 2011). Yale Journal of International Law. v. 36. 2011. Disponível em: <http://ssrn.com/abstract=1674565>. Acesso em: 24 fev. 2012.

legítima defesa, é incompatível com a realidade cibernética e ineficiente para lidar com protagonistas que atuam sem as restrições impostas pela legalidade. O diálogo das fontes jurídicas e técnicas deverá ajudar a comunidade internacional a definir as cautelas necessárias.

A relativamente baixa exposição das ações e reações no espaço cibernético pode dificultar o processo de evolução normativa, ou seja, as vedações da Carta da ONU podem constituir restrições ineficientes para os ataques cibernéticos, considerando a dificuldade de serem atribuídos aos seus verdadeiros patrocinadores, os quais podem utilizar inúmeros atores não estatais. Isso também pode explicar as dificuldades das negociações de acordos internacionais para a regulamentação da guerra cibernética.

Percebe-se que as disposições da Carta da ONU, particularmente os conceitos de uso da força, legítima defesa, necessidade e proporcionalidade e os critérios para identificação de autoria e caracterização da hostilidade precisam ser repensados para o espaço cibernético.

4.1.2 Convenções de Genebra e Protocolos Adicionais

Os esforços do suíço Henry Dunant para prestar assistência aos feridos na batalha de Solferino, em 1859, deflagraram os primeiros passos para a fundação da Cruz Vermelha Internacional, em 1864, e construção do Direito Humanitário Internacional, arcabouço de normas internacionais que disciplinam os métodos e meios de guerra, além de proteger pessoas e bens afetados ou que possam ser atingidos em conflitos. As quatro Convenções de Genebra de 1949 e os dois Protocolos Adicionais de 1977[245] constituem a essência do Direito Internacional Humanitário.

[245] Convenções de Genebra I (Melhoria da Sorte dos Feridos e Enfermos dos Exércitos em Campanha), II (Melhoria da Sorte dos Feridos, Enfermos e Náufragos das Forças Armadas no Mar),

De tais normas convencionais, serão destacadas regras que dispõem sobre a proteção de bens e pessoas, normas de precaução e limites para os ataques e para o emprego de novas armas, além das regras que tutelam a condição dos combatentes.

4.1.2.1 Armas Cibernéticas

As armas convencionais são aquelas que atendem a usos e costumes da guerra e por isso não geram contestações. Atualmente, não são consideradas convencionais as armas nucleares, radiológicas, biológicas e químicas, exceto as que produzem fumaça, incendiárias e as utilizadas contra o controle de distúrbios[246].

Das vantagens enumeradas para a utilização de armas cibernéticas, destacam-se a preservação de vidas, a assimetria, o fator surpresa e a redução de custos em relação a uma guerra convencional. O desenvolvimento de um vírus ou de um sistema de defesa custa menos do que qualquer outra arma ou estratégia. Além disso, as possibilidades de camuflar a origem de um ataque ou mesmo a dificuldade de vincular o seu autor a um governo está abrindo a discussão a respeito da terceirização do ataque[247].

Considerando a potencial gravidade das técnicas de ataques cibernéticos, não há como negar que eles podem ser considerados novas armas de guerra, submetendo-se, por tal razão, ao respectivo regramento, não obstante os desafios técnicos e jurídicos relativos à identificação da origem e à atribuição de autoria.

III (Tratamento dos Prisioneiros de Guerra) e IV (Proteção dos Civis em Tempo de Guerra), de 1949. (Decreto nº 42.121, de 21 de agosto de 1957); Protocolos Adicionais I e II às Convenções de Genebra, de 12 de Agosto de 1949, adotado pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário Aplicável aos Conflitos Armados. (Decreto nº 849, de 25 de junho de 1993)

[246] Glossário das Forças Armadas. Disponível em: <https://www.defesa.gov.br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/MD35_G_01_GlossarioFA_4aEd2007.pdf>. Acesso em 24 fev. 2012.

[247] Disponível em: <http://www.teletime.com.br/4/2011/guerra-cibernetica/tt/226285/revista.aspx>. Acesso em 24 fev. 2012.

A despeito da necessidade de revisitar as regras existentes para uma adaptação à nova realidade, os atuais parâmetros e limites para a utilização de novas armas aplicáveis às armas cibernéticas podem ser extraídas dos artigos 35 a 37 dos Protocolos Adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados, os quais dispõem sobre os métodos e meios de combate[248].

De acordo com Kevin Coleman[249], as armas cibernéticas já estão sendo desenvolvidas e utilizadas por governos há vários anos e se intensificou a partir de 2005, quando o Pentágono começou a investir no desenvolvimento de ferramentas para possível aplicação bélica. Despontam no arsenal cibernético os *botnets* e os *exploits*.

Em 2000, durante as discussões relativas à Convenção de Budapeste sobre crimes cibernéticos, o Conselho da Europa chegou a estudar a possibilidade de

---

[248] ARTIGO 35 Normas Fundamentais
1. Em todo conflito armado, o direito das Partes em conflito, a escolha dos métodos ou meios de combate não é ilimitado.
2. É proibido o emprego de armas, projéteis, materiais e MÉTODOS de combate de tal índole que causem males supérfluos ou sofrimentos desnecessários.
3. É proibido o emprego de métodos ou meios de combate que tenham sido concebidos para causar, ou dos quais se pode prever que causem, danos extensos, duradouros e graves ao meio ambiente natural.
ARTIGO 36 Novas Armas
Quando uma Alta Parte Contratante estude, desenvolva, adquira ou adote uma nova arma, ou novos meios ou métodos de combate, terá a obrigação de verificar se seu emprego, em certas condições ou em todas as circunstâncias, estaria proibido pelo presente Protocolo ou por qualquer outra norma de Direito Internacional aplicável a essa Alta Parte Contratante.
ARTIGO 37 Proibição da Perfídia
1. É proibido matar, ferir ou capturar um adversário valendo-se de meios perfídios. Constituirão perfídia os atos que, apelando para boa-fé de um adversário e com a intenção de atraiçoá-lo, dêem a entender a este que tem direito à proteção, ou que está obrigado a concedê-la, em conformidade com as normas de Direito Internacional aplicáveis nos conflitos armados. São exemplos de perfídia os seguintes atos:
a) simular a intenção de negociar sob uma bandeira de armistício ou de rendição:
b) simular incapacidade por ferimentos ou enfermidades:
c) simular a condição de pessoa civil, não combatente; e
d) simular que possui condição de proteção, pelo uso de sinais, emblemas ou uniformes das Nações Unidas ou de Estados neutros ou de outros Estados que não sejam Partes em conflito.
2. **Os estratagemas não são proibidos. São estratagemas os atos que têm por objeto induzir a erro um adversário ou fazer com que este cometa imprudências, porém <u>que não infrinjam nenhuma norma de Direito Internacional aplicável aos conflitos armados</u>, <u>nem sejam perfídios</u> já que não apelam para a boa-fé de uma adversário com respeito à proteção prevista nesse direito**. São exemplos de estratagemas os seguintes atos: a camuflagem, os engodos, as operações simuladas e as informações falsas.

[249] COLEMAN, Kevin G. *The cyber commander's ehandbook, a downloadable guide*. 2011.

estabelecer um controle sobre armas cibernéticas que possam afetar a confidencialidade, a disponibilidade e a integridade de informações e sistemas. Em tal época, a Rússia já era defensora da criação de regras internacionais para restringir o desenvolvimento e a utilização de armas cibernéticas pela Organização das Nações Unidas[250].

O Reino Unido admitiu, em dezembro de 2011, que sua estratégia de defesa cibernética inclui medidas de segurança e desenvolvimento de armas cibernéticas, táticas, técnicas e planos para ataques contra invasores, além de *softwares* capazes de sabotar a capacidade militar convencional ou nuclear de nações inimigas[251].

No início de 2012, além de acusar os Estados Unidos e a China de realizar invasões, o Japão divulgou que promoverá alterações legislativas para poder utilizar armas cibernéticas que está desenvolvendo, em parceria com a empresa Fujitsu - um sistema de vírus e equipamentos para monitorar ameaças, além de rastrear a origem e neutralizar um ataque cibernético[252].

De acordo com informações divulgadas, em maio de 2011, pela imprensa americana com base em declarações de oficiais militares americanos, o Pentágono teria diversas armas e ferramentas cibernéticas, incluindo vírus capazes de sabotar redes críticas de adversários – os quais poderiam ser instalados em redes estrangeiras para posterior ativação mediante autorização prévia do Presidente, a qual seria desnecessária para outras finalidades, como estudar as capacidades de outras redes[253].

Em novembro de 2011, a DARPA – *Defense Advanced Research Projects Agency*, órgão de pesquisa do Pentágono que participou da gestação da Internet,

---

[250] DOROTHY Denning. *Reflections on cyberweapons controls.* Disponível em: < http://faculty.nps.edu/dedennin/publications/reflections_on_cyberweapons_controls.pdf>. Acesso em: 24 fev. 2012.

[251] Disponível em: <http://idgnow.uol.com.br/seguranca/2011/12/02/governo-ingles-admite-preparar-armas-ciberneticas-contra-estados-inimigos/>. Acesso em: 24 fev. 2012.

[252] Disponível em: <http://asian-defence-news.blogspot.com/2012/01/japan-developing-cyber-weapon.html>. Acesso em: 24 fev. 2012.

[253] Disponível em: <http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html>. Acesso em: 24 fev. 2012.

convocou “*hackers* visionários” para o desenvolvimento de novas armas e mudar a dinâmica da defesa cibernética das infraestruturas críticas[254].

A China, que tem 420 milhões de internautas, o maior número do mundo, já foi acusada por diversos países de praticar espionagem e desenvolver armas cibernéticas, especialmente após a criação da base militar cibernética em julho de 2011, conhecida como *On Line Blue Army* ou *Cyber Blue Team*[255].

Recentemente, o Exército Brasileiro divulgou a contratação de duas empresas nacionais para desenvolver um simulador de guerra cibernética e um antivírus a ser usado a partir de 2012[256]. Além de reduzir a dependência de fornecedores internacionais, tais medidas foram adotadas com o intuito de evitar que os dados da rede do Exército sejam avaliados fora do ambiente militar, reduzindo, assim, o risco de vazamento de dados. Além disso, objetiva-se criar um sistema nacional de *Honeypots* (computadores na rede configurados para atrair vírus), para atrair os vírus e manter uma lista nacional atualizada, sem depender de listas internacionais – pois o antivírus só elimina ameaças conhecidas. Um país pode criar um novo vírus e, em contexto de guerra, evocar leis de segurança nacional para impedir que suas empresas coloquem a “arma cibernética” em listas de ameaças, daí a relevância do banco de dados nacional.

Estudo realizado a pedido do Comitê de Assuntos Exteriores do Parlamento Europeu classificou as ameaças cibernéticas em quatro níveis, seguindo uma graduação: crime de baixo nível ou individual (*hacking*), criminalidade grave e organizada, extremismo político ou ideológico e ataques cibernéticos patrocinados pelo Estado[257]. Em comunicado realizado em 2011 ao Parlamento Europeu sobre o plano de ação para proteção das infraestruturas críticas da informação na Europa, a Comissão agrupou as ameaças cibernéticas em três categorias conforme a finalidade:

---

[254] Disponível em: <http://www.darpa.mil/NewsEvents/Releases/2011/2011/09/12_DARPA_ENLISTS_CYBER_COMMUNITY_FOR_FRANK_DISCUSSION.aspx>. Acesso em: 24 fev. 2012.

[255] Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1167/China-confirma--Cyber-Blue-Team>. Acesso em: 24 fev. 2012.

[256] Disponível em: <http://www.valor.com.br/empresas/2496658/exercito-quer-arma-nacional-para-travar-guerra-line>. Acesso em: 24 fev. 2012.

[257] Disponível em: <http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em: 24 fev. 2012. , págs. 132 e seguintes.

> - as que têm por finalidade a exploração, como as 'ameaças avançadas persistentes' para fins de espionagem econômica e política (por exemplo, GhostNet), o roubo de identidades, os recentes ataques ao sistema de comércio de emissões ou os ataques contra os sistemas TI dos Estados;
>
> - as que têm por finalidade introduzir perturbações, como os ataques de Recusa Distribuída de Serviço ou 'spamming' gerado via 'botnets' (por ex., a rede Conficker de 7 milhões de máquinas e a rede Mariposa, com base em Espanha, de 12,7 milhões de máquinas), a Stuxnet e o corte de meios de comunicação;
>
> - as que têm por finalidade a destruição. Trata-se de um cenário ainda não materializado, mas que não pode ser de todo excluído no futuro, dada a crescente presença das TIC nas infraestruturas críticas (como as redes eléctricas e os sistemas de abastecimento de água inteligentes).[258]

Além de tais distinções de motivação e gravidade, que variam conforme os protagonistas e objetivos envolvidos, algumas ferramentas e técnicas de ataques cibernéticos, bem como as técnicas para dificultar as investigações, podem ser utilizadas para fins criminosos, terroristas ou bélicos, diferenciação que será feita adiante.

Portanto, pode ser bastante difícil associar um ataque a um responsável apenas com as informações relacionadas ao ataque cibernético, pois, além do caráter transnacional do espaço cibernético, existem diversas etapas e técnicas de "camuflagem", muitas das quais podem inclusive envolver usuários inocentes.

Com maior razão, pode ser difícil comprovar a intenção, que também tem relevância jurídica, se o ataque não puder ser atribuído ou não for assumido oficialmente por um ator estatal, daí a dificuldade de estabelecer regras para a guerra cibernética.

4.1.2.2 Distinção, Precauções e Vedação de Ataques Indiscriminados

Com o objetivo de evitar ataques que vitimizem a população civil e causem danos aos bens civis, o artigo 51 do Protocolo I de 1977 define de forma detalhada

[258] Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:PT:HTML>. Acesso em: 24 fev. 2012.

os ataques indiscriminados, que são proibidos pelo direito humanitário. Além disso, os artigos 57 e 58 do Protocolo I estabelecem que devem ser adotadas diversas precauções no ataque para limitar os efeitos negativos sobre bens e pessoas civis.

São considerados indiscriminados os ataques que não são dirigidos contra uma alvo militar determinado, os que utilizam métodos ou meios de combate que não permitem dirigir os ataques contra um alvo militar determinado, os que utilizam métodos e meios de combate cujos efeitos não podem ser limitados, os que podem causar acidentalmente a perda de vidas humanas na população civil, ferimentos a civis, danos aos bens civis, ou uma combinação destas perdas e danos, que seriam excessivos relativamente à vantagem militar concreta e esperada. Por tais razões, as seguintes precauções devem ser adotadas:

> "a) Os que preparam ou decidem um ataque devem:
>
> - Fazer tudo o que for praticamente possível para verificar que os objectivos a atacar não são pessoas civis, nem bens de caráter civil e não beneficiam de uma protecção especial, mas que são objectivos militares [...];
>
> - Tomar todas as precauções praticamente possíveis quanto à escolha dos meios e métodos de ataque com vista a evitar e, sempre, reduzir ao mínimo a perda de vidas humanas na população civil, ferimentos às pessoas civis e danos nos bens de carácter civil que possam ser causados acidentalmente;
>
> - Abster-se de lançar um ataque de que se possa esperar que venha a causar acidentalmente perda de vidas humanas na população civil, ferimentos nas pessoas civis, danos nos bens de caráter civil ou uma combinação destas perdas e danos, que seriam excessivos relativamente à vantagem militar concreta e directa esperada.
>
> b) Um ataque deve ser anulado ou interrompido quando pareça que o seu objectivo não é militar ou que beneficie de uma protecção especial ou que possa esperar que venha a causar incidentalmente perdas de vidas humanas na população civil, ferimentos em pessoas civis, danos nos bens de carácter civil ou uma combinação dessas perdas e danos que seriam excessivos relativamente à vantagem militar concreta e directa esperada.
>
> c) Nos casos de ataques que podem afectar a população civil, deve ser dado um aviso em tempo útil e através de meios eficazes, a menos que as circunstâncias não o permitam.
>
> Quando for possível escolher entre vários objectivos militares para obter uma vantagem militar equivalente, a escolha deverá recair sobre o objectivo cujo ataque seja susceptível de provocar o menor perigo para as pessoas civis ou para os bens de carácter civil [...]. Nenhuma disposição do presente artigo poderá ser interpretada como autorizando ataques contra a população civil, as pessoas civis ou bens de carácter civil." [259]

[259] BOUCHET-SAULNIER, Françoise. Dicionário Prático do Direito Humanitário. Lisboa: Instituto Piaget, 1998, p. 57-59.

A propósito, o Comitê Internacional da Cruz Vermelha realça o dever que recai sobre os responsáveis pelos ataques de adotar as medidas mais eficazes possíveis para minimizar os possíveis prejuízos e danos às infraestruturas civis e aos civis - o que inclui a verificação de possíveis estragos que podem resultar dos ataques e da natureza dos sistemas alvejados para saber se os sistemas militares são separados dos sistemas civis, bem como o cancelamento quando se verificar que poderão causar prejuízos incidentais excessivos aos civis.

Todavia, dependendo do alvo militar, pode ser praticamente impossível levar a efeito um ataque cibernético sem envolver infraestruturas civis, considerando as características do espaço cibernético e interdependência entre sistemas civis e militares. Como realça a Cruz Vermelha, “o uso de um *worm* que se replica e não pode ser controlado e pode, desta forma, causar estragos importantes a infraestruturas civis, seria uma violação ao DIH.” Não obstante, é interessante realçar o aparente entendimento de que a tecnologia de informação poderia limitar os estragos incidentais aos civis e às infraestruturas civis “na medida em que pode ser menos danoso interromper determinados serviços usados para fins militares e civis do que destruir a infraestrutura por completo”. Em outras palavras, à luz do princípio da precaução, se os Estados devem escolher meios menos nocivos para alcançar um objetivo militar, essa escolha poderia, teoricamente, recair nos ataques cibernéticos[260].

4.1.2.3 Participação de Civis nas Hostilidades

Atores não estatais podem deflagrar ou se envolver direta ou indiretamente nas hostilidades cibernéticas, como ocorreu em setembro de 2000, quando *hackers* adolescentes israelenses criaram um *website* para interferir nos sítios do Hezbollah

[260] DROEGE, Cordula. *Não há brechas jurídicas no ciberespaço.* Disponível em: <http://www.icrc.org /por/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>. Acesso em: 24 fev. 2012.

e do Movimento de Resistência Islâmica Hamas, no Líbano, bloqueando e interferindo em seis *websites* de tais organizações e à Autoridade Nacional Palestina. O que poderia parecer um incidente corriqueiro tomou proporções de um incidente internacional.

Embora não tragam o conceito da participação direta em hostilidades, à luz das Convenções de Genebra, a participação direta de atores não estatais[261] nos conflitos cibernéticos pode implicar não apenas a perda da proteção destinada aos civis (exceto se feridos ou na condição de prisioneiros), mas também consequências jurídicas na seara dos crimes de guerra na medida em que podem assumir o *status* de combatentes[262].

Existem várias classificações e categorias de autores dos ataques cibernéticos[263], conforme o nível de conhecimento, de organização e dos objetivos, os quais podem variar entre a simples busca de desafios ou motivações ideológicas até razões criminosas, financeiras, espionagem ou bélicas.

A participação de civis não configura, necessariamente, uma prática indevida. Aliás, pelo contrário, na guerra cibernética, ela pode se tornar indispensável, tanto que muitos países já cogitam o recrutamento de tais atores[264] e tal ideia também já foi teorizada no Brasil, com base na Lei nº 11.631, de 21 de dezembro de 2007, que criou o Sistema Nacional de Mobilização[265].

É preciso distinguir, portanto, as ações defensivas ou ofensivas desencadeadas à luz das normas dos conflitos armados daquelas realizadas à revelia dos limites legais, em contexto de beligerância, sujeitando-os a todas as consequências legais, conforme o Guia Interpretativo da Noção de Participação

---

[261] DELIBASIS, Dimitrios. *Cyberspace warfare attacks and non state actors*. 2011. Disponível em: <http://ssrn.com/abstract=1942283>. Acesso em: 25 fev. 2012.
[262] WATTS, Sean. *Combatant status and computer network attacks*. Fevereiro de 2010. Disponível em: <http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=sean_watts>. Acesso em: 24 fev. 2012.
[263] A respeito das distinções entre *hackers*, *crackers*, *phreakers* e outras categorias, organizações e modos de atuação, vide Raphael Mandarino, ob. cit., págs. 81/104.
[264] BRENNER, Susan W.; CLARKE, Leo L. *Civilians in cyberwarfare: casualties***.** SMU Science and Technology Law Review, v. 13. p. 249-282. 2009-2010.
[265] STOPATTO, Sérgio Luiz. *A guerra cibernética e a mobilização nacional.* Caderno de Estudos Estratégicos de Logística e Mobilização. Escola Superior de Guerra: 2010, p.. 211. Disponível em: <http://www.esg.br/uploads/2010/12/CadernoSALMob2010_r.pdf>. Acesso em: 24 fev. 2012.

Direita nas Hostilidades à Luz do Direito Humanitário Internacional da Cruz Vermelha[266].

O Protocolo Adicional I define que os membros das Forças Armadas envolvidas em conflito - exceto serviço religioso e de saúde - são combatentes, têm o direito de participar diretamente das hostilidades e de invocar o estatuto de prisioneiro de guerra - nos termos dos artigos 43 (2) e 44 (1) – o que não é conferido aos espiões – artigo 46 - e aos mercenários, que não são parte das Forças Armadas e são recrutados para atuar de forma direta nas hostilidades; também não têm direito ao estatuto do combatente - artigo 47 - e à proteção destinada aos civis pelas Convenções de Genebra, exceto se feridos; respondem por crimes de guerra ou penalmente se cometerem violações graves ao direito humanitário.

De acordo com o artigo 50 do Protocolo Adicional I de 1977, civil é a pessoa que não pertence a nenhuma das categorias definidas no seu artigo 43 (combatentes) e no artigo 4º - A, alíneas 1, 2, 3 e 6) da Convenção III de Genebra (membros de Forças Armadas regulares, milícias e corpo de voluntários que façam parte das Forças Armadas, outras milícias e outros corpos voluntários, incluindo movimentos de resistência organizados, população não organizada em força armada regular que combate tropas de invasão).

Tais definições permitem concluir que os civis protegidos pelas Convenções de Genebra não se confundem com os civis que integram corpo de voluntários ou milícias integrantes ou não das Forças Armadas, os quais podem invocar as proteções do estatuto dos combatentes e do prisioneiro de guerra - o que não ocorre com mercenários e espiões. Tais civis podem também ser agentes de crimes de guerra se não forem observadas as leis, os usos e os costumes da guerra.

---

[266] MELZER, Nils. *Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law*. 2009. Disponível em: <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>. Acesso em: 22 fev. 2012.
A propósito: *If war is defined as a state of armed conflict between States it follows, to those who accept this definition, that the 'subjects' of belligerence can only be States. But even traditionalists admit, on reflection, that groups of citizens, for example those recognised as belligerents in civil war, can wage war. Even other groups, if they have some consolidated structure, can be classified as belligerents, as is amply demonstrated in contemporary warfare […]. International organisations cal also be belligerents. […] There is no reason why other organisations could not be belligerents and no a priori reason why such entities should be excluded as subjects of the Law of War.* DETTER, Ingrid. The law of war. UK: Cambridge University Press, 2000, p. 132-133.

Tais noções precisam ser pensadas à luz dos conceitos de nacionalidade e do caráter transnacional do espaço cibernético[267], bem como avaliados enquanto possível brecha para a terceirização da guerra, com todas as questões éticas decorrentes.

4.1.3 O Direito de Haia e o Direito de Nova Iorque

A necessidade de limitar o desenvolvimento de armas, as inovações tecnológicas e a complexidade dos conflitos armados contemporâneos têm contribuído para a aproximação e interdependência entre as Convenções de Genebra e de Haia, pois a proteção de bens e pessoas nos conflitos armados está ligada à proibição e limitação do uso de determinados meios e métodos de combate[268].

Adotadas durante as Conferências da Paz realizadas em Haia em 1899 e 1907, as Convenções de Haia congregam leis e costumes de guerra e regras que devem ser observadas na condução das hostilidades, ou seja, os métodos de guerra, impondo limitações aos meios e às armas utilizados para provocar danos aos inimigos.

O Direito de Nova Iorque contempla aspectos das Convenções de Haia e de Genebra refletidos nas normas da Organização das Nações Unidas, as quais refletem os esforços de incentivar os países signatários a cumprirem os preceitos de Genebra e de Haia na proteção dos soldados e da população civil nos conflitos armados, postura formalmente inaugurada na Resolução XXIII de 1968.

---

[267] BRENNER, Susan W.; CLARKE, Leo L. *Civilians in cyberwarfare: conscripts* (July 29, 2010). Vanderbilt Journal of Transnational Law. v. 43. 2010.

[268] Manual de Emprego do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas, aprovado pela Portaria Normativa nº 1.069, de 5 de maio de 2011, do Ministério da Defesa, publicada no Diário Oficial da União nº 87, de 9 de maio de 2011, Seção I, p. 5.

Na mesma trilha das indagações e possíveis interpretações do Direito de Genebra, o Direito de Haia e o Direito de Nova Iorque precisam amadurecer e repensar seus conceitos com o mesmo propósito de elucidar quais ações defensivas e ofensivas podem ser deflagradas ou não no espaço cibernético, preservando bens e pessoas civis.

4.1.4 Princípios, Usos e Costumes do Direito Internacional

Considerando que não existem usos e costumes consolidados a respeito das hostilidades cibernéticas[269], ainda não podem ser invocados como uma fonte normativa específica. É provável que as diferentes políticas nacionais de segurança e defesa cibernética passem a formatar os usos e costumes da guerra cibernética.

De acordo com a Cláusula Martens, prevista no preâmbulo da IV Convenção de Haia de 1907, na ausência de regras específicas de direito para contornar os conflitos, “os habitantes e combatentes permanecem sob a proteção dos princípios do direito das nações decorrentes dos costumes das nações civilizadas, do princípio da humanidade e dos ditames da consciência pública”. Tal noção foi confirmada no artigo 1º do I Protocolo Adicional de 1977 à Convenção de Genebra, segundo o qual “nos casos não previstos pelo presente Protocolo ou por outros acordos internacionais, os civis e os combatentes ficarão sob a proteção e a autoridade dos princípios de direito internacional, tal como resulta do costume estabelecido, dos princípios humanitários e das exigências da consciência pública.”

O Comitê Internacional da Cruz Vermelha publica, em seu portal, as “práticas geralmente aceitas como lei”, as quais constituem normas do Direito

[269] JURICH, Jon P. *Cyberwar and customary international law: the potential of a ‘bottom-up’ approach to an international law of information operations***.** Chicago Journal of International Law. v. 9. Nr 1. p. 275-295. Citation: 9 Chi. J. Int'l L. 275 2008-2009

Internacional Humanitário Consuetudinário[270]. Além disso, os princípios que regem o Direito Humanitário Internacional também são relevantes para sua aplicação, especialmente nas situações em que as regras positivadas não podem ser cumpridas: princípio da humanidade, necessidade, proporcionalidade, distinção, proibição dos males supérfluos e independência do *jus ad bellum* e *jus in bello.*[271]

4.1.5 Tratados Internacionais e Normas Internas

Os compromissos bilaterais ou multilaterais assumidos pelos Estados no plano internacional e as suas normas internas de segurança da informação e doutrinas militares também constituem inequívocas fontes normativas aplicáveis à guerra cibernética, com a ressalva de que a sua aplicabilidade ao espaço cibernético e a possibilidade de colidências normativas são desafios aos estrategistas e juristas.

O Acordo Internacional de Telecomunicações e Organizações de Satélites de 1973 (INTELSAT), ao prever que os satélites devem ser usados para propósitos pacíficos, permite concluir que proíbe o tráfego de dados para guerra cibernética, porém, suas disposições não se aplicam ao estabelecimento, aquisição ou utilização de segmentos e instalações espaciais exclusivos para propósitos de segurança nacional. A Convenção a respeito da Organização Internacional de Satélites Marítimos de 1976 (INMARSAT) também restringe o uso de satélites alugados ou de propriedade do INMARSAT para propósitos pacíficos, o que evidencia uma tradição em matéria de telecomunicações de não interferência. A Convenção Internacional de Telecomunicações de Málaga – Terremolinos de 1973 estabelece, no artigo 35, que todas as estações, quaisquer que sejam seus propósitos, devem operar de maneira que não causem interferência nociva nos serviços de rádio ou comunicações de

[270] Disponível em: <http://www.icrc.org/por/war-and-law/treaties-customary-law/customary-law/index.jsp>. Acesso em: 24 fev. 2012.
[271] BOUVIER, Antoine A.; SASSÓLI, Marco. *How does law protect in war?* p. 115.

outros Membros, porém, os satélites militares estão expressamente excluídos de tal regra[272].

O Brasil é signatário de diversos atos internacionais relativos ao Direito da Guerra[273], Defesa e Desarmamento[274], Assuntos Militares[275] e diversos outros relacionais aos Direitos Humanos e ao Direito Humanitário Internacional, além de contar com uma densa legislação vocacionada à segurança da informação[276]. Diversas ações e regras militares também estão sendo desenvolvidas para o espaço cibernético, definido como setor estratégico pela Doutrina Nacional de Defesa.

4.1.6 Tribunal Penal Internacional

As Convenções de Haia e de Genebra fixam as principais regras, limites e interdições relacionados à violência e aos métodos de guerra, além de definirem os comportamentos que constituem crimes de guerra e mecanismos de sanção. Alguns crimes são qualificados como graves infrações às Convenções de Genebra e caem na alçada da jurisdição universal, que permite a qualquer país julgar seus autores. A antiguidade e a repetição de tais normas convencionais lhe atribuem um caráter consuetudinário, tornando-se, por tal razão, obrigatórias aos não signatários[277].

Regido pelo princípio da subsidiariedade[278], o Tribunal Penal Internacional é um tribunal permanente que tem competência para julgar indivíduos acusados da prática de crime de genocídio, crimes contra a humanidade, crimes de guerra e

---

[272] Disponível em: <http://www.airpower.au.af.mil/apjinternational/apj-p/2000/4tri00/dicenso.htm>. Acesso em: 24 fev. 2012.
[273] Disponível em: <http://www2.mre.gov.br/dai/guerra.htm >. Acesso em: 24 fev. 2012.
[274] Disponível em: <http://www2.mre.gov.br/dai/dearm.htm>. Acesso em: 24 fev. 2012.
[275] Disponível em: <http://www2.mre.gov.br/dai/assumilitar.htm>. Acesso em: 24 fev. 2012.
[276] Disponível em: <http://dsic.planalto.gov.br/legislacaodsic>. Acesso em: 24 fev. 2012.
[277] BOUCHET-SAULNIER, Françoise, ob. cit. p. 304.
[278] Ou da *ultima ratio*, segundo o qual a jurisdição do TPI pode ser acionada após o esgotamento ou inércia da jurisdição dos países signatários. Consagra o princípio da responsabilidade penal internacional do indivíduo. O TPI não tem uma polícia investigativa, razão pela qual o procurador-geral e seus adjuntos dependem da cooperação dos países.

crime de agressão - o único que não é definido pelo Estatuto de Roma[279], mas que pode ser materializado nos ataques cibernéticos[280]. Alguns dos crimes de guerra previstos no artigo 8º do Estatuto do TPI podem resultar de ataques cibernéticos:

> 1. O Tribunal terá competência para julgar os crimes de guerra, em particular quando cometidos como parte integrante de um plano ou de uma política ou como parte de uma prática em larga escala desse tipo de crimes.
>
> 2. Para os efeitos do presente Estatuto, entende-se por "crimes de guerra":
>
> a) As violações graves às Convenções de Genebra, de 12 de Agosto de 1949, a saber, qualquer um dos seguintes atos, dirigidos contra pessoas ou bens protegidos nos termos da Convenção de Genebra que for pertinente:
>
> iv) Destruição ou a apropriação de bens em larga escala, quando não justificadas por quaisquer necessidades militares e executadas de forma ilegal e arbitrária;
>
> b) Outras violações graves das leis e costumes aplicáveis em conflitos armados internacionais no âmbito do direito internacional, a saber, qualquer um dos seguintes atos:
>
> i) Dirigir intencionalmente ataques à população civil em geral ou civis que não participem diretamente nas hostilidades;
>
> ii) Dirigir intencionalmente ataques a bens civis, ou seja, bens que não sejam objetivos militares;
>
> iv) Lançar intencionalmente um ataque, sabendo que o mesmo causará perdas acidentais de vidas humanas ou ferimentos na população civil, danos em bens de caráter civil ou prejuízos extensos, duradouros e graves no meio ambiente que se revelem claramente excessivos em relação à vantagem militar global concreta e direta que se previa;
>
> v) Atacar ou bombardear, por qualquer meio, cidades, vilarejos, habitações ou edifícios que não estejam defendidos e que não sejam objetivos militares;
>
> ix) Dirigir intencionalmente ataques a edifícios consagrados ao culto religioso, à educação, às artes, às ciências ou à beneficência, monumentos históricos, hospitais e lugares onde se agrupem doentes e feridos, sempre que não se trate de objetivos militares;
>
> xiii) Destruir ou apreender bens do inimigo, a menos que tais destruições ou apreensões sejam imperativamente determinadas pelas necessidades da guerra;
>
> xx) Utilizar armas, projéteis; materiais e métodos de combate que, pela sua própria natureza, causem ferimentos supérfluos ou sofrimentos desnecessários ou que surtam efeitos indiscriminados, em violação do direito internacional aplicável aos conflitos armados, na medida em que tais armas, projéteis, materiais e métodos de combate sejam objeto de uma proibição geral e estejam incluídos em um anexo ao presente Estatuto, em virtude de uma alteração aprovada em conformidade com o disposto nos artigos 121 e 123;

---

[279] Decreto nº 4.388, de 25 de setembro de 2002 (promulga o Estatuto de Roma do Tribunal Penal Internacional). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4388.htm>. Acesso em: 25 fev. 2012.

[280] OPHARDT, Jonathan A. *Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow´s battlefield.* Duke Law & Technology Review, Nr 3. p. 275-295. 2010

> e) As outras violações graves das leis e costumes aplicáveis aos conflitos armados que não têm caráter internacional, no quadro do direito internacional, a saber qualquer um dos seguintes atos:
>
> i) Dirigir intencionalmente ataques à população civil em geral ou civis que não participem diretamente nas hostilidades;

A Resolução 3314, de dezembro de 1974, da Assembleia Geral da ONU[281] elenca alguns exemplos e define agressão como o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado ou ainda qualquer atitude incompatível com a Carta da Organização das Nações Unidas.

À luz do princípio da jurisdição universal, todos os países signatários das Convenções de Genebra têm jurisdição para julgar graves violações e crimes de guerra (inclusive outros não definidos pelas Convenções) e a obrigação de adequar as normas nacionais e de buscar supostos violadores, independentemente da nacionalidade e do país em que tenha ocorrido a violação, para levá-los a julgamento nos tribunais nacionais ou entregá-los a outro país signatário[282].

4.2 Desafios e Tendências para a Regulamentação da Guerra Cibernética

A despeito da possibilidade de aplicação das regras dos conflitos armados e do direito humanitário internacional aos ataques cibernéticos, é certo que elas foram elaboradas para outro contexto e não foram pensadas para as armas cibernéticas, razão pela qual se faz necessária uma releitura de deve enfrentar desafios jurídicos e técnicos.

---

[281] Disponível em: <http://www.unidir.org/pdf/articles/pdf-art2642.pdf>. Acesso em: 19 fev. 2012.
[282] Disponível em: <http://www.icrc.org/por/resources/documents/statement/united-nations-universal-jurisdiction-statement-2010-10-15.htm>. Acesso em: 19 fev. 2012.

É preferível enfrentar tais complexidades a relegar para o acaso as consequências de uma ameaça efetiva à paz e à segurança internacional. Em tal direção, algumas iniciativas de governos, organismos internacionais, universidades e setor privado já estão em curso, embora distantes de um consenso.

De acordo com relatório disponibilizado por Raphael Mandarino, na 1ª Conferência sobre Segurança da Informação realizado pela Interpol, em 2010, no Departamento de Polícia de Hong Kong, na China[283], foi debatida a necessidade de ampliar a cooperação nas investigações de crimes e de criar leis para desenvolver um sistema internacional de verificação de identidade no espaço cibernético; percebeu-se que os temas relacionados à defesa cibernética, aos crimes cibernéticos e à proteção das infraestruturas críticas costumam ser tratados como sinônimos ou complementares em razão da falta de uma taxonomia internacional a respeito do assunto. As diferentes visões a respeito das políticas de segurança cibernética decorrem fundamentalmente das distintas formas de tratar do fluxo de informações, da liberdade na Internet e das ações estatais relacionadas aos crimes cibernéticos.

Atualmente, quatro grandes modelos de segurança no espaço cibernético estão sendo construídos no cenário mundial[284]. O modelo americano considera que o espaço cibernético não tem fronteiras, razão pela qual não há barreiras para a circulação da informação; conforme visto anteriormente, o governo americano defende a política de que os ataques cibernéticos podem ser respondidos por força militar convencional. O modelo europeu também defende que a informação no espaço cibernético não tem fronteiras, que seu fluxo é livre e que o foco deve estar na proteção das infraestruturas críticas, na cooperação internacional e no combate aos crimes cibernéticos. No modelo russo[285], o espaço cibernético não tem fronteiras, mas o fluxo de informações não é absolutamente livre; qualquer investigação no espaço cibernético pressupõe um acordo bilateral. No modelo chinês, o espaço cibernético tem fronteiras e a circulação de informações não é livre.

---

[283] http://www.interpol.int/News-and-media/News-media-releases/2010/PR070

[284] Palestra proferida por Raphael Mandarino no II Seminário de Defesa Cibernética, novembro de 2011.

[285] A Rússia integra a Organização para Cooperação de Xangai, criada em 2001, juntamente com a China, Cazaquistão, Quirguistão, Tadjiquistão e Uzbequistão.

Em abril de 2011, o EastWest Institute dos Estados Unidos e o Information Security Institute of Moscou State University da Rússia firmaram um acordo sobre a taxonomia ou terminologia crítica para a segurança cibernética, denominado “Russia – U.S. Bilateral on Cybersecurity Critical Terminology Foundations” [286]; diversas definições técnicas relativas ao espaço cibernético (“the theatre”), às circunstâncias agravantes (“the modes of aggravation”) - diferenciando a guerra cibernética do crime, do terrorismo e dos demais conflitos cibernéticos – e à arte da segurança (“the art”) - no qual traz definições de ataque e contra-ataque, capacidade ofensiva e defensiva, exploração e intimidação, contramedidas e estado de guerra no espaço cibernético.

Em 2010, o Brasil e a Rússia firmaram um Acordo de Proteção Mútua e Não Agressão por Armas de Informação, ainda não ratificado pelo Congresso Nacional, o qual prevê a troca de informações sigilosas, capacitação de pessoal e realização de exercícios conjuntos de guerra cibernética[287]. Outros acordos similares já foram assinados pelo Brasil com outros países, como Portugal, Espanha, França, Itália e Israel; outros estão em negociação com Alemanha, Dinamarca, Estados Unidos, Luxemburgo, República Checa e Ucrânia[288].

A criação de regras para o emprego de armas cibernéticas ou de um tratado de não proliferação de armas de informação encontra na UIT – União Internacional de Telecomunicações e na Rússia os seus maiores defensores. Em 1998, a Rússia propôs à Organização das Nações Unidas uma Resolução, que previa uma chamada aos Estados para apresentar suas visões a respeito da conveniência de elaborar normas internacionais de proibição do desenvolvimento de armas de informação, mas a iniciativa nunca foi levada para votação pela Assembleia Geral; em 2001, a Federação Russa, preocupada com os possíveis efeitos das armas cibernéticas[289], propôs a criação de um grupo de peritos governamentais para

[286] Disponível em http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2).pdf, acesso em 22.02.2012.
[287] http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=22683&sid=18
[288] De acordo com dados de maio de 2011 apresentados ao Tribunal de Contas da União por Raphael Mandarino. Disponível em: <www.ticontrole.gov.br/portal/pls/portal/docs/1957157.PPT>. Acesso em: 25 fev. 2012.
[289] No inverno europeu, por exemplo, um ataque cibernético ao sistema de energia elétrica pode representar, teoricamente, risco de genocídio.

estudar a criação de regras internacionais. Na reunião realizada em 2005, um grupo de países, integrado pelos representantes do Brasil, já reconhecia o potencial catastrófico das armas cibernéticas e defendia a necessidade de levar a questão ao Conselho de Segurança. Outros países vislumbraram a necessidade de regulamentação, porém, não consideravam a ameaça catastrófica. Os Estados Unidos e o Reino Unido defenderam a suficiência das normas existentes[290]. Em 2010, o grupo reconheceu a interdependência dos países para enfrentar as ameaças cibernéticas[291].

Vale lembrar que, na época da elaboração da Convenção de Budapeste sobre crimes cibernéticos, o Conselho Europeu também estudou a questão.

O Doutor Alexander Merezhko, professor de direito internacional da Ucrânia, desenvolveu uma proposta de Convenção Internacional para a Proibição da Guerra Cibernética, na qual caracteriza a Internet como ferramenta para o desenvolvimento tecnológico, informacional e econômico da comunidade internacional, constituindo patrimônio comum da humanidade que não pode ser objeto de apropriação nacional. Por tal razão, propõe que a comunidade internacional deve usar a Internet exclusivamente para fins pacíficos, em prol da segurança e da liberdade, abstendo-se de prejudicar a segurança, economia, política e soberania de qualquer Estado. Além disso, estabelece que os Estados não devem recorrer ou apoiar a guerra cibernética e que se comprometem a criar disposições penais específicas para prevenir e proibir a guerra cibernética e a envidar esforços para o desenvolvimento de um sistema global de segurança na Internet, respeitando os sistemas nacionais de segurança cibernética[292].

Um grupo de juristas e peritos do Centro de Excelência e Cooperação em Defesa Cibernética da OTAN, baseado em Tallin, na Estônia, coordenados pelo Professor Michael N. Schmitt, está desenvolvendo o “MILCW – Manual on Internacional Law Applicable to Cyber Warfare”, divulgado como Tallinn

---

[290] ALMEIDA, José Eduardo Portella. *A tendência mundial para a defesa cibernética*. p. 86. Disponível em: <http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em: 25 fev. 2012.

[291] Disponível em: <http://www.reachingcriticalwill.org/political/1com/1com10/reports/201.pdf>. Acesso em: 25 fev. 2012.

[292] Disponível em: <http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57>. Acesso em: 25 fev. 2012.

Manual[293].Thomas Wingfield, do Centro Marshall da Alemanha, compõe o grupo e defende a tese de que ataques cibernéticos podem ser respondidos com ataques militares convencionais e de que, a despeito das dificuldades técnicas para a identificação da autoria e da origem de um ataque, não seria necessária a certeza absoluta, bastando 75% (setenta e cinco) de provas claras e convincentes[294]. Não obstante a indiscutível necessidade de criar normas de proteção aos Estados, tal raciocínio, todavia, pode gerar inúmeras controvérsias e manipulações, além de ataques temerários e indevidos, em detrimento de outros interesses e valores do mesmo calibre de importância.

De autoria de Daniel Ryan, da National Defense University, Julie Ryan, da George Washington University, Maeve Dion, da Stockholm University, e Eneken Tikk, quando integrante do Centro de Excelência e de Cooperação em Defesa Cibernética, a proposta do "Ten Rules of Behavior for Cyber Security"[295] enunciam os seguintes princípios: Territorialidade, Responsabilidade, Cooperação,

[293] Disponível em: <http://www.ccdcoe.org/249.html>. Acesso em: 25 fev. 2012.
[294] Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/2214/Empresas-e-governos-fazem-investimentos-bilionarios-em-ciberdefesa->. Acesso em: 25 fev. 2012.
[295] Apresentação de Eneken Tik no II Seminário de Defesa Cibernética, CITEX, Brasília, Novembro de 2011.
- **Territoriality**: Information Infrastructure located within a State's territory is subject to that State's territorial sovereignty. Make use of the regulatory framework and remedies within your jurisdiction;
- **Responsability**: The fact that a cyber attack has been launched from an information system located in a State's territory invokes the responsibility of that State for the attack;
- **Cooperation**: The fact that a cyber attack has been conducted via the information system located in a State's territory creates a duty to cooperate with the victim State. There are no options for investigating cross-border incidents without cooperation, the duty of cooperation also applies between public and private sector and between different disciplines;
- **Self-Defence**: Everyone has the right to self-defense when facing a clear and imminent danger. This right has strict limitations in criminal law and law of armed conflicts;
- **Early Warning**: Everyone has to notify the potential victims about an upcoming cyber attack;
- **Data Protection**: Information infrastructure monitoring data is perceived personal unless provided for otherwise. Information infrastructure monitoring data is perceived personal unless provided for otherwise. Prevalent interpretation in the EU (Data Protection Directive);
- **Duty of Care**: Everyone has the responsibility to implement a reasonable level of security in their information infrastructure. Due diligence duties arise from the legal framework of data protection, information society services, consumer protection etc;
- **Access to Information**: The public has the right to be informed about threats to their life, security and well-being. Whistle-blowing, classified information Private sector conflict of interest;
- **Criminalization**: Every nation has the responsibility to include the most common cyber offences in its criminal law. Council of Europe Cyber Crime Convention contains the basic framework for cross-border investigation and prosecution;
- **Mandate**: An Organization's capacity to act (and regulate) derives from its mandate. Currently, significant overlaps and gaps exist between the focus areas of major international organizations as well between national authorities.

Autodefesa, Alerta Oportuno, Proteção da Informação, Dever de Cuidado, Acesso à Informação, Criminalização e Mandato.

Finalmente, será imprescindível definir as regras técnicas de preservação de evidências digitais e investigação dos ataques cibernéticos para efeito de identificação da origem e da autoria. Para tanto, alguns critérios da Convenção de Budapeste podem ser utilizados, embora a lógica da cooperação internacional possa não funcionar no contexto da guerra cibernética.

Além disso, será fundamental avaliar a adequação e a extensão dos mandatos da Organização das Nações Unidas, especialmente do Conselho de Segurança, e do Tribunal Penal Internacional para conduzir investigações, deliberar sobre atos de guerra cibernética e julgar eventuais crimes dela decorrentes.

Ao Direito Humanitário Internacional incumbirá fomentar esforços para evitar ou minimizar os efeitos da guerra cibernética.

5 CONCLUSÃO

As informações colhidas no decorrer da pesquisa não deixam dúvidas de que os ataques cibernéticos podem ser equiparados a armas cibernéticas, inclusive com grande potencial destrutivo, razão pela qual sua utilização pode configurar agressão ou uso da força à luz da Carta da ONU, a despeito de ser necessária a identificação da autoria para que a legítima defesa ou o sistema de segurança coletiva sejam autorizados. Qualquer resposta deve ser orientada pelos princípios da necessidade e da proporcionalidade, conceitos que também precisam de amadurecimento para o espaço cibernético.

A utilização das armas cibernéticas deve ser guiada pelos preceitos do direito internacional humanitário que protegem bens e pessoas civis, observando-se o princípio da distinção, as precauções e a proibição de ataques indiscriminados dos quais possam resultar consequências imprevisíveis e danos superiores ou desproporcionais aos objetivos militares. A participação de civis e atores não estatais nas hostilidades, na condição de voluntários ou mercenários, além de retirar a proteção destinada aos civis (exceto na condição de feridos), pode acarretar a prática de crimes de guerra e levar à responsabilização, inclusive pelo Tribunal Penal Internacional, observado o princípio da subsidiariedade. Todavia, tal participação não é, necessariamente, indevida, desde que observadas as normas e os limites dos conflitos armados.

Enquanto não for possível construir um consenso internacional a respeito da regulamentação da guerra cibernética, além da aplicabilidade das regras existentes – *quando e se houver critérios técnicos seguros que permitam identificar a autoria e a origem, a necessidade e a proporcionalidade da resposta a um ataque cibernético, bem como para a sua eventual adoção no decorrer de hostilidades se eles forem menos nocivos ou não apresentarem riscos de danos aos bens e à população civil* - o Movimento Internacional da Cruz Vermelha e a Corte Internacional de Justiça (embora sua vocação natural seja outra) poderão exercer suas atribuições interpretativas para minimizar as dúvidas e lacunas normativas.

Como possível critério de interpretação e proteção, a Cláusula Martens, da Convenção de Haia de 1907, assegura que, na ausência de regras específicas de direito para contornar os conflitos, os habitantes e combatentes permanecem sob a proteção e a autoridade dos princípios de direito internacional que resultam do costume estabelecido, dos princípios humanitários e das exigências da consciência pública.

Os principais desafios técnicos e jurídicos para a regulamentação da guerra cibernética decorrem do seu caráter transnacional e das constantes inovações tecnológicas que permitem camuflar ou dificultar a identificação da origem e da autoria de um ataque cibernético.

Para superar tais desafios, será necessário identificar antes os critérios técnicos e jurídicos, além de definir mandato para conduzir as investigações relacionadas aos ataques cibernéticos e para julgar os eventuais crimes de guerra deles decorrentes. O Tribunal Penal Internacional não tem polícia investigativa própria e a cooperação internacional pode restar frustrada em contexto de beligerância.

Além disso, a despeito da universalidade da jurisdição do Direito Humanitário Internacional, o que atribui a todos os países a competência para sua aplicação, uma solução poderia ser a inclusão das armas cibernéticas e dos atos de guerra cibernética no anexo ao Estatuto de Roma, na forma dos artigos 121 e 123, conforme autoriza seu artigo 2, alínea “b”, xx.

Para o futuro das relações internacionais e da humanidade, seria melhor poder discutir apenas a cooperação e a paz cibernética, mas as inúmeras lacunas jurídicas e vulnerabilidades tecnológicas não permitem acreditar que elas não serão exploradas para fins não pacíficos, razão pela qual os desafios de aplicação e interpretação das atuais normas precisam ser enfrentados urgentemente pela comunidade internacional.

GLOSSÁRIO

Backbone (tradução: espinha dorsal) - no contexto de redes de computadores, o backbone designa o esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho. Na Internet, uma rede de escala planetária, podem-se encontrar hierarquicamente divididos, vários *backbones*: os de ligação intercontinental, que derivam nos *backbones* internacionais, que por sua vez derivam nos *backbones* nacionais.

Blog - contração do termo inglês *Web log* (diário da Web), é um site cuja estrutura permite a atualização rápida a partir de acréscimos dos chamados artigos ou *posts*. Estes são, em geral, organizados de forma cronológica inversa, tendo como foco a temática proposta do *blog*, podendo ser escritos por um número variável de pessoas, de acordo com a política do *blog*.

Botnet - é uma coleção de agentes de *software* ou *bots* que são executados autônoma e automaticamente. O termo é geralmente associado com o uso de *software* malicioso (vírus, por exemplo), mas também pode se referir a uma rede de computadores utilizando *software* de computação distribuída.

Cracker - é o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por *hackers* em defesa contra o uso jornalístico do termo *hacker*. Podem ser classificados em *crackers* de criptografia, *crackers* de *softwares* e desenvolvedores de vírus, *worms*, *trojans* e outros *malwares*.

Exploit - em segurança da informação, é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional – como o próprio sistema operacional ou serviços de interação de protocolos (ex: servidores Web). São geralmente elaborados por *hackers* como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por *crackers* a fim de ganhar acesso não autorizado a sistemas.

Gadget (tradução: geringonça, dispositivo) - pronuncia-se *gad-jet*; é um equipamento que tem um propósito e uma função específica, prática e útil no cotidiano. São comumente chamados de *gadgets* dispositivos eletrônicos portáteis como celulares, *smartphones*, leitores de mp3, entre outros. Pode identificar algum pequeno *software*, pequeno módulo, ferramenta ou serviço que pode ser agregado a um ambiente maior.

GhostNet - Rede de ciberespiões com sede no sul da China, responsável pela invasão e disseminação de vírus em mais de 1300 computadores em mais de 100 países. Tinha o objetivo de capturar pastas, arquivos, imagens e sons de computadores localizados em embaixadas, bancos e outras instalações sensíveis, concentrando-os em seu Centro de Comando.

Hacker - são indivíduos que elaboram e modificam *software* e *hardware* de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas, além de terem muito conhecimento em informática. Os *hackers* utilizam todo o seu conhecimento para melhorar *softwares* de forma legal.

Hardware - o termo *hardware* é bastante utilizado para identificar a unidade central de processamento, a memória e os dispositivos de entrada e saída. Em um conceito mais abrangente, identifica todo o arcabouço físico de um sistema computacional. Em complemento ao *hardware*, o *software* é a parte lógica, ou seja, o conjunto de instruções e dados processado pelos circuitos eletrônicos do *hardware*.

Peering - é um esforço colaborativo, seja de pessoas ou organizações, onde cada parte contribui voluntariamente e de forma aberta para a formação de determinado conteúdo. Essa definição é mais adequada para sua utilização no tráfego de dados na Internet, significando uma interconexão onde as partes envolvidas não necessitam de um acordo explícito. As transformações que a Internet sofreu ao longo dos anos, resultando no barateamento e nas inovações de sua infraestrutura, correspondem ao surgimento de estruturas colaborativas de baixo custo, como a telefonia via Internet, *softwares* de código aberto e plataformas globais de terceirização.

Script - Linguagem de *script* (também conhecido como linguagem de *scripting*, ou linguagem de extensão) são linguagens de programação executadas do interior de programas e/ou de outras linguagens de programação, não se restringindo a esses ambientes. As linguagens de *script* servem para estender a funcionalidade de um programa e/ou controlá-lo.

SIGINT - abreviatura de *signals intelligence*, é o termo inglês usado para descrever a atividade de colheita de informações ou inteligência através da interceptação de sinais de comunicações entre pessoas ou máquinas. Configura-se, na atualidade, como a maior fonte de informação dos serviços de inteligência, ao contrário do passado, quando a *HUMINT* (*human intelligence*) dominava.

Software - é uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado/informação ou acontecimento. *Software* também é o nome dado ao comportamento exibido por essa sequência de instruções quando executada em um computador ou máquina semelhante, além de um produto desenvolvido pela Engenharia de *software*. Inclui não só o programa de computador propriamente dito, mas também manuais e especificações.

Spam - abreviação em inglês de *spiced ham* (presunto condimentado), é uma mensagem eletrônica não solicitada enviada em massa. Em sua forma mais popular, um *spam* consiste em uma mensagem de correio eletrônico com fins publicitários. O termo *spam*, no entanto, pode ser aplicado a mensagens enviadas por outros meios e em outras situações. Geralmente os *spams* têm caráter apelativo e na maioria das vezes são incômodos e inconvenientes.

Switch (tradução: comutador) - é um dispositivo utilizado em redes de computadores para reencaminhar módulos (*frames*) entre os diversos nós. Possuem portas, assim como os concentradores (*hubs*) e a principal diferença entre um comutador e um concentrador é que o comutador segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá

colisões entre os pacotes de segmentos diferentes — ao contrário dos concentradores, cujas portas partilham o mesmo domínio de colisão.

Tablet - Um *tablet*, também conhecido como *tablet PC*, ou ainda em português, tablete, é um dispositivo pessoal em formato de prancheta que pode ser usado para acesso à Internet, organização pessoal, visualização de fotos, vídeos, leitura de livros, jornais e revistas e para entretenimento com jogos. Apresenta uma tela *touchscreen* (tela sensível ao toque) que é o dispositivo de entrada principal. A ponta dos dedos ou uma caneta aciona suas funcionalidades. É um novo conceito e não deve ser igualado a um computador completo ou um *smartphone*, embora possua diversas funcionalidades dos dois.

Token - é um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB. Esses dispositivos são, geralmente, utilizados como um fator de segurança adicional em transações financeiras realizadas em canais remotos/Internet. São empregados como um segundo fator de autenticação, pois elevam o nível de segurança e privacidade em caso de roubo de senhas, através de programas espiões. Ataques recentes, entretanto, mostram que os *tokens* são pouco efetivos como demonstrado na invasão da Lockheed Martin, fabricante dos caças F22 e F35 do governo dos EUA, em que foram utilizados *tokens* "falsos" para invadir o sistema.

REFERÊNCIAS

ALMEIDA, José Eduardo Portella. *A tendência mundial para a defesa cibernética*. p. 86. Disponível em: <http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em: 25 fev. 2012.

AUGUST, Ray. *International cyber-jurisdiction: a comparative analysis.* American Business Law Journal. p. 533.

BENATAR, Marco. *The use of cyber force: need for legal justification?* HeinOnline, 1 Goettingen J. Int´l L 375, 2009.

BOUCHET-SAULNIER, Françoise. Dicionário Prático do Direito Humanitário. Lisboa: Instituto Piaget, 1998.

BRENNER, Susan W.; CLARKE, Leo L. *Civilians in cyberwarfare: casualties*. SMU Science and Technology Law Review, v. 13, 2010.

CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura.* Lisboa: Fundação Calouste Gulbenkian, v.1, 2002.

CHAINOGLOU, Kalliopi. *An assessment of jus in bello issues concerning computer network attacks: a threat reflected in national security agendas* (April 13, 2011). Romanian Journal of International Law, v. 12. p. 25-63. 2010. Disponível em: <Available at SSRN: http://ssrn.com/abstract =1809127>. Acesso em: 25 fev. 2012.

CLARKE, Richard A.; KNAKE, Robert K., *Cyber War: The Next Threat to Nacional Security and What to do About it*. Estados Unidos: HarperCollins, 2010.

COLEMAN, Kevin G. *The cyber commander's ehandbook, a downloadable guide*. 2011.

DELIBASIS, Dimitrios. *Cyberspace warfare and self-defence* (October 10, 2011). Disponível em: <http://ssrn.com/abstract=1942279>. Acesso em: 25 fev. 2012.

_____. *Cyberspace warfare attacks and non state actors*. 2011. Disponível em: <http://ssrn.com/abstract=1942283>. Acesso em: 25 fev. 2012.

DETTER, Ingrid. The law of war. UK: Cambridge University Press, 2000.

DINSTEIN, Yoram. *Guerra, agressão e legítima defesa*. 3. ed. Tradução: Mauro Raposo de Mello. Barueri, SP: Manole, 2004.

DOROTHY Denning. *Reflections on cyberweapons controls.* Disponível em: < http://faculty.nps.edu/dedennin/publications/reflections_on_cyberweapons_controls.pdf>. Acesso em: 24 fev. 2012.

DROEGE, Cordula. *Não há brechas jurídicas no ciberespaço.* Disponível em: <http://www.icrc.org /por/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>. Acesso em: 24 fev. 2012.

DYSON, Esther. *Release 2.0 – A design for living in the digital age*. Estados Unidos: Broadway Books, 1997.

GEERS, Kenneth. Stra*tegic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence*. Talin, Estônia. 2011. p. 87-94. Disponível em: <http://pt.scribd.com/doc/62478319/Strategic-Cyber-Security-K-Geers >. Acesso em: 25 fev. 2012.

_____. *Sun Tzu and cyber war. NATO Cooperative Cyber Defence Centre of Excellence*. Talin, Estônia. 2011. p. 20-21. Disponível em: <http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf>. Acesso em: 26 fev. 2012.

GERVAIS, Michael. *Cyber attacks and the laws of war.* 2011 Disponível em: < http://ssrn.com/abstract=1939615 or http://dx.doi.org/10.2139/ssrn.1939615>. Acesso em 25 fev. 2012.

GLENNY, Misha. *Mercado sombrio: o cibercrime e você*. Tradução de Augusto Pacheco Calil; George Schlesinger; Luiz Antonio de Araújo. 1. ed. São Paulo: Companhia das Letras, 2011.

GRAHAM, David E. *Cyber threats and the law of war*. 2010.

HALPIN, Edward et al. *Cyberwar, netwar and the revolution in military affairs*. New York: Palgrave Macmillan, 2006.

HAYDEN, Michael. *The battlefield of cyberspace: the inevitable new military branch – the cyber force.* ALB. L.J. SCI. & TECH. 2011. v. 18. p. 295-324.

HOISINGTON, Matthew. *Cyberwarfare and the use of force giving rise to the right of self-defence*. Boston College International & Comparative Law Review. v. 32. p. 439-454.

HOLLIS, Duncan B., Why States Need an International Law for Information Operations. Lewis & Clark Law Review, Vol. 11, p. 1023, 2007; Temple University Legal Studies Research Paper No. 2008-43. Disponível em: <http://ssrn.com/abstract=1083889>. Acesso em: 24 fev. 2012.

_____. *New tools, new rules: international law and information operations. The message of war: information, influence and perception in armed conflict.* G. David and T. McKeldin, eds., 2008; Temple University Legal Studies Research Paper No. 2007-15. Disponível em: <http://ssrn.com/abstract=1009224>. Acesso em: 24 fev. 2012.

JURICH, Jon P. *Cyberwar and customary international law: the potential of a 'bottom-up' approach to an international law of information operations*. Chicago Journal of International Law. v. 9. Nr 1. p. 275-295. Citation: 9 Chi. J. Int'l L. 275 2008-2009

KERR, Orin S. *Internet surveillance law after the USA Patriot Act: the big brother that isn´t.* Northwestern University Law Review, v. 97. 2003. Disponível em: <http://papers.ssrn.com/sol3 /papers.cfm?abstract_id=317501>. Acesso em: 25 fev. 2012.

KESAN, Jay P.; HAYES, Carol M. *Mitigative counterstriking: self-defense and deterrence in cyberspace.* (April 7, 2011). Illinois Public Law Research Paper No. 10-35; Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Harvard Journal of Law and Technology, Forthcoming. Disponível em: <http://ssrn.com/abstract=1805163>. Acesso em: 25 fev. 2012.

LESSIG, Laurence. *Code.* New York: Basic Books, 2006, p. 1. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 24 fev. 2012.

LÉVY, Pierre. *O que é o virtual?* São Paulo: Editora 34, 1996.

LUCERO, Everton. *Governança na internet: aspectos da formação de um regime global e oportunidades para a ação diplomática*. Brasília: Fundação Alexandre Gusmão, 2011.

MANDARINO JÚNIOR, Raphael. *Segurança e defesa do espaço cibernético brasileiro*. Recife: Cubzac, 2010.

MELZER, Nils. *Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law*. 2009. Disponível em: <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>. Acesso em: 22 fev. 2012

OIKAWA, Alysson Hautsch, no artigo "*Conflito de leis e de jurisdição em casos envolvendo a internet: da necessidade de regulamentação internacional sobre a matéria*". In: MENEZES, Wagner (Org.). In: 2º CONGRESSO BRASILEIRO DE DIREITO INTERNACIONAL. Estudos de Direito Internacional. v.1. Curitiba. *Anais.* Curitiba: Juruá, 2004.

OPHARDT, Jonathan A. *Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow´s battlefield.* Duke Law & Technology Review, Nr 3. p. 275-295. 2010.

OPPENHEIM, L. *International Law*. 7ª ed., v II, Lauterpacht, 1952, p. 202.

PAPANASTASIOU, Afroditi. *Application of international law in cyber warfare operations* (September 8, 2010). Disponível em: <http://ssrn.com/abstract=1673785> ou em: <http://dx.doi.org/10.2139/ssrn.1673785>. Acesso em: 25 fev. 2012.

RAMOS, Albenides. *Metodologia da pesquisa científica: como uma monografia pode abrir o horizonte do conhecimento.* São Paulo: Atlas, 2009.

REMUS, Titiriga. *Cyber warfare and law of the nations.* (Jus Ad Bellum) (October 19, 2011). Disponível em: <http://ssrn.com/abstract=1946470 or http://dx.doi.org/10.2139/ssrn.1946470>. Acesso em: 25 fev. 2012.

REZEK, Francisco. *Direito internacional público: curso elementar*. São Paulo: Saraiva, 2000.

RICHARDSON, John C. *Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield* 2011. Disponível em: <http://ssrn.com/abstract=1892888> ou em: <http://dx.doi.org/10.2139/ssrn.1892888>. Acesso em: 25 fev. 2012.

ROSCINI, Marco. *World wide warfare - 'jus ad bellum' and the use of cyber force* (June 30, 2010). Max Planck Yearbook of United Nations Law. v. 14. p. 85-130. 2010. Disponível em: <http://ssrn.com/abstract=1683370>. Acesso em: 25 fev. 2012.

SCHMITT, Michael N. *Computer network attack and the use of force in international law: thoughts on a normative framework*. Columbia Journal of Transnational Law. v. 37. 1998-99. Disponível em: <http://ssrn.com/abstract=1603800>. Acesso em: 25 fev. 2012.

STOPATTO, Sérgio Luiz. *A guerra cibernética e a mobilização nacional.* Caderno de Estudos Estratégicos de Logística e Mobilização. Escola Superior de Guerra: 2010, p. 211. Disponível em: < http://www.esg.br/uploads/2010/12/Caderno SALMob2010_r.pdf>. Acesso em: 24 fev. 2012.

SWINARSKI, Christophe. *A norma e a guerra: palestras sobre direito internacional humanitário. competências e funções do comitê internacional da cruz vermelha - órgão da ação internacional humanitária.* Porto Alegre: Sergio Antonio Fabris, 1991.

TAKAHASHI, Tadao. *Sociedade da informação no Brasil: livro verde.* Brasília: Ministério da Ciência e Tecnologia, 2000.

WALKER, Paul A. *Traditional military activities in cyberspace: preparing for netwar*. Journal of International Law, . nr 3. v. 22. 2010. p. 337-359.

WATTS, Sean. *Combatant status and computer network attacks*. Fevereiro de 2010. Disponível em: <http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=sean_watts>. Acesso em: 24 fev. 2012.

WAXMAN, Matthew C. *Cyber-attacks and the use of force: back to the future of article 2.* (March 16, 2011). Yale Journal of International Law. v. 36. 2011. Disponível em: <http://ssrn.com/abstract=1674565>. Acesso em: 24 fev. 2012.