PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós-Graduação em Relações Internacionais

Jussara de Oliveira Machado

**CIBERGUERRA:
conceitos, doutrinas, estratégias, operações, instituições
e o caso dos Estados Unidos**

Belo Horizonte

2014

Jussara de Oliveira Machado

**CIBERGUERRA:
conceitos, doutrinas, estratégias, operações, instituições
e o caso dos Estados Unidos**

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Mestre em Relações Internacionais.

Orientador: Eugenio Pacelli Lazzarotti Diniz Costa

Belo Horizonte

2014

FICHA CATALOGRÁFICA

Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

M149c Machado, Jussara de Oliveira
Ciberguerra: conceitos, doutrinas, estratégias, operações, instituições e o caso dos Estados Unidos / Jussara de Oliveira Machado. Belo Horizonte, 2014. 139f.:il.

Orientador: Eugenio Pacelli Lazzarotti Diniz Costa
Dissertação (Mestrado)- Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Relações Internacionais.

1. Ciberespaço. 2. Processamento de dados - Medidas de segurança. 3. Estratégia. 4. Redes de informação. 5. Estados Unidos - Relações internacionais. I. Costa, Eugenio Pacelli Lazzarotti Diniz. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Relações Internacionais. III. Título.

SIB PUC MINAS

CDU: 301.175.1

Jussara de Oliveira Machado

**CIBERGUERRA:
conceitos, doutrinas, estratégias, operações, instituições
e o caso dos Estados Unidos**

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Mestre em Relações Internacionais.

Prof. Dr. Eugenio Pacelli Lazzarotti Diniz Costa (Orientador) – PUC Minas

Prof. Dr. Salvador Ghelfi Raza (Avaliador) – U.S. Naval Postgraduate School

Prof. Dr. Cristiano Garcia Mendes (Avaliador) – PUC Minas

Belo Horizonte, 25 de abril de 2014.

Ao meu pai, à minha mãe e ao meu amor,
com carinho.

AGRADECIMENTOS

Agradeço a Deus pela vida; aos meus pais, por tudo que sou, pelo amor incondicional e pelas doses diárias de carinho; ao meu irmão e à Pri, pelo apoio e admiração; ao Fábio, pela descoberta do amor, pelo exemplo de coragem e pela cura; à Lana, pelo começo; ao Denilson Feitoza, meu herói, e à FESMPMG, minhas maiores motivações para esta nova etapa; ao Marco Cepik, pela ideia e pelo essencial, sempre; ao CEEIG e à Priscila Brandão, pela prontidão em ajudar com os eventos; ao Renato, à Cris e a todos do TFLA, pela compreensão; ao Vlad, pelas notícias sempre atualizadas e pelo autógrafo instigador no livro; à Daila, pela ajuda com a prova de ingresso, à Lenise, por me ajudar com o primeiro projeto de pesquisa; ao Diego Canabarro e ao Thiago Borne, pela minibanca de qualificação e pelo material; aos colegas do curso na ECEME, Bernardo Wahl, Sandro Teixeira e Marco Túlio Freitas, por terem causado uma reviravolta em minhas ideias; a todos da PUC-MG, principalmente às funcionárias Paula e Bianca, pela paciência e carinhosa acolhida; aos professores e colegas, particularmente à Rosane, minha companheira de estudos, pela amizade construída nesta difícil jornada; ao Thiago Malafaia, pela ajuda com as teorias; ao Chris, pelo entusiasmo encorajador e pelo exemplo de dedicação; ao Cristiano Mendes, Otávio Dulci, Jorge Lasmar, Gabriel Pimenta, Rogério Giordano, Roberto Vinicius Gama, Manoela Vasconcelos, Renato Pires, Andrea Tsuruta e Cecília Oliveira, pela rica troca de experiências; à PUC-MG e à FAPEMIG, por terem custeado parte deste sonho; a todos de quem tive que me ausentar; a todos aqueles que sonharam junto comigo e, em especial, ao meu professor e orientador, Eugenio Diniz, por ter acreditado no meu potencial, investido no meu trabalho e ter me feito ir muito além do que eu mesma acreditava que poderia.

Sobre o princípio de tudo:
Fiz a tese e este livro, barcos de papel [...] como parte de nossa travessia. (CEPIK, 2003).

Porque os nossos sonhos são o que nos move
e nos impulsiona para além do impossível,
nos tornando pessoas melhores a cada ciclo da vida.

RESUMO

O principal objetivo deste estudo é tentar responder à seguinte pergunta: quais são as doutrinas, estratégias e operações de ciber guerra estadunidenses? Além desse objetivo geral, o estudo tem por objetivo específico sistematizar alguns conceitos relacionados aos ciberconflitos da atualidade e apresentar as principais mudanças institucionais ocorridas no aparato governamental estadunidense relacionadas à ciber guerra. Para tal, primeiramente retoma-se o processo histórico em que alguns dos conceitos utilizados hoje foram criados, como os conceitos de ciber, cibernética, ciberespaço, cibersegurança, ciber guerra, guerra na rede, guerra de informações, operações de informação e guerra centrada em rede, apresentando a evolução do debate ciber. Em seguida, apresentam-se as doutrinas, estratégias e operações de ciber guerra estadunidenses, recuperando um pouco o processo histórico em que surgiram e mostrando seus principais conteúdos. Por fim, apresentam-se as principais mudanças institucionais relacionadas à ciber guerra ocorridas no aparato governamental estadunidense, a partir da perspectiva da história dos ciberconflitos da atualidade. A pesquisa tem o intuito não só de aprofundar o debate que gira em torno da ciber guerra, mas também de contribuir para os estudos de política externa, política internacional, relações internacionais, defesa, segurança e estudos estratégicos relacionados aos conflitos internacionais da atualidade.

Palavras-chave: ciberespaço – cibersegurança – ciber guerra – conceitos – doutrinas – estratégias – operações – instituições – Estados Unidos

ABSTRACT

The main objective of this study is to try to answer the following question: what are the doctrines, strategies, and operations of cyberwar of the United States? In addition to this broad objective, the study aims specifically at systematizing some concepts related to today's cyber conflicts and to present the main institutional changes in the United States state apparatus related to the cyberwar. In order to do this, we first look at the historical process in which some of the concepts used today were created, such as the concepts of cyber, cybernetics, cyberspace, cybersecurity, cyberwar, netwar, information warfare, information operations and network-centric warfare, presenting the evolution of the cyber debate in retrospect. Next, we present the doctrines, strategies, and operations of cyberwar of the United States, referring back to the historical process in which they arose and showing its main contents. Finally, we present the main institutional changes, related to the cyberwar, which occurred in the United States state apparatus, from a historical perspective of today's cyber conflicts. The research is intended not only to deepen the debate that revolves around cyberwar, but also to contribute to foreign policy, international politics, international relations, defense, security and strategic studies related to the international conflicts of today.

Keywords: cyberspace - cybersecurity - cyberwar - concepts - doctrines - strategies - operations - institutions - United States

LISTA DE SIGLAS

- AF** – Air Force (Força Aérea)
- AFCENT** – Air Forces Central (Comando Central da Força Aérea)
- AFCYBER** – Air Force Cyber Command (Comando Ciber da Aeronáutica)
- ANPOCS** – Associação Nacional de Pós-Graduação e Pesquisa em Ciências Sociais
- APT** – Advanced Persistent Threat (Ameaça Persistente Avançada)
- ARFORCYBER** – Army Cyber Command (Comando Ciber do Exército)
- C2** – Command and Control (Comando e Controle)
- C2W** – Command-and-Control Warfare (Guerra de Comando e Controle)
- CA** – Civil Affairs (Assuntos Cíveis)
- CCDCOE** – Cooperative Cyber Defence Centre of Excellence (Centro de Excelência para a Cooperação em Defesa Ciber)
- CENTAF** – Central Command Air Forces (Comando Central da Força Aérea)
- CENTCOM** – Central Command (Comando Central)
- CERT** – Computer Emergency Response Team (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança)
- CI** – Counterintelligence (Contraineligência)
- CIA** – Central Intelligence Agency (Agência Central de Inteligência)
- CNA** – Computer Network Attack (Ataque a Redes de Computadores)
- CNCI** – Comprehensive National Cybersecurity Initiative (Iniciativa Global Nacional para a Cibersegurança)
- CND** – Computer Network Defense (Defesa de Redes de Computadores)
- CNE** – Computer Network Exploitation (Espionagem a Redes de Computadores)
- CNO** – Computer Network Operations (Operações de Redes de Computadores)
- CO** – Cyberspace Operations (Operações no Ciberespaço)
- CSIS** – Center for Strategic and International Studies (Centro para Estudos Estratégicos e Internacionais)
- DCEO** – Defensive Cyber Effects Operations (Operações de Efeitos Ciber Defensivos)
- DDoS** – Distributed Denial of Service (Ataques de Negação de Serviço Distribuídos)
- DHS** – Department of Homeland Security (Departamento de Segurança Interna)
- DISA** – Defense Information Systems Agency (Agência de Defesa de Sistemas de Informação)

DNS – Domain Name Server (Servidor de Nome de Domínio)

DNS – Domain Name System (Sistema de Nome de Domínio)

DoD – Department of Defense (Departamento de Defesa)

DoS – Denial of Service (Ataques de Negação de Serviço)

DRP – Disaster Recovery Planning (Planejamento de Recuperação de Desastres)

EIW – Economic Information Warfare (Guerra de Informação Econômica)

ER – ELIGIBLE RECEIVER (Receptor Elegível)

EUA – Estados Unidos da América

EW – Electronic Warfare (Guerra Eletrônica)

FAS – Federation of American Scientists (Federação Americana de Cientistas)

FBI – Federal Bureau of Investigation (Agência Federal de Investigação)

FLTCYBERCOM – Navy Fleet Cyber Command (Comando Ciber da Frota Naval)

FOIA – Freedom of Information Act (Lei de Liberdade da Informação)

GAO – Government Accountability Office (Escritório de Auditoria do Governo)

GPS – Global Positioning System (Sistema Global de Posicionamento)

HSPD – Homeland Security Presidential Directive (Diretiva Presidencial de Segurança Interna)

HUMINT – Human Intelligence (Inteligência Humana)

IA – Information Assurance (Garantia da Informação)

IBM – International Business Machines

IBW – Intelligence-based Warfare (Guerra baseada na Inteligência)

IDS – Intrusion Detection System (Sistema de Detecção de Intrusão)

IE – Information Environment (Ambiente de Informações)

IFSH – Institute for Peace Research and Security Policy (Instituto para Pesquisa sobre Paz e Política de Segurança)

IO – Information Operations (Operações de Informação)

IOTC – Information Operations Technology Center (Centro de Tecnologia de Operações de Informação)

IP – Internet Protocol (Protocolo de Internet)

IPS – Intrusion Prevention System (Sistema de Prevenção de Intrusão)

IRCs – Information-related Capabilities (Capacidades relacionadas com a Informação)

ISAC – Information Sharing and Analysis Centers (Centros de Compartilhamento de Informações e Análises)

IW – Information Warfare (Guerra de Informações)

IXP – Internet Exchange Point (Ponto de Troca de Tráfego)

JFC – Joint Forces Command (Comando das Forças Conjuntas)

JFCC-NW – Joint Functional Component Command – Network Warfare (Comando Conjunto de Componente Funcional – Guerra em Rede)

JIACG – Joint Interagency Coordination Group (Grupo de Coordenação Conjunto das Interagências)

JP – Joint Publication (Publicação Conjunta)

JPT – Joint Test Publication (Publicação Conjunta de Teste)

JTF-CND – Joint Task Force for Computer Network Defense (Força Tarefa Conjunta para a Defesa de Redes de Computadores)

JTF-CNO – Joint Task Force for Computer Network Operations (Força Tarefa Conjunta para Operações em Redes de Computadores)

JTF-GNO – Joint Task Force for Global Network Operations (Força Tarefa Conjunta para as Operações em Rede Globais)

JTRB – Joint Telecommunications Resources Board (Conselho Conjunto de Recursos de Telecomunicação)

JWICS – Joint Worldwide Intelligence Communications System (Sistema Conjunto Mundial de Comunicação de Inteligência)

KGB – Komitet Gosudarstvennoy Bezopasnosti (Comitê de Segurança do Estado)

LBL – Lawrence Berkeley Laboratory (Laboratório Lawrence Berkeley)

MARFORCYBER – Marine Forces Cyber Command (Comando Ciber das Forças Marítimas)

MILDEC – Military Deception (Dissimulação Militar)

MILNET – Military Network (Rede Militar)

MISO – Military Information Support Operations (Operações de Informação de Suporte às Forças Armadas)

NASA – National Aeronautics and Space Administration (Administração Nacional da Aeronáutica e do Espaço)

NATO – North Atlantic Treaty Organization (Organização do Tratado do Atlântico Norte)

NCCIC – National Cybersecurity and Communications Integration Center (Centro Integrado Nacional de Cibersegurança e Comunicações)

NCRCG – National Cyber Response Coordination Group (Grupo de Coordenação Nacional de Resposta Ciber)

NCSD – National Cyber Security Division (Divisão Nacional de Cibersegurança)

NCW – Network Centric Warfare (Guerra Centrada em Rede)

NDCM – Nonintrusive defensive countermeasures (Contramedidas Defensivas Não Intrusivas)

NDU – National Defense University (Universidade de Defesa Nacional)

NIPC – National Infrastructure Protection Center (Centro de Proteção da Infraestrutura Nacional)

NIPRNET – Non-classified Internet Protocol Router Network

NMS – National Military Strategy (Estratégia Militar Nacional)

NMS-CO – National Military Strategy for Cyberspace Operations (Estratégia Militar Nacional para Operações no Ciberespaço)

NSA – National Security Agency (Agência de Segurança Nacional)

NSC – National Security Council (Conselho de Segurança Nacional)

NSD – National Security Directive (Diretiva de Segurança Nacional)

NSPD – National Security Presidential Directive (Diretiva Presidencial de Segurança Nacional)

NSSA – National Security Strategy Archive (Arquivo de Estratégias Nacionais de Segurança)

OCEO – Offensive Cyber Effects Operations (Operações de Efeitos Ciber Ofensivos)

OCO – Offensive Cyberspace Operations (Operações Ofensivas no Ciberespaço)

OPLAN – Operation Plan (Plano de Operação)

OPSEC – Operations Security (Segurança das Operações)

OSINT – Open Source Intelligence (Inteligência de Fontes Ostensivas)

P2P – Peer-to-peer (Ponto-a-ponto)

PCCIP – President’s Commission on Critical Infrastructure Protection (Comissão Presidencial para a Proteção da Infraestrutura Crítica)

PCIPB – President’s Critical Infrastructure Protection Board (Conselho para a Proteção da Infraestrutura Crítica do Presidente)

PLA – People’s Liberation Army (Exército de Libertação Popular)

PPD – Presidential Policy Directive (Diretiva Política Presidencial)

PR – Public Relations (Relações Públicas)

PSYOPS – Psychological Operations (Operações Psicológicas)

PSYW – Psychological Warfare (Guerra Psicológica)

RAT – Remote Access Trojan (Trojan de Acesso Remoto)

RMA – Revolution in Military Affairs (Revolução nos Assuntos Militares)

SC – Strategic Communication (Comunicação Estratégica)

SCC – IT Sector Coordinating Council (Conselho Coordenador do Setor de TI)

SECDEF – Secretary of Defense (Secretário de Defesa)

SIGINT – Signals Intelligence (Inteligência de Sinais)

SIO – Special Information Operations (Operações Especiais de Informação)

SIPRNET – Secret Internet Protocol Router Network

STOD – Special Technical Operations Division (Divisão Especial de Operações Técnicas)

TCP – Transmission Control Protocol (Protocolo de Controle de Transmissão)

TI – Tecnologia da Informação

TIC – Tecnologias da Informação e Comunicação

TO – Theater Operations (Teatro de Operações)

UNIDIR – United Nations Institute for Disarmament Research (Instituto das Nações Unidas para Pesquisa sobre o Desarmamento)

US – United States (Estados Unidos)

USA – United States Army (Exército dos Estados Unidos)

USAF – United States Air Force (Força Aérea dos Estados Unidos)

USCERT – United States Computer Emergency Readiness Team (Equipe de Respostas a Incidentes de Emergência dos Estados Unidos)

USCYBERCOM – US Cyber Command (Comando Ciber dos Estados Unidos)

USG – United States Government (Governo dos Estados Unidos)

USSPACECOM – US Space Command (Comando Espacial dos Estados Unidos)

USSTRATCOM – US Strategic Command (Comando Estratégico dos Estados Unidos)

SUMÁRIO

1 INTRODUÇÃO	29
2 CIBERGUERRA E CONCEITOS ASSOCIADOS: O PARADIGMA INFORMACIONAL E A GUERRA NO SÉCULO XXI	31
2.1 Debate inicial.....	32
2.1.1 <i>Ciber (Cyber), Cibernética (Cybernetics) e Ciberespaço (Cyberspace)</i>	32
2.1.2 <i>Ciberguerra (Cyberwar) e Guerra na Rede (Netwar) segundo Arquilla e Ronfeldt</i>	34
2.1.3 <i>Guerra de Informações (Information Warfare) e Operações de Informação (Information Operations) segundo Libicki e Schmitt</i>	38
2.1.4 <i>Guerra Centrada em Rede (Network Centric Warfare)</i>	41
2.2 Debate atual	42
2.2.1 <i>Securitização do Ciberespaço e Relações Internacionais</i>	43
<u>2.2.1.1 <i>Ciberterrorismo (Cyber terror or Cyberterrorism), Hacktivismo (Hacktivism) e Cibercrime (Cyber crime or Cybercrime)</i></u>	46
2.2.2 <i>Analogias, metáforas e inconsistência conceitual</i>	48
<u>2.2.2.1 <i>Ciberespaço (Cyberspace), Internet (Internet) e Web (World Wide Web)</i></u>	50
2.2.3 <i>Thomas Rid: Ciberguerra (Cyberwar) Vs. Sabotagem (Sabotage), Espionagem (Espionage) e Subversão (Subversion)</i>	52
2.2.4 <i>Guerra baseada na Internet (iWar)</i>	55
2.3 Definindo Ciberguerra.....	56
3 DOCTRINAS, ESTRATÉGIAS E OPERAÇÕES DE CIBERGUERRA: ATACANDO E SE DEFENDENDO NO CIBERESPAÇO	58
3.1 Doutrinas de Ciberguerra.....	60
3.2 Estratégias de Ciberguerra.....	72
3.3 Operações de Ciberguerra.....	80
3.3.1 <i>Operações de Coleta de Inteligência</i>	83
3.3.2 <i>Operações Ofensivas</i>	89
3.3.3 <i>Operações Defensivas</i>	93
4 CIBERGUERRA E A HISTÓRIA DOS CIBERCONFLITOS: MUDANÇAS INSTITUCIONAIS E LIÇÕES APRENDIDAS	100
4.1 Três grandes períodos de mudanças institucionais e políticas ocorridas nos Estados Unidos segundo Healey	102
4.1.1 <i>Tomada de Consciência (Realization) (1986-1998)</i>	104
4.1.2 <i>Decolagem (Takeoff) (1998-2003)</i>	108
4.1.3 <i>Militarização (Militaryization) (2003-2012)</i>	110
4.2 Lições aprendidas e breves reflexões	118
5 CONSIDERAÇÕES FINAIS	125
REFERÊNCIAS	127

1 INTRODUÇÃO

No dia 20 de maio de 2013 um empregado da Booz Allen Hamilton, empresa prestadora de serviços para a Agência de Segurança Nacional (NSA) dos Estados Unidos, chega a Hong Kong. Primeiro de junho, os jornalistas do jornal *The Guardian* Glenn Greenwald e Ewen MacAskill, juntamente com a produtora e diretora de filmes e documentários Laura Poitras voam de Nova York até Hong Kong para encontrá-lo. No dia 5 de junho o jornal *The Guardian* anuncia o vazamento de documentos classificados da NSA, revelando que a empresa Verizon havia fornecido ao governo dos Estados Unidos milhões de metadados telefônicos sobre os cidadãos americanos. Em 6 de junho o programa secreto estadunidense de monitoramento global denominado PRISM é revelado. Oito de junho, a ferramenta Boundless Informant, que grava e analisa de onde todos os dados captados pela NSA vêm, é apresentada. Nove de junho de 2013: o mundo, então, conhece Edward Snowden, que, por meio de uma entrevista em vídeo, se apresenta como o responsável pelo vazamento de todas as informações confidenciais da NSA (GIDDA, 2013).

Essas revelações se inserem no nosso tema de pesquisa, que abrange contexto nacional e internacional, está ligado a situações vivenciadas por países de todo o mundo, relacionadas à defesa nacional e tecnologia, e diretamente associado ao debate recente sobre o uso cada vez mais ofensivo do ciberespaço pelos governos e pela sociedade para criar vantagens e influenciar eventos em todo o mundo (KUEHL, 2009; STARR, 2009; RATTRAY, 2009; HEALEY, 2013; CAVELTY, 2012; SHELDON, 2012; REVERON, 2012).

Embora tenha trazido benefícios incalculáveis para a humanidade e não obstante tenha proporcionado uma unificação e digitalização cada vez mais intensa das plataformas de informação e comunicação que a ele encontram-se interligadas, o ciberespaço também é palco de fortes ameaças (GUIMARÃES JR., 1999; CEPIK; CANABARRO; BORNE, 2014; REVERON, 2012).

Apesar das vulnerabilidades serem universais, as nações tecnologicamente desenvolvidas, cuja dependência é maior em relação ao que o ciberespaço pode lhes oferecer, têm se visto cada vez mais vulneráveis neste ambiente. Além disso, acredita-se que a própria natureza difusa das ameaças, que variam de ataques *hacker* efetuados por adolescentes até o uso da internet para fins terroristas, espionagem corporativa e governamental, passando pelo roubo de identidade por cibercriminosos, ações de subversão na rede, sabotagem industrial, dentre outros (ANDRESS; WINTERFELD, 2011; CANABARRO; BORNE, 2013b), tenha contribuído para uma intensificação do senso de vulnerabilidade frente a essas ameaças,

fazendo com que os governos de vários países passassem a buscar, cada vez mais, mecanismos para defender seus interesses e intensificar sua proteção através da realização de inúmeras mudanças em seu aparato governamental, mais especificamente, aquelas voltadas para as Forças Armadas (HANSEN; NISSENBAUM, 2009; CANABARRO; BORNE, 2013b; HEALEY, 2013).

Dentre os Estados com um alto nível de desenvolvimento tecnológico, os Estados Unidos, alvo de vários dos grandes ciberconflitos da atualidade, têm se destacado internacionalmente na reunião de esforços para a criação de instrumentos capazes não só de defender o país contra as ameaças da atualidade, mas garantir o uso das capacidades totais que o ciberespaço pode lhes oferecer para fazer prevalecer seus interesses nacionais diante, ou não, da ocorrência de uma guerra (HEALEY, 2013).

Tendo em vista a participação peculiar dos Estados Unidos nesse contexto e no intuito de apresentar e ampliar um pouco mais o debate que gira em torno desse tema, insere-se o seguinte problema de pesquisa, objeto de nosso estudo: quais são as doutrinas, estratégias e operações de ciberguerra estadunidenses?

A pesquisa tem por objetivo geral investigar quais são as doutrinas, estratégias e operações de ciberguerra estadunidenses e trazer breves reflexões sobre as mesmas. Além desse objetivo geral, o estudo tem por objetivo específico sistematizar alguns conceitos relacionados aos ciberconflitos da atualidade que se encontram um pouco confusos dentro da literatura a eles direcionada, bem como apresentar as principais mudanças institucionais relacionadas à ciberguerra ocorridas no aparato governamental estadunidense, com a finalidade não só de aprofundar o debate ciber, mas também de trazer reflexões para os estudos de política externa, política internacional, relações internacionais, defesa, segurança e estudos estratégicos relacionados aos conflitos internacionais da atualidade.

Para alcançar os objetivos aqui traçados, primeiramente, tenta-se retomar o processo histórico em que alguns dos conceitos relacionados aos ciberconflitos da atualidade foram criados, mostrando a evolução do debate ciber. Logo em seguida, no intuito de aprofundar o debate, apresentam-se as doutrinas, estratégias e operações de ciberguerra estadunidenses, recuperando um pouco o processo histórico em que surgiram, mostrando seu conteúdo e acompanhando a sua evolução até os dias de hoje. Por fim, adentrando mais no debate, apresentam-se as principais mudanças institucionais no aparato governamental estadunidense relacionadas à ciberguerra, a partir da perspectiva da história dos ciberconflitos da atualidade.

2 CIBERGUERRA E CONCEITOS ASSOCIADOS: O PARADIGMA INFORMACIONAL E A GUERRA NO SÉCULO XXI

Na melhor das hipóteses, as guerras poderão ser ganhas ao se atingir o coração estratégico de uma ciberestrutura do inimigo – seus sistemas de conhecimento, informação e comunicações.¹ (ARQUILLA; RONFELDT, 1997, p. 45, tradução nossa).

Muitos estudos têm sido desenvolvidos acerca das ameaças no ciberespaço da atualidade (KRAMER; STARR; WENTZ; 2009; CLARKE; KNAKE, 2010; ANDRESS; WINTERFELD, 2011; BETZ; STEVENS, 2011; REVERON, 2012; HEALEY, 2013). Contudo, percebe-se que ainda existe certa nebulosidade em relação aos conceitos que permeiam a literatura direcionada a esses estudos (KUEHL, 2009; BETZ; STEVENS, 2011, 2013; CANABARRO; BORNE, 2013a,b; RID, 2012, 2013). O principal objetivo deste capítulo é tentar trazer breves esclarecimentos sobre alguns dos conceitos que giram em torno dos ciberconflitos² (*cyber conflicts*) atuais, como os conceitos de ciber, cibernética, ciberespaço, cibersegurança, ciberguerra, guerra na rede, guerra de informações, operações de informação, guerra centrada em rede, ciberterrorismo, hacktivismo, cibercrimes, internet, web, sabotagem, espionagem, subversão e guerra baseada na internet, bem como apresentar, quando pertinente, sucintas reflexões sobre os mesmos. Para isso, tentaremos retomar o processo histórico em que alguns desses conceitos hoje utilizados foram criados e mostrar a evolução do debate ciber,³ que se originou nos anos 1990 e que permanece acirrado até os dias de hoje. Certamente este capítulo não tem o intuito de abordar todo o debate, mas apontar discussões que permitirão elucidar alguns conceitos. O esclarecimento desses conceitos contribuirá para o entendimento do contexto atual em que se insere o objeto de nosso estudo, a Ciberguerra (*Cyberwar*).⁴

¹ In the best circumstances, wars may be won by striking at the strategic heart of an opponent's cyber structures – his systems of knowledge, information, and communications.

² Ciberconflitos (*cyber conflicts*) são conflitos entre atores estatais ou grupos não estatais que, no uso de capacidades ciber ofensivas e defensivas atacam, se defendem ou espionam uns aos outros, geralmente para fins políticos ou de defesa nacional. Esses conflitos englobam as operações de ciberguerra e não abrangem cibercrimes que não envolvam objetivos políticos (HEALEY, 2013, p. 14-15).

³ Aqui preferimos utilizar o prefixo ciber como um substantivo autônomo (HEALEY, 2013), assim como o faremos várias vezes ao longo do texto, pois, como veremos mais adiante, o debate ciber envolve questões que vão além da cibernética ou do ciberespaço, envolvendo também questões relacionadas à cibersegurança.

⁴ Neste trabalho optamos por utilizar o termo “ciberguerra” para nos referirmos aos termos *cyberwar/cyber war*, *cyberwarfare/cyber warfare*, indistintamente, embora haja uma pequena diferença entre eles. A palavra *warfare* tem um significado um pouco mais abrangente que a palavra *war* e significa tudo o que engloba a vida militar de maneira geral, incluindo a preparação para a guerra, enquanto a palavra *war* diz respeito à guerra propriamente dita (SOUZA, 2013, p. 29). Nossa escolha se deu não apenas pelo fato de não termos encontrado no nosso vocabulário palavra que melhor traduzisse essas últimas (*cyberwarfare/cyber warfare*), mas também pelo fato de entendermos que, para a presente pesquisa, essa distinção não é relevante, já que

2.1 Debate inicial

Muitos dos conceitos que permeiam os estudos relacionados à ciberguerra, hoje, surgiram dentro de um contexto que muitos teóricos denominam de Era da Informação (CASTELLS, 1996). Também conhecida como Era Digital (RYAN, 2010), representa a era em que vivemos atualmente e se caracteriza, principalmente, pela reestruturação do capitalismo (flexibilização organizacional, diversificação das relações de trabalho e integração econômica global dos mercados financeiros, por exemplo); modernização, universalização e digitalização dos sistemas de comunicação (com redes de computadores interativas e uso de mídias sociais, por exemplo) e geração e acumulação do conhecimento como principal fonte de produção (CASTELLS, 1996, p. 1-28). Suas origens estão relacionadas, especialmente, com a “revolução tecnológica centrada em torno das tecnologias de informação”⁵ (CASTELLS, 1996, p. 1, tradução nossa) que se intensificou com o fim da Guerra Fria, a invenção dos microcomputadores e a expansão da internet nas décadas de 1960, 1970 e 1980 (RYAN, 2010). Em decorrência disso, os anos 1990 foram marcados por uma vasta produção intelectual voltada para a análise das influências da Revolução da Informação em todas as áreas das ciências (CASTELLS, 1996). Além dos conceitos de Cibernética (*Cybernetics*) (WIENER, 1970), Ciberespaço (*Cyberspace*) (GIBSON, 1984), Ciberguerra (*Cyberwar*) (ARQUILLA; RONFELDT, 1993), Guerra na Rede (*Netwar*) (ARQUILLA; RONFELDT, 1993), Guerra de Informações (*Information Warfare*) (LIBICKI, 1995a,b) e Operações de Informação (*Information Operations*) (SCHMITT, 1999), também permeou o debate inicial sobre a Revolução da Informação o conceito de Guerra Centrada em Rede (*Network Centric Warfare*) (CEBROWSKI; GARSTKA, 1998).

2.1.1 Ciber (*Cyber*), Cibernética (*Cybernetics*) e Ciberespaço (*Cyberspace*)

Originalmente, o prefixo “ciber” (*cyber*) surgiu como uma redução da palavra “cibernética” (*cybernetics*), cujo conceito foi introduzido por um cientista estadunidense

nosso objetivo é tentar abordar as principais questões que envolvem a ciberguerra de forma geral, estejam elas relacionadas com a sua preparação, condução, impacto etc. No que se refere ao uso do termo “ciberguerra”, bem como de outros como “ciberespaço”, “ciberconflitos”, “ciberterrorismo”, “cibercrimes” e “armas ciber”, por exemplo, em detrimento dos termos utilizados na língua portuguesa como “guerra cibernética”, “espaço cibernético”, “conflitos cibernéticos”, “terrorismo cibernético”, “crimes cibernéticos” e “armas cibernéticas” (CARNEIRO, 2012), a escolha se dá pelo fato de que, como já mencionamos, o prefixo ciber está deixando de ser um adjetivo para a palavra “cibernética” e, aos poucos, tem sido usado como um substantivo autônomo, indicando “qualquer coisa que tenha a ver com o ciberespaço ou, mais especificamente, com a *cibersegurança*”. (HEALEY, 2013, p. 280, tradução nossa, destaque do autor).

⁵ technological revolution, centered around information technologies

chamado Norbert Wiener em 1948 no seu livro “Cibernética; ou controle e comunicação no animal e na máquina” (no original, *Cybernetics; or the Control and Communication in the Animal and the Machine*) (ARQUILLA; RONFELDT, 1997, p. 57). Logo em seguida, o termo ciber passou a ser utilizado como um adjetivo para cunhar termos, expressões e palavras cujos significados estariam relacionados à informação ou à teoria cibernética (HEALEY, 2013, p. 280).

Wiener (1970, p. 36) e um grupo de cientistas⁶ que pesquisavam sobre a informação, a importância da sua quantidade, seu comando e transmissão perceberam uma “falta de unidade da literatura relativa a esses domínios” e também uma “ausência de qualquer terminologia comum, ou mesmo de um nome único para o campo”. Assim, para preencher essa lacuna, decidiram “designar o campo inteiro da teoria de comunicação e controle, seja na máquina ou no animal, com o nome de Cibernética” (WIENER, 1970, p. 36).

A palavra “cibernética” (*cybernetics*) tem sua origem nos prefixos das palavras gregas *kybernan*, que significa dirigir ou governar e *kybernetes*, que significa “piloto”, “governador”, ou “timoneiro”. Também está relacionada com o termo *cybernetique*, palavra francesa que significa “a arte de governar” (ARQUILLA; RONFELDT, 1997, p. 57). De acordo com Wiener (1970, p. 36-37), a escolha do termo quis, ao mesmo tempo, reconhecer o primeiro trabalho significativo sobre mecanismos de realimentação, um artigo sobre reguladores, publicado por Clerk Maxwell em 1868 e, também, referir-se “ao fato de que os engenhos de pilotagem de um navio são na verdade uma das primeiras e mais desenvolvidas formas de mecanismos de realimentação.” (WIENER, 1970, p. 37).

Sobre esse conceito, esclarece Wiener (1962 apud SAMPAIO, 2001, p. 2):

A cibernética não se ocupa primordialmente nem de organismos nem de produtos técnicos, mas sim daquilo que é comum a ambos, ou seja, a cibernética se centraliza não na eletrotécnica, mas no conceito mais fundamental de informação, quer ela seja transmitida por meios elétricos, mecânicos ou nervosos. (WIENER, 1962 apud SAMPAIO, 2001, p. 2. Destaque do autor).

O termo “ciberespaço” (*cyberspace*) (GIBSON, 1984, p. 12), por sua vez, não surgiu como um termo técnico, científico ou acadêmico (RYAN, 2010, p. 60), mas sim da obra de ficção científica “Neuromante” (*Neuromancer*), de William Gibson (1984), e designava, no seu livro “um ambiente de computador fictício em que se podia navegar ‘Uma representação

⁶ Para saber mais sobre esses pesquisadores e seus trabalhos em torno da criação da Teoria Cibernética veja a introdução do livro de Wiener (1970), versão brasileira traduzida da edição original de 1948, principalmente as páginas 35 a 53.

gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano”⁷ (GIBSON, 1984, p. 67, tradução nossa), um tipo de internet tangível”⁸ (RYAN, 2010, p. 60, tradução nossa), o universo das redes digitais, um espaço de dados que tornava “sensível a geografia móvel da informação, normalmente invisível” (LÉVY, 1999, p. 92).

2.1.2 Ciberguerra (Cyberwar) e Guerra na Rede (Netwar) segundo Arquilla e Ronfeldt

No campo dos Estudos de Segurança, Defesa e Estratégicos, o advento da Revolução da Informação impulsionou o debate sobre as questões de segurança nacional⁹ relacionadas à cibernética e ao ciberespaço que, apesar de não serem novas, começaram a receber, de forma mais concisa, uma maior atenção dos governos (WARNER, 2012, p. 781). Foi dentro desse contexto da Revolução da Informação que o conceito de “ciberguerra” (*cyberwar*) surgiu. O artigo intitulado *Cyberwar is Coming!* (“A Ciberguerra está vindo!”, em tradução livre), escrito em 1993 por John Arquilla e David Ronfeldt,¹⁰ foi o responsável por introduzir formalmente o prefixo ciber ao léxico dos Estudos de Segurança, Defesa e Estratégicos, criando o conceito de ciberguerra (CANABARRO; BORNE, 2013b, p. 2).

Arquilla e Ronfeldt (1997, p. 57-58), assim como outros visionários e tecnólogos da época, estavam em busca de termos que melhor se adequassem aos novos conceitos relacionados à Revolução da Informação. Assim, entenderam que a utilização do prefixo ciber na criação do conceito de ciberguerra era mais apropriada que a utilização de outros termos como Guerra de Informações (*Information Warfare*), uma vez que, para eles, o prefixo conectava melhor o campo da informação com o campo da governança (ARQUILLA; RONFELDT, 1997, p. 57-58): “A ciberguerra se refere à condução e à preparação para

⁷ A graphic representation of data abstracted from the banks of every computer in the human system.

⁸ a fictional computer environment in which one could navigate ‘a graphic representation of data abstracted from the banks of every computer in the human system’, a sort of tangible Internet.

⁹ Para essa pesquisa, segurança nacional é a prerrogativa do Estado de manter a sua sobrevivência perante os outros Estados através da proteção de seu território, sua população e seus interesses nacionais por meio do uso de todos os seus instrumentos de poder (políticos, diplomáticos, econômicos, militares e informacionais) (PALERI, 2008, p. 24-25; KUEHL, 2009, p. 38; STARR, 2009, p. 48; RATTRAY, 2009, p. 255).

¹⁰ O texto *Cyberwar is Coming!*, de John Arquilla e David Ronfeldt foi escrito em 1993 e publicado primeiramente pela editora Taylor & Francis, Inc. em seu periódico *Comparative Strategy*. Em 1997, entretanto, foi republicado pela Rand Corporation no livro *In Athena's Camp: Preparing for Conflict in the Information Age* (em tradução livre, “No campo de Atenas: preparando-se para o conflito na Era da Informação”), uma publicação editada por Arquilla e Ronfeldt que reuniu obras de vários autores acerca dos pensamentos sobre os conflitos que permeavam o início da Era da Informação. Curiosamente, o título do livro se referia ao fato de que, agora, os conflitos do futuro deveriam ter como patrona Atena, a deusa da sabedoria, e não Marte, uma vez que essa última representava o antigo modo de se fazer a guerra, através da força bruta. Disponível em: <http://www.rand.org/pubs/monograph_reports/MR880.html>. Acesso em: 02 out. 2013.

condução de operações militares, conforme os princípios relacionados com a informação.”¹¹ (ARQUILLA; RONFELDT, 1997, p. 30, tradução nossa).

Para Arquilla e Ronfeldt (1997, p. 30-32), a ciberguerra seria a “guerra do futuro”, a “guerra do século XXI”, e consistia em um complexo de mudanças expressivas na forma de se fazer a guerra¹² (ARQUILLA; RONFELDT, 1997, p. 24). **Essas mudanças baseavam-se não apenas no desenvolvimento tecnológico, mas na utilização de princípios relacionados ao controle da informação na preparação e condução da guerra através da implementação de significativas mudanças organizacionais, doutrinárias, estratégicas e operacionais dentro do setor militar.**

De fato, Arquilla e Ronfeldt (1997, p. 24-25) não descartavam a ideia de que, ao longo da história, avanços tecnológicos teriam continuamente servido de base para profundas mudanças na doutrina, organização e estratégia militares. Muitos desses avanços, inclusive, faziam parte do que se entendia na época por Revolução Militar Tecnológica (*Military Technical Revolution*) ou Revolução nos Assuntos Militares (*Revolution in Military Affairs - RMA*),¹³ como é hoje conhecida.¹⁴ Entretanto, para esses autores, a própria história já havia demonstrado que, quando do surgimento de novas tecnologias, as pessoas tendiam a enfatizar as melhorias em termos de eficiência e subestimar os potenciais efeitos sociais sistêmicos que essas novas tecnologias poderiam causar (SPROULL; KIESLER, 1991, p. 15-16 apud ARQUILLA; RONFELDT 1997, p. 26). Na visão de Arquilla e Ronfeldt (1997, p. 25), o que estava em pauta nesse momento era maior do que simples avanços,¹⁵ constituindo a Revolução da Informação como o grande salto tecnológico que modificaria a natureza dos conflitos e da guerra. Para eles, naquela época, a informação estava se mostrando ser um

¹¹ Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.

¹² “Num sentido mais profundo, ciberguerra significa uma transformação na natureza da guerra.” (ARQUILLA; RONFELDT, 1997, p. 31, tradução nossa).

¹³ Acredita-se que as ideias advindas da Revolução nos Assuntos Militares estão no cerne do conceito original de ciberguerra (CANABARRO; BORNE, 2013b, p. 3).

¹⁴ As origens da Revolução nos Assuntos Militares (*Revolution in Military Affairs*) remontam das décadas de 1970 e 1980 na antiga União Soviética (FITZGERALD, 1987, p. i) e, segundo Chapman (2003, p. 2), o general soviético Nikolai Vasilyevich Ogarkov foi um dos seus principais teóricos, que a denominou, inicialmente, de Revolução Militar Tecnológica (*Military Technical Revolution*). Seu núcleo reside na “reflexão sobre o papel das tecnologias digitais para as Forças Armadas e as reformas institucionais e organizacionais relacionadas, que devem advir para melhor atender essa tendência.” (RUMSFELD, 2002 apud CANABARRO; BORNE, 2013b, p. 3, tradução nossa).

¹⁵ “a ciberguerra não é simplesmente um conjunto de medidas baseadas na tecnologia. E não deve ser confundida com os significados passados de guerra computadorizada, automatizada, robotizada, ou eletrônica.” (ARQUILLA; RONFELDT, 1997, p. 30, tradução nossa).

recurso estratégico¹⁶ tão valioso e influente na Era Digital quanto o capital e o trabalho o foram na Era Industrial (ARQUILLA; RONFELDT, 1997, p. 25).

Dentre as mudanças sugeridas por Arquilla e Ronfeldt (1997) para a “guerra do futuro” podemos destacar a centralização estratégica e a descentralização hierárquica dos sistemas de comando e controle militares no nível tático, a fim de aperfeiçoar a visão estratégica informacional (*top sight*) no campo de batalha (ARQUILLA; RONFELDT, 1997, p. 23, 45), a superioridade informacional no campo de batalha, não só em termos táticos, mas também em termos doutrinários e organizacionais (ARQUILLA; RONFELDT, 1997, p. 23), uma relativa redução da força militar (exércitos menores) (ARQUILLA; RONFELDT, 1997, p. 24, 46), uma maior flexibilidade hierárquica organizacional (ARQUILLA; RONFELDT, 1997, p. 27) e a realização de operações militares de maneira mais conjunta pelas Forças Armadas (ARQUILLA; RONFELDT, 1997, p. 46).

Arquilla e Ronfeldt (1997, p. 44-45) também acreditavam, embora não estivessem ainda certos disto, que a vitória poderia ser alcançada sem que houvesse a necessidade de destruir uma força em oposição.

De acordo com Canabarro e Borne (2013b, p. 4), a perspectiva visionária de Arquilla e Ronfeldt (1997, p. 30) também foi influenciada pelas ideias e estudos desenvolvidos por Manuel Castells nos anos 1990, mais precisamente as que foram solidificadas em sua obra “A sociedade em rede” (*The Rise of the Network Society*) (1996), primeiro volume de sua trilogia “A Era da Informação: economia, sociedade e cultura” (*The Information Age: Economy, Society and Culture*).¹⁷ A teoria de Castells (CASTELLS, 1996, p. 5) parte do pressuposto de que “a tecnologia não determina a sociedade: ela a incorpora. Mas a sociedade também não determina os avanços tecnológicos: ela os utiliza”¹⁸ (CANABARRO; BORNE, 2013b, p. 4, tradução nossa). “Isso significa que ‘a capacidade de utilizar tecnologias avançadas de informação e comunicação¹⁹ [...] requer uma reorganização de toda a sociedade’ para lidar com o caráter descentralizado das redes que dão forma às sociedades em uma ‘Era da

¹⁶ “No sentido de Clausewitz, caracteriza-se pelo esforço de transformar conhecimento em capacidade.” (ARQUILLA; RONFELDT, 1997, p. 31, tradução nossa).

¹⁷ A trilogia de Manuel Castells consiste nas obras “A sociedade em rede” (*The Rise of the Network Society*) (1996), “O poder da identidade” (*The Power of Identity*) (1997) e “Fim do Milênio” (*End of Millennium*) (1998).

¹⁸ technology does not determine society: it embodies it. But neither does society determine technological innovation: it uses it.

¹⁹ Arquilla e Ronfeldt (1997, p. 32) defendiam a ideia de que, embora fossem necessárias tecnologias avançadas para que a ciberguerra fosse implementada, ela não dependia de tais tecnologias para acontecer, já que as dimensões organizacionais e psicológicas eram tão importantes quanto a técnica.

Informação”²⁰ (CASTELLS, 1999, p. 3 apud CANABARRO; BORNE, 2013b, p. 4, tradução nossa).

Em suma, o conceito original de ciberguerra pressupunha uma mudança no modo de se fazer a guerra. Para isso, seria necessária uma reorganização militar a fim de que se pudesse fazer uma real utilização das capacidades tecnológicas evolutivas que a Revolução da Informação estava trazendo.

Juntamente com o conceito de ciberguerra, no texto *Cyberwar is Coming!*, aqui mencionado, Arquilla e Ronfeldt também criaram o conceito de Guerra na Rede (*Netwar*) (CANABARRO; BORNE, 2013b, p. 3). A Guerra na Rede partia do pressuposto de que a Revolução da Informação estava trazendo mudanças de caráter global, afetando não só a forma como as Forças Armadas das nações faziam a guerra, mas também na própria forma com que as sociedades entravam em conflito, fossem eles de caráter militar ou não (ARQUILLA; RONFELDT, 1997, p. 27).

De acordo com Arquilla e Ronfeldt (1997), a Guerra na Rede não era uma guerra real, no sentido tradicional da palavra (ARQUILLA; RONFELDT, 1997, p. 30), mas tinha por objetivo tentar “interromper, danificar ou modificar o que uma população-alvo sabe ou pensa que sabe sobre si mesma e o mundo ao seu redor.”²¹ (ARQUILLA; RONFELDT, 1997, p. 28, tradução nossa). Para alcançar seus objetivos, os atores poderiam se valer de “medidas diplomáticas públicas, propaganda e campanhas psicológicas, subversão política e cultural, dissimulação (*deception*) ou interferência com a mídia local, infiltração em redes de computadores e bancos de dados”²², dentre outros (ARQUILLA; RONFELDT, 1997, p. 28, tradução nossa). Envolveria atores estatais e não estatais²³, englobaria conflitos das mais variadas dimensões, fossem eles políticos, econômicos, sociais ou militares. Seriam, a princípio, conflitos não violentos ou de baixa intensidade violenta, podendo evoluir para o

²⁰ It means that the “ability to use advanced information and communication technologies [...] requires an entire reorganization of society” to cope with the decentralized character of networks that give shape to societies in an “information age”

²¹ disrupt, damage, or modify what a target population “knows” or thinks it knows about itself and the world around it.

²² public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks.

²³ Quanto aos atores não estatais, Arquilla e Ronfeldt (1997, p. 28-29, 40, 49) se referiam a grupos ou organizações envolvidas com terrorismo, proliferação de armas de destruição em massa ou tráfico de drogas, bem como grupos ativistas engajados em movimentos religiosos, étnicos ou a favor do meio ambiente ou dos direitos humanos, por exemplo, que tivessem, ou não, ligações com países específicos, ou que fizessem parte, ou não de redes ou coligações transnacionais. De acordo com os autores, a estrutura-base de ação desses grupos ou organizações era descentralizada e não hierarquizada como nas instituições que as combatiam (forças armadas ou policiais) e que talvez fossem necessárias mudanças organizacionais de caráter descentralizado nessas instituições para que se pudesse combatê-los de forma mais efetiva.

nível de ciberguerra quando envolvessem alvos e assuntos militares,²⁴ podendo, também, ocorrer paralelamente à guerra convencional, como uma forma de evitá-la ou, também, de dar suporte à mesma (ARQUILLA; RONFELDT, 1997, p. 28-30).²⁵

Fica claro, portanto, que, para Arquilla e Ronfeldt (1997), num primeiro momento, a ciberguerra (*cyberwar*) se referia especificamente às mudanças no setor militar, enquanto a Guerra na Rede (*netwar*) estava voltada para as mudanças na sociedade direcionadas aos conflitos de forma geral (CANABARRO; BORNE, 2013b, p. 4). Ambas, entretanto, tinham algo em comum: giravam em torno da informação e da comunicação e eram “formas de guerra sobre o ‘conhecimento’ – sobre quem sabe o quê, quando, onde e por que, e sobre quão segura uma sociedade ou suas Forças Armadas estão em relação ao seu conhecimento de si mesmas e de seus adversários.”²⁶ (ARQUILLA; RONFELDT, 1997, p. 27).

2.1.3 Guerra de Informações (*Information Warfare*) e Operações de Informação (*Information Operations*) segundo Libicki e Schmitt

Libicki (1995ab), assim como outros pesquisadores da época (MOLANDER; RIDDILE; WILSON, 1996) diferentemente de Arquilla e Ronfeldt (1993), mas também influenciados sob o mesmo debate dos anos 1990 acerca dos efeitos da Revolução da Informação na guerra, optaram por utilizar o termo Guerra de Informações (*Information Warfare*) para tratar das mudanças relativas à Revolução da Informação. Embora o conceito não fosse novo, assim como afirmou Libicki (1995b, p. ix, tradução nossa), ele estava “enraizado no fato indiscutível de que as informações e as tecnologias de informação [estavam se tornando] cada vez mais importantes para a segurança nacional em geral, e, especificamente, para a guerra”.²⁷

Libicki (1995a, p. 1, tradução nossa) apresentou, em um Fórum promovido pela Universidade de Defesa Nacional (*National Defense University* – NDU), em março de 1995, taxonomias e definições alternativas para a “guerra do século XXI”, tendo designado **a Ciberguerra como um “combate no mundo virtual”²⁸, um aspecto “novo” da Guerra de**

²⁴ Arquilla e Ronfeldt (1997, p. 29, tradução nossa) se referem à proliferação nuclear, ao contrabando de drogas e às ações terroristas, por representarem potenciais ameaças à “ordem internacional e aos interesses de segurança nacional.”

²⁵ O conceito de Guerra na Rede (*Netwar*) sugerido por Arquilla e Ronfeldt (1997) se aproxima do conceito de ciberconflitos (*cyber conflicts*) utilizado por Healey (2013, p. 13-14).

²⁶ forms of war about “knowledge” — about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries.

²⁷ rooted in the indisputable fact that information and information technologies are increasingly important to national security in general and to warfare specifically.

²⁸ combat in the virtual realm

Informações (*Information Warfare – IW*). Essa definição de ciberguerra difere totalmente da apresentada por Arquilla e Ronfeldt (1993). Assim como explicou Libicki (1995b, p. 7), Arquilla e Ronfeldt viam a ciberguerra como uma guerra de comando e controle que amplamente incluía operações psicológicas contra o adversário. Libicki (1995b, p. 75) ao contrário, via a ciberguerra como uma simples categoria da Guerra de Informações.

Conforme Libicki (1995b, p. x, tradução nossa), a Guerra de Informações envolvia “a proteção, a manipulação, a degradação e a negação de informações”²⁹ e englobava (1) Guerra de Comando e Controle (*Command-and-Control Warfare – C2W*); (2) Guerra Baseada na Inteligência (*Intelligence-based Warfare – IBW*); (3) Guerra Eletrônica (*Electronic Warfare – EW*); (4) Guerra Psicológica (*Psychological Warfare – PSYW*); (5) Guerra Hacker (*Hacker Warfare*); (6) Guerra de Informação Econômica (*Economic Information Warfare – EIW*) e (7) Ciberguerra (*Cyberwar*) (LIBICKI, 1995b, p. x).

No texto de Libicki (1995b), Guerra de Comando e Controle (C2W) significava uma estratégia militar que tinha por objetivo destruir o inimigo a partir de suas forças de comando (LIBICKI, 1995b, p. 9); Guerra Baseada na Inteligência (IBW) ocorria quando a inteligência³⁰ era alimentada diretamente pelas operações militares, ao invés de ser usada apenas como uma ferramenta de apoio à Guerra de Comando e Controle (LIBICKI, 1995b, p. 19); Guerra Eletrônica (EW) tinha por objetivo afetar as comunicações do inimigo e englobava técnicas operacionais de radioeletrônica e criptografia (LIBICKI, 1995b, p. 27); Guerra Psicológica

²⁹ the protection, manipulation, degradation, and denial of information

³⁰ O termo inteligência pode ser entendido a partir de três concepções: como conhecimento, como organização e como atividade (KENT, 1967, p. 9 apud MACHADO, 2010, p. 14): “a) Inteligência como conhecimento produzido: consiste no conhecimento (seja ele descritivo, narrativo ou especulativo-avaliativo) resultante da atividade desempenhada por organizações especializadas, que sirva de base para que ‘idealizadores, planejadores e executores’ (‘utilizadores primordiais do produto final das informações’), em seus mais variados níveis funcionais, possam tomar decisões mais completas, precisas e oportunas e, assim, garantir o bem-estar e a segurança do Estado (KENT, 1967, p. 17-23 apud MACHADO, 2010, p. 15). b) Inteligência como organização: consiste em uma organização composta por um ‘pessoal ativo que busca uma categoria especial de conhecimentos’ (indisponíveis ou negados), devendo tal pessoal ser conhecedor das necessidades da organização (devem ‘saber o que se deseja, o que tem e o que não tem importância’) e possuir capacidades profissionais suficientes para produzir esses conhecimentos e salvaguardá-los. Tais instituições devem dispor de instalações adequadas à produção e armazenamento dos conhecimentos já produzidos e devem possuir uma estrutura funcional sólida e ao mesmo tempo flexível, para evitar o sobrecarregamento, no caso do surgimento de imprevisibilidades (KENT, 1967, p. 77-84 apud MACHADO, 2010, p. 15). c) Inteligência como atividade ou processo: é a atividade ou o processo de pesquisa que a organização desempenha para produzir certos tipos de conhecimentos. Esse processo, que possui metodologia própria, pode iniciar-se com uma requisição ou com uma sugestão de pesquisa dos interessados, consistindo-se em procedimentos para a coleta ou busca de dados, a fim de que sejam analisados e apresentados em forma de hipóteses prováveis aos tomadores de decisão (KENT, 1967, 147-153 apud MACHADO, 2010, p. 15).” “São exemplos de conhecimentos descritivos e narrativos: informes sobre ‘terreno, hidrografia e clima’ (imutáveis) e população (relativamente mutáveis). São exemplos de conhecimentos especulativo-avaliativos: informes relacionados ‘com o futuro, suas possibilidades e probabilidades’” (KENT, 1967, p. 20-21 apud MACHADO, 2010, p. 14).

(PSYW) tinha por objetivo utilizar a informação como forma de controlar a mente do inimigo (LIBICKI, 1995b, p. 35); Guerra *Hacker* tinha como alvo as redes de computadores civis do adversário, que também deveriam ser protegidas (LIBICKI, 1995b, p. 50-51); Guerra de Informação Econômica (EIW) representava tanto o bloqueio da informação quanto o monopólio da informação, com o objetivo de desestabilizar uma nação através da sua economia (LIBICKI, 1995b, p. 68); Ciberguerra englobava terrorismo informacional, ataques semânticos, simulação de guerra e a guerra Gibson (LIBICKI, 1995b, p. 75).

O terrorismo informacional tinha por objetivo explorar sistemas de computador para atacar indivíduos (LIBICKI, 1995b, p. 76). Ataques semânticos consistiam na realização de atividades para manipular os sistemas do adversário ao invés de torná-los inoperativos, a fim de conduzi-los para tomadas de decisões desfavoráveis (LIBICKI, 1995b, p.77). Simulações de guerra consistiam em modelar o campo de batalha através do computador (LIBICKI, 1995b, p. 80-81). A guerra Gibson seria aquela que ocorreria no mundo virtual, uma guerra fictícia, assim como descreveu Gibson em seu livro *Neuromancer* (LIBICKI, 1995b, p. 81).

Apesar de sugerir essa taxonomia para a ciberguerra, Libicki (1995b, p. 75) acreditava que ela fosse algo intangível, uma vez que a infraestrutura global de informação existente teria que passar por uma grande evolução para que tais atividades pudessem vir a acontecer.

A Guerra de Informações, segundo Healey (2013, p. 18), passou a constar na doutrina militar no final da década de 1990 como parte de um conjunto mais amplo de atividades denominado Operações de Informação (*Information Operations*) (SCHMITT, 1999, p. 7). De acordo com Schmitt (1999, p. 7), a Guerra de Informações passou a ser compreendida como “operações de informação conduzidas durante tempos de crise ou conflito com a intenção de afetar os resultados específicos contra um adversário em particular”³¹ (SCHMITT, 1999, p. 7, tradução nossa), e as Operações de Informação teriam um caráter mais abrangente, compreendendo não só as atividades realizadas dentro de um contexto específico de guerra ou crise, mas também todas aquelas que eram realizadas em tempos de paz (SCHMITT, 1999, p. 7). Sendo assim, **Operações de Informação seriam todas as ações tomadas para afetar as informações ou os sistemas de informação do adversário, bem como aquelas tomadas para defender suas próprias informações e sistemas de informação (SCHMITT, 1999, p. 7), em tempos de paz ou de guerra, possuindo um caráter tanto ofensivo quanto defensivo.**

³¹ information operations conducted during times of crisis or conflict intended to effect specific results against a particular opponent

Quanto ao seu caráter defensivo, as atividades incluíam Garantia da Informação (*Information Assurance – IA*), Segurança das Operações (*Operations Security – OPSEC*), Segurança Física (*Physical Security*), Ações Anti-dissimulação (*Counterdeception*), Ações Antipropaganda (*Counterpropaganda*), Contrainteligência (*Counterintelligence - CI*), Guerra Eletrônica (*Electronic Warfare – EW*) e Operações Especiais de Informação (*Special Information Operations – SIO*) (ESTADOS UNIDOS, 1998, p. I-10), que tinham por objetivo geral garantir acesso à informação oportuna, precisa e relevante e, ao mesmo tempo, negar aos inimigos a exploração de suas informações ou dos seus sistemas de informação (ESTADOS UNIDOS, 1998, p. I-10).

No que se refere ao seu caráter ofensivo, de acordo com Schmitt (1999, p. 7), as operações de informação incluíam uma variedade de atividades, sendo elas: Ataque a Redes de Computadores (*Computer Network Attack – CNA*), Dissimulação Militar (*Military Deception*), Operações Psicológicas (*Psychological Operations - PSYOPS*), Guerra Eletrônica (*Electronic Warfare – EW*), Ataque Físico (*Physical Attack*) e Operações Especiais de Informação (*Special Information Operations – SIO*) (SCHMITT, 1999, p. 7). Essas atividades tinham por objetivo geral auxiliar as operações de informação de caráter defensivo, enganar os adversários quanto às capacidades militares e missões, transmitir informações falsas à população de um país ou ao seu governo, influenciando o comportamento de ambos, e atacar – tanto as informações armazenadas, quanto os próprios computadores, seus sistemas e suas redes (ESTADOS UNIDOS, 1998, p. II-3-II7).

2.1.4 Guerra Centrada em Rede (Network Centric Warfare)

Reflexões geradas pela teoria da Revolução nos Assuntos Militares trouxeram à tona outro conceito que também nos ajuda a compreender algumas discussões acerca da ciberguerra hoje: o conceito de Guerra Centrada em Rede (*Network Centric Warfare – NCW*). Esse conceito apareceu pela primeira vez na literatura desclassificada num artigo escrito por Cebrowski e Garstka em 1998 (MITCHELL, 2006, p. 7). Entretanto, suas origens datam da Segunda Guerra Mundial, cujo ambiente operacional caracterizado pelo aparecimento de aeronaves modernas de combate exigiu uma maior coordenação entre as missões terrestres, navais e aéreas (MITCHELL, 2006, p. 28). Embora seja um conceito ainda em desenvolvimento, tem sido adotado pelas Forças Armadas de vários países no mundo, assim como os demais conceitos aqui citados (MITCHELL, 2006, p. 7).

A ideia da Guerra Centrada em Rede apoia-se no princípio da ubiquidade da informação (capacidade de estar, ao mesmo tempo, em vários lugares) e num modelo de interoperabilidade (capacidade dos sistemas de se comunicarem uns com os outros, proporcionando a troca de informações ou dados) (MITCHELL, 2006, p. 7-8). Baseia-se na maximização do poder através da distribuição da informação (MITCHELL, 2006, p. 31) e consiste no emprego de recursos de tecnologias da informação e comunicação (TIC) para conectar comandantes e combatentes de todos os níveis hierárquicos numa grande rede operativa, cujo propósito “é aumentar a velocidade de comando, ou seja, o ritmo do processo de tomada de decisões, bem como o grau de consciência situacional, que se concretiza pela apurada compilação e ampla compreensão do quadro tático do Teatro de Operações (TO)”³² (DIAS, 2006, p. 44). A transformação da informação em consciência compartilhada (*shared awareness*) faz com que as unidades combatentes interajam de maneira articulada, tanto fisicamente quanto virtualmente, através de uma rede de informações ou intranet (MOFFAT, 2003, p. 49).

Mitchell (2006, p. 8) acredita que, num plano estratégico global, a integração entre forças militares multinacionais no compartilhamento de informações pode afetar não só o ambiente operacional militar, mas, principalmente, o panorama estratégico da guerra, fazendo com que o uso político da força militar convencional se veja subordinado às alianças em rede estabelecidas entre os países (MITCHELL, 2006, p. 8).

2.2 Debate atual

Mais de duas décadas depois desse debate inicial, o que se verifica hoje é que, ao contrário do que muitos pensadores afirmaram nos anos 1990 (ARQUILLA; RONFELDT, 1993), a Revolução da Informação não fez com que a natureza da guerra se modificasse (BETZ; STEVENS, 2011, p. 96). De fato, as novas tecnologias têm trazido contribuições importantes para as capacidades militares até então existentes (ZIMET; BARRY, 2009, p. 299), mas muitas das mudanças organizacionais, estratégicas, doutrinárias e operacionais que foram sugeridas para a “guerra do futuro” nos anos 1990 ainda não ocorreram.

Alguns estudiosos (BETZ; STEVENS, 2011) sustentam que tais mudanças não vão acontecer, uma vez que são previsões de um debate enviesado e influenciado por uma

³² O compartilhamento de “informações entre combatentes e comandantes de todos os níveis hierárquicos, conectando fuzileiros, carros de combate, centros de comando, aeronaves e navios em uma única e grande rede” (DIAS, 2006, p. 44) pode proporcionar aos combatentes “um maior entendimento da situação” (DIAS, 2006, p. 46) em que se encontram durante a guerra, facilitando, assim, o planejamento e a tomada de decisões imediatas.

tendência cíclica de pensamento ligada à ideia do “novo”, que aparece sempre que avanços tecnológicos significativos acontecem, como ocorreu com o debate especulativo em torno do poder aéreo na guerra na década de 1920 (BETZ; STEVENS, 2011, p. 82-88).

De fato, a “tecnologia tem sempre impulsionado a guerra e tem sempre sido conduzida por ela”,³³ mas, “Por milênios, entretanto, ela foi incapaz de mudar a natureza da guerra ou o propósito a que ela servia.”³⁴ (CREVELD, 2007, tradução nossa). Até o momento, o uso do ciberespaço para atacar o “pessoal, instalações ou equipamentos com o objetivo de degradar, neutralizar ou destruir a capacidade combatente do inimigo”³⁵ (ALEXANDER, 2007, p. 60, tradução nossa) ainda não aconteceu. Atos de “Degradação de páginas do governo, ataques de negação de serviço e roubo de dados têm sido realizados na Internet, mas estes atos não constituem atos de guerra”³⁶ (REVERON, 2012, p. 13, tradução nossa).

Na realidade, acredita-se que “a ideia de utilizar capacidades ciber na guerra esteja aos poucos emergindo”³⁷ (REVERON, 2012, p. 3, tradução nossa) e que os governos estejam cada vez mais “buscando novas formas e meios para defender seus interesses no ciberespaço e desenvolver suas próprias capacidades ofensivas para nele competir”³⁸ (REVERON, 2012, p. 3, tradução nossa), mas “A questão não é de ciberguerra [uma guerra travada no ciberespaço], mas sim do uso de ciber *na* guerra”³⁹ (SHELDON, 2012, p. 208, tradução nossa, destaque do autor), ou seja, está relacionada ao uso da capacidade ciber na guerra.

2.2.1 Securitização do Ciberespaço e Relações Internacionais

Acredita-se que as teorizações acerca da ocorrência de uma guerra no ciberespaço aumentaram com o fenômeno da securitização e consequente redução da concepção da “ideia mais ampla de ciber-”⁴⁰ (CANABARRO; BORNE, 2013b, p. 5, tradução nossa) que permeou o debate inicial nos anos 1990. A ideia mais ampla de ciber, para Canabarro e Borne (2013b, p. 5, tradução nossa) residia nas “interações complexas de tecnologia e governança em rede

³³ technology has always driven war, and been driven by it

³⁴ For millennia, however, it was incapable of changing either the nature of war or the purpose that it served.

³⁵ personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability

³⁶ Defacement of government websites, denial-of-service attacks, and data stealing have been conducted over the Internet, but these do not constitute warfare.

³⁷ the concept of using cyber capabilities in war is slowly emerging.

³⁸ seek new ways and means to defend their interests in cyberspace and to develop their own offensive capabilities to compete in cyberspace.

³⁹ The issue, therefore, is not cyberwar, but cyber *in* war

⁴⁰ the broad idea of “cyber-”

no século XXI”.⁴¹ Essa ideia “tem se tornado cada vez mais subordinada à estreita concepção de ‘ciber-’ como algo relacionado ao ciberespaço apenas (e cada vez mais, à Internet).”⁴² (CANABARRO; BORNE, 2013b, p. 5, tradução nossa). Assim como afirmou Healey (2013, p. 280), o prefixo ciber tem se tornado “seu substantivo próprio autônomo, indicando qualquer coisa que tenha a ver com o ciberespaço ou, mais especificamente, com *cibersegurança*.”^{43,44} (HEALEY, 2013, p. 280, tradução nossa, destaque do autor).

Para Canabarro e Borne (2013b, p. 4-5), o estreitamento do conceito de ciber se deu não tanto em virtude da crescente importância que as agendas acadêmica e política de Estudos de Segurança, Defesa e Estratégicos têm dado aos aspectos tecnológicos e organizacionais sugeridos pelo debate inicial gerado pela Revolução da Informação (WEIMANN, 2004; ERIKSSON; GIACOMELLO, 2007; GILES, 2011; HSIAO, 2010; KRAMER; STARR, 2009 apud CANABARRO; BORNE, 2013b, p. 4-5), mas, principalmente em virtude de um processo paralelo de securitização do ciberespaço (NISSENBAUM, 2005; HANSEN; NISSENBAUM, 2009).

O conceito de securitização foi desenvolvido por Buzan, Weaver e Wilde (1998), da Escola de Copenhague, e é bastante utilizado nos Estudos de Segurança das Relações Internacionais para explicar aspectos imateriais de interpretação de ameaças (CEPIK; CANABARRO; BORNE, 2014, p. 2):

Segundo a teoria, quando determinado assunto é legitimamente percebido como ameaça existencial, justifica-se a adoção de medidas extraordinárias que extrapolam a ordem regular do processo de decisão política daquele país diante da urgência de medidas que garantam a segurança do objeto ameaçado (CEPIK; CANABARRO; BORNE, 2014, p. 2).

No que tange à ligação desse fenômeno com a Era Digital, Hansen e Nissenbaum (2009) “se propuseram a ampliar o ferramental teórico dos estudos de segurança da Escola de Copenhague, a partir da avaliação de eventos de securitização relacionados ao ciberespaço e à Internet, agregando assim o setor cibernético à análise” (CEPIK; CANABARRO; BORNE, 2014, p. 2).

⁴¹ complex interactions of technology and networked governance in the 21st century

⁴² has become subordinated to the narrow conception of “cyber-” as something merely related to cyberspace (and increasingly, to the Internet).

⁴³ “Cibersegurança: Também usada como sinônimo de duas palavras: segurança ciber. Geralmente significa todas as ações para proteger computadores e redes contra ataques à sua confidencialidade, integridade e disponibilidade. No entanto, à medida que os campos ‘ciber’ se expandem, a cibersegurança está mais associada com os aspectos mais técnicos de defesa. Alguém que sabe de cibersegurança, por exemplo, pode não ser um especialista em ciberconflitos e vice-versa.” (HEALEY, 2013, p. 281, tradução nossa).

⁴⁴ its own standalone noun to indicate anything having to do with cyberspace or, more specifically, *cybersecurity*.

É importante notar que, no campo das Relações Internacionais, esses estudos teóricos sobre a Era Digital e Segurança só começaram a ser desenvolvidos no final da primeira década dos anos 2000. Isso se deu, principalmente, com a intensificação do processo de securitização do ciberespaço, a partir de vários acontecimentos que marcaram o início do século, como os ataques DDoS à Estônia em 2007 e o ataque do vírus Stuxnet às usinas nucleares iranianas em 2010 (CANABARRO; BORNE, 2013b, p. 5).

De acordo com Eriksson e Giacomello (2007), organizadores de *International Relations and Security in the Digital Age* (em tradução livre, “Relações Internacionais e Segurança na Era Digital”) (2007), a obra teve por objetivo principal “contribuir para preencher a lacuna⁴⁵ existente entre as Teorias das Relações Internacionais e a prática da Segurança da Era Digital”⁴⁶ (ERIKSSON; GIACOMELLO, 2007, p. i, tradução nossa). O livro

abrange uma série de temas-chave, tais como: proteção da infraestrutura crítica, questões relacionadas à privacidade, cooperação internacional; ciberterrorismo e política de segurança. Ele tem como objetivo analisar o impacto da revolução da informação na segurança internacional e doméstica; examinar o que as teorias de relações internacionais existentes podem dizer sobre este desafio, e discutir como as teorias de relações internacionais podem ser desenvolvidas para melhor enfrentar esse desafio.

A análise sugere que o foco do liberalismo no pluralismo, na interdependência e na globalização, a ênfase do construtivismo na linguagem, símbolos e imagens (incluindo ‘virtualidade’), e alguns elementos dos estudos estratégicos realistas (sobre o tema específico de guerra de informação) contribuem para uma melhor compreensão da segurança da Era Digital.⁴⁷ (ERIKSSON; GIACOMELLO, 2007, p. i, tradução nossa).

Além desses temas, alguns estudos de Relações Internacionais e Política Internacional também têm abordado tópicos como o uso de *soft-power* na ciberguerra (NYE, 2013), o impacto da energia nuclear na construção de armas ciber (NYE, 2013), o uso de armas ciber como armas de destruição em massa (CARR, 2013), o uso de armas ciber em sistemas

⁴⁵ Acácio e Souza (2012) fizeram uma recente contribuição para esses estudos no 36º Encontro Anual da Anpocs (Associação Nacional de Pós-Graduação e Pesquisa em Ciências Sociais), apresentando discussões sobre quatro abordagens teóricas das Relações Internacionais, quais sejam, Realismo, Escola Inglesa, Neoliberalismo e Escola de Copenhague.

⁴⁶ contribute towards filling the gap between theories of international relations and the practice of digital-age security.

⁴⁷ covers a range of key topics, including: critical infrastructure protection; privacy issues; international cooperation; cyberterrorism; and security policy. It aims to analyse the impact of the information revolution on international and domestic security; examine what existing international relations theories can say about this challenge; and discuss how international relations theory can be developed to better meet this challenge. The analysis suggests that liberalism’s focus on pluralism, interdependence and globalization, constructivism’s emphasis on language, symbols and images (including ‘virtuality’), and some elements of realist strategic studies (on the specific topic of information warfare) contribute to a better understanding of digital-age security.

industriais (BRENNER, 2013) e a participação de atores não estatais na ciberguerra (NYE, 2012; CANABARRO; BORNE, 2013b).

Acredita-se que a natureza difusa das ameaças ciber em potencial (CAVELTY, 2012, p. 103), que variam desde a execução de ataques *hacker* efetuada por adolescentes, roubo de identidade por cibercriminosos, ações de subversão na rede, sabotagem industrial, uso da internet para fins terroristas, espionagem corporativa e governamental, dentre outros (ANDRESS; WINTERFELD, 2011, p. xix), tenha contribuído para uma intensificação do senso de vulnerabilidade governamental frente a essas ameaças, fazendo com que o ciberespaço passasse a incorrer em uma visível militarização (CAVELTY, 2012, p. 103). Entretanto, exceto no que a eles for comum, não se pode “tratar ativismo, atividades criminosas, terrorismo e atos de guerra de forma intercambiável”,⁴⁸ pois além de ser “algo que ignora a própria complexidade desses fenômenos”⁴⁹ (CANABARRO; BORNE, 2013b, p. 13-14, tradução nossa), “impõe graves ameaças às liberdades civis e aos direitos políticos dos indivíduos em todo o mundo, tanto em democracias quanto em regimes autoritários”⁵⁰, já que lança “diferentes categorias de atores sob o mesmo guarda-chuva”⁵¹ (CANABARRO; BORNE, 2013b, p. 14, tradução nossa). Por mais que os ciberconflitos inseridos dentro do conceito de cibersegurança sejam eventos relevantes para a segurança nacional, como o ciberterrorismo, o hacktivismo e os cibercrimes, não podemos classificá-los como atos de ciberguerra nem dar a eles igual tratamento, uma vez que as respostas políticas a eles endereçadas podem ter caráter distinto (CANABARRO; BORNE, 2013b, p. 13-14). Se vistos como atos de guerra, os ciberconflitos devem ser combatidos com o uso de métodos militares, se vistos como atividades criminosas, pressupõem o uso de técnicas policiais, por exemplo (SEDERBERG, 2003 apud LUTZ; LUTZ, 2007, p. 291). Sendo assim, antes de tudo, é preciso compreendê-los nos seus próprios termos.

2.2.1.1 Ciberterrorismo (*Cyber terror or Cyberterrorism*), Hacktivismo (*Hactivism*) e Cibercrime (*Cyber crime or Cybercrime*)

Ciberterrorismo (*Cyber terror or Cyberterrorism*) é a “convergência dos termos terrorismo e ciberespaço”⁵² (DENNING, 2000, tradução nossa). “É geralmente entendido

⁴⁸ treating activism, criminal activities, terrorism, and acts of war interchangeably

⁴⁹ something that ignores the complexity of those phenomena

⁵⁰ poses severe threats to the civil liberties and political rights of individuals all around the world, both in democratic and in autocratic regimes.

⁵¹ throwing different categories of actors under the same umbrella

⁵² the convergence of terrorism and cyberspace.

como ataques ilegais e ameaças de ataque contra computadores, redes e as informações neles armazenadas, quando feitos com o intuito de intimidar ou coagir um governo ou o seu povo em prol de objetivos políticos ou sociais.”⁵³ (DENNING, 2000, tradução nossa). Além disso, de acordo com Denning (2000), para se qualificar como ciberterrorismo, “um ataque deve resultar em violência contra pessoas ou bens, ou pelo menos causar dano suficiente para gerar medo.”⁵⁴ (DENNING, 2000, tradução nossa).

O termo ciberterrorismo tem sido frequentemente utilizado para se referir a ações que não têm caráter terrorista, como as ações hacktivistas. Esses fenômenos são bastante diferentes. Hacktivismismo (*Hacktivism*) é o termo utilizado por estudiosos para descrever a junção de *hacking* com o ativismo político (WEIMANN, 2004). De acordo com Weimann (2004),

enquanto o principal objetivo dos hacktivistas é protestar e perturbar politicamente um governo através do uso de bloqueios virtuais⁵⁵, bombardeios de *e-mail*, invasões de computadores e do uso de vírus e *worms*⁵⁶ para infectar redes computacionais, [por exemplo], o principal objetivo dos ciberterroristas é matar ou aterrorizar (WEIMANN, 2004, p. 5 apud MACHADO, 2011, p. 288).

Essa diferença pode, em algum momento, tornar-se um pouco confusa, “especialmente se grupos terroristas forem capazes de recrutar ou contratar hacktivistas especialistas em computadores ou se hacktivistas decidirem elevar suas ações, atacando sistemas que operam elementos críticos da infraestrutura nacional, tais como redes de energia elétrica e serviços de emergência”⁵⁷ (WEIMANN, 2004, p. 5, tradução nossa), mas ela existe.

O Cibercrime (*Cyber crime or cybercrime*) ou crime de informática, por sua vez, “é a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material. Ao primeiro

⁵³ It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

⁵⁴ an attack should result in violence against persons or property, or at least cause enough harm to generate fear.

⁵⁵ “Bloqueios virtuais, de acordo com o autor, são tentativas de gerar tráfego para o site que está sendo visitado de forma a impossibilitar que outros usuários o acessem, e assim, causar a interrupção das operações normais do site.” (WEIMANN, 2004, p. 4 apud MACHADO, 2011, p. 288).

⁵⁶ “Vírus são *malwares* (*softwares* maliciosos) criados com o objetivo de danificar arquivos armazenados no disco rígido (especialmente arquivos críticos para o funcionamento do sistema), tornando o sistema inoperante. *Worms* são como os vírus, mas têm a capacidade de se propagar para outros computadores. Normalmente, os *worms* geram um aumento considerável no tráfego de dados, prejudicando o acesso aos serviços de rede. Os *worms* costumam se propagar buscando vulnerabilidades em sistemas e em e-mails.” (BRASIL, 2006, p. 14 apud MACHADO, 2011, p. 288).

⁵⁷ especially if terrorist groups are able to recruit or hire computer-savvy hacktivists or if hacktivists decide to escalate their actions by attacking the systems that operate critical elements of the national infrastructure, such as electric power networks and emergency services.

chamaremos de crime de informática impróprio ou comum, ao segundo de próprio ou autêntico.” (ROQUE, 2000 apud CRISPIN, 2010, p. 12).

“O cibercrime é usualmente viabilizado e conduzido através de uma conexão com a internet, mas também pode envolver a remoção não autorizada de dados em dispositivos pequenos e portáteis de armazenamento (conhecidos como *flash drives* ou *pen drives*).”⁵⁸ (WILSON, 2009, p. 416, tradução nossa).

De acordo com o documento que resultou do acordo bilateral entre a Rússia e os Estados Unidos sobre terminologia em cibersegurança denominado *Critical Terminology Foundations* (“Fundamentos de Terminologia Crítica”, tradução livre), editado por Karl Frederick Rauscher e Valery Yaschenko e publicado em abril de 2011, cibercrime “é o uso do ciberespaço para propósitos criminais definidos por leis nacionais ou internacionais.”⁵⁹ (RAUSCHER; YASCHENKO, 2011, p. 27, tradução nossa).

2.2.2 Analogias, metáforas e inconsistência conceitual

A crescente dependência das nações em relação ao ciberespaço e a atmosfera de insegurança e tensão que desencadearam o processo de securitização do ciberespaço também têm contribuído para que, assim como explicam Canabarro e Borne (2013b), “Grande parte da produção intelectual sobre o assunto [careça] de um consenso em torno dos conceitos básicos, [avance] em analogias insatisfatórias e [crie] quadros analíticos sem consistência teórica, lógica e empírica.”⁶⁰ (CANABARRO; BORNE, 2013b, p. 5, tradução nossa). A inconsistência conceitual se verifica não apenas no meio acadêmico, mas, sobretudo, no uso indiscriminado de termos, conceitos e metáforas pela mídia, por órgãos governamentais e pela população em geral (CEPIK; CANABARRO; BORNE, 2014, p. 1). Dessa forma, “paradoxalmente, [o estreitamento do conceito de ciber tem implicado em] um alargamento dos desafios para os estudos e as práticas de Segurança na Era Digital”⁶¹ (CANABARRO; BORNE, 2013b, p. 5, tradução nossa).

Embora o uso de analogias e metáforas (espaciais, biológicas, com a ficção científica, com a Segunda Guerra Mundial, por exemplo), seja recorrente no campo da cibersegurança,

⁵⁸ Cyber crime is usually enabled and conducted through a connection to the Internet but can also involve unauthorized removal of data on small, portable storage devices (known as flash drives or thumb drives).

⁵⁹ is the use of cyberspace for criminal purposes as defined by national or international law.

⁶⁰ Much of the intellectual production in the field lacks consensus surrounding basic concepts, advances unsatisfactory analogies and creates analytical frameworks without theoretical, logical, and empirical consistency.

⁶¹ Paradoxically, this narrow conception implies an enlargement of the challenges for the study and the practices of security in the Digital Era.

sua utilização tem sido bastante questionada, principalmente devido ao caráter influente e catalisador que esses recursos possuem (BETZ; STEVENS, 2013, p. 148).

Para Brito e Watkins (2011, p. 38), comparar os ciberataques com os ataques à Pearl Harbor ou aos ataques de 11 de setembro é “inútil e perigoso”⁶² (BETZ; STEVENS, 2013, p. 148, tradução nossa), além de ser incongruente com o pensamento analítico intelectual (BETZ; STEVENS, 2013, p. 148-149; LIBICKI, 1997, p. 6). O mesmo verifica-se no uso de conceitos relacionados com a Guerra Fria ou ao holocausto nuclear (BETZ; STEVENS, 2013, p. 149; SHACHTMAN; SINGER, 2011). O repetido uso dessas analogias e metáforas pelos governos resulta mais em opacificação das faculdades críticas dos indivíduos do que em real mobilização de suporte para a causa (EDELMAN, 1964, p. 124-125 apud BETZ; STEVENS, 2013, p. 149).

Libicki (2012) também discute a utilidade da designação do ciberespaço como um novo domínio operacional para se fazer a guerra, juntamente com a terra, o mar, o ar e o espaço e acredita que o uso dessa designação deve ser cauteloso. Para ele, essa é uma “forma errônea de visualizar o ciberespaço, [pois] leva estrategistas e operadores a presunções ou conclusões que não derivam da observação e da experiência,”⁶³ mas sim de conotações (LIBICKI, 2012, p. 322, tradução nossa). Assim, imaginar o ciberespaço repleto de tropas de ciberguerreiros (*cyber warriors*) entrando em sistemas e redes para atacar seus adversários não passa de uma metáfora, já que “Na prática, grande parte do que os ciberguerreiros ofensivos fazem é reconhecimento ou exploração”⁶⁴ (LIBICKI, 2012, p. 330, tradução nossa). Além disso, a natureza dos domínios de combate difere totalmente da natureza do ciberespaço, não tanto pelo fato de ele ter sido criado pelo homem, mas principalmente por ser um meio maleável e múltiplo, passível de ser controlado por uma variedade de operadores, em sua grande parte, privados (LIBICKI, 2012, p. 324). Presumir que a defesa do ciberespaço pode ser feita assim como nos outros domínios é equivocado, já que os comandantes não possuem um total domínio desse meio, nem podem retaliar da mesma forma que o fazem quando estão sendo atacados na terra, no ar ou no espaço (LIBICKI, 2012, p. 324, 330).

No campo da Segurança, a “escolha de uma metáfora traz consigo implicações sobre o conteúdo, causas, expectativas, normas e escolhas estratégicas”⁶⁵ (BOBROW, 1996, p. 436

⁶² “unhelpful and dangerous”

⁶³ the wrong way to view cyberspace [...] it leads strategists and operators to presumptions or conclusions that are not derived from observation and experience

⁶⁴ In practice, a great deal of what offensive cyber warriors do is reconnaissance, or exploration

⁶⁵ ‘choice of a metaphor carries with it implications about contents, causes, expectations, norms, and strategic choices’

apud BETZ; STEVENS, 2013, p. 149, tradução nossa) que, muitas vezes, podem ser utilizadas para manipular a “estruturação da realidade política”⁶⁶ (HOOK, 1984, p. 259 apud BETZ; STEVENS, 2013, p. 149, tradução nossa). Sendo assim, o uso de analogias e metáforas nessa área deve ser cauteloso, afirmam Betz e Stevens (2013, p. 149).

Para Cepik, Canabarro e Borne (2014, p. 1), a inconsistência conceitual se agravou com a intensificação do processo de securitização do ciberespaço. De acordo com os autores, “A exploração do ciberespaço para fins político-estratégicos, seja por atores estatais, seja por atores não estatais, integra há tempos a agenda de pesquisa dos estudos de segurança” (ARQUILLA; RONFELDT, 1997; 2001 apud CEPIK; CANABARRO; BORNE, 2014, p. 1), mas foi somente

a partir do desencadeamento da guerra global ao terrorismo a partir dos atentados terroristas de 11 de Setembro de 2001 – diante do comprovado emprego da Internet e de outras tecnologias da informação e da comunicação pela Al Qaeda – que um rol bastante variado de atividades levadas a cabo através de redes computacionais passou a ser indiscriminadamente tratado como assunto de segurança. (WEIMANN, 2006; STARR, 2009; CLARKE; KNAKE, 2010 apud CEPIK; CANABARRO; BORNE, 2014, p. 1).

Um simples exemplo de falta de consenso em torno de conceitos básicos se dá no emprego impreciso dos termos ciberespaço, internet e web, que “compõem o cerne dos estudos de cibersegurança.” (CANABARRO; BORNE, 2013a).

2.2.2.1 Ciberespaço (Cyberspace), Internet (Internet) e Web (World Wide Web)

Apesar da origem do termo “ciberespaço” (*cyberspace*) estar relacionada com uma obra de ficção científica (GIBSON, 1984) e estar claramente associada à tecnologia computacional, justamente por ter surgido dentro do contexto da Revolução da Informação, a existência do ciberespaço precede em muito a sua criação e utilização terminológica (BETZ; STEVENS, 2011, p. 13). Cientificamente, o ciberespaço se caracteriza por ser

um domínio global dentro do ambiente informacional que se destaca pelo uso da eletrônica e do espectro eletromagnético a fim de criar, armazenar, modificar, trocar e explorar a informação através de redes interdependentes e interconectadas que utilizam tecnologias de comunicação e informação.⁶⁷ (KUEHL, 2009, p. 28, tradução nossa).

⁶⁶ structuring political reality

⁶⁷ a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.

Sendo assim, ele também abrange outras redes que já existiam antes da invenção do computador e da internet (BETZ; STEVENS, 2011, p. 13). Dessa forma, aparelhos eletrônicos pertencentes a diferentes instâncias de comunicação, como telefones celulares, *paggers*, aparatos de videoconferência, rádios, telégrafo, televisão via satélite, *video games* etc., bem como os dados e informações associados a esses dispositivos, que estão sendo armazenados ou transportados por eles, também fazem parte do ciberespaço (MATHERS, 2007, p. 2; GUIMARÃES JR., 1999; BETZ; STEVENS, 2011, p. 13; KUEHL, 2009, p. 28-31).

O termo ciberespaço tem sido amplamente utilizado como um equivalente à “internet” (*Internet*) (BETZ; STEVENS, 2011, p. 13). Isso se deu, principalmente, devido à “revolução científico-tecnológica da década de 1970 e a invenção dos circuitos eletrônicos integrados (os populares microchips)” (CEPIK; CANABARRO; BORNE, 2014, p. 3), que fizeram com que todas as redes passassem “a se apoiar em tecnologias da informação e comunicação (TIC) centradas na computação” (CEPIK; CANABARRO; BORNE, 2014, p. 3). Essa tendência à unificação da esfera global de telecomunicações a partir de plataformas digitais (GUIMARÃES JR., 1999), de acordo com Betz e Stevens (2011, p. 13) fez com que a internet se tornasse “não apenas a principal rede que compõe o ciberespaço, mas a plataforma para a qual têm convergido as demais tecnologias” (SERRA, 2006 apud CEPIK; CANABARRO; BORNE, 2014, p. 3). Porém, apesar da internet ser o principal ambiente do ciberespaço (GUIMARÃES JR., 1999), os limites entre ambos não podem se confundir. A internet nada mais é do que uma solução tecnológica para interligar computadores e redes de computadores (KUROSE; ROSS, 2007; CANABARRO; BORNE, 2013a), cujas “características intrínsecas (padrões abertos, governança, técnica participativa, e neutralidade, dentre outras) permitiram seu crescimento e transformaram-na em ponto focal para o desenvolvimento de redes computacionais” (ABBATE, 2001; GREWAL, 2009; KURBALIJA; GELBSTEIN, 2005 apud CANABARRO; BORNE, 2013a), tendo-se tornado, “ao final do século passado, a rede das redes” (CANABARRO; BORNE, 2013a). Dessa forma, o termo ciberespaço possui um significado muito mais amplo, enquanto a internet funciona apenas “como a principal porta de entrada”⁶⁸ para ele (CANABARRO; BORNE, 2013b, p. 4, tradução nossa).

Para compreender melhor a dinâmica da internet, podemos visualizá-la a partir de camadas (ZITTRAIN, 2008, p. 22):

A camada inferior é composta pelos elementos físicos que dão suporte às conexões, ao fluxo e ao armazenamento de dados que circulam em formato digital. São

⁶⁸ the main entry door for cyberspace

componentes da camada inferior, por exemplo, as linhas telefônicas, os cabos de conexão, as antenas de transmissão, os satélites, os servidores, etc. A camada superior, por sua vez, é composta por informação. A informação é codificada e decodificada por padrões técnicos e lógicos que compõem a camada intermediária da Internet. Em outras palavras, a informação é traduzida na camada intermediária, de padrões compreensíveis por seres humanos para padrões computacionais, e vice-versa. O uso e a partilha da informação por diferentes usuários através de diferentes aplicações (e-mail, sítios Web, telefonia VoIP⁶⁹, troca de arquivos P2P⁷⁰, entre outras) gera ainda uma quarta camada, um espaço vastíssimo de interações e formação de redes sociais, econômicas e políticas que se desenvolve de forma transnacional e impõe múltiplos desafios aos processos de governança política nos planos nacional e internacional (EISENBERG; CEPIK, 2002; MUELLER, 2002; MALCOM, 2008 apud CANABARRO; BORNE, 2013a).

A utilização do termo “web” (*world wide web*) como um sinônimo do termo ciberespaço também ocorre. Entretanto, a web nada mais é que uma dentre várias outras aplicações que dão acesso ao conteúdo que está armazenado em computadores, utilizando-se de um sistema de documentos de hipertexto interligados (BETZ; STEVENS, 2011, p. 13; CANABARRO; BORNE, 2013a). A criação da web foi bastante relevante para a internet pelo fato de ter simplificado o acesso à informação e ter aumentado o uso da internet pelo usuário não especializado, mas a internet nunca precisou da web para funcionar (CANABARRO; BORNE, 2013a; ANDERSON; WOLFF, 2010). “Atualmente, o modelo de Internet móvel adotado por telefones e *tablets* representa o principal candidato de superação da Web, já que muitos desses dispositivos fazem uso de outros padrões e protocolos de acesso à Rede” (CANABARRO; BORNE, 2013a). Dessa forma, a web é apenas uma das formas de se ter acesso à internet e está longe de possuir o caráter tão abrangente do termo ciberespaço.

2.2.3 Thomas Rid: Ciberguerra (*Cyberwar*) Vs. Sabotagem (*Sabotage*), Espionagem (*Espionage*) e Subversão (*Subversion*)

Mais além das confusões semânticas simples, as principais controvérsias conceituais giram em torno do uso da palavra ciberguerra. Thomas Rid (2012, 2013) lidera esse debate e sustenta que o uso de conceitos que dão ênfase à guerra distrai os governos do real desafio que o ciberespaço lhes apresenta: os confrontos não violentos, que podem ser tão catastróficos quanto os violentos ou, até mesmo, piores que esses, em alguns casos (RID, 2012, 2013).

⁶⁹ VoIP (*Voice over Internet Protocol*) é um tipo de tecnologia de transmissão de comunicação de voz através de uma rede de dados usando um endereço na internet (*Internet Protocol – IP*). (GENERAL DYNAMICS..., 2014, p. 1).

⁷⁰ P2P (*Peer-to-peer*) significa ponto-a-ponto e é uma “Arquitetura de rede onde cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, em que alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via programas P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, etc.” (PEER-TO-PEER, 2014).

Em 2012, Rid escreveu um artigo intitulado *Cyber war will not take place* (“A Ciberguerra não vai acontecer”, tradução livre) (2012) com o objetivo de refutar o artigo de Arquilla e Ronfeldt de 1993 (“A Ciberguerra está vindo!”). Em 2013, Rid publicou um livro de mesmo nome, com o objetivo de aprofundar seus fundamentos e oferecer uma contribuição mais sólida para o debate (RID, 2013, p. ix).

De acordo com Rid (2012, p. 6-7), os ciberataques que ocorreram no passado, que ocorrem hoje e que, potencialmente, virão a ocorrer no futuro, não se caracterizam como atos de guerra. Isso porque, segundo as premissas de Clausewitz, renomado teórico da guerra, um ato ofensivo precisa atender a certos critérios que, segundo Rid (2012), não estão presentes na maioria dos ciberataques da atualidade. Esses critérios seriam a presença, real ou potencial, de violência; a instrumentalidade do ato, ou seja, o uso da força para alcançar um objetivo, e a existência de vontades políticas opostas, que se reflete na atribuição (CLAUSEWITZ, 1832, 1980 apud RID, 2012, p. 6-7).

Rid (2012) descreve e analisa vários ciberataques ocorridos nos últimos tempos, demonstra a inexistência dos elementos sugeridos por Clausewitz nesses ataques (violência, instrumentalidade e atribuição) e vai além: argumenta que o uso da palavra guerra para denominá-los têm “mais valor metafórico que descritivo”⁷¹ (RID, 2012, p. 15, tradução nossa), como em “Guerra contra o Terror” ou “Guerra contra o câncer”. Ademais, **ressalta que os conhecidos conceitos de sabotagem, espionagem e subversão são mais apropriados para caracterizar tais ataques que o termo ciberguerra** (RID, 2012, p. 6).

Sabotagem (*Sabotage*) “é uma tentativa deliberada de enfraquecer ou destruir um sistema econômico ou militar”⁷² (RID, 2012, p. 16, tradução nossa), possuindo um caráter predominantemente técnico: “*Se a violência é usada, coisas são os primeiros alvos, não seres humanos*”⁷³ (RID, 2012, p. 16, tradução nossa, destaque do autor). O termo tem sua origem na palavra francesa *sabots*, espécie de madeira que sustenta os trilhos de uma ferrovia, e data da greve ferroviária de 1910 na França, quando trabalhadores retiraram e destruíram os *sabots* como forma de protesto (RID, 2012, p. 16).

Rid (2012, p. 17) considera que o Stuxnet, vírus que atingiu o programa de enriquecimento de urânio iraniano descoberto em 2010, foi um dos atos de cibernsabotagem mais complexos e sofisticados que já existiu, não só pela sua natureza operativa

⁷¹ it has more metaphoric than descriptive value.

⁷² is a deliberate attempt to weaken or destroy an economic or military system.

⁷³ If violence is used, things are the prime targets, not humans

autoexecutável, mas também pela sua capacidade de localizar o alvo, camuflar sua atuação e se autodeletar, quando necessário.

Espionagem (*Espionage*) “é uma tentativa de penetrar um sistema adversário a fim de extrair informações sensíveis ou protegidas.”⁷⁴ (RID, 2012, p. 20, tradução nossa). Pode ter natureza social (inteligência humana⁷⁵) ou técnica (inteligência de sinais⁷⁶) e tem como principal objetivo coletar informações (RID, 2012, p. 20). De acordo com Rid (2012, p. 20), “o uso mais comum de capacidades ciber patrocinadas pelo Estado é para fins de espionagem. Empiricamente, a grande maioria dos incidentes de cibersegurança de caráter político tem sido de espionagem.”⁷⁷ (RID, 2012, p. 20, tradução nossa).

Rid (2012, p. 21) cita a invasão à intranet do Departamento de Defesa (*Department of Defense – DoD*) estadunidense chamada SIPRNET (*Secret Internet Protocol Router Network*), ocorrida em novembro de 2008, como a violação mais significativa de computadores que se tem conhecimento. Utilizada para transmitir informações classificadas, a intranet era protegida contra conexões inseguras, mas através de um *malware* inserido na rede desclassificada denominada NIPRNET (*Non-classified Internet Protocol Router Network*) foi possível alcançá-la.

Subversão (*Subversion*) “é a tentativa deliberada de minar a autoridade, a integridade e a constituição de uma autoridade ou ordem estabelecida [...] ao corroer laços *sociais*, crenças e a confiança no Estado ou em outras entidades coletivas.”⁷⁸ (RID, 2012, p. 22, tradução nossa). Na subversão, “*As mentes humanas são os alvos, não as máquinas*”⁷⁹ (RID, 2012, p. 22, tradução nossa, destaque do autor).

Rid (2012, p. 22) chama a atenção para a diferença entre subversão e insurgência (*insurgency*). Para que a insurgência seja bem sucedida é preciso que tenha havido violência e derrubada de uma ordem pré-estabelecida. Na subversão, embora esses critérios possam existir, não são necessários para que um ato seja considerado subversivo.

⁷⁴ is an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information.

⁷⁵ “Humint (*Human Intelligence*) – informações obtidas a partir de fontes humanas.” (CEPIK, 2003, p. 36).

⁷⁶ “Sigint (*Signals Intelligence*) – informações obtidas a partir da interceptação e decodificação de comunicações e sinais eletromagnéticos.” (CEPIK, 2003, p. 36).

⁷⁷ The most widespread use of state-sponsored cyber capabilities is for purposes of espionage. Empirically, the vast majority of all political cyber security incidents have been cases of espionage.

⁷⁸ is the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order [...] eroding *social* bonds, beliefs, and trust in the state and other collective entities.

⁷⁹ Human minds are the targets, not machines.

2.2.4 Guerra baseada na Internet (*iWar*)

Enquanto alguns (RID, 2012, 2013) buscam apresentar conceitos alternativos para caracterizar os ciberconflitos atuais, outros (RYAN, 2010) continuam a utilizar termos que utilizam a palavra guerra para se referir a conflitos de caráter não militar, como ocorre com o conceito de Guerra baseada na Internet (*iWar*).

Para Ryan (2010, p. 195), na Guerra baseada na Internet o principal alvo dos ataques são os consumidores e toda a infraestrutura a eles direcionada e não as infraestruturas militares. Segundo Ryan (2010, p. 195), a Guerra baseada na Internet gera uma mudança elementar no equilíbrio da capacidade ofensiva, uma vez que pode ser travada não só por nações, empresas ou comunidades, mas principalmente “por qualquer indivíduo que tenha um conhecimento razoável de tecnologia”⁸⁰ (RYAN, 2010, p. 195, tradução nossa). Isso dota qualquer pessoa com poder de ameaçar as atividades dos governos e grandes empresas, embora, diante dessa concepção, qualquer um possa ser prejudicado por um ataque de Guerra baseada na Internet (RYAN, 2010, p. 195).

A complexidade da Guerra baseada na Internet é a mesma que se verifica na maioria dos incidentes ocorridos no ciberespaço e gira em torno da facilidade em obter o conhecimento necessário para realizar os ataques, do caráter anônimo desses ataques, do alcance global da internet e da falta de aparatos para punir tais ataques. Assim como dispôs Ryan (2010, p. 195-196, tradução nossa), a Guerra baseada na Internet

pode causar danos partindo de qualquer ponto do globo e atingindo um alvo em qualquer lugar do mundo sem praticamente nenhum custo.⁸¹ [...] novas ferramentas e *know-how* necessários para conduzir a *iWar* proliferam facilmente através da Internet.⁸² [...] pode ser travada de forma anônima e é difícil de punir.⁸³ [...] Mesmo se a culpa oficial pudesse ser provada, não está claro como um Estado deve responder a um ataque *iWar* feito por outro. A investigação criminal não seria menos problemática.⁸⁴

E conclui: “A potência dessa forma de guerra crescerá na proporção em que as economias, os governos e as comunidades do mundo adotarem a internet para interagir e oferecer serviços”⁸⁵ (RYAN, 2010, p. 196, tradução nossa).

⁸⁰ by any reasonably tech-savvy individual.

⁸¹ can inflict damage from any point on the globe at a target anywhere on the globe at virtually no cost.

⁸² new tools and know-how necessary to wage *iWar* proliferate easily across the Internet.

⁸³ can be waged anonymously and is difficult to punish.

⁸⁴ Even if official culpability could be proven, it is unclear how one state should respond to an *iWar* attack by another. A criminal investigation would be no less problematic.

⁸⁵ The potency of this form of warfare will grow as the economies, governments and communities of the world embrace the Internet to interact and deliver services.

Ao que tudo indica o conceito de Guerra na Rede (*Netwar*) de Arquilla e Ronfeldt (1993) não se equipara ao conceito de Guerra baseada na Internet (*iWar*). Embora ambas não possuam um caráter primordialmente militar, a primeira diz respeito a um conflito informacional, ou seja, visa o controle de informações, enquanto a segunda diz respeito a uma série de ações que têm por objetivo causar danos, fazer protestos, indisponibilizar serviços, prejudicar não só a reputação, mas também financeiramente, tanto indivíduos como grupos ou governos.

Sobre o uso da palavra guerra para denominar conflitos de caráter não militar como esses, esclarecem Hansen e Nissenbaum (2009): “a rotulagem de fenômenos intrinsecamente não militares com o termo ‘guerra’ pode levar a eventos injustificados de securitização, que são uma característica potencial das políticas de cibersegurança em geral.”⁸⁶ (CANABARRO; BORNE, 2013b, p. 4, tradução nossa).

2.3 Definindo Ciberguerra

Apresentado um breve panorama da origem e evolução do debate ciber, contexto em que se insere a ciberguerra, faz-se, agora, necessário defini-la.

Como observamos, o termo ciberguerra tem sido utilizado das mais variadas formas (convencionalmente, estrategicamente, analogicamente, metaforicamente etc.) e alternativas conceituais para o seu uso também já foram apresentadas (sabotagem, espionagem e subversão) (RID, 2012, 2013). Apesar de entendermos que o uso da palavra guerra nos estudos de segurança internacional deve ser cauteloso (BETZ; STEVENS, 2013) e apesar de reconhecermos que os argumentos de Rid (2012, 2013) procedem, já que os ciberataques da atualidade não consistem em atos de guerra, mas sim, em grande parte, em atos de sabotagem e espionagem de um país contra o outro, optamos, neste trabalho, por adotar a palavra ciberguerra para nos referirmos a esses ataques, bem como às atividades desempenhadas pelos governos para realizá-los ou se defender deles, tanto pela ubiquidade do termo, que já vem sendo utilizado pela mídia, pelos governos e por grande parte da literatura que trata das questões ciber há algum tempo, como, principalmente, pela real necessidade de esclarecê-lo.

Sendo assim, dentro da perspectiva dos estudos de Defesa, Segurança e Estratégicos entendemos que a ciberguerra deve ser entendida como o uso do poder ciber (*cyber power*)

⁸⁶ the labeling of inherently non-military phenomena as “war” can lead to unjustified events of securitization, which are a potential feature of cybersecurity policies in general.

pelos governos para “manipular o ambiente estratégico”⁸⁷ (SHELDON, 2012, p. 208, tradução nossa), em tempos de paz ou no âmbito da preparação e condução da guerra, com a finalidade de “alcançar os objetivos políticos da nação”⁸⁸ (SHELDON, 2012, p. 208, tradução nossa).

O poder ciber (*cyber power*) se perfaz na “habilidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais [ar, terra, mar e espaço] e através dos instrumentos de poder [políticos, diplomáticos, econômicos, militares e informacionais]”⁸⁹ (KUEHL, 2009, p. 38; STARR, 2009, p. 48; RATTRAY, 2009, p. 255, tradução nossa).

As atividades de ciberguerra, por sua vez, devem ser vistas como operações no ciberespaço (*cyberspace operations*), incluindo aquelas que têm por objetivo viabilizar ou dar suporte a operações militares “cinéticas (*kinetic operations*), informacionais (*information operations*) ou outros tipos de operações”⁹⁰ (ESTADOS UNIDOS, 2012b, p. 4, tradução nossa), constituindo-se um recurso, uma especialidade ou uma ferramenta estratégica (SHELDON, 2012, p. 2009) e não uma nova forma distinta de guerra travada no ciberespaço. Como afirmou Cepik (2003, p. 69), referindo-se à Guerra de Informações (*Information Warfare – IW*), essas operações “não devem ser tomadas como configurando uma ‘guerra’ à parte. A guerra permanece una e indivisível enquanto realidade.”

De fato, “Por causa do papel da informação na guerra (veja, por exemplo, Clausewitz, 2007, Livro I, Capítulo VI)”⁹¹ (CANABARRO; BORNE, 2013b, p. 2, tradução nossa), “as operações de informação [e, mais recentemente, as operações no ciberespaço] têm sido reconhecidas [cada vez mais] como uma forma distinta de guerra, possuindo doutrina, política e táticas próprias em separado,”⁹² (SCHMITT, 1999, p. 32, tradução nossa), “uma tendência que se intensificou após a revolução científica da década de 1970”⁹³ (FREEMAN; LOUÇÃ, 2001; RENNSTICH, 2008 apud CANABARRO; BORNE, 2013b, p. 2, tradução nossa). No entanto, embora possuam doutrina, política e táticas próprias, as operações de informação e as operações no ciberespaço são apenas parte de uma série de esforços que são empregados por um Estado para a consecução de seu objetivo maior, ou seja, fazer prevalecer seus interesses perante os demais Estados diante, ou não, da existência de uma guerra.

⁸⁷ manipulate the strategic environment

⁸⁸ for achieving the policy objectives of the nation.

⁸⁹ ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power

⁹⁰ kinetic, information, or other types of operations.

⁹¹ Because of the role of information in war (see, e.g., Clausewitz, 2007, Book I, Chapter VI)

⁹² information operations has been recognized as a distinct form of warfare meeting its own separate doctrine, policy, and tactics,

⁹³ a trend that has been intensified after the scientific revolution of the 1970s.

3 DOCTRINAS, ESTRATÉGIAS E OPERAÇÕES DE CIBERGUERRA: ATACANDO E SE DEFENDENDO NO CIBERESPAÇO

Essas ferramentas não são únicas, nem muitas delas são de difícil acesso, e o processo é simples, mas para se levar a cabo uma guerra no nível de um Estado-nação é preciso uma grande dose a mais de recursos, esforço e conhecimento.⁹⁴ (ANDRESS; WINTERFELD, 2011, p. 178, tradução nossa).

No capítulo anterior, tentamos esclarecer alguns conceitos apresentando a evolução do debate ciber. Neste capítulo, com o intuito de aprofundar esse debate e partindo do pressuposto de que as atividades de ciber guerra devem ser vistas como operações no ciberespaço, incluindo aquelas que têm por objetivo viabilizar ou dar suporte a operações militares cinéticas, informacionais ou outros tipos de operações (ESTADOS UNIDOS, 2012b, p. 4), cabe-nos discorrer, brevemente, sobre o que seriam essas operações no ciberespaço (*cyberspace operations*) e em que tipo de doutrinas e estratégias elas se encontram fundamentadas.

Muitas questões ciber já se encontram bastante evoluídas em vários países ao redor do mundo, como na China,⁹⁵ na Rússia,⁹⁶ no Japão e no Reino Unido (ANDRESS,

⁹⁴ These tools are not unique, nor are many of them difficult to access, and the process is simple, but to carry out warfare at the level of a nation-state requires a great deal more resources, effort, and knowledge.

⁹⁵ Sobre a China, tivemos acesso a um estudo bastante conciso feito por Inkster (2012). De acordo com ele, na China, o governo tem tentado conciliar sua política de rigoroso controle de acesso e fluxo de informações com a busca por crescente modernização econômica, um de seus recentes objetivos estratégicos. Para isso, tem promovido a internet como um recurso competitivo indispensável para o país e, ao mesmo tempo, tem desenvolvido normas e mecanismos mais robustos de censura que bloqueiam o acesso a determinados websites, filtram informações pesquisadas e responsabilizam provedores de internet pelo conteúdo que está sendo transmitido em suas redes. A tecnologia tem tornado a tarefa de monitoramento cada vez mais fácil de ser executada pelo governo chinês, mas também tem servido como um meio favorecedor da realização de manifestações e protestos online. Entretanto, principalmente aqueles de cunho nacionalista têm sido manipulados pelo governo antes que possam significar uma ameaça real ao regime (INKSTER, 2012, p. 191-198). A dominância da internet pelo ocidente no que se refere à posse da maioria dos *hardwares* e *softwares*, bem como o uso da internet para espalhar a subversão são as principais preocupações atuais do governo chinês. As políticas desse país, portanto, têm sido direcionadas ao fomento da indústria nacional para a produção de *softwares*, de forma a minar a pirataria ocidental, que também traz vulnerabilidades à propriedade intelectual do país; à promoção da soberania dos países na rede, sugerindo a implementação de uma administração internacional da internet e o desenvolvimento de ferramentas de segurança da informação pelo governo (INKSTER, 2012, p. 198-200). No que concerne à espionagem na rede e à ciber guerra, Inkster (2012, p. 200-203) aponta que “Formalmente, a China tem duas autoridades responsáveis pela espionagem e cibersegurança. Estas são o 3º Departamento de Estado-Maior General do PLA (*People’s Liberation Army - Exército de Libertação Popular*) (3/PLA), a agência de inteligência de sinais (SIGINT) da China, e o 4º Departamento de Estado-Maior General do PLA (4/PLA), que é responsável pela guerra eletrônica.” (INKSTER, 2012, p. 201, tradução nossa). “Este último é responsável por uma nova Base de Salvaguarda da Informação - *xinxi baozhang jidi* - cuja criação se tornou pública em julho de 2010 e cujo objetivo foi descrito como enfrentar as ameaças ciber e salvaguardar a segurança da informação e a infraestrutura de informação da China.” (PU, 2010 apud INKSTER, 2012, p. 201-202, tradução nossa). De acordo com Inkster (2012, p. 202-203), desde os anos 1990 as Forças Armadas chinesas estão alertas às vulnerabilidades estadunidenses (como a sua crescente dependência em sistemas de TIC) e que sua doutrina chinesa enfatiza a necessidade de desenvolver capacidades ofensivas para destruir os sistemas de comando e controle do inimigo no campo de batalha, visualizando a internet como um novo domínio para se fazer a guerra, assim como vê os Estados Unidos. Além disso, afirma que, antigamente, a atividade de coleta de inteligência

WINTERFELD, 2011, p. 43-46; HEALEY, 2013, p. 233-264; GVOSDEV, 2012, p. 173-189; INKSTER, 2012, p. 191-205). Contudo, a maioria das informações que aqui apresentaremos irão se referir aos Estados Unidos, não só pelo pioneirismo desse país no assunto (HEALEY, 2013), mas também pela facilidade com que se tem acesso a grande parte de documentos sobre essa área que ali são produzidos. Vale lembrar, entretanto, que embora tenhamos escolhido a perspectiva estadunidense para apresentar parte do conteúdo das doutrinas, estratégias e operações no ciberespaço, a essência desses documentos reflete e se aproxima, em grande parte, do que está sendo produzido, desenvolvido e realizado por muitos outros países (ANDRESS; WINTERFELD, 2011, p. 43-44), já que a maioria dos governos também está preocupada em adequar conceitos, reestruturar instituições, estabelecer políticas satisfatórias, operacionalizar esforços e obter um domínio mais efetivo das capacidades que o ciberespaço pode lhes oferecer.⁹⁷

Não obstante a disponibilidade online de grande parte das doutrinas e estratégias ciber estadunidenses, recurso por nós utilizado, devido aos propósitos a que são direcionadas, quais sejam, guiar as ações de todo país em prol de seus interesses nacionais, grande parte desse material permanece classificado, ou seja, indisponível na internet. Além disso, o caráter atual do assunto tem intensificado as publicações sobre o tema, fazendo com que documentos com

chinesa era muito mais aleatória e em larga escala, mas que hoje é mais direcionada e estruturada (INKSTER, 2012, p. 203). Inkster (2012, p. 203) considera que a inovação chinesa será percebida em pouco mais tempo do que se imagina e que o país exercerá maior influência em assuntos relacionados com a governança global da internet, mas acredita que haverá uma continuidade da política de controle do conteúdo que circula na rede.

⁹⁶ Govsdev (2012) recentemente apresentou um estudo pertinente sobre as capacidades ciber da Rússia. De acordo com ele, embora a Rússia não esteja mais na “vanguarda dos países tecnologicamente mais avançados do mundo” (GOVSDEV, 2012, p. 173, tradução nossa), seus *hackers* patriotas vêm demonstrando grande habilidade ciber, como nos últimos ataques à Estônia (2007) e à Geórgia (2008). Para ele, o uso de ciberataques patrocinados pelo governo representa uma recente mudança do pensamento estratégico russo. Antes, o governo dava mais ênfase às capacidades militares tradicionais, mas nas últimas três décadas, as capacidades ciber têm se destacado como um importante instrumento de poder (GOVSDEV, 2012, p. 173). A doutrina militar russa atual apela para “a implementação prioritária de medidas de guerra de informação a fim de alcançar objetivos políticos sem a utilização da força militar” (RÚSSIA, 2010 apud GOVSDEV, 2012, p. 177, tradução nossa) e o governo russo tem adotado o monitoramento do ciberespaço, a contratação de *hackers* e o incentivo à inovação tecnológica como políticas prioritárias, a fim de, com essas medidas, evitar ataques terroristas, evitar a entrada maciça de tecnologia de informação estrangeira no país e expandir suas capacidades operacionais informacionais (GOVSDEV, 2012, P. 178-182). Govsdev (2012, p. 182-184) considera, entretanto, que a Rússia ainda é bastante vulnerável às ameaças e que seus recursos financeiros não são suficientes para acompanhar os investimentos em capacidades ciber feitos pelos Estados Unidos e pela China.

⁹⁷ A título de exemplo, um estudo recente feito em conjunto pelo Centro para Estudos Estratégicos e Internacionais (*Center for Strategic and International Studies – CSIS*), pelo Instituto para Pesquisa sobre Paz e Política de Segurança (*Institute for Peace Research and Security Policy – IFSH*) e pelo Instituto das Nações Unidas para Pesquisa sobre o Desarmamento (*United Nations Institute for Disarmament Research - UNIDIR*) revelou que, com base em informações obtidas por fontes abertas, doze dos quinze países com os maiores orçamentos militares têm ou estão desenvolvendo unidades de ciber guerra e, desses doze, dez parecem possuir ou estar desenvolvendo capacidades ciber ofensivas (LEWIS; NEUNECK, 2013, p. 3).

datas recentes já estejam em desuso (ANDRESS; WINTERFELD, 2011, p. 38-39). Essas questões dificultam o acompanhamento da evolução desses documentos e tornam o nosso estudo algo bastante desafiador, limitando-o; embora isso não o torne menos útil, como veremos.

Para direcionar os nossos esforços, no que diz respeito às doutrinas e estratégias relacionadas às Operações no Ciberespaço, nos limitaremos a responder a essas duas questões: “Quais são seus principais conteúdos?” e “Quais são as doutrinas e estratégias mais recentes?” No que se refere às operações, tentaremos responder às seguintes perguntas: “Quais são as operações?”, “Quem as conduz?”, “O que se utiliza para realizá-las?”, “Como são realizadas?”, “Quais são os seus principais objetivos?” (ANDRESS; WINTERFELD, 2011).

Apesar de a literatura pesquisada (ESTADOS UNIDOS, 1998-2014; ANDRESS; WINTERFELD, 2011; HEALEY, 2013) trazer grandes detalhes a respeito das nomenclaturas, siglas e metodologias utilizadas nas doutrinas, estratégias e operações que existem ou estão sendo criadas, devido ao caráter mutante e evolutivo desses documentos que, conforme observamos, estão sob constante revisão e aperfeiçoamento, optamos aqui por dar maior destaque ao conteúdo central abordado, ou seja, os conceitos, sem prejuízo, é claro, de alguns dados que contribuirão para uma melhor compreensão dos propósitos deste capítulo.

3.1 Doutrinas de Ciberguerra

As doutrinas militares compreendem o conjunto de princípios, diretrizes, valores, conceitos, normas, métodos e processos; são influenciadas “por tradições, guias, táticas, técnicas e procedimentos”⁹⁸ e têm por objetivo orientar as Forças Armadas “a guiar suas ações para dar suporte aos objetivos nacionais.”⁹⁹ (ANDRESS; WINTERFELD, 2011, p. 37, tradução nossa).

O conteúdo da doutrina estadunidense que fala sobre operações no ciberespaço¹⁰⁰ direciona-se a definir conceitos e estabelecer diretrizes e prioridades, bem como organizar as funções e responsabilidades dentro da estrutura hierárquica das Forças Armadas e de seus órgãos governamentais de apoio. Para essa pesquisa, interessa-nos, precipuamente, os conceitos.

⁹⁸ by tradition, guides, and tactics, techniques, and procedures (TTPs).

⁹⁹ guide their actions in support of national objectives.

¹⁰⁰ Além dos documentos aqui mencionados, também podemos destacar o “Plano de Conceituação e Capacitação de Operações no Ciberespaço” (*Cyberspace Operations Concept Capability Plan 2016-2028*) do Exército dos Estados Unidos, de 22 de fevereiro de 2010 (ESTADOS UNIDOS, 2010d).

Para compreender os conceitos existentes na doutrina de ciberguerra estadunidense mais recente é preciso lembrar sua origem, que coincide com a produção intelectual dos anos 1990 marcada pela chegada da Era da Informação.

Assim como observou Healey (2013, p. 18), dos anos 1980 até as primeiras décadas dos anos 1990 a doutrina estadunidense utilizou o termo Guerra de Informações (*Information Warfare*) para se referir às operações militares, ofensivas ou defensivas, que lidavam com questões relativas à informação.

A partir de 1998, a doutrina estadunidense central JP 3-13 (*Joint Publication 3-13*) (ESTADOS UNIDOS, 1998) passou a utilizar o termo Operações de Informação (*Information Operations – IO*) para se referir a essas operações (HEALEY, 2013, p. 18; ESTADOS UNIDOS, 1998, p. I-1), tendo ainda mantido o termo Guerra de Informações (*Information Warfare*) para se referir àquelas operações específicas de informação, “conduzidas durante tempos de crise ou conflitos (incluindo a guerra) para alcançar ou promover objetivos específicos sobre um adversário ou adversários específicos.”¹⁰¹ (ESTADOS UNIDOS, 1998, p. I-1, tradução nossa).

A JP 3-13 de 1998 já se referia a Ataques a Redes de Computadores (*Computer Network Attack – CNA*) como “operações para interromper, negar, degradar ou destruir informações residentes em computadores e redes de computadores ou os próprios computadores e suas redes.”¹⁰² (ESTADOS UNIDOS, 1998, p. I-9, tradução nossa). Essas operações, entretanto, apareciam como uma opção quando da condução de Operações de Informação (*Information Operations – IO*):

“Operações de informação” são ações tomadas para afetar as informações e os sistemas de informação do adversário, ao defender as próprias informações e sistemas de informação. IOs exigem uma integração estreita e contínua das capacidades e atividades ofensivas e defensivas, assim como um modelo efetivo de integração e interação de C2 [comando e controle], com o apoio da inteligência. IOs são realizadas através da integração de muitas capacidades e atividades relacionadas. As principais capacidades para conduzir IOs incluem, mas não estão limitadas a, OPSEC (segurança das operações – *operations security*), PSYOP (operações psicológicas – *psychological operations*), dissimulação militar (*military deception*), EW (guerra eletrônica – *electronic warfare*) e ataque físico/destruição (*physical attack/destruction*), **podendo incluir CNA (ataque a redes de computadores – *computer network attack*)**. Atividades relacionadas com as IOs incluem, mas não estão limitadas a, relações públicas (*public relations – PR*) e atividades de assuntos

¹⁰¹ conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries.

¹⁰² operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

civis (*civil affairs* – CA).¹⁰³ (ESTADOS UNIDOS, 1998, p. I-9-I-10, tradução nossa, destaque nosso).¹⁰⁴

Em 2006, a doutrina JP-3-13 (ESTADOS UNIDOS, 2006a) foi atualizada e estabeleceu uma diferenciação nítida entre as Capacidades Centrais (*Core Capabilities*), as Capacidades de Suporte (*Supporting Capabilities*) e as Capacidades Relacionadas (*Related Capabilities*) das Operações de Informação (*Information Operations*), incluindo as Operações de Redes de Computadores (*Computer Network Operations* – CNO) como uma das cinco capacidades centrais das Operações de Informação, junto com as operações de Guerra Eletrônica (*Electronic Warfare* – EW), Operações Psicológicas (*Psychological Operations* – PSYOP), Segurança das Operações (*Operations Security* – OPSEC) e Dissimulação Militar (*Military Deception* – MILDEC). (ESTADOS UNIDOS, 2006a, p. iii).

Essas transformações tiveram por objetivo alinhar a doutrina de Operações de Informação existente com as orientações de planejamento trazidas pelo Roteiro de Operações de Informação (*Information Operations Roadmap*) do Departamento de Defesa, de outubro de 2003 (ESTADOS UNIDOS, 2006a, p. iii), que afirmou:

O Roteiro surge como mais um exemplo do compromisso do Departamento [de Defesa] de transformar as nossas capacidades militares para acompanhar as ameaças emergentes e explorar novas oportunidades oferecidas pela inovação e o rápido desenvolvimento das tecnologias da informação.¹⁰⁵ (ESTADOS UNIDOS, 2003a, p. 1, tradução nossa).

¹⁰³ “Information operations” are actions taken to affect adversary information and information systems, while defending one’s own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. IO are conducted through the integration of many capabilities and related activities. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CNA. IO-related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities.

¹⁰⁴ Na doutrina JP 3-13 de 1998, as “IOs ofensivas envolvem o uso integrado de capacidades e atividades atribuídas e de suporte, mutuamente apoiadas pela inteligência, para afetar os tomadores de decisão do adversário e alcançar ou promover objetivos específicos. Essas capacidades e atividades atribuídas e de suporte incluem, mas não estão limitadas a, OPSEC, dissimulação militar, PSYOP, EW, ataque físico/destruição e operações especiais de informação (*special information operations* – SIO), e podem incluir CNA. IOs defensivas integram e coordenam as políticas e procedimentos, operações, pessoal e tecnologia para proteger e defender as informações e os sistemas de informação. IOs defensivas são conduzidas e assistidas através da garantia da informação (*information assurance* – IA), OPSEC, segurança física, contradissimulação (*counterdeception*), contrapropaganda, contra-inteligência (*counterintelligence* – CI), EW e SIO. IOs defensivas garantem o acesso à informação de forma oportuna, precisa e relevante, negando aos adversários a oportunidade de explorar informações favoráveis e os sistemas de informação para seus próprios propósitos. IOs ofensivas também podem dar suporte às IOs defensivas.” (ESTADOS UNIDOS, 1998, p. I-10, tradução nossa).

¹⁰⁵ The Roadmap stands as another example of the Department’s commitment to transform our military capabilities to keep pace with emerging threats and to exploit new opportunities afforded by innovation and rapidly developing information technologies.

Na JP 3-13 de 2006, as funções das Operações de Redes de Computadores (*Computer Network Operations* – CNO) se assemelhavam às das operações de Guerra Eletrônica e consistiam em Ataques a Redes de Computadores (*Computer Network Attack* – CNA), Defesa de Redes de Computadores (*Computer Network Defense* – CND) e Espionagem a Redes de Computadores (*Computer Network Exploitation* – CNE) (ESTADOS UNIDOS, 2006a, p. iii):

(1) As CNO são um dos recursos mais recentes desenvolvidos para dar suporte às operações militares. As CNO derivam do aumento do uso de computadores em rede e dos sistemas de apoio à infraestrutura de TI por organizações militares e civis. **As CNO, juntamente com a EW, são usadas para atacar, enganar, degradar, interromper, negar, explorar e defender a informação e a infraestrutura eletrônicas. Para os propósitos das operações militares, as CNO são divididas em CNA, CND e espionagem (CNE) a redes de computadores relacionadas, que viabilizam operações.** As CNA consistem em ações realizadas através do uso de redes de computadores para interromper, negar, degradar ou destruir a informação encontrada em computadores e redes de computadores ou os próprios computadores e suas redes. As CND envolvem ações realizadas através do uso de redes de computadores para proteger, monitorar, analisar, detectar e responder a atividade não autorizada dentro dos sistemas de informação e redes de computadores do DoD [Departamento de Defesa]. Ações de CND não só protegem os sistemas do Departamento de Defesa contra um adversário externo, mas também contra a espionagem, e são agora uma função necessária em todas as operações militares. As CNE são operações viabilizadoras e capacidades de coleta de inteligência realizadas através do uso de redes de computadores para coletar dados dos sistemas de informação automatizados de redes do alvo ou adversário. Note-se que, devido à contínua expansão das redes sem fio e devido à integração de computadores e comunicações de radiofrequência, **haverá operações e capacidades que tornarão opaca a linha divisória entre as CNO e as EW**, o que pode exigir uma determinação caso a caso, quando as EW e as CNO forem atribuídas a autoridades em separado.

(2) **As CNO como capacidades centrais das IOs.** A dependência crescente de Forças Armadas pouco sofisticadas e de grupos terroristas em computadores e redes de computadores para passar informações para as forças C2 reforça a importância das CNO nos planos e atividades de IO. À medida que a capacidade dos computadores e a variedade de seu emprego ampliam, novas vulnerabilidades e oportunidades continuarão a se desenvolver. Isto oferece oportunidades tanto para atacar e espionar as fraquezas do sistema de computadores de um adversário, como um requisito para identificar e proteger o nosso próprio de ataques ou espionagem similares.¹⁰⁶ (ESTADOS UNIDOS, 2006a, p. II4-II5, tradução nossa, destaque nosso).

¹⁰⁶ (1) CNO is one of the latest capabilities developed in support of military operations. CNO stems from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations. CNO, along with EW, is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. For the purpose of military operations, CNO are divided into CNA, CND, and related computer network exploitation (CNE) enabling operations. CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. CND actions not only protect DoD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations. CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Note that due to the continued expansion of wireless networking and the integration of computers and radio frequency communications, there will be operations and capabilities that blur the line between CNO and EW and that may require case-by-case determination when EW and CNO are assigned separate release

Também nesse documento a palavra ciberespaço aparece pela primeira vez na doutrina, significando um “ambiente fictício em que a informação digitalizada é comunicada através das redes de computadores.”¹⁰⁷ (ESTADOS UNIDOS, 2006a, p. GL-6, tradução nossa).

Em novembro de 2010, um documento específico sobre Operações no Ciberespaço foi elaborado, através de um memorando, tendo sido denominado Terminologia Conjunta para Operações no Ciberespaço (*Joint Terminology for Cyberspace Operations*) (ESTADOS UNIDOS, 2010c). Nesse momento, o termo CNO (*Computer Network Operations*) foi substituído por Operações no Ciberespaço (*Cyberspace Operations – CO*)¹⁰⁸ (ESTADOS UNIDOS, 2010c, p. 8), que significava “O emprego de capacidades ciber, cujo principal propósito é alcançar objetivos no ou através do ciberespaço. Tais operações incluem operações de rede de computadores e atividades para operar e defender a Rede Mundial de Computadores (*Global Information Grid*).”¹⁰⁹ (ESTADOS UNIDOS, 2010c, p. 8, tradução nossa). O documento também modificou as definições existentes de CNA, CND e CNE (ESTADOS UNIDOS, 2010c, p. 2) incluindo, no rol, várias outras atividades, como as Operações de Força Avançadas (*Advance Force Operations*),¹¹⁰ as Operações Ofensivas no Ciberespaço (*Offensive Cyberspace Operations – OCO*),¹¹¹ as atividades de Categorização do

authorities. (2) CNO as an IO Core Capability. The increasing reliance of unsophisticated militaries and terrorist groups on computers and computer networks to pass information to C2 forces reinforces the importance of CNO in IO plans and activities. As the capability of computers and the range of their employment broadens, new vulnerabilities and opportunities will continue to develop. This offers both opportunities to attack and exploit an adversary’s computer system weaknesses and a requirement to identify and protect our own from similar attack or exploitation.

¹⁰⁷ the notional environment in which digitized information is communicated over computer networks.

¹⁰⁸ Ao lado do termo operações no ciberespaço existe a seguinte informação “CM-0856-09 1 Sep 2009” (ESTADOS UNIDOS, 2010c, p. 8), o que nos leva a crer que essa definição de Operações no Ciberespaço deve ter sido elaborada anteriormente e publicada em setembro de 2009 através de um documento que desconhecemos.

¹⁰⁹ The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

¹¹⁰ “Uma operação que antecede o principal esforço em uma área objetiva, a fim de preparar o objetivo para o ataque principal através da condução de operações tais como reconhecimento, tomada de posições de apoio – incluindo os principais sistemas de rede ou nós – pré-armazenagem ou ajuste de armas – tais como remoção de minas navais, bombardeio preliminar, demolições submarinas ou o implante de acessos e/ou armas ciber – e apoio aéreo.” (ESTADOS UNIDOS, 2010c, p. 2, tradução nossa).

¹¹¹ “Atividades que, através do uso do ciberespaço, reúnem ativamente informações de computadores, sistemas de informação ou redes, ou manipulam, interrompem, negam, degradam ou destroem computadores, sistemas de informação ou redes específicas.” (ESTADOS UNIDOS, 2010c, p. 13, tradução nossa).

Armamento (*Weapon Categorization*)¹¹² e as operações de Ciberataque (*Cyber attack*)¹¹³, a título de exemplo.

Nesse documento, o ciberespaço (*cyberspace*) passou a significar um “domínio caracterizado pelo uso da eletrônica e do espectro eletromagnético para armazenar, modificar e trocar dados através de sistemas de rede e infraestruturas físicas associadas”¹¹⁴ (ESTADOS UNIDOS, 2010c, p. 7, tradução nossa).

Em janeiro de 2011, o secretário de defesa publicou um memorando denominado Comunicação Estratégica e Operações de Informação no DoD (*Strategic Communication and Information Operations in the DoD*) (ESTADOS UNIDOS, 2011c) ampliando o conceito de Operações de Informação. Esse documento retirou do conceito de Operações de Informação as suas cinco capacidades centrais (*core capabilities*). Essa alteração se deu, principalmente, devido ao fato de que, ao nomeá-las, as unidades por ela responsáveis deram ênfase a cada uma dessas capacidades de forma isolada, enquanto o principal objetivo era integrá-las. Ao retirar o rol explícito de capacidades “as ferramentas disponíveis [estariam] agora limitadas apenas pela imaginação do comandante e sua equipe.”¹¹⁵ (ESTADOS UNIDOS, 2011d, p. 6, tradução nossa). O novo texto ficou assim:

[Operações de Informação consistem no] ‘emprego integrado, durante as operações militares, de capacidades relacionadas com a informação (*information-related capabilities*), em conjunto com outras linhas de operações, para influenciar, interromper, corromper ou usurpar a tomada de decisão de adversários e potenciais adversários e, ao mesmo tempo, proteger a nossa.’¹¹⁶ (ESTADOS UNIDOS, 2011c, p. 2, tradução nossa).

¹¹² “Um complexo de capacidades de armas ciber colocadas em categorias, baseadas na avaliação de risco e na autoridade de autorização necessária para o seu uso, que são usadas para determinar o nível de autorização para a sua utilização. Um exemplo de categorias poderia ser: Categoria I – Autorização do Comandante em combate, Categoria II – Autorização pré-aprovada para uso do comandante em combate em OPLANs específicos ou sob o estado de alerta específico/status de arma ROE, Categoria III – Autorizada apenas pelo Presidente/SECDEF.” (ESTADOS UNIDOS, 2010c, p. 15, tradução nossa).

¹¹³ “Um ato hostil usando o computador ou redes ou sistemas relacionados e destinado a interromper e/ou destruir sistemas, ativos ou funções ciber críticas do adversário. Os efeitos pretendidos de um ciberataque não estão necessariamente limitados aos sistemas de computadores-alvo ou aos dados em si – por exemplo, ataques contra sistemas de computadores que se destinam a degradar ou destruir a infraestrutura ou capacidade C2. Um ciberataque pode utilizar veículos de entrega intermediários incluindo dispositivos periféricos, transmissores eletrônicos, códigos incorporados ou operadores humanos. A ativação ou o efeito de um ciberataque podem ser amplamente separados temporalmente e geograficamente da sua entrega.” (ESTADOS UNIDOS, 2010c, p. 5, tradução nossa).

¹¹⁴ domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures.

¹¹⁵ the tools available are now constrained only by the imagination of the commander and his staff.

¹¹⁶ “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”

Embora as capacidades centrais das Operações de Informação tivessem sido retiradas do conceito, elas não deixaram de existir. De acordo com o documento Cartilha de Operações de Informação: Fundamentos das Operações de Informações (*Information Operations Primer: Fundamentals of Information Operations*) (ESTADOS UNIDOS, 2011d) produzido pela Escola de Guerra do Exército dos EUA (*US Army War College*) em novembro de 2011, os planos eram de que essas capacidades fossem incorporadas ao corpo da doutrina então em revisão (ESTADOS UNIDOS, 2011d, p. 6), o que ocorreu.

Em novembro de 2012, a doutrina central JP 3-13 (ESTADOS UNIDOS, 2012a) incorporou a nova definição de Operações de Informação sugerida pelo memorando de 2011 e aprofundou o significado de capacidades relacionadas com a informação (*information-related capabilities – IRCs*): “são ferramentas, técnicas ou atividades empregadas dentro de uma dimensão do ambiente de informações, que podem ser utilizadas para alcançar um fim específico/fins específicos.”¹¹⁷ (ESTADOS UNIDOS, 2012a, p. iii, tradução nossa).

De forma abrangente, o texto da JP 3-13 de 2012 enumerou várias IRCs, que se resumem nas capacidades tradicionais existentes, como as OPSEC, as MILDEC e as MISO,¹¹⁸ por exemplo, e em outras novas capacidades, como a Comunicação Estratégica (*Strategic Communication – SC*)¹¹⁹ e as Operações Espaciais (*Space Operations*),¹²⁰ deixando claro que esse rol de capacidades não era exaustivo (ESTADOS UNIDOS, 2012a, p. ix).

¹¹⁷ tools, techniques or activities employed within a dimension of the information environment, which can be used to achieve a specific end(s).

¹¹⁸ A expressão Operações Psicológicas (*Psychological Operations - PSYOP*) foi substituída pela expressão Operações de Informação de Suporte às Forças Armadas (*Military Information Support Operations - MISO*) em 2010. Assim, as MISO são consideradas capacidades tradicionais. A modificação na terminologia foi feita por um memorando em dezembro de 2010 (ESTADOS UNIDOS, 2011c, p. 2), mas só foi incorporada ao texto da doutrina central JP 3-13 em novembro de 2012, significando “operações planejadas para transmitir informações e indicadores selecionados para o público estrangeiro para influenciar suas emoções, motivos, raciocínio objetivo e, em última instância, o comportamento de governos estrangeiros, organizações, grupos e indivíduos.” (ESTADOS UNIDOS, 2012a, p. II-9-II-10, tradução nossa).

¹¹⁹ “(1) Comunicação Estratégica. (a) O processo de SC consiste em esforços focados do Governo dos Estados Unidos (USG) para criar, fortalecer ou preservar condições favoráveis para o avanço dos interesses, políticas e objetivos nacionais ao compreender e engajar audiências-chave através do uso de programas coordenados, planos, temas, mensagens e produtos sincronizados com as ações de todos os instrumentos de poder nacionais. A SC é uma abordagem governamental global (*whole-of-government approach*) impulsionada por processos de interagências e de integração que estão focados em uma estratégia nacional de comunicação eficaz. (b) Os elementos e organizações que implementam a orientação estratégica, tanto internos como externos à força conjunta, devem não só entender e estar cientes dos objetivos das IOs da força conjunta, mas também devem trabalhar em estreita colaboração com os membros da comunidade interagências, a fim de assegurar plena coordenação e sincronização dos esforços do Governo dos EUA. Assim, os objetivos do Comando das Forças Conjuntas (*Joint Forces Command - JFC*) das IOs devem complementar os objetivos gerais de acordo com a orientação estratégica. O Grupo de Coordenação Conjunto das Interagências (*Joint Interagency Coordination Group - JIACG*) representativo dentro da célula de IOs facilita a coordenação para cumprir a orientação estratégica e facilitar a SC.” (ESTADOS UNIDOS, 2012a, p. II-5-II-6, tradução nossa).

¹²⁰ “(7) Operações Espaciais. Capacidades espaciais são um multiplicador de força significativo quando integrado com as operações conjuntas. As operações espaciais dão suporte às IOs através das funções de melhoria de força espacial de inteligência, monitoramento e reconhecimento, alerta de mísseis, monitoramento ambiental;

No que tange ao ciberespaço e às Operações no Ciberespaço (*Cyberspace Operations* – CO) a doutrina JP 3-13 de 2012 afirmou:

(a) O ciberespaço é um domínio global dentro do ambiente de informações consistindo na rede interdependente de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, as redes de telecomunicações, os sistemas de computadores e os processadores e controladores embutidos. **As COs são o emprego de capacidades do ciberespaço, cujo principal propósito é alcançar os objetivos no ou através do ciberespaço.** As capacidades do ciberespaço, quando em apoio às IOs, negam ou manipulam a tomada de decisão do adversário ou adversário em potencial, através de um meio de informação-alvo (como um ponto de acesso sem fio na dimensão física), através da mensagem em si (uma mensagem criptografada na dimensão informacional) ou através de uma ciber-persona (uma identidade online que torna possível a comunicação, a tomada de decisão e a influência do público na dimensão cognitiva). **Quando empregadas em apoio às IOs, as COs geralmente têm como foco a integração de capacidades ofensivas e defensivas exercidas no e através do ciberespaço, em conjunto com outras IRCs e em coordenação com várias linhas de operação e linhas de esforço.**

(b) Como um processo que integra o emprego de IRCs através das múltiplas linhas de esforço e linhas de operação para afetar um tomador de decisão adversário ou adversário em potencial, as IOs podem direcionar o meio (um componente dentro da dimensão física, como uma torre de microondas) ou a mensagem em si (por exemplo, uma mensagem codificada na dimensão informacional). As COs são uma das várias IRCs à disposição do comandante.¹²¹ (ESTADOS UNIDOS, 2012a, p. II-9, tradução nossa, destaque nosso).

Embora tenha sido publicada em novembro de 2012, acreditamos que a última JP 3-13 já esteja desatualizada, pelo menos no que se refere aos conceitos. Através da Diretiva 3600.01 do Departamento de Defesa (*Department of Defense Directive 3600.01*) (ESTADOS UNIDOS, 2013a), de maio de 2013, o Departamento de Defesa dos Estados Unidos apresentou uma definição mais atualizada para as Operações de Informação:

a. As IOs serão o principal mecanismo utilizado durante as operações militares para integrar, sincronizar, empregar e avaliar uma grande variedade de

comunicações por satélite e de posicionamento espacial, navegação e cronometragem. A célula IO é um lugar-chave para a coordenação e soluções de controvérsias (*deconflicting*) das funções de melhoria da força espacial com outras IRCs.” (ESTADOS UNIDOS, 2012a, p. II-9, tradução nossa).

¹²¹ (a) Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities, when in support of IO, deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension). When employed in support of IO, CO generally focus on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort. (b) As a process that integrates the employment of IRCs across multiple lines of effort and lines of operation to affect an adversary or potential adversary decision maker, IO can target either the medium (a component within the physical dimension such as a microwave tower) or the message itself (e.g., an encrypted message in the informational dimension). CO is one of several IRCs available to the commander.

capacidades relacionadas com a informação (IRCs), em conjunto com outras linhas de operações para afetar a tomada de decisões dos adversários ou potenciais adversários, protegendo a nossa.

b. **As IRCs constituem ferramentas, técnicas ou atividades empregadas dentro de uma dimensão do ambiente de informações (*information environment – IE*)¹²², que podem ser usadas para atingir um fim específico, em um tempo e lugar específico.** IRCs podem incluir, mas não se limitam, a uma variedade de atividades técnicas e não técnicas que se cruzam com as áreas tradicionais de guerra eletrônica (*electronic warfare – EW*)¹²³, **operações no ciberespaço (*cyberspace operations – CO*)¹²⁴**, operações de informação de suporte às Forças Armadas (*military information support operations – MISO*)¹²⁵, dissimulação militar (*military deception – MILDEC*)¹²⁶, atividades de influência (*influence activities*), segurança das operações (*operations security – OPSEC*)¹²⁷ e inteligência (*intelligence*)¹²⁸ (ESTADOS UNIDOS, 2013a, p. 1, tradução nossa, destaque nosso).

A despeito dessas recentes alterações, revelações publicadas pelo jornal *The Guardian* em junho de 2013 (GREENWALD; MACASKILL, 2013a) mostram que a doutrina sobre as Operações no Ciberespaço continua em evolução. O documento, de caráter classificado, denominado Diretiva Política Presidencial/PPD 20 (*Presidential Policy Directive/PPD-20*) (ESTADOS UNIDOS, 2012b) de outubro de 2012 foi apresentado em sua íntegra pelo jornal *The Guardian* no dia 7 de junho de 2013 (GREENWALD; MACASKILL, 2013b), como parte das revelações em massa feitas por Edward Snowden, ex-consultor da Agência de Segurança Nacional estadunidense (*National Security Agency – NSA*) e apresenta novas definições para as Operações no Ciberespaço.

¹²² O ambiente de informações (*information environment – IE*) “é o agregado de indivíduos, organizações e sistemas que coletam, processam, disseminam ou agem sobre a informação.” (ESTADOS UNIDOS, 2010b, p. 127, tradução nossa).

¹²³ “Ação militar envolvendo o uso de energia eletromagnética e dirigida para controlar o espectro eletromagnético ou para atacar o inimigo. Também chamada de EW.” (ESTADOS UNIDOS, 2010b, p. 84, tradução nossa).

¹²⁴ Operações no Ciberespaço consistem no “emprego de capacidades do ciberespaço, cujo propósito principal é alcançar os objetivos no ou através do ciberespaço.” (ESTADOS UNIDOS, 2010b, p. 64, tradução nossa).

¹²⁵ As MISO são “operações planejadas para transmitir informações e indicadores selecionados para o público estrangeiro para influenciar suas emoções, motivos, raciocínio objetivo e, em última instância, o comportamento de governos estrangeiros, organizações, grupos e indivíduos de uma forma favorável aos objetivos de seu originador.” (ESTADOS UNIDOS, 2010b, p. 171-172, tradução nossa).

¹²⁶ As MILDEC consistem em “ações executadas para enganar deliberadamente um adversário militar, paramilitar ou tomadores de decisão de organização extremista violenta, fazendo com que o adversário tenha ações específicas (ou inércia) que contribuirão para a realização da missão favorável.” (ESTADOS UNIDOS, 2010b, p. 171, tradução nossa).

¹²⁷ A OPSEC é “um processo de identificação de informação crítica e subsequente análise de ações favoráveis que atendem às operações militares e outras atividades.” (ESTADOS UNIDOS, 2010b, p. 197, tradução nossa).

¹²⁸ a. IO will be the principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of operations to effect adversaries' or potential adversaries' decision-making while protecting our own. b. IRCs constitute tools, techniques, or activities employed within a dimension of the information environment (IE) that can be used to achieve a specific end at a specific time and place. IRCs can include, but are not be limited to, a variety of technical and non-technical activities that intersect the traditional areas of electronic warfare, cyberspace operations, military information support operations (MISO), military deception (MILDEC), influence activities, operations security (OPSEC), and intelligence.

Na PPD-20 as Operações no Ciberespaço constituem atividades no ciberespaço e incluem aquelas operações que dão suporte ou viabilizam Operações de Informação (*Information Operations*), operações cinéticas (*kinetic operations*) ou outros tipos de operações (ESTADOS UNIDOS, 2012b, p. 4), e compreendem as operações de coleta ciber (*cyber collection*), as operações de efeitos ciber defensivos (*defensive cyber effects operations* – DCEO), incluindo as contramedidas defensivas não intrusivas (*nonintrusive defensive countermeasures* – NDCM), e as operações de efeitos ciber ofensivos (*offensive cyber effects operations* – OCEO) (ESTADOS UNIDOS, 2012b, p. 3).

O efeito ciber (*cyber effect*) consiste na “manipulação, interrupção, negação, degradação ou destruição de sistemas de computadores, de informação ou de sistemas de comunicação, de redes, de infraestrutura física ou virtual controlada por computadores ou sistemas de informação, ou informações neles residentes.”¹²⁹ (ESTADOS UNIDOS, 2012b, p. 2, tradução nossa).

As operações de coleta ciber (*cyber collection*) são

Operações e programas relacionados ou atividades realizadas pelo ou em nome do Governo dos Estados Unidos, no ou através do ciberespaço, com o principal propósito de coletar inteligência – incluindo a informação que pode ser usada para operações futuras – de computadores, sistemas de informação ou de comunicação ou redes com a finalidade de permanecer ocultas. A coleta ciber implica em acessar um computador, um sistema de informação ou rede sem autorização do proprietário ou do operador do computador, sistema de informação, ou rede ou de uma parte para uma comunicação ou para exceder o acesso autorizado. A coleta ciber inclui aquelas atividades essenciais e inerentes à viabilização da coleta ciber, tais como a inibição de detecção ou atribuição, mesmo que criem efeitos ciber.¹³⁰ (ESTADOS UNIDOS, 2012b, p. 2-3, tradução nossa, destaque nosso).

As operações de efeitos ciber defensivos (*defensive cyber effects operations* – DCEO) são

Operações e programas relacionados ou atividades – diferentes de defesa de rede (*network defense*)¹³¹ ou coleta ciber – conduzidas pelo ou em nome do Governo dos

¹²⁹ manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

¹³⁰ Operations and related programs or activities conducted by or on behalf of the United States Government, in or through cyberspace, for the primary purpose of collecting intelligence – including information that can be used for future operations – from computers, information or communications systems, or networks with the intent to remain undetected. Cyber collection entails accessing a computer, information system, or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access. Cyber collection includes those activities essential and inherent to enabling cyber collection, such as inhibiting detection or attribution, even if they create cyber effects.

¹³¹ Defesa de Rede (*Network Defense*) consiste em “programas, atividades e o uso de ferramentas necessárias para facilitá-los (incluindo aqueles governados pelas NSPD-54/HSPD-23 e NSD-42), conduzidos em um computador, rede ou sistema de comunicação ou informações pelo proprietário ou com o consentimento do

Estados Unidos, no ou através do ciberespaço, que **se destinam a viabilizar ou produzir efeitos ciber fora das redes do Governo dos Estados Unidos com o objetivo de defender ou proteger [os Estados Unidos] contra ameaças iminentes ou ataques em curso ou atividades ciber maliciosas contra os interesses nacionais dos Estados Unidos de dentro ou de fora do ciberespaço.**¹³² (ESTADOS UNIDOS, 2012b, p. 3, tradução nossa, destaque nosso).

As contramedidas defensivas não intrusivas (*nonintrusive defensive countermeasures* – NDCM) são

O subconjunto de DCEOs que **não requerem acesso** a computadores, informações ou sistemas de comunicação, ou redes **sem autorização** dos proprietários ou operadores de sistemas de computadores alvo, informação ou sistemas de comunicação, ou redes ou **acesso autorizado excedente**, e **só cria os efeitos ciber mínimos necessários para mitigar as atividades relacionadas com a ameaça.**¹³³ (ESTADOS UNIDOS, 2012b, p. 3, tradução nossa, destaque nosso).

As operações de efeitos ciber ofensivos (*offensive cyber effects operations* – OCEO) são

Operações e programas relacionados ou atividades – diferentes de defesa de rede, coleta ciber, ou DCEO – **conduzidas pelo ou em nome do Governo dos Estados Unidos, no ou através do ciberespaço, que se destinam a viabilizar ou produzir efeitos ciber fora das redes do Governo dos Estados Unidos.**¹³⁴ (ESTADOS UNIDOS, 2012b, p. 3, tradução nossa, destaque nosso).

Como podemos observar, as novas concepções dão um caráter mais ativo às operações no ciberespaço, permitindo que mesmo as operações de defesa produzam efeitos ciber, desde que fora das redes do Governo dos Estados Unidos.

Mesmo após as revelações, a nova terminologia ainda não apareceu no Dicionário de Termos Militares e Associados do Departamento de Defesa JP 1-02 (*Department of Defense Dictionary of Military and Associated Terms* – JP 1-02) de 2010 (ESTADOS UNIDOS,

proprietário e, quando apropriado, os usuários, para o objetivo principal de proteger (1) aquele computador, rede ou sistema, (2) os dados nele armazenados, processados ou que transitam nesse computador, rede ou sistema, ou (3) a infraestrutura física e virtual controlada por um computador, rede ou sistema. Defesa da rede não envolve ou requer o acesso ou a condução de atividades em computadores, redes ou sistemas de informação ou de comunicação sem a autorização dos proprietários ou ultrapassagem do acesso autorizado pelos proprietários.” (ESTADOS UNIDOS, 2012b, p. 2, tradução nossa).

¹³² Operations and related programs or activities – other than network defense or cyber collection – conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace.

¹³³ The subset of DCEO that does not require accessing computers, information or communications systems, or networks without authorization from the owners or operators of the targeted computers, information or communications systems, or networks or exceeding authorized access and only creates the minimum cyber effects needed to mitigate the threat activity.

¹³⁴ Operations and related programs or activities – other than network defense, cyber collection, or DCEO – conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks.

2010b), que foi atualizado em dezembro de 2013. Entretanto, o dicionário já contém algumas definições que constam no último documento direcionado especificamente às Operações no Ciberespaço de que se tem conhecimento, a publicação conjunta denominada Operações Conjuntas no Ciberespaço JP 3-12 (*Joint Cyberspace Operations JP 3-12*) (ESTADOS UNIDOS, 2013b), assinada em 5 de fevereiro de 2013, o que confirma a evolução contínua da doutrina (ESTADOS UNIDOS, 2010b, p. 64, 69, 192)¹³⁵. Essa última publicação, contudo, é classificada e encontra-se disponível apenas na rede fechada SIPRNET JDEIS (ESTADOS UNIDOS, 2013b, p. iii).

De acordo com o Compêndio de Publicações da Doutrina Conjunta Central (*Compendium of Key Doctrine Publications*) (ESTADOS UNIDOS, 2013b), de junho de 2013, a JP 3-12 adveio do Plano de Implementação da Estratégia Militar Nacional para Operações no Ciberespaço (*National Military Strategy for Cyberspace Operations Implementation Plan*). Ela teve início como uma Publicação Conjunta de Teste (*Joint Test Publication – JPT*), tendo evoluído para uma Publicação Conjunta (*Joint Publication – JP*) devido ao esforço coletivo da comunidade destinada a desenvolvê-la (ESTADOS UNIDOS, 2013b, p. iii).¹³⁶ O Compêndio também afirma que essa publicação “aborda a singularidade das operações militares no ciberespaço, esclarece o comando de operações relacionadas ao ciberespaço, bem como as inter-relações operacionais, e incorpora as lições operacionais aprendidas.”¹³⁷ (ESTADOS UNIDOS, 2013b, p. iii, tradução nossa).

A doutrina que fundamenta as Operações no Ciberespaço, portanto, originou-se dentro da doutrina de Operações de Informação e, ao longo do tempo, à medida que essa capacidade

¹³⁵ A título de exemplo, o dicionário traz as seguintes definições constantes na JP 3-12: “Superioridade no ciberespaço – O grau de domínio do ciberespaço por uma força que permite a condução segura e confiável de operações por essa força e por suas respectivas forças terrestres, aéreas, marítimas e espaciais, em um determinado tempo e lugar, sem a interferência proibitiva de um adversário. (JP 3-12)” (ESTADOS UNIDOS, 2010b, p. 64, tradução nossa). “Ações de resposta às operações defensivas no ciberespaço – Medidas deliberadas e autorizadas ou ações tomadas fora da rede defendida, para proteger e defender as capacidades do ciberespaço do Departamento de Defesa ou de outros sistemas designados. Também chamadas de DCO-RA. (JP 3-12)” (ESTADOS UNIDOS, 2010b, p. 69, tradução nossa). “Operações Defensivas no Ciberespaço – Operações no Ciberespaço passivas e ativas destinadas a preservar a habilidade de utilizar capacidades do ciberespaço favoráveis e a proteger dados, redes, capacidades centradas na rede (*net-centric capabilities*) e outros sistemas designados. Também chamadas de DCO. (JP 3-12)” (ESTADOS UNIDOS, 2010b, p. 69, tradução nossa). “Operações Ofensivas no Ciberespaço – Operações no Ciberespaço destinadas a projetar poder através da aplicação de força no ou através do ciberespaço. Também chamadas de OCO. (JP 3-12)” (ESTADOS UNIDOS, 2010b, p. 192, tradução nossa).

¹³⁶ A doutrina da Força Aérea estadunidense possui um documento de denominação semelhante: Operações no Ciberespaço – Documento 3-12 da Doutrina da Força Aérea (*Cyberspace Operations – Air Force Doctrine Document 3-12*) (ESTADOS UNIDOS, 2010a) publicado em julho de 2010 e atualizado em novembro de 2011. Acredita-se que esse documento tenha feito parte dos esforços conjuntos para a elaboração da Publicação Conjunta JP 3-12, cujo conteúdo ainda encontra-se classificado.

¹³⁷ addresses the uniqueness of military operations in cyberspace, clarify cyberspace operations-related command and operational interrelationships, and incorporate operational lessons learned.

foi se tornando mais relevante, ela passou a ser desenvolvida na doutrina de forma mais autônoma, embora a doutrina de Operações de Informação ainda seja o principal mecanismo utilizado durante as operações militares para coordenar as capacidades do ciberespaço com as outras capacidades existentes em todas as linhas de operações militares (ESTADOS UNIDOS, 2013a, p. 1).

3.2 Estratégias de Ciberguerra

Estratégias governamentais também têm como objetivo guiar “ações para dar suporte aos objetivos nacionais.”¹³⁸ (ANDRESS; WINTERFELD, 2011, p. 37, tradução nossa), definindo diretrizes e prioridades dentro de cada âmbito de atuação do governo.

No que se refere às estratégias governamentais mais recentes que tratam especificamente sobre Operações no Ciberespaço (*Cyberspace Operations*), os Estados Unidos possuem duas estratégias basilares, quais sejam: a Estratégia Militar Nacional para Operações no Ciberespaço (*National Military Strategy for Cyberspace Operations – NMS-CO*) (ESTADOS UNIDOS, 2006b), publicada em dezembro de 2006 e a Estratégia para Operar no Ciberespaço do Departamento de Defesa (*Department of Defense Strategy for Operating in Cyberspace*) (ESTADOS UNIDOS, 2011a) de julho de 2011.

Para apresentar o conteúdo relevante dessas duas estratégias, acreditamos que seja pertinente fazê-lo através de um breve relato sobre as estratégias nacionais estadunidenses direcionadas ao ciberespaço¹³⁹ até então existentes, mostrando a sua evolução.¹⁴⁰ Esse relato se faz importante não só para que possamos visualizar o contexto em que as estratégias para operar no ciberespaço surgiram, baseadas na produção intelectual sobre as relações entre governança e Revolução da Informação que se iniciou nos anos 1990, mas também para que

¹³⁸ actions in support of national objectives.

¹³⁹ Além dos documentos aqui citados, também podemos destacar: Plano Nacional de Proteção às Infraestruturas (*National Infrastructure Protection Plan*) (ESTADOS UNIDOS, 2009c) de 2009; Projeto de Estratégia Nacional para Identidades Confiáveis no Ciberespaço (*National Strategy for Trusted Identities in Cyberspace. Draft*) (ESTADOS UNIDOS, 2010f), de 25 de junho de 2010; Iniciativa Nacional para Educação em Cibersegurança (*The National Initiative for Cybersecurity Education*) (ESTADOS UNIDOS, 2010g), de 19 de abril de 2010; Ciberespaço Confiável: Plano Estratégico para o Programa Federal de Pesquisa e Desenvolvimento em Cibersegurança (*Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*) (ESTADOS UNIDOS, 2011e), de dezembro de 2011; Ato de Conscientização Pública sobre a Cibersegurança (*Cyber Security Public Awareness Act of 2011*) (ESTADOS UNIDOS, 2011f), de abril de 2011.

¹⁴⁰ Para informações mais detalhadas sobre a evolução das Estratégias Nacionais relacionadas à cibersegurança, ver o relatório elaborado pelo Escritório de Auditoria do Governo dos Estados Unidos (*Government Accountability Office – GAO*) (ESTADOS UNIDOS, 2013c) em fevereiro de 2013, mais especificamente as páginas 18 a 28.

possamos comparar a evolução do conteúdo dessas duas estratégias operacionais no tempo e vislumbrar breves reflexões.

A primeira iniciativa do governo estadunidense de estabelecer diretrizes nacionais relacionadas ao ciberespaço resultou no Plano Nacional para a Proteção de Sistemas de Informação (*National Plan for Information Systems Protection*) lançado pela Casa Branca em 2000 (ESTADOS UNIDOS, 2013c, p. 21). Embora limitado à proteção dos sistemas e infraestruturas críticas do país contra ciberataques, o plano foi concebido como um primeiro esforço do governo para defender o ciberespaço (ESTADOS UNIDOS, 2000, p. ii, iii).

Em fevereiro de 2003 foi lançada a Estratégia Nacional para Proteger o Ciberespaço (*The National Strategy to Secure Cyberspace*), cujo objetivo principal se resumia em “aperfeiçoar a cibersegurança em todo o país, não só dos sistemas do governo, mas também das infraestruturas críticas pertencentes ao setor privado”¹⁴¹ (CHEN, 2013, p. 3). Esse documento destacou três prioridades estratégicas que se consubstanciam no “[combate] aos ciberataques contra as infraestruturas críticas estadunidenses, na [redução] da vulnerabilidade nacional frente aos ciberataques e na [minimização] dos danos e redução do tempo de recuperação pós-ataques”¹⁴² (ESTADOS UNIDOS, 2003b, p. viii, tradução nossa). Além disso, a Estratégia identificou prioridades nacionais críticas e enumerou várias ações e iniciativas que podemos, assim, condensar: implementar um sistema nacional de resposta a incidentes de segurança no ciberespaço e incentivar as parcerias público-privadas na troca de informação e nas respostas a incidentes ciber; aumentar a conscientização nacional sobre cibersegurança através de treinamentos, programas de educação, pesquisas e desenvolvimento em cibersegurança e reforçar a cooperação internacional para proteger o ciberespaço (ESTADOS UNIDOS, 2003b, p. viii-x).

Em 2004, foi publicada a Estratégia Militar Nacional (*National Military Strategy - NMS*)¹⁴³ dos Estados Unidos. Essa estratégia consistiu em um plano de ação para as Forças Armadas darem suporte às novas Estratégias de Segurança e Defesa Nacional¹⁴⁴ (ESTADOS UNIDOS, 2004, p. iv). A Estratégia Militar destacou três prioridades basilares: combater o terrorismo, aperfeiçoar o combate conjunto das Forças Armadas e transformar a força

¹⁴¹ improve cyber security nationwide, not only government systems but also critical infrastructures owned by the private sector.

¹⁴² Prevent cyber attacks against America’s critical infrastructures; Reduce national vulnerability to cyber attacks; and Minimize damage and recovery time from cyber attacks that do occur

¹⁴³ A Estratégia Militar Nacional (*National Military Strategy – NMS*) dos Estados Unidos mais recente que encontramos online foi publicada em 8 de fevereiro de 2011 (ESTADOS UNIDOS, 2011b).

¹⁴⁴ Para ter acesso a algumas Estratégias Nacionais de Segurança estadunidenses, veja o Arquivo de Estratégias Nacionais de Segurança (*National Security Strategy Archive – NSSA*) (ESTADOS UNIDOS, 2014b).

conjunta das Forças Armadas para atender aos objetivos militares futuros (ESTADOS UNIDOS, 2004, p. iv, v).

Apesar de não ser uma estratégia direcionada especificamente ao ciberespaço, ela é relevante para esta pesquisa, pois constituiu o ciberespaço como o mais novo domínio para se fazer a guerra, assim como a terra, o mar, o ar e o espaço: “As Forças Armadas devem ter a capacidade para operar através dos domínios ar, terra, mar, espaço e ciberespaço do campo de batalha.”¹⁴⁵ (ESTADOS UNIDOS, 2004, p. 5, 18, tradução nossa).

Em dezembro de 2006, a Estratégia Militar Nacional para Operações no Ciberespaço (*National Military Strategy for Cyberspace Operations – NMS-CO*) foi publicada. Parcialmente desclassificada desde a sua publicação, a NMS-CO tem por escopo contribuir para o alcance do objetivo estratégico militar fundamental, que é garantir a superioridade estratégica militar dos Estados Unidos no ciberespaço (ESTADOS UNIDOS, 2006b, p. 1). Para isso, ela “descreve o domínio do ciberespaço, articula ameaças e vulnerabilidades no ciberespaço e fornece um quadro estratégico para a ação”¹⁴⁶ (ESTADOS UNIDOS, 2006b, p. vii, tradução nossa) que orienta e focaliza as ações do Departamento de Defesa nas áreas militar, de inteligência e de operações de negócios no e através do ciberespaço (ESTADOS UNIDOS, 2006b, p. ix). A NMS-CO também visa promover “um entendimento comum sobre o ciberespaço”¹⁴⁷ e ser referência para o planejamento, execução e obtenção de recursos relacionados às operações no ciberespaço (ESTADOS UNIDOS, 2006b, p. ix, tradução nossa).

A NMS-CO possui as seguintes prioridades estratégicas: obter e manter a iniciativa para operar dentro do ciclo decisório adversário; desenvolver capacidades para operar no ciberespaço e integrá-las com toda a gama de operações militares existentes; gerenciar o risco das operações no ciberespaço (ESTADOS UNIDOS, 2006b, p. F-1-F3).

Em agosto de 2007, o governo estabeleceu a Comissão sobre Cibersegurança para a 44ª Presidência (*Commission on Cybersecurity for the 44th Presidency*)¹⁴⁸ por meio do Centro para Estudos Estratégicos e Internacionais (*Center for Strategic and International Studies – CSIS*), uma instituição de pesquisa dedicada a analisar os impactos de políticas públicas em todo o mundo. O objetivo era analisar os planos e estratégias ciber existentes e avaliar o que

¹⁴⁵ The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace.

¹⁴⁶ describes the cyberspace domain, articulates threats and vulnerabilities in cyberspace, and provides a strategic framework for action.

¹⁴⁷ a common understanding of cyberspace

¹⁴⁸ Para ter acesso a outros documentos produzidos por essa comissão, além do relatório aqui citado, veja o site do Centro para Estudos Estratégicos e Internacionais (*Center for Strategic and International Studies – CSIS*) (COMMISSION..., 2014).

deveria ser mantido ou modificado (SECURING..., 2008, p. 1). Os trabalhos dessa comissão resultaram num relatório denominado Proteção do Ciberespaço para a 44^a Presidência (*Securing Cyberspace for the 44th Presidency*) (SECURING..., 2008), publicado em dezembro de 2008, que concluiu: a cibersegurança é um grande problema de segurança nacional para os Estados Unidos, as decisões e ações sobre cibersegurança devem respeitar a privacidade e as liberdades civis e apenas uma estratégia de abrangência nacional e internacional pode tornar o país mais seguro (SECURING..., 2008, p. 1).

De todas as recomendações estabelecidas pelo relatório podemos ressaltar as seguintes: criar uma estratégia de segurança de abrangência nacional e internacional; criar, organizar ou reestruturar agências, instituições, cargos e funções destinadas à cibersegurança, nos âmbitos legal, militar e dos serviços de inteligência; fazer parcerias com o setor privado; rever os parâmetros legais de segurança da informação e estabelecer padrões técnicos de segurança universais tanto para os sistemas públicos quanto para os sistemas privados; promover educação, realizar treinamentos, desenvolver a força de trabalho e conduzir pesquisas em cibersegurança (SECURING..., 2008, p. 5-9).

Enquanto isso, em janeiro de 2008, o governo dos Estados Unidos estabeleceu a Iniciativa Global Nacional para a Cibersegurança (*The Comprehensive National Cybersecurity Initiative – CNCI*) com o objetivo de implementar as responsabilidades estabelecidas pelas diretivas políticas Diretiva Presidencial de Segurança Nacional 54 / Diretiva Presidencial de Segurança Interna 23 (*National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – NSPD-54/HSPD-23*)¹⁴⁹, ambas parcialmente classificadas.¹⁵⁰

De acordo com o Relatório do Escritório de Auditoria do Governo dos Estados Unidos (*United States Government Accountability Office – GAO*)¹⁵¹ (ESTADOS UNIDOS, 2013c) de fevereiro de 2013, os projetos a serem implementados pela CNCI se alinham, em grande parte, com as recomendações apontadas nas estratégias anteriores (ESTADOS UNIDOS,

¹⁴⁹ Para uma lista das diretivas presidenciais dos últimos governos dos Estados Unidos veja o website da Federação Americana de Cientistas (*Federation of American Scientists - FAS*) (PRESIDENTIAL..., 2014).

¹⁵⁰ Em março de 2009 emitiu-se um relatório sobre a CNCI no que se refere aos seus aspectos legais e políticos (ESTADOS UNIDOS, 2009a), mas, tendo em vista o caráter parcialmente classificado das Diretivas que lhe deram origem, detalhes da CNCI não foram então publicados nesse relatório. Entretanto, com a finalidade de tornar públicos os esforços governamentais que estavam sendo realizados em relação à cibersegurança, a Casa Branca resolveu desclassificar parte das Diretivas publicando, em março de 2010, um documento detalhando as iniciativas da CNCI (ESTADOS UNIDOS, 2010e, p. 2). O detalhamento dessas iniciativas também pode ser encontrado no website da Casa Branca (ESTADOS UNIDOS, 2014d).

¹⁵¹ *Accountability*, segundo Cepik (2003, p. 158), é a avaliação posterior das ações dos governantes pelos governados. Entendemos não existir no nosso vocabulário palavra que possa melhor traduzir esse termo, mas consideramos útil, aqui, a palavra “auditoria” para proporcionar uma melhor compreensão do texto.

2013c, p. 22), tratando-se de iniciativas para aumentar a consciência situacional compartilhada sobre as vulnerabilidades no ciberespaço, ao conectar centros especializados em cibersegurança; aumentar a capacidade de agir rapidamente para evitar invasões, ao criar sistemas de monitoramento e ao aumentar a segurança das redes classificadas; aumentar as capacidades de contrainteligência; difundir educação em cibersegurança e coordenar esforços para pesquisas e desenvolvimento em cibersegurança; elaborar programas e estratégias de dissuasão (*deterrence*) e prevenção contra ataques; gerenciar riscos e realizar parcerias entre os setores públicos e privados (ESTADOS UNIDOS, 2010e, p. 1-2).

Em fevereiro de 2009, o presidente determinou a realização de uma revisão da política, estratégias e organizações voltadas para a cibersegurança, a fim de avaliar se as iniciativas propostas pela CNCI estavam sendo devidamente implementadas. A revisão durou 60 dias e foi realizada não só por especialistas em cibersegurança, mas também por membros dos setores industrial, acadêmico, comunidades de proteção às liberdades civis e aos direitos de privacidade, das organizações não governamentais, dos governos estaduais, parceiros internacionais e dos poderes legislativo e executivo (ESTADOS UNIDOS, 2009d, p. iii) e resultou num documento denominado Revisão da Política para o Ciberespaço (*Cyberspace Policy Review*) (ESTADOS UNIDOS, 2009d), publicado em maio de 2009.

A Revisão apresentou as principais vulnerabilidades dos Estados Unidos face às ameaças ciber da época e sugeriu planos de ação de curto, médio e longo prazo com recomendações para serem seguidas pelo governo, pelo setor privado, pelos cidadãos estadunidenses e pelos demais países no mundo (ESTADOS UNIDOS, 2009d).

Dentre as vulnerabilidades podemos destacar a falta de um órgão central que coordenasse as atividades de cibersegurança de âmbito nacional, estadual e local (ESTADOS UNIDOS, 2009d, p. 7), falta de um padrão global de resposta a incidentes significativos (ESTADOS UNIDOS, 2009d, p. 23), pouco investimento em pesquisa na área ciber (ESTADOS UNIDOS, 2009d, p. i) e falta de padronização entre as leis nacionais e regionais no que se refere aos cibercrimes (ESTADOS UNIDOS, 2009d, p. iv).

Dentre as recomendações, podemos ressaltar a nomeação de um responsável pela coordenação das políticas e atividades de cibersegurança da nação, a elaboração de uma estratégia nacional para proteger as infraestruturas de informações e comunicação, o fortalecimento da parceria público-privada para proteger as infraestruturas críticas que estão nas mãos do setor privado e a elaboração de uma campanha de conscientização pública para os riscos no ciberespaço (ESTADOS UNIDOS, 2009d, p. vi).

Como podemos observar, os relatórios que analisam e avaliam as estratégias e políticas para a proteção do ciberespaço, bem como os planos de ação a elas atrelados, tanto os mais antigos quanto os mais recentes, demonstram que, embora várias vulnerabilidades e prioridades tenham sido identificadas há muito tempo, o processo de implementação de mudanças mais concretas, capazes de garantir a proteção do ciberespaço de forma mais efetiva foi e ainda é bastante lento.

Em maio de 2011, lançou-se a Estratégia Internacional para o Ciberespaço (*International Strategy for Cyberspace*) (ESTADOS UNIDOS, 2011g) como mais uma tentativa do governo de compilar suas diretrizes fundamentais de atuação e dar cumprimento a uma parte das recomendações estabelecidas nas estratégias anteriores.

A Estratégia Internacional enfatizou a necessidade de cooperação internacional na proteção do ciberespaço e aprofundou os princípios de conduta no ciberespaço não apenas dos Estados Unidos, mas de todos os demais países do globo. Dentre esses princípios, destacam-se a não violação das liberdades fundamentais, a não violação da privacidade e a garantia do livre fluxo de informações de forma a fortalecer a segurança internacional e promover o livre comércio entre as nações, a liberdade de expressão e a inovação (ESTADOS UNIDOS, 2011g, p. 8).

Para isso, a estratégia determinou como prioritárias as seguintes políticas (ESTADOS UNIDOS, 2011g, p. 17-24):

Economia:¹⁵² promover padrões internacionais e mercados abertos e inovadores; **Redes:**¹⁵³ aprimorar a segurança, confiabilidade e resiliência; **Imposição da lei:**¹⁵⁴ estender a colaboração e o Estado de Direito; **Área militar:**¹⁵⁵ preparar para os

¹⁵² “Manter um ambiente de livre-comércio que incentive a inovação tecnológica em redes acessíveis e globalmente conectadas; Proteger a propriedade intelectual, incluindo os segredos comerciais, contra roubo; Assegurar a primazia de padrões técnicos interoperáveis e seguros, determinados por peritos técnicos.” (ESTADOS UNIDOS, 2011g, p. 17-18, tradução nossa).

¹⁵³ “Promover a cooperação no ciberespaço, em especial sobre normas de comportamento para os Estados e a cibersegurança, bilateralmente e em uma variedade de organismos multilaterais e parcerias multinacionais; Reduzir intrusões e interrupções de redes dos EUA; Assegurar uma gestão robusta de incidentes, resiliência e capacidade de recuperação da infraestrutura de informações; Melhorar a segurança da cadeia de fornecimento de alta tecnologia, em consulta com a indústria.” (ESTADOS UNIDOS, 2011g, p. 18-19, tradução nossa).

¹⁵⁴ “Participar plenamente no desenvolvimento de políticas contra o cibercrime internacional; Harmonizar as leis de cibercrime internacionalmente ao expandir a adesão à Convenção de Budapeste; Concentrar as leis sobre o cibercrime no combate às atividades ilegais, sem restringir o acesso à internet; Negar aos terroristas e outros criminosos a capacidade de explorar a internet para o planejamento operacional, financiamento ou ataques.” (ESTADOS UNIDOS, 2011g, p. 19-20, tradução nossa).

¹⁵⁵ “Reconhecer e se adaptar à crescente necessidade militar de operar em redes confiáveis e seguras; Construir e reforçar alianças militares existentes para enfrentar potenciais ameaças no ciberespaço; Expandir a cooperação no ciberespaço com aliados e parceiros para aumentar a segurança coletiva.” (ESTADOS UNIDOS, 2011g, p. 20-21, tradução nossa).

desafios de segurança do século XXI; **Governança da Internet:**¹⁵⁶ promover estruturas eficazes e inclusivas; **Desenvolvimento internacional:**¹⁵⁷ construir capacidade, segurança e prosperidade; **Liberdade na Internet:**¹⁵⁸ apoiar as liberdades fundamentais e a privacidade.¹⁵⁹ (ESTADOS UNIDOS, 2011g, p. 17-24, tradução nossa, destaque nosso).

Na área de defesa, especificamente, o documento apontou como objetivos prioritários incentivar um comportamento responsável dos Estados e indivíduos no ciberespaço e estabelecer diretrizes para dissuadir e impedir intervenções maliciosas no ciberespaço (ESTADOS UNIDOS, 2011g, p. 12-13). Diferentemente das estratégias anteriores, a Estratégia Internacional falou, pela primeira vez, sobre o direito de autodefesa (HEALEY, 2013, p. 77-78) e demonstrou, de forma direta, o posicionamento estadunidense de resposta aos ciberconflitos da atualidade:

Quando justificadamente, os Estados Unidos irão responder aos atos hostis no ciberespaço como faria para qualquer outra ameaça ao nosso país. **Reservamo-nos o direito de utilizar todos os meios necessários – diplomáticos, informacionais, militares e econômicos – adequados e compatíveis com o direito internacional aplicável, a fim de defender a nossa nação, nossos aliados, nossos parceiros e nossos interesses.** Ao fazê-lo, vamos esgotar, sempre que possível, todas as opções disponíveis antes de utilizar a força militar, vamos pesar cuidadosamente os custos e os riscos de ação contra os custos da inércia e vamos agir de uma maneira que reflita nossos valores e fortaleça a nossa legitimidade, buscando amplo apoio internacional sempre que possível.¹⁶⁰ (ESTADOS UNIDOS, 2011g, p. 14, tradução nossa, destaque nosso).

¹⁵⁶ “Priorizar a abertura e a inovação na internet; Preservar a segurança e a estabilidade da rede global, incluindo o sistema de nome de domínio (DNS); Promover e aperfeiçoar espaços multilaterais para a discussão de questões relacionadas à governança da internet.” (ESTADOS UNIDOS, 2011g, p. 21-22, tradução nossa).

¹⁵⁷ “Fornecer conhecimento, treinamento e outros recursos necessários para países que procuram desenvolver suas capacidades técnica e de cibersegurança; Desenvolver de forma continuada e compartilhar regularmente as melhores práticas internacionais de cibersegurança; Melhorar a capacidade dos Estados de combater o cibercrime – incluindo treinamento para a aplicação da lei, especialistas forenses, juristas e legisladores; Desenvolver relacionamentos com os tomadores de decisão para melhorar a capacitação técnica, proporcionando um contato regular e permanente com os especialistas e os seus pares do governo dos Estados Unidos.” (ESTADOS UNIDOS, 2011g, p. 22-23, tradução nossa).

¹⁵⁸ “Dar suporte aos atores da sociedade civil em alcançar plataformas confiáveis, protegidas e seguras para as liberdades de expressão e de associação; Colaborar com a sociedade civil e organizações não governamentais para estabelecer salvaguardas que protegem suas atividades na internet contra invasões digitais ilegais; Incentivar a cooperação internacional para a proteção efetiva da privacidade de dados comerciais; Garantir a interoperabilidade de extremo a extremo de uma internet acessível a todos.” (ESTADOS UNIDOS, 2011g, p. 23-24, tradução nossa).

¹⁵⁹ Economy: Promoting International Standards and Innovative, Open Markets; Networks: Enhancing Security, Reliability, and Resiliency; Law Enforcement: Extending Collaboration and Rule of Law; Military: Preparing for 21st Century Security Challenges; Internet Governance: Promoting Effective and Inclusive Structures; International Development: Building Capacity, Security, and Prosperity; Internet Freedom: Supporting fundamental Freedoms and Privacy.

¹⁶⁰ When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests In so doing, we will exhaust all options before military force whenever we can;

Meses após o lançamento da Estratégia Internacional, em julho de 2011, o Departamento de Defesa lançou a Estratégia para Operar no Ciberespaço do Departamento de Defesa (*Department of Defense Strategy for Operating in Cyberspace*)¹⁶¹ (ESTADOS UNIDOS, 2011a) que, para Chen (2013, p. 8), representou, de forma direta, o reconhecimento oficial pelo DoD da importância estratégica do ciberespaço para a segurança nacional, além de comprovar a tendência atual de uma crescente militarização do ciberespaço, como vimos no capítulo anterior (CAVELTY, 2012, p. 103):

Embora as redes e sistemas que compõem o ciberespaço sejam, muitas vezes, de propriedade privada, e primariamente de uso civil, tratar o ciberespaço como um domínio é uma concepção organizadora fundamental para as missões de segurança nacional do DoD. Isso permite que o DoD se organize, treine e se equipe para o ciberespaço como o fazemos no ar, na terra, no mar e no espaço, de forma a dar suporte aos interesses de segurança nacional.¹⁶² (ESTADOS UNIDOS, 2011a, p. 5, tradução nossa).

A estratégia do DoD para proteger os Estados Unidos contra as ameaças ciber emergentes apresentou cinco iniciativas estratégicas de atuação:

1. Tratar o ciberespaço como um domínio operacional [equivalente ao ar, a terra, ao mar e ao espaço] para organizar, treinar e equipar, fazendo com que o DoD tire total proveito do potencial do ciberespaço;
2. Empregar novos conceitos operacionais de defesa para proteger as redes e os sistemas do DoD;
3. Cooperar com outras agências do governo dos EUA e com o setor privado para viabilizar uma estratégia de cibersegurança abrangente;
4. Construir relacionamentos fortes com os aliados e parceiros internacionais dos Estados Unidos para reforçar a cibersegurança coletiva, e,
5. Alavancar a engenhosidade da nação através da capacitação da força de trabalho ciber e de uma rápida inovação tecnológica.¹⁶³ (ESTADOS UNIDOS, 2011a, p. 5-12, tradução nossa).

Para isso, a Estratégia sugere que sejam realizadas operações utilizando todas as capacidades do ciberespaço, que devem concentrar seus esforços: na preservação da

will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

¹⁶¹ Para um estudo aprofundado sobre essa Estratégia veja CHEN (2013).

¹⁶² Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.

¹⁶³ Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential. Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems. Strategic Initiative 3: DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy. Strategic Initiative 4: DoD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity. Strategic Initiative 5: DoD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

capacidade crítica de operação; na realização de treinamentos, exercícios e jogos de guerra; na construção de sistemas capazes de se recuperarem prontamente (resiliência); na criação de medidas que garantam a segurança e a proteção da missão; na realização de uma defesa ativa, ao agir preventivamente contra invasões; na promoção de boas práticas de cibersegurança, como a constante atualização de antivírus e sistemas operacionais; na mitigação dos riscos através de parcerias com o setor privado; no desenvolvimento de armas ciber (*cyber weapons*) através da promoção de inovações tecnológicas; no reforço da cooperação internacional entre os aliados voltada para a dissuasão (*deterrence*) e o compartilhamento da consciência situacional sobre as vulnerabilidades no ciberespaço, através do estabelecimento de alianças e treinamentos internacionais; na promoção de programas que vislumbrem e treinem possíveis futuros ciberguerreiros (ESTADOS UNIDOS, 2011a, p. 5-12).

Como vimos, ao longo da trajetória das Estratégias Nacionais relacionadas com a cibersegurança “Alguns temas foram repetidos várias vezes, tais como a necessidade de cooperação entre os setores públicos e privados, a redução das vulnerabilidades, [a necessidade de] mais treinamento em cibersegurança e cooperação internacional”¹⁶⁴ (CHEN, 2013, p. 2, tradução nossa). Entretanto, apesar da pouca inovação de ideias (CHEN, 2013, p. 45) e da lenta operacionalização das recomendações, o conteúdo das duas últimas estratégias demonstra que os Estados Unidos estão, cada vez mais, incluindo a participação das Forças Armadas nas estratégias de proteção do ciberespaço, buscando, numa parceria constante com o setor privado, estabelecer procedimentos mais eficientes de ação contra as ameaças emergentes, de forma a garantir a predominância de seus interesses nacionais no ciberespaço.

3.3 Operações de Ciberguerra

Como vimos nas doutrinas e estratégias de Ciberguerra estadunidenses, as Operações no Ciberespaço (*Cyberspace Operations*) envolvem uma série de atividades de natureza bastante distintas. A literatura consultada (ANDRESS; WINTERFELD, 2011; LIN, 2012; RID, 2013), conseqüentemente, traz questões bastante variadas sobre essas operações, envolvendo discussões acerca dos efeitos diretos e indiretos dos ciberataques, sua comparação com os ataques cinéticos, os possíveis objetivos dos ciberataques, a importância da inteligência nesses ataques, a complexidade do seu planejamento, a avaliação dos danos etc. Contudo, em meio a essa literatura, Andress e Winterfeld (2011) abordaram de forma mais

¹⁶⁴ Some themes have been repeated often, such as a need for public-private sector cooperation, reduction of vulnerabilities, more cyber security training, and international cooperation.

abrangente e objetiva o conteúdo de que propusemos tratar nesta parte da pesquisa, motivo pelo qual utilizaremos, aqui, sua obra. Vale lembrar, porém, que é praticamente inviável saber que tipos exatos de atividades e ferramentas estão sendo utilizadas, seja pelos Estados Unidos, seja por qualquer outra nação, tendo em vista o grau classificado dessas atividades. Mesmo as revelações em massa feitas no ano passado pelo ex-consultor da NSA, Edward Snowden, sobre o programa PRISM estadunidense não mostram de forma efetiva toda a gama de recursos que é utilizada. Entretanto, de acordo com a literatura consultada (ANDRESS; WINTERFELD, 2011), podemos incluir nesse trabalho breves noções do que seriam essas operações no ciberespaço e que tipo de ferramentas são necessárias para conduzi-las.

De acordo com Andress e Winterfeld (2011), as atividades centrais das operações no ciberespaço que estão relacionadas com as operações de informação estão baseadas em três operações-chave: as operações de coleta de inteligência, as operações de ataque e as operações de defesa (ANDRESS; WINTERFELD, 2011, p. 155-191). Embora a doutrina estadunidense desclassificada atual (JP 3-13) tenha excluído as operações de CNE, CNA e CND do cerne de seu conceito central de Operações no Ciberespaço, essas operações não deixaram de existir (ESTADOS UNIDOS, 2012a). Além disso, a doutrina classificada estadunidense mais recente (PPD-20) fala em operações de coleta ciber, operações de efeitos ciber defensivos, incluindo as contramedidas defensivas não intrusivas, e operações de efeitos ciber ofensivos (ESTADOS UNIDOS, 2012b), confirmando a tendência da centralidade desses três tipos de atividades, motivo pelo qual iremos, aqui, descrevê-las.

As ferramentas ou armas de ciberguerra denominadas, assim, por Andress e Winterfeld (2011, p. 83-152), podem ter natureza lógica (*logical weapons*), física (*physical weapons*) ou psicológica (*psychological weapons*), mas, neste trabalho, iremos nos ater às ferramentas lógicas, por serem aquelas que claramente refletem as capacidades ciber emergentes e cuja operacionalização e funcionalidades ainda estão em processo de construção e aperfeiçoamento. Essas ferramentas, em sua maioria, possuem um caráter dual, ou seja, uma mesma ferramenta pode ser utilizada de forma diferente para propósitos de natureza diferentes, servindo tanto para atacar como para se defender no ciberespaço, motivo pelo qual devem ser observadas sob essas duas perspectivas (ANDRESS; WINTERFELD, 2011, p. 83).

As operações no ciberespaço são conduzidas pelos chamados ciberguerreiros (*cyber warriors*). Pelo fato de ser um campo relativamente novo, a maioria das pessoas que conduzem as operações de ciberguerra hoje não foram, desde sempre, treinadas para fazê-lo (ANDRESS; WINTERFELD, 2011, p. 61). Essas pessoas geralmente possuem graduação e

especialização em ciência da computação, engenharia de computação, tecnologia da informação, segurança da informação e afins, além de certificações profissionais em “segurança da informação [em geral], testes de penetração e investigação forense”¹⁶⁵ (ANDRESS; WINTERFELD, 2011, p. 62), treinamento em tratamento de incidentes, direito, auditoria (ANDRESS; WINTERFELD, 2011, p. 64), bem como conhecimentos doutrinários, estratégicos e operacionais adquiridos na academia militar. Por mais que o campo exija pessoas cada vez mais especializadas nas novas dinâmicas trazidas pelo ciberespaço, em se tratando de guerra, as lições aprendidas com a história e transmitidas por pessoas com experiência militar são imprescindíveis para a formação dos ciberguerreiros (HEALEY, 2013, p. 14).

Nos Estados Unidos, a NSA, Agência de Segurança Nacional (*National Security Agency*) estadunidense verifica currículos de instituições universitárias cadastradas¹⁶⁶ em seus programas e oferece certificados de qualidade para aqueles cursos que alcançam os critérios por ela estabelecidos (ANDRESS; WINTERFELD, 2011, p. 63-64).

As experiências e habilidades para executar operações de ciberguerra diferem em muito das habilidades tradicionais exigidas pelas Forças Armadas, como idade, comportamento, condições físicas e credenciamento. Os ciberguerreiros precisam, de maneira geral, possuir três tipos de habilidades: as de reconhecimento, as ofensivas e as defensivas (ANDRESS; WINTERFELD, 2011, p. 64-69).

As habilidades de reconhecimento podem ser comumente encontradas em pessoas que lidam com soluções de problemas relacionados aos sistemas, aos aplicativos e às redes (ANDRESS; WINTERFELD, 2011, p. 64). Ao possuir o domínio de monitoramento de tráfego de rede passivo (*sniffing*), de análise de pacotes, de mapeamento de redes e sistemas e de investigação forense, por exemplo, o ciberguerreiro será capaz de examinar a infraestrutura, os sistemas de tráfego e os dados dos adversários no campo de batalha virtual (ANDRESS; WINTERFELD, 2011, p. 64).

As habilidades ofensivas podem ser encontradas em *hackers* ou pessoas que trabalham com engenharia de rede e desenvolvimento, ou aquelas que têm por função manter infraestruturas, sistemas e aplicações funcionando, mas cujo objetivo, agora, é derrubá-los (ANDRESS; WINTERFELD, 2011, p. 65).

¹⁶⁵ information security, penetration testing, and forensics

¹⁶⁶ Para uma lista de algumas dessas instituições divulgada em dezembro de 2013, veja o Website da NSA (ESTADOS UNIDOS, 2013d).

As habilidades defensivas podem ser encontradas em administradores de sistemas, realizadores de testes de penetração e engenheiros de rede, por exemplo, embora as habilidades para combater ataques em larga escala ainda sejam bastante limitadas (ANDRESS; WINTERFELD, 2011, p. 65).

3.3.1 Operações de Coleta de Inteligência

A inteligência como atividade é desempenhada no intuito de produzir conhecimentos que serão utilizados para fins variados, mas destinados, principalmente, aos tomadores de decisão de qualquer nível hierárquico governamental. Essa atividade segue uma metodologia própria e consiste em procedimentos de coleta ou busca de informações para que sejam analisadas e, posteriormente, disseminadas (KENT, 1967, p. 147-153 apud MACHADO, 2010, p. 15). A contrainteligência como “função indissociável da inteligência” (GONÇALVES, 2009, p. 60) se perfaz na reunião e análise de dados sobre as capacidades do adversário e suas atividades, bem como na realização de atividades que frustrem ou neutralizem as ações do adversário de forma a proteger a nação (SHULSKY; SCHMITT, 2002, p. 99 apud GONÇALVES, 2009, p. 6; LOWENTAL, 2003, p. 113 apud GONÇALVES, 2009, p. 61).

As operações de coleta de inteligência no ciberespaço consistem em capacidades operacionais viabilizadoras e realizadoras de coleta de informações existentes em computadores, em sistemas de informação ou de comunicação e em redes, sobretudo operações de reconhecimento e monitoramento, efetuadas no ou através do ciberespaço, sem autorização do proprietário ou operador, executadas de forma a inibir sua detecção ou atribuição, com a finalidade de identificar o inimigo, obter informações sobre ele, explorar suas vulnerabilidades, combater e preparar ataques e refinar estratégias de defesa, de forma a dar suporte a todos os tipos de operações militares, sejam elas cinéticas ou informacionais (ESTADOS UNIDOS, 2006a, p. II4-II5, 2012b, p. 2-4; ANDRESS; WINTERFELD, 2011, p. 155-156).

Para Andress e Winterfeld (2011, p. 155), “Tais operações são o equivalente ciber da boa espionagem à moda antiga”¹⁶⁷ e, dessa forma, a maioria delas estão sujeitas a leis e tratados bastante rigorosos, caso sejam descobertas. Porém, afirma Libicki (2009, p. 24), num contexto internacional em que atos de espionagem são praticados por todos os governos, a

¹⁶⁷ Such operations are the cyber equivalent of good old-fashioned spying.

postura de intimidação de uma nação contra essas ações é hipócrita, já que é inconcebível estabelecer políticas dissuasivas sobre práticas que também realizam. Em se tratando de relações entre nações soberanas, os interesses de cada Estado é que vão prevalecer. As recentes revelações feitas pelo ex-consultor da NSA Edward Snowden sobre o programa de monitoramento estadunidense PRISM comprovam esse comportamento. Embora vários chefes de nações tenham se voltado contra o governo dos Estados Unidos, nenhuma ação mais concreta desses países pôde ser tomada no sentido de parar ou punir o comportamento estadunidense. A Casa Branca publicou no dia 17 de janeiro deste ano a Diretiva Política Presidencial 28 (*Presidential Policy Directive 28 – PPD 28*) (ESTADOS UNIDOS, 2014c), que restringe algumas das atividades de coleta de inteligência de sinais, mas deixou claro que elas não serão interrompidas:

Os Estados Unidos devem manter e continuar a desenvolver uma capacidade de inteligência de sinais robusta e tecnologicamente avançada para proteger a nossa segurança e a de nossos parceiros e aliados. Os nossos recursos de inteligência de sinais também devem ser ágeis o suficiente para permitir que nos concentremos em oportunidades fugazes ou crises emergentes e para que enfrentemos não só as questões atuais, mas também os problemas de amanhã, que não somos capazes de prever.¹⁶⁸ (ESTADOS UNIDOS, 2014c, tradução nossa).

As operações de coleta de inteligência no ciberespaço podem ser divididas em duas categorias centrais: operações de reconhecimento (*reconnaissance*) e operações de monitoramento (*surveillance*) (ANDRESS; WINTERFELD, 2011, p. 155).

As operações de reconhecimento podem ser divididas em três grandes categorias: Inteligência de Fontes Ostensivas (*Open Source Intelligence – OSINT*), Reconhecimento Passivo (*Passive Reconnaissance*) e Ameaça Persistente Avançada (*Advanced Persistent Threat – APT*). Esses métodos são geralmente utilizados de forma progressiva, à medida que a obtenção de informações mais específicas e detalhadas se fizer necessária (ANDRESS; WINTERFELD, 2011, p. 157).

As atividades de OSINT constituem o uso de ferramentas de reconhecimento (*reconnaissance tools*)¹⁶⁹ e, até certo ponto, de técnicas de monitoramento de rede (*network*

¹⁶⁸ The United States must preserve and continue to develop a robust and technologically advanced signals intelligence capability to protect our security and that of our partners and allies. Our signals intelligence capabilities must also be agile enough to enable us to focus on fleeting opportunities or emerging crises and to address not only the issues of today, but also the issues of tomorrow, which we may not be able to foresee.

¹⁶⁹ Para informações mais detalhadas sobre ferramentas de reconhecimento (*reconnaissance tools*), tais como “Websites”, “Search Engines”, “Google Hacking”, “The Deep Web”, “Whois”, “DNS”, “Metadata”, “Metagoofil”, “Exiftool”, “Strings” e “Maltego”, veja Andress e Winterfeld (2011, p. 84-94). Essas ferramentas são geralmente utilizadas em combinação umas com as outras, para garantir um melhor resultado (ANDRESS; WINTERFELD, 2011, p. 85).

monitoring tools),¹⁷⁰ de forma a não alertar o alvo de que este está sendo observado ou monitorado (ANDRESS; WINTERFELD, 2011, p. 157).

As ferramentas de reconhecimento

são aquelas que usamos para reunir informações, geralmente em um estado passivo, contra redes e sistemas onde planejamos agir, num sentido lógico. Tais esforços podem incluir a reunião de informações a partir de sites públicos, observação de registros de Servidores de Nome de Domínio (*Domain Name Servers – DNS*), coleta de metadados de documentos acessíveis, obtenção de informações muito específicas com o uso de ferramentas de busca ou qualquer outra de uma série de atividades similares.¹⁷¹ (ANDRESS; WINTERFELD, 2011, p. 84-85, tradução nossa).

Com as ferramentas de reconhecimento é possível ter acesso a uma variedade infinita de informações sobre o alvo, tais como senhas de fácil decodificação, endereços IP das redes em que se encontram localizados, seus nomes de domínio, endereço físico, telefones, nome de alguém diretamente associado ao domínio, uma lista de máquinas associadas ao domínio, a localização do servidor de e-mail; dados sobre dados, como nomes de usuários que criaram, editaram ou armazenaram arquivos, o local onde uma foto foi tirada, o material utilizado para criar uma imagem, a sua localização geográfica através de dispositivos com GPS e dados escondidos em arquivos ou dados que foram deletados (ANDRESS, WINTERFELD, 2011, p. 84-94).

Para se defender contra as ações dessas ferramentas é preciso “limitar as fontes de dados e os dados que estão disponíveis a partir de cada fonte, na medida do possível”¹⁷² (ANDRESS; WINTERFELD, 2011, p. 94, tradução nossa), tendo cuidado para não divulgar informações detalhadas de forma excessiva, não extrapolar o compartilhamento de dados, implementar políticas de divulgação de informações sensíveis, negar a transferência de dados para máquinas desconhecidas, limitar as funcionalidades de edição e visualização de documentos e utilizar ferramentas que controlem o conteúdo compartilhado (ANDRESS; WINTERFELD, 2011, p. 94).

¹⁷⁰ O uso prolongado dessas ferramentas deve ser cauteloso, de forma a não permitir que a atividade seja descoberta (ANDRESS; WINTERFELD, 2011, p. 161).

¹⁷¹ are those that we use to gather information, usually in a passive state, about the networks and systems that we might plan to take action against in a logical sense. Such efforts may include gathering information from public websites, looking up Domain Name Server (DNS) records, collecting metadata from accessible documents, retrieving very specific information through the use of search engine, or any of a number of other similar activities.

¹⁷² limit the sources of data and the data that is available from each source to the greatest extent that is reasonable.

As operações de Reconhecimento Passivo (*Passive Reconnaissance*) consistem no uso de ferramentas de varredura (*scanning tools*)¹⁷³ com o objetivo de “interrogar diretamente uma rede ou sistema a fim de descobrir as suas particularidades.”¹⁷⁴ (ANDRESS, WINTERFELD, 2011, p. 160, tradução nossa). Medidas mais incisivas dentro do ambiente-alvo são executadas com o objetivo de extrair informações sobre ele, os sistemas que o compõem e os detalhes desses sistemas, sem que o alvo, em si, seja afetado (ANDRESS; WINTERFELD, 2011, p. 94, 159-160).

Com as ferramentas de varredura é possível ter acesso a uma variedade infinita de informações sobre o ambiente-alvo, tais como “enumerar os dispositivos de infraestrutura, redes e sistemas ali localizados, avaliar as portas abertas e os serviços que operam nessas portas, identificar configurações de sistemas operacionais e avaliar as vulnerabilidades”¹⁷⁵ (ANDRESS; WINTERFELD, 2011, p. 160, tradução nossa).

Para se defender contra as ações dessas ferramentas é preciso “não enviar o tráfego para fora do sistema de uma forma que seja facilmente visível para os ouvintes não autorizados, não executar serviços em portas padrão, não enviar tráfego não criptografado e qualquer uma de uma série de medidas de proteção semelhantes.”¹⁷⁶ (ANDRESS; WINTERFELD, 2011, p. 100, tradução nossa).

As operações de reconhecimento passivo são distintas das atividades de teste de penetração (*penetration testing*)¹⁷⁷ já que, enquanto os testes de penetração são atividades autorizadas, que não oferecem nenhum risco de retaliação ou contra-ataque e que têm geralmente como alvo final informações superficiais disponibilizadas para esse exercício, no reconhecimento passivo as ações são executadas no ambiente-alvo real, estando sujeitas a todas as dificuldades que ele possa oferecer, bem como a qualquer reação do adversário (ANDRESS; WINTERFELD, 2011, p. 160).

A Ameaça Persistente Avançada (*Advanced Persistent Threat – APT*) “é um ataque organizado e de longo prazo, projetado especificamente para acessar e retirar informações dos

¹⁷³ Para informações mais detalhadas sobre as ferramentas de varredura (*scanning tools*), tais como “Nmap” e “Nessus”, utilizadas para realizar “ping sweeps”, “network mapping”, “port scanning”, “enumeration”, “vulnerability analysis” e “operating system fingerprinting”, veja Andress e Winterfeld (2011, p. 94-100).

¹⁷⁴ involve directly interrogating a network or system, in order to discover its particulars.

¹⁷⁵ enumerate the infrastructure devices, networks, and systems in place in the environment, assess the ports open and services operating on those ports, fingerprint operating systems, and assess vulnerabilities

¹⁷⁶ not sending traffic out in ways that it is easily visible to unauthorized listeners, not running services on standard ports, not sending unencrypted traffic, and any of a number of similar hardening measures.

¹⁷⁷ O teste de penetração (*penetration testing*) é uma operação defensiva, que consiste na intrusão autorizada de forma a que se possa descobrir vulnerabilidades no sistema (ANDRESS; WINTERFELD, 2011, p. 188).

sistemas de destino.”¹⁷⁸ (ANDRESS; WINTERFELD, 2011, p. 162, tradução nossa). Esse tipo de ataque pode ter como finalidade última apenas o reconhecimento, mas devido à sua natureza mais complexa e duradoura também pode ser utilizado como uma atividade de monitoramento (*surveillance*) ou até mesmo como um meio para se conduzir um ataque ofensivo (*assault*) ao alvo final. Para cumprir essas várias utilidades, o ataque APT pode fazer uso de ferramentas de reconhecimento, ferramentas de varredura, ferramentas de acesso e escalonamento (*access and escalation tools*), ferramentas de sustentação (*sustainment tools*) e ferramentas de extração (*exfiltration tools*).

As ferramentas de acesso e escalonamento¹⁷⁹ “estão focalizadas em obter acesso a sistemas e escalar o nível de privilégio assim que forem capazes de acessar o sistema.”¹⁸⁰ (ANDRESS; WINTERFELD, 2011, p. 100, tradução nossa). Elas podem ser capazes de adivinhar ou decodificar senhas e facilitar o acesso a sistemas de forma automatizada (ANDRESS; WINTERFELD, 2011, p. 100-105).

A defesa contra as ações dessas ferramentas, “em grande parte, gira em torno de políticas de implementação de senhas bem escritas, a aplicação de *patches*¹⁸¹ e o fortalecimento do sistema.”¹⁸² (ANDRESS; WINTERFELD, 2011, p. 105, tradução nossa).

As ferramentas de sustentação¹⁸³ são utilizadas para que, depois de acessado, seja possível manter o acesso àquele sistema no futuro. Essas ferramentas são capazes de adicionar usuários ao sistema, adicionar portas de acesso (*backdoors*), criar acesso a aplicações e redes dentro do sistema ou conectar a ele outros sistemas de forma a garantir que se tenha legitimidade para acessá-lo novamente (ANDRESS; WINTERFELD, 2011, p. 109-110).

A defesa contra as ações dessas ferramentas consiste em dificultar a instalação de portas de acesso (*backdoors*) no sistema. Isso pode ser feito através do fortalecimento do sistema, da restrição do tráfego de dados, da limitação de privilégios administrativos do sistema e de uma constante busca no sistema por essas *backdoors* (ANDRESS; WINTERFELD, 2011, p. 110).

¹⁷⁸ is an organized and long-term attack, designed specifically to access and exfiltrate information from the target systems

¹⁷⁹ Para informações mais detalhadas sobre as ferramentas de acesso e escalonamento (*access and escalation tools*), tais como “*Password Tools*”, “*The Metasploit Project*” e “*Immunity CANVAS*”, veja Andress e Winterfeld (2011, p. 100-105).

¹⁸⁰ are focused on gaining access to systems and escalating our level of privilege once we are able to access the system.

¹⁸¹ *Patches* são avanços, otimizações e funcionalidades para correção de erros.

¹⁸² largely revolves around well-written and implemented password policy, patching, and system hardening.

¹⁸³ Para informações mais detalhadas sobre as ferramentas de sustentação (*sustainment tools*), tais como “*Adding ‘Authorized’ Access*” e “*Backdoors*”, veja Andress e Winterfeld (2011, p. 109-110).

As ferramentas de extração¹⁸⁴ têm por objetivo retirar dados de um ambiente-alvo sem que a extração, em si, seja detectada. Essas ferramentas são capazes de diminuir o tamanho do armazenamento de dados para facilitar o seu transporte físico, esconder dados em formatos de difícil visualização, criptografá-los, armazená-los de forma oculta em arquivos comuns, codificar informações e enviá-las através de protocolos comuns e até mesmo retirá-los do alcance de mecanismos de segurança contra atividades suspeitas, utilizando métodos que são incapazes de serem detectados, como tirar uma foto da informação exibida ou imprimi-la em formato de papel (ANDRESS; WINTERFELD, 2011, p. 106-108).

A defesa contra as ações dessas ferramentas consiste na implementação de bases de dados seguras, realizando um controle físico ou lógico mais rígido sobre as atividades das pessoas que transitam dentro do ambiente organizacional (ANDRESS; WINTERFELD, 2011, p. 108).

“A principal diferença entre o reconhecimento e o monitoramento é a de que o reconhecimento tende a significar uma única observação de um determinado ambiente, enquanto o monitoramento implica em uma observação contínua.”¹⁸⁵ (U.S. MARINE CORPS, 2002 apud ANDRESS; WINTERFELD, 2011, p. 161, tradução nossa). O monitoramento do tráfego de voz e dados é geralmente utilizado como base para a detecção de padrões de comportamento suspeitos (ANDRESS; WINTERFELD, 2011, p. 165).

Várias ferramentas utilizadas no reconhecimento podem ser utilizadas também no monitoramento, tomando-se as devidas cautelas, já que seu uso será prolongado. Assim, são utilizadas no monitoramento ferramentas de reconhecimento (*reconnaissance tools*), ferramentas de varredura (*scanning tools*), ferramentas de acesso e escalonamento (*access and escalation tools*), ferramentas de sustentação (*sustainment tools*) e ferramentas de extração (*exfiltration tools*) através do uso de Ameaça Persistente Avançada (*Advanced Persistent Threat – APT*) e demais ferramentas específicas de monitoramento de tráfego de voz¹⁸⁶ e de dados, além de programas de monitoramento em larga escala, como o Echelon,¹⁸⁷

¹⁸⁴ Para informações mais detalhadas sobre as ferramentas de extração (*exfiltration tools*), tais como métodos para facilitar seu transporte físico, o uso de esteganografia ou criptografia para disfarçar os dados, o uso de protocolos comuns que normalmente são autorizados a deixar o ambiente alvo, ou o uso de métodos de saída da banda (*out of band methods*), veja Andress e Winterfeld (2011, p. 106-108).

¹⁸⁵ The major difference between reconnaissance and surveillance is that reconnaissance tends to imply a single observation of a given environment, whereas surveillance implies an ongoing observation.

¹⁸⁶ Como exemplo, podemos citar o monitoramento de tráfego de voz na rede (*voice over IP – Voip*) (ANDRESS; WINTERFELD, 2011, p. 163).

¹⁸⁷ O Echelon é um programa de monitoramento de tráfego de voz e dados em larga escala cujo propósito inicial era monitorar as comunicações da União Soviética com os seus aliados nos anos 1960, mas que atualmente é utilizado para monitorar atividades ligadas ao terrorismo ou tráfico de drogas e coletar inteligência de forma geral (ANDRESS; WINTERFELD, 2011, p. 164).

“a rede de coleta e análise de inteligência de sinais operada pelas partes do Acordo de Segurança EUA-Reino Unido, a saber, Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia”¹⁸⁸ (ANDRESS; WINTERFELD, 2011, p. 161-165, tradução nossa) e o mais recentemente revelado PRISM, programa ultrassecreto dos Estados Unidos iniciado em 2007 e operado pela Agência de Segurança Nacional (*National Security Agency – NSA*) que permite que a comunidade de inteligência dos EUA tenha acesso a dados de alvos que operam fora dos Estados Unidos fornecidos por nove empresas que oferecem serviços na internet: Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube, Skype e AOL (NSA..., 2013b).

3.3.2 Operações Ofensivas

As operações ofensivas no ciberespaço consistem em capacidades operacionais para realizar ciberataques com a finalidade de manipular, interromper, negar, degradar ou destruir computadores, os sistemas de informação ou comunicação e as redes do adversário, bem como as informações ali residentes, de forma a dar suporte a todos os tipos de operações militares, sejam elas cinéticas ou informacionais (ESTADOS UNIDOS, 2006a, p. II4-II5, 2012b, p. 3; ANDRESS; WINTERFELD, 2011, p. 167-178).

Essas atividades são viabilizadas através de operações de reconhecimento, varredura, acesso, escalonamento, extração, sustentação e ofuscação, efetuadas no ou através do ciberespaço, sem a autorização do proprietário ou operador do sistema ou rede, executadas de forma a inibir sua detecção ou atribuição (ANDRESS; WINTERFELD, 2011, p. 167-178).

Nas operações de ofuscação, utilizam-se as ferramentas para ofuscar (*obfuscation tools*):¹⁸⁹ “ferramentas que podemos utilizar para encobrir os nossos rastros quando operando em um sistema ou em um ambiente.”¹⁹⁰ (ANDRESS; WINTERFELD, 2011, p. 113, tradução nossa). Essas ferramentas geralmente tentam ocultar a localização do atacante, através do uso de *Proxy*,¹⁹¹ por exemplo, bem como manipular registros e arquivos, de forma a apagar seus rastros naquele sistema ou rede (ANDRESS; WINTERFELD, 2011, p. 113-116).

Para nos defender, podemos utilizar ferramentas que monitoram a manipulação de arquivos em tempo real, enviando alertas, ou enviar cópias dos registros para locais mais

¹⁸⁸ the network of signals intelligence collection and analysis operated by the parties to the U.S.-UK Security Agreement, namely the United States, Canada, United Kingdom, Australia, and New Zealand.

¹⁸⁹ Para informações mais detalhadas sobre as ferramentas para ofuscar (*obfuscation tools*), tais como “*Tor*”, “*Bitblinder*”, “*Perfect Dark*”, “*I2P*”, o uso de “*Virtual Private Networks – VPN*”, “*log manipulation*”, “*file manipulation*” e “*Tripwire*”, veja Andress e Winterfeld (2011, p. 113-117).

¹⁹⁰ tools that we might use to cover our tracks when operating on a system or in an environment.

¹⁹¹ “Um servidor *proxy* é um computador intermediário situado entre o computador do usuário e a Internet.” (JAVA..., 2014).

seguros contra ataques, de forma a garantir que, se algo for alterado, isso não passará despercebido (ANDRESS; WINTERFELD, 2011, p. 117).

As atividades ofensivas não se configuram como uma nova modalidade de guerra, mas sim como uma nova capacidade para dar suporte às operações militares, assim como todas as outras operações no ciberespaço aqui descritas. Entretanto, são realizadas com maior complexidade e cautela, já que têm um caráter mais intrusivo que as atividades de coleta de inteligência e defesa. A destruição dos sistemas de controle e comando de um adversário, por exemplo, pode resultar em retaliação severa durante uma guerra ou, dependendo do impacto, pode dar fim à mesma, mudando todo o curso de ação (ANDRESS; WINTERFELD, 2011, p. 167-168).

Ciberataques lógicos de um país contra o outro são geralmente mais complexos do que os comumente realizados por *hackers* no dia a dia e também tendem a ser realizados de forma mais lenta, já que necessitam de atividades viabilizadoras que garantam o seu sucesso, como as atividades de reconhecimento, varredura, acesso, escalonamento, extração, sustentação e ofuscação. São direcionados a um alvo específico, geralmente aquele contra o qual se faria um ataque usando os meios convencionais ou contra aquele cujas relações diplomáticas não são tão boas. São provavelmente realizados de forma não isolada, ou seja, são empregados conjuntamente com outras operações militares, como uma capacidade de apoio (ANDRESS; WINTERFELD, 2011, p. 169-170).

Os ataques lógicos podem ser reativos ou proativos. São reativos quando auxiliam na defesa ou na resposta às ações do inimigo. São proativos quando executados com o objetivo de obter condições vantajosas sobre o inimigo, como rendê-lo prontamente quando ele decidir atacar (ANDRESS; WINTERFELD, 2011, p. 169).

A identificação do inimigo pode ser feita através do rastreamento do ataque, observando atentamente o alvo, as fontes do ataque, os atacantes e seus patrocinadores (ANDRESS; WINTERFELD, 2011, p. 156).

Em se tratando de ataques lógicos, utiliza-se “o termo fonte para indicar o ponto inicial a partir do qual o ataque real veio.”¹⁹² (ANDRESS; WINTERFELD, 2011, p. 156, tradução nossa). Essa denominação é pertinente uma vez que a origem dos ataques pode ser camuflada, “devido à relativa facilidade em comprometer um sistema e utilizá-lo como um *proxy* para atacar outro alvo.”¹⁹³ (ANDRESS; WINTERFELD, 2011, p. 156, tradução nossa).

¹⁹² the term source to indicate the endpoint from which the actual attack arrived.

¹⁹³ due to the relative ease of compromising a system and using it as a proxy to attack another target.

Nos ataques diretos, ou seja, “conduzidos diretamente do sistema que está sob controle direto do atacante”¹⁹⁴ (ANDRESS; WINTERFELD, 2011, p. 156, tradução nossa), existe a vantagem de o caminho percorrido ficar livre de conexões potencialmente instáveis, mas nesse tipo de ataque não existe nenhum mecanismo que possa ocultar a sua origem. Descoberta a origem do ataque, o atacante corre o risco de perder a conexão, sofrer retaliação por parte do alvo ou tornar-se um alvo de coleta de informações (ANDRESS; WINTERFELD, 2011, p. 156).

Nos ataques indiretos, ou seja, com o uso de *proxy*, fica mais fácil encobrir a atribuição, já que o atacante pode utilizar um ou vários sistemas diferentes, cada um localizado em regiões geograficamente diferentes, por exemplo, como camadas de proteção, ocultando o sistema de origem. Entretanto, ao utilizar esse tipo de ataque, o atacante também corre riscos não apenas técnicos causados pelas conexões a uma série de sistemas diferentes, mas também de ser descoberto, já que pode ficar exposto aos administradores ou usuários dos sistemas que utilizar (ANDRESS; WINTERFELD, 2011, p. 156-157).

O processo de ataque segue uma sequência de ações que pode variar, mas que geralmente acontece da seguinte forma: reconhecer (*recon*), varrer (*scan*), acessar (*access*), escalonar (*escalate*), extrair (*exfiltrate*), atacar (*assault*) e sustentar (*sustain*), possuindo também a ação de ofuscar (*obfuscate*), que ocorre durante todo o processo de ataque (ANDRESS; WINTERFELD, 2011, p. 170-170).

As ferramentas para reconhecer, varrer, acessar, escalonar, extrair e sustentar são praticamente as mesmas utilizadas nas operações de coleta de inteligência. Entretanto, aqui elas se diferenciam com relação ao objetivo e à profundidade. Enquanto nas atividades de coleta o reconhecimento e monitoramento são feitos para a obtenção de informações de cunho geral sobre o ambiente-alvo, no processo de ataque essas atividades são direcionadas à realização do ataque, em si, possuindo um caráter muito mais específico. Para o ataque, muitas das informações adquiridas quando da coleta de inteligência serão úteis, mas uma análise muito mais detalhada do sistema é necessária para buscar e monitorar dados e vulnerabilidades bem mais específicos, acessar e alcançar níveis de privilégios adicionais dentro do sistema, e facilitar ainda mais a extração de dados que contribuirão para a reconfiguração do sistema de modo que seja possível acessá-lo novamente para, no futuro, realizar o ataque final (ANDRESS; WINTERFELD, 2011, p. 170-178). Durante todo esse processo devem ser utilizadas ferramentas para ofuscar a trajetória percorrida e as ações

¹⁹⁴ conducted directly from the system that is directly controlled by the attacker

realizadas, de modo a evitar não apenas que a origem do ataque seja descoberta, mas, também, que outros atacantes interfiram nessas atividades (ANDRESS; WINTERFELD, 2011, p. 177).

Os efeitos de um ataque lógico podem variar entre dissimulação (*deception*), interrompimento (*disruption*), negação (*denial*), degradação (*degradation*) ou destruição (*destruction*) (ANDRESS; WINTERFELD, 2011, p. 175).

Ataques que visam a dissimulação de dados podem “falsificar comunicações, alterar aquelas que estão em trânsito ou simplesmente fazer com que esse tipo de tráfego desapareça quando estiver a caminho.”¹⁹⁵ (ANDRESS; WINTERFELD, 2011, p. 176, tradução nossa). A crescente dependência da sociedade em relação aos mecanismos de comunicação modernos aumenta o potencial desse tipo de ataque. “No mundo moderno, o computador é rei e não é questionado frequentemente.”¹⁹⁶ (ANDRESS; WINTERFELD, 2011, p. 176, tradução nossa).

Ataques que visam a interrupção de sistemas ou processos sendo executados por esses sistemas, especialmente durante um evento específico, como a execução de uma operação militar, “podem causar pânico e perturbar os usuários e os administradores dos sistemas”¹⁹⁷ envolvidos (ANDRESS; WINTERFELD, 2011, p. 176, tradução nossa).

Ataques de negação de serviço (*Denial of Service* – DoS) e ataques de negação de serviço distribuídos (*Distributed Denial of Service* – DDoS) podem ser facilmente executados contra servidores web, servidores de e-mail e de transferência de arquivos, por exemplo, para sobrecarregar seus sistemas com um grande número de requisições de acesso de forma a inviabilizar o acesso, pelos seus usuários, aos recursos oferecidos (ANDRESS; WINTERFELD, 2011, p. 176).

Ataques que visam degradar podem atingir o desempenho de um sistema, fazendo com que partes dele se tornem esporadicamente inoperativas ou degradar sutilmente os dados produzidos por esse sistema, alterando resultados e decisões (ANDRESS; WINTERFELD, 2011, p. 176).

Ataques que visam a destruição podem “destruir dados, aplicativos ou o sistema operacional do sistema, em nível de *software*, o que poderia ser muito prejudicial no caso de dados valiosos ou sistemas críticos.”¹⁹⁸ (ANDRESS; WINTERFELD, 2011, p. 177, tradução nossa).

¹⁹⁵ falsify communications, alter those that are in transit, or simply make such traffic disappear while en route.

¹⁹⁶ In the modern world, the computer is king and is not often questioned.

¹⁹⁷ can cause panic and disruption among users and system administrators

¹⁹⁸ destroy data, applications, or the operating system of the system in a software sense, which could potentially be very damaging in the case of valuable data or critical systems.

O processo de ataque “é simples, mas para se levar a cabo uma guerra no nível de um Estado-nação é preciso uma grande dose a mais de recursos, esforço e conhecimento.”¹⁹⁹ (ANDRESS; WINTERFELD, 2011, p. 178, tradução nossa).

3.3.3 Operações Defensivas

As operações defensivas no ciberespaço consistem em capacidades operacionais para proteger e defender os computadores, sistemas de informação ou comunicação e as redes governamentais e militares, bem como as informações ali residentes, principalmente as informações sensíveis, contra ações adversas, de forma a evitar que as operações militares ou os interesses nacionais sejam frustrados (ESTADOS UNIDOS, 2006a, p. II4-II5, 2012b, p. 3; ANDRESS; WINTERFELD, 2011, p. 179-191).

A proteção e defesa de informações constantes em computadores, sistemas de informação ou comunicação e redes governamentais e militares, principalmente informações sensíveis, geralmente se baseiam em três princípios básicos: *confidencialidade* (*confidentiality*), *integridade* (*integrity*) e *disponibilidade* (*availability*) (ANDRESS; WINTERFELD, 2011, p. 181-183):

A **confidencialidade** dos dados refere-se a mantê-los fora das mãos das pessoas que não estão autorizadas a vê-los [...]. Em termos de implementações de segurança específicas, isso muitas vezes significa controles de acesso e criptografia de forma a fornecer tais proteções. Ao aplicar essas medidas, é preciso considerar tanto os dados em repouso quanto os dados em trânsito. Dependendo de onde os dados estão em um determinado ponto no tempo, talvez seja necessário usar diferentes controles de segurança ou métodos diferentes dentro de um determinado controle.

[...] Quando queremos proteger a **integridade** dos dados, estamos tentando impedir que eles sejam manipulados de forma não autorizada. [...] podemos usar criptografia para ajudar a assegurar a integridade dos dados, tornando difícil de manipulá-los com sucesso sem a devida autorização. [...] *hashes*²⁰⁰ ou mensagens resumidas [...] muitas vezes são usadas para garantir que as mensagens ou arquivos não foram alterados a partir do original, criando uma impressão digital dos dados originais, que pode ser rastreada com o tempo. Falhas na integridade podem ter efeitos graves se não tivermos consciência de que elas têm acontecido, já que dados em forma de comunicações ou arquivos podem ser livremente alterados para reverter o seu significado ou para alterar o resultado de decisões com base nos dados em questão.

[...] A **disponibilidade** de dados significa, simplesmente, a possibilidade de acessá-los quando for necessário. Assegurar a disponibilidade significa que devemos ser resilientes em face de ataques que podem corromper ou apagar os nossos dados ou nos negar o acesso a eles, atacando o ambiente no qual eles repousam. Isso também significa que nós precisamos ter um ambiente suficientemente robusto para lidar com interrupções do sistema, problemas de comunicação, problemas de alimentação,

¹⁹⁹ is simple, but to carry out warfare at the level of a nation-state requires a great deal more resources, effort, and knowledge.

²⁰⁰ “Um *hash* é um algoritmo em forma matemática que, quando executado em um arquivo ou disco rígido, cria uma assinatura em cadeia de bits ou uma mensagem codificada.” (ANDRESS; WINTERFELD, 2011, p. 220, tradução nossa).

e quaisquer outros problemas que podem nos impedir de acessar os nossos dados. A disponibilidade é muitas vezes realizada através do uso de redundância e *backups* para os nossos dados e para os nossos ambientes.²⁰¹ (ANDRESS; WINTERFELD, 2011, p. 181-183, tradução nossa, destaque nosso).

Para assegurar os dados, também é necessário seguir os princípios de autenticação (*authentication*), autorização (*authorization*) e auditoria (*auditing*). (ANDRESS; WINTERFELD, 2011, p. 182). “Estes são os meios através dos quais podemos controlar e monitorar como os nossos dados estão sendo acessados, e por quem, permitindo-nos, assim, fazer cumprir as políticas que criamos para manter os dados seguros.”²⁰² (ANDRESS; WINTERFELD, 2011, p. 182, tradução nossa).

Autenticar é limitar o acesso de um indivíduo ou sistema a um determinado ambiente ao verificar a sua identidade, através, por exemplo, do uso da combinação de *login* e senha:

Uma das principais chaves para o futuro da autenticação é a utilização de dados biométricos, como impressões digitais, exames de íris e outros meios com base em atributos físicos. Esses identificadores são onipresentes, portáteis e difíceis de falsificar, desde que os sistemas de autenticação sejam adequadamente projetados.²⁰³ (ANDRESS; WINTERFELD, 2011, p. 182-183, tradução nossa).

Autorizar é verificar quais atividades uma determinada identidade pode realizar e, se for preciso, limitá-las. O administrador do sistema, por exemplo, provavelmente pode realizar operações que um usuário comum não está autorizado a executar (ANDRESS; WINTERFELD, 2011, p. 183):

O princípio do menor privilégio afirma que para qualquer camada em um ambiente de computação, como uma pessoa, um processo ou um sistema, a essa camada deve

²⁰¹ The confidentiality of data refers to keeping it out of the hands of those that are not authorized to see it [...]. In terms of specific security implementations, this often means access controls and encryption in order to provide such protections. When applying these measures, we need to consider both data at rest and data in motion. Depending on where the data is at any given point in time, we may need to use different security controls, or different methods within a given control. [...] When we look to protect the integrity of data, we are trying to prevent it from being manipulated in an unauthorized manner. [...] we can use encryption to help provide integrity by making the data difficult to successfully manipulate without the proper authorization [...] hashes or messages digests [...] are often used to ensure that messages or files have not been altered from the original by creating a fingerprint of the original data that can be tracked over time. Failures in integrity can have serious effects if we are not aware that they have happened, as data in the form of communications or files can be freely altered to reverse their meaning or to alter the outcome of decisions based on the data in question. [...] The availability of data simply means that we can access it when we need to do so. Ensuring availability means that we must be resilient in the face of attacks that might corrupt or delete our data or deny us access to it by attacking the environment in which it rests. It also means that we need to have a sufficiently robust environment in order to cope with system outages, communication problems, power issues, and any number of issues that might prevent us from accessing our data. Availability is often accomplished through the use of redundancy and backups for our data and for our environments.

²⁰² These are the means through which we can control and track how our data is being accessed, and by who, thus enabling us to enforce the policies that we have created to keep the data secure.

²⁰³ One of the main keys to the future of authentication is the use of biometric identifiers, such as fingerprints, iris scans, and other means based on physical attributes. Such identifiers are ubiquitous, portable, and difficult to forge, given properly designed authentication systems.

ser dado apenas o nível mínimo de privilégio que é necessário para que ela funcione corretamente. Seguir este princípio evita muitas das questões de segurança comuns que podemos enfrentar.²⁰⁴ (ANDRESS; WINTERFELD, 2011, p. 183, tradução nossa).

Auditar é monitorar as atividades que foram realizadas em um determinado sistema ou ambiente, mantendo um registro do que foi feito. “Isso nos permite equilibrar o carregamento do sistema e da rede de forma correta, bem como monitorar atividades autorizadas, mas inapropriadas ou indesejadas.”²⁰⁵ (ANDRESS; WINTERFELD, 2011, p. 183, tradução nossa).

As operações de proteção e defesa de dados são viabilizadas através de operações de coleta de inteligência e operações ofensivas, efetuadas no ou através do ciberespaço, bem como treinamento e conscientização em segurança, já que “As pessoas representam o que provavelmente é a única maior vulnerabilidade de segurança que temos ou teremos, em qualquer sistema ou ambiente determinado.”²⁰⁶ (ANDRESS; WINTERFELD, 2011, p. 183, tradução nossa).

Para se defender contra um ciberataque é preciso, antes de qualquer coisa, fortalecer o sistema e monitorar as atividades que ali ocorrem. Além disso, devem ser criadas e implementadas políticas satisfatórias de segurança, monitoramento, *data mining*²⁰⁷ e *pattern matching*.²⁰⁸ Tendo em vista que, atualmente, “as redes que compõem a internet não são segmentadas de acordo com as fronteiras nacionais, em sua maior parte”²⁰⁹ (ANDRESS; WINTERFELD, 2011, p. 187, tradução nossa), a detecção e prevenção contra intrusões a níveis satisfatórios ficam bastante prejudicadas. A reestruturação dessas redes é, hoje, algo economicamente inviável e mesmo um monitoramento robusto pode ser falho. No entanto, a rotineira atividade de avaliação de vulnerabilidades e a realização de testes de penetração

²⁰⁴ The Principle of Least Privilege states that for any given layer in a computing environment, such as a person, process, or a system, that layer be given only the minimum level of privilege that is needed for it to operate properly. Following this principle negates many of the common security issues that we might face.

²⁰⁵ This allows us to balance system and network loads properly, as well as monitor for authorized but inappropriate or unwanted activities.

²⁰⁶ People pose what is likely the single largest security vulnerability that we have, or will ever have, in any given system or environment.

²⁰⁷ “*Data Mining* ou Mineração de Dados consiste em um processo analítico projetado para explorar grandes quantidades de dados (tipicamente relacionados a negócios, mercado ou pesquisas científicas), na busca de padrões consistentes e/ou relacionamentos sistemáticos entre variáveis e, então, validá-los aplicando os padrões detectados a novos subconjuntos de dados.” (DATA..., 2014).

²⁰⁸ *Pattern Matching* é o ato de verificação da presença de um padrão em um conjunto de dados. “Padrões são regras para transformar os dados de entrada. Eles são utilizados em toda a linguagem F # para comparar os dados com uma estrutura ou estruturas lógicas, decompor os dados em partes constituintes, ou extrair informações a partir de dados de várias maneiras.” (PATTERN..., 2013).

²⁰⁹ the networks that comprise the Internet are not segmented along national boundaries, for the most part

podem minimizar os riscos de ocorrência de um ataque (ANDRESS; WINTERFELD, 2011, p. 187-188).

No que concerne aos testes de penetração, Andress e Winterfeld (2011, p. 188) explicam que, quando realizados corretamente, podem se assemelhar, em muito, às atividades de um ataque real. Em alguns testes o atacante invade sem que lhe seja fornecida nenhuma informação adicional ao que um atacante normal teria, mas, mesmo nos casos em que o teste seja direcionado a afetar informações específicas, é possível avaliar vulnerabilidades e falhas, desde que as restrições impostas a esse tipo de teste não os tornem inúteis, passando uma falsa ideia de que estamos seguros (ANDRESS; WINTERFELD, 2011, p. 188).

O planejamento de recuperação de desastres (*disaster recovery planning* – DRP) é útil quando não se consegue evitar um ataque, interrupções ou desastres. Quando bem feito, o planejamento pode contribuir para uma rápida recuperação do sistema. Ele é mais bem operacionalizado “através da utilização de *backups* para os nossos dados e através da utilização de diferentes graus de sistemas redundantes e infraestrutura.”²¹⁰ (ANDRESS; WINTERFELD, 2011, p. 188, tradução nossa).

A aplicação do princípio da defesa em profundidade (*defense in depth*) (ANDRESS; WINTERFELD, 2011, p. 179-191) também é bastante útil nas operações de proteção e defesa. Ele consiste na securitização compartimentada das diferentes camadas: a de rede, a de hospedagem, a de aplicações e a de dados. “Podemos ter, como exemplo, *firewalls* e IDS/IPS²¹¹ no nível de rede, *firewalls* e ferramentas *anti-malware* no nível de *host*, controles de acesso no nível de aplicativos e criptografia no nível de dados.”²¹² (ANDRESS; WINTERFELD, 2011, p. 189, tradução nossa). Tendo em vista que a criação de um ambiente impenetrável é impossível, “devemos configurar nossas defesas em camadas, para que possamos diminuir a velocidade de um atacante tanto quanto pudermos, a fim de termos tempo suficiente para detectar e lidar com seus ataques.”²¹³ (ANDRESS; WINTERFELD, 2011, p. 190, tradução nossa).

²¹⁰ through the use of backups for our data and through the use of varying degrees of redundant systems and infrastructure.

²¹¹ IDS/IPS - *Intrusion Detection Systems/Intrusion Prevention Systems* (Sistemas de Detecção de Intrusão/Sistemas de Prevenção de Intrusão) (ANDRESS; WINTERFELD, 2011, p. 187, 202).

²¹² We might have, as an example, firewalls and IDS/IPS at the network level, software firewalls and anti-malware tools at the host level, access controls at the application level, and encryption at the data level.

²¹³ we should configure our layered defenses so that we can slow an attacker as much as we can in order to have time to detect and deal with their attacks.

Por último, dentre as operações de proteção e defesa, faz-se necessário mencionar uma seara ainda pouco conhecida, denominada investigação digital forense (*digital forensics*).²¹⁴ Não obstante seja uma “disciplina da ciência dedicada à reunião e análise sistemática de evidências para demonstrar fatos que podem ser apresentados em tribunais”²¹⁵ (ANDRESS; WINTERFELD, 2011, p. 219, tradução nossa), ela se faz essencial para a defesa de um país. “Embora as evidências acabem não sendo enviadas a tribunais de justiça”²¹⁶, a aplicação dos princípios básicos de investigação digital forense, quando da execução de operações no ciberespaço, pode dar suporte aos tomadores de decisão e “pode representar o que é necessário para se autorizar um contra-ataque (virtual ou físico).”²¹⁷ (ANDRESS; WINTERFELD, 2011, p. 219, tradução nossa).

São princípios básicos da investigação digital forense a preservação de evidências, a coleta e análise constante de evidências, a documentação da investigação e a fundamentação das conclusões (ANDRESS; WINTERFELD, 2011, p. 219).

A investigação digital forense segue quatro passos básicos: preparação, aquisição, análise e relatório. Na preparação, táticas, técnicas, procedimentos, ferramentas e metodologias são desenvolvidas. Na aquisição, faz-se a coleta, preservação e exame da evidência. Na análise, constroem-se fatos a partir das evidências, de forma a tentar descobrir o que de fato aconteceu e, se possível, quem o fez. No relatório, as conclusões são materializadas de forma a facilitar a tomada de decisões (ANDRESS; WINTERFELD, 2011, p. 220).

Atribuir responsabilidade a ciberataques tem sido uma das mais difíceis tarefas desempenhadas no ciberespaço, sendo, “contudo, o aspecto mais importante da ciberdefesa.”²¹⁸ (HEALEY, 2013, p. 265, tradução nossa). Healey (2013, p. 265-266), numa tentativa de atribuir responsabilidade às nações pelo início de alguns dos ciberconflitos da atualidade, quais sejam os ataques à Estônia e à Geórgia e o Stuxnet, apresentou, recentemente, uma análise de atribuição²¹⁹ baseada num “espectro do estado de responsabilidade” (*spectrum of state responsibility*) elaborado pelo Conselho do Atlântico

²¹⁴ Para informações mais detalhadas sobre as ferramentas de análise digital forense, tais como “Encase”, “Forensic Tool Kit” ou “Helix”, veja Andress e Winterfeld (2011, p. 219-222). Para um manual completo sobre as ferramentas de análise digital forense veja Davidoff e Ham (2012).

²¹⁵ the discipline of science dedicated to the systematic gathering and analysis of evidence to establish facts that can be presented in court.

²¹⁶ Although the evidence may not end up in a court of law

²¹⁷ it may be what is needed to authorize a counterattack (virtual or physical).

²¹⁸ yet the most important, aspect of cyber defense.

²¹⁹ Para informações detalhadas sobre essa análise, bem como sobre o espectro do estado de responsabilidade (*spectrum of state responsibility*), veja Healey (2012) e Healey (2013, p. 265-274).

(*Atlantic Council*). Essa análise, de cunho não técnico, está direcionada a identificar que nações estariam mais propensas a ignorar, incentivar ou conduzir ciberataques, correlacionando essas informações com os tipos de ataques que estariam mais propensos a serem patrocinados por governos, de acordo com evidências apoiadas em múltiplas fontes e categorias independentes.

Rid (2013, p. 139-162) também dedicou um capítulo de seu livro para discutir a atribuição. Para Rid (2013), a atribuição é a principal mudança ocorrida entre os conflitos tradicionais e os conflitos digitais e sustenta “que o problema da atribuição, no seu núcleo, é mais um problema político que um problema técnico.”²²⁰ (RID, 2013, p. 140, tradução nossa).

Rid (2013) argumenta que nos conflitos militares tradicionais, com exceção das operações encobertas e do terrorismo, a autoria quase sempre foi revelada (RID, 2013, p. 141). No caso dos cyberconflitos, porém, “a não revelação da atribuição é a regra, não a exceção.”²²¹ (RID, 2013, p. 142, tradução nossa).²²² Isso se deve ao fato de o rastreamento ter uma dimensão territorial que exige a cooperação de várias instituições estrangeiras que nem sempre estão interessadas em cooperar, além de ser tecnicamente difícil de ser realizado e muito menos preciso do que se imagina (RID, 2013, p. 141-146).

Para Rid (2013, p. 153), outra grande questão que limita a atribuição é o fato de se tomar a inteligência produzida como evidência nos mesmos moldes da prova criminal. De acordo com ele,

Os padrões de prova que podem ser alcançados em uma operação de inteligência, sem recursos humanos no terreno, muito menos sem o apoio de agências legais locais, são obrigatoriamente menores do que o ideal – mas as estimativas que são “prováveis” ou “quase certas”, para usar duas das mais altas graduações de inteligência, ainda podem ser suficientes para justificar uma ação política significativa, mesmo uma ação que tenha consequências graves.²²³ (RID, 2013, p. 156, tradução nossa).

Para Rid (2013, p. 162, tradução nossa), “A atribuição é sempre uma questão de julgamento,”²²⁴ e um problema intrinsecamente político, pois “Mesmo que um ataque possa ser atribuído a um determinado Estado, e mesmo que a motivação desse Estado para atacar

²²⁰ that the attribution problem, as its core, is a political problem more than it is a technical problem.

²²¹ non-attribution is the rule, not the exception.

²²² Rid (2013, p. 159-160) atenta para o fato de a natureza dos ciberataques também ser propensa à falsa atribuição que, segundo Libicki (2009, p. 44), pode levar um Estado a atacar outro Estado ou um grupo ou organização de forma equivocada.

²²³ The standards of proof that can be achieved in an intelligence operation without human resources on the ground, let alone without support by local law enforcement agencies, are bound to be lower than ideal – but estimates that are “probable” or “almost certain”, to use two of the highest gradations of intelligence, may still be sufficient to take meaningful political action, even action with serious consequences.

²²⁴ Attribution is always a call of judgment.

pareça clara, a arquitetura técnica, social e política do problema da atribuição dá ao Estado acusado negação plausível”²²⁵ (RID, 2013, p. 161, tradução nossa) que, num contexto internacional, pode ser até desejável para alguns.

Segundo Rid (2013, p. 160), uma investigação digital forense direcionada a encontrar falhas deixadas pelos invasores, a limitação da motivação do ataque, a busca por evidências do planejamento do ataque e a determinação do grau de especialização do ataque podem facilitar a atribuição.

²²⁵ Even if an attack can be traced to a particular state, and even if that state's motivation to attack seems clear, the attribution problem's technical, social, and political architecture gives the accused state sufficient deniability.

4 CIBERGUERRA E A HISTÓRIA DOS CIBERCONFLITOS: MUDANÇAS INSTITUCIONAIS E LIÇÕES APRENDIDAS

Ciberconflitos são novidade, mas não tanto que não tenham acumulado a sua própria história.²²⁶ (HEALEY, 2013, p. 10, tradução nossa).

No segundo capítulo, tentamos esclarecer alguns conceitos apresentando a evolução do debate ciber. No terceiro capítulo, com o intuito de aprofundar esse debate, tentamos tecer breves noções sobre as doutrinas, estratégias e operações de ciberguerra estadunidenses no ciberespaço. Neste capítulo, seguimos no intuito de adentrar um pouco mais no debate, apresentando as principais mudanças institucionais ocorridas nos Estados Unidos relacionadas à ciberguerra, sob a perspectiva histórica dos ciberconflitos (HEALEY, 2013).

Embora tenhamos escolhido trabalhar sob uma perspectiva estadunidense, sabemos que, de certa forma, a história mundial dos ciberconflitos se confunde, em vários aspectos, com a própria história estadunidense desses conflitos²²⁷, uma vez que, pelo seu intenso desenvolvimento tecnológico e consequente crescente vulnerabilidade no ciberespaço, vivenciou vários conflitos que ficaram conhecidos no mundo inteiro, tendo, assim, sido um país pioneiro em criar as primeiras instituições especializadas em combater cada tipo de ameaça no ciberespaço (HEALEY, 2013, p. 13).

O livro *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (em tradução livre, “Um domínio feroz: conflito no ciberespaço, de 1986 a 2012”), editado por Jason Healey (2013), diretor da Iniciativa Política Ciber (*Cyber Statecraft Initiative*) do Conselho do Atlântico dos Estados Unidos (*Atlantic Council of the United States*), ex-vice-presidente da Goldman Sachs²²⁸ e ex-diretor da Política Ciber (*Cyber Policy*) estadunidense na Casa Branca (HEALEY, 2013, p. 14), representa a primeira iniciativa de abordagem histórica dos ciberconflitos, motivo pelo qual iremos nos valer, aqui, desse recurso. As informações editadas por Healey (2013), mesmo possuindo um caráter ostensivo ou desclassificado

²²⁶ Cyber conflict is new, but not so new that it has failed to accumulate its own history.

²²⁷ Para uma lista detalhada dos principais incidentes ciber significativos entre maio de 2006 e setembro de 2013, veja o documento Incidentes Ciber significativos desde 2006 (*Significant Cyber Incidents Since 2006*) produzido pelo Centro para Estudos Estratégicos e Internacionais (*Center for Strategic and International Studies - CSIS*) (SIGNIFICANT..., 2014). Healey (2013, p. 344-349) também apresentou uma linha do tempo da história dos ciberconflitos bastante concisa, que vai de fevereiro de 1970 a maio de 2012. Andress e Winterfeld (2011, p. 273-275) também o fizeram, mas sob uma perspectiva dos eventos que moldaram ou impactaram a cibersegurança, de 1912 a 2010.

²²⁸ “Fundada em 1869, a *Goldman Sachs Groups Inc.* é uma empresa com liderança global em gerenciamento de investimentos que oferece uma grande variedade de serviços financeiros para uma base substancial e diversificada de clientes, incluindo corporações, instituições financeiras, governos e indivíduos com patrimônio líquido elevado. A empresa está sediada em Nova York e mantém escritórios em todos os principais centros financeiros do mundo.” Disponível em: <<http://www.goldmansachs.com/who-we-are/at-a-glance/index.html>>. Acesso em: 01 dez. 2013.

(HEALEY, 2013, p. 12), substanciam, em grande parte, o nosso debate (HEALEY, 2013).

Assim como afirmou o autor,

Felizmente ainda não houve nenhum *feedback* de que as lições da história apresentadas aqui seriam diferentes se tivessem se baseado em fontes classificadas. Este livro foi necessariamente construído em cima de histórias da mídia, informações solicitadas ao FOIA,²²⁹ entrevistas²³⁰ e outros materiais de pesquisa não classificados, e ele fornece, sim, uma visão geral abrangente.²³¹ (HEALEY, 2013, p. 16, tradução nossa).

Segundo Healey (2013, p. 14), ao observar a ainda tão recente história dos ciberconflitos, podemos tirar algumas lições valiosas para o presente e para o futuro. Embora Healey tenha reunido informações que se referem a fatos que vão muito além da nossa aceção de ciberguerra e não obstante esses fatos serem bastante relevantes para compreendê-la, limitamo-nos a relatar apenas aqueles que estão diretamente relacionados a ela, no intuito de permanecer no debate que ora tentamos aprofundar.

²²⁹ FOIA (*Freedom of Information Act*), “Lei de Liberdade da Informação”, é uma lei que dá o direito de acesso à informação contida nos bancos de dados do governo federal dos Estados Unidos. Ela foi promulgada em 4 de julho de 1966 e passou a ter efeito um ano depois. Ela prevê que “qualquer pessoa tem o direito, executável pelos tribunais, de obter acesso aos registros de agências federais, exceto na medida em que tais registros (ou parte deles) estejam protegidos contra a divulgação por uma das nove isenções ou por uma das três exclusões especiais de aplicação da lei. Um pedido FOIA pode ser direcionado a qualquer registro das agências [federais].” (FOIA, 2014) Disponível em: <<http://www.foia.gov/about.html>>. Acesso em: 31 jan. 2014.

²³⁰ Healey (2013, p. 39, 40, 55-63, 79-84) incluiu no livro trechos de entrevistas de várias autoridades que participaram da criação das primeiras unidades ciber (*cyber units*) dos Estados Unidos, como Walter “Dusty” Rhoads, Coronel reformado da Força Aérea dos Estados Unidos (USAF), comandante fundador do 609^o Esquadrão de Guerra de Informações (*609th Information Warfare Squadron*), em 1995; John H. “Soup” Campbell, Tenente General reformado da Força Aérea dos Estados Unidos (USAF), comandante fundador da Força Tarefa Conjunta para a Defesa de Redes de Computadores (*Joint Task Force for Computer Network Defense - JTF-CND*), em 1998 e James D. Bryan, Major General reformado do Exército dos Estados Unidos (USA), comandante fundador da Força Tarefa Conjunta para Operações em Redes de Computadores (*Joint Task Force for Computer Network Operations - JTF-CNO*), em 2000. Essas entrevistas foram colhidas através de um *workshop* realizado pelo Conselho do Atlântico dos Estados Unidos (*Atlantic Council of the United States*) em 5 de março de 2012, cujas transcrições completas podem ser acessadas no website do Conselho (LESSONS..., 2012a). Healey (2013) também incluiu trechos de entrevistas com o Ex-Vice-Diretor Adjunto da Divisão Ciber do FBI (*Federal Bureau of Investigation*), Steve Chabinsky e com o Coordenador de Assuntos Ciber do Departamento de Estado dos Estados Unidos (*US State Department*), Christopher Painter. Essas entrevistas também foram colhidas através de um evento sediado pelo Conselho do Atlântico (*Atlantic Council*), realizado em 16 de maio de 2012, cujas transcrições completas também podem ser encontradas no website do conselho (LESSONS..., 2012b).

²³¹ Fortunately there has been no feedback yet that the lessons from history presented here would be any different if it had relied on classified sources. This book is necessarily built upon on media stories, FOIA requested information, interviews, and other non-classified research material, and it does provide a comprehensive overview.

4.1 Três grandes períodos de mudanças institucionais e políticas ocorridas nos Estados Unidos segundo Healey

Healey (2013, p. 17, 30) considera que existiram, até o presente momento, sete grandes alertas ciber (*cyber wake-up calls*) que marcaram três grandes períodos de mudanças institucionais e políticas nos Estados Unidos:

1. Tomada de Consciência (*Realization*) (1986 a 1998)
 - (1º) Morris Worm
2. Decolagem (*Takeoff*) (1998 a 2003)
 - (2º) ELEGIBLE RECEIVER e SOLAR SUNRISE²³²
 - (3º) MOONLIGHT MAZE
3. Militarização (*Militarization*) (2003 a 2012)
 - (4º) Chinese Espionage
 - (5º) Estonia and Georgia
 - (6º) BUCKSHOT YANKEE
 - (7º) Stuxnet

Esses três grandes períodos podem ser mais bem visualizados no quadro abaixo:

	Tomada de Consciência	Decolagem	Militarização
Data de início	Anos 1980	1998-	2003-
Dinâmicas	O>D: ²³³ Os atacantes possuem vantagem sobre os defensores	O>D: Os atacantes possuem vantagem sobre os defensores	O>D: Os atacantes possuem vantagem sobre os defensores
Quem tem capacidades	EUA e alguns outros	EUA, Rússia e muitos outros	EUA, Rússia, China e muitos e muitos outros
Adversários	<i>Hackers</i>	Hacktivistas, <i>Hackers</i> Patriotas, Vírus e <i>Worms</i>	Neo-Hacktivistas, Agências de espionagem, <i>Malware</i> , Forças Armadas Nacionais, Espiões e seus representantes, Hacktivistas
Incidentes mais importantes	Morris Worm (1998) Cuckoo's Egg (1989) Dutch Hackers (1991) ²³⁴	ELIGIBLE RECEIVER, SOLAR SUNRISE, MOONLIGHT	TITAN RAIN, Estônia, Geórgia, BUCKSHOT YANKEE

²³² De acordo com Healey (2013, p. 23), as Forças Armadas dos Estados Unidos utilizam letras maiúsculas para escrever exercícios e operações militares e, tendo em vista que seu livro conta parte da história militar estadunidense, resolveu seguir o mesmo formato para descrever tais exercícios e operações, motivo pelo qual também utilizaremos esse formato em nosso trabalho.

²³³ O>D (*Offence > Defense*).

	Rome Labs (1994) ²³⁵ Citibank (1994) ²³⁶	MAZE, ALLIED FORCE ²³⁷ , <i>Hackers</i> Patriotas Chineses ²³⁸	
Política motriz/ Políticas	Várias, abrangendo segurança da comunicação, guerra de comando e controle	PDD-63 ²³⁹	HSPD-7/HSPD-23, ²⁴⁰ NSPD/NSPD-54, ²⁴¹ CNCI ²⁴²
Organizações Defensivas dos EUA	CERT, ²⁴³ NSA, ²⁴⁴ Centro de Guerra de Informações da AF ²⁴⁵ (1993), 609º Esquadrão de IW ²⁴⁶ da AF (1995)	JTF-CND, ²⁴⁷ JTF-CNO, ²⁴⁸ USSPACE, ²⁴⁹ NSA, CERT	JTF-GNO, ²⁵⁰ USSTRAT, ²⁵¹ Comando Ciber dos EUA, ²⁵² DHS ²⁵³ /NCSD, ²⁵⁴ NSA e USCERT ²⁵⁵

²³⁴ “*Hackers* holandeses invadiram as redes de mais de 30 instalações militares dos EUA durante a preparação para a primeira Guerra do Golfo. Usando métodos bastante sofisticados, os *hackers* adolescentes da Holanda estavam em busca de informações sobre mísseis, armas nucleares e a operação DESERT SHIELD.” (HEALEY, 2013, p. 344, tradução nossa).

²³⁵ Jovens *hackers* britânicos invadiram o Laboratório da Força Aérea estadunidense localizado em Rome, no estado de Nova York, e utilizaram os sistemas militares estadunidenses para invadir um instituto nuclear coreano. As Forças Armadas dos Estados Unidos ficaram apreensivas com esse incidente, pois poderia ser visto pela Coreia do Norte (país que estava envolvido em difíceis negociações nucleares com os Estados Unidos naquele momento), como um ataque ou ato de espionagem do governo dos Estados Unidos contra a Coreia do Norte e, dessa maneira, levar a uma retaliação (HEALEY, 2013, p. 37).

²³⁶ “Invasões ao Citibank: o hacker russo Vladimir Levin é preso em Londres [no dia 3 de março de 1995] por hackear o Citibank, que perdeu dezenas de milhões de dólares. Isso levou o Citibank a criar o primeiro Diretor de Segurança da Informação (*Chief Information Security Officer*) para supervisionar a segurança das suas redes, uma posição agora comum no mundo todo.” (HEALEY, 2013, p. 344, tradução nossa).

²³⁷ “ALLIED FORCE e Ataques a NATO: A Aliança começou esta operação em 24 de março [de 1999] para expulsar as tropas iugoslavas de Kosovo. No dia 26 de março, o servidor web da NATO ficou indisponível em consequência de ataques de negação de serviço. Muitos outros ataques contra a NATO e membros das Forças Armadas se seguiram, a maioria conduzida por *hackers* patrióticos da Iugoslávia ou da Rússia.” (HEALEY, 2013, p. 346, tradução nossa).

²³⁸ “Durante a Operação ALLIED FORCE, os EUA bombardearam a Embaixada da China em Belgrado. Isso conduziu uma onda de hacktivismo patriota chinês em sistemas de informação do DoD dos EUA e marcou o surgimento da famosa Aliança dos Hackers Vermelhos (*Red Hackers Alliance*).” (HEALEY, 2013, p. 346, tradução nossa).

²³⁹ PPD-63 – *Presidential Policy Directive 63* (Diretiva Política Presidencial 63).

²⁴⁰ HSPD-7 – *Homeland Security Presidential Directive 7* (Diretiva Presidencial de Segurança Interna 7).

²⁴¹ HSPD-23 – *Homeland Security Presidential Directive 23* (Diretiva Presidencial de Segurança Interna 23).

²⁴² NSPD – *National Security Presidential Directive* (Diretiva Presidencial de Segurança Nacional). NSPD-54 – *National Security Presidential Directive 54* (Diretiva Presidencial de Segurança Nacional 54).

²⁴³ CNCI – *Comprehensive National Cybersecurity Initiative* (Iniciativa Global Nacional para a Cibersegurança).

²⁴⁴ CERT – *Computer Emergency Response Team* (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança).

²⁴⁵ NSA – *National Security Agency* (Agência de Segurança Nacional).

²⁴⁶ AF – *Air Force* (Força Aérea).

²⁴⁷ IW – *Information Warfare* (Guerra de Informações).

²⁴⁸ JTF-CND – *Joint Task Force for Computer Network Defense* (Força Tarefa Conjunta para a Defesa de Redes de Computadores).

²⁴⁹ JTF-CNO – *Joint Task Force for Computer Network Operations* (Força Tarefa Conjunta para Operações em Redes de Computadores).

²⁵⁰ USSPACECOM – *US Space Command* (Comando Espacial dos Estados Unidos).

²⁵¹ JTF-GNO – *Joint Task Force for Global Network Operations* (Força Tarefa Conjunta para as Operações em Rede Globais).

²⁵² USSTRATCOM – *US Strategic Command* (Comando Estratégico dos Estados Unidos).

²⁵³ USCYBERCOM – *US Cyber Command* (Comando Ciber dos Estados Unidos).

²⁵⁴ DHS – *Department of Homeland Security* (Departamento de Segurança Interna).

²⁵⁵ NCSD – *National Cyber Security Division* (Divisão Nacional de Cibersegurança).

Organizações Ofensivas dos EUA	Programas de Acesso Especial	JTF-CNO, USSTRAT	JFCC-NW, ²⁵⁶ USSTRAT, Comando Ciber dos EUA
Organizações Coordenadoras	IOTC, ²⁵⁷ CERT, JTRB ²⁵⁸	IOTC, NIPC ²⁵⁹ e ISACs ²⁶⁰	NCRCG, ²⁶¹ SCCs, ²⁶² ISACs, USCERT
Doutrina dos EUA	Guerra de Informações	Operações de Informação	Ciber
Governança dos EUA	Alguns NSC ²⁶³	J-39 ²⁶⁴ , NSC, PCIPB ²⁶⁵	Conselho de Segurança Nacional

Quadro 1. Fases da História dos Ciberconflitos. HEALEY (2013, p. 18, tradução nossa).

4.1.1 Tomada de Consciência (Realization) (1986-1998)

Embora o uso da eletroeletrônica e das tecnologias de telecomunicação e informação na guerra seja bastante antigo e embora a inteligência de sinais (*signals intelligence* – SIGINT)²⁶⁶ tenha avançado tanto a ponto de, na Segunda Guerra Mundial “ter impulsionado o desenvolvimento de computadores eletrônicos programáveis e redes de comunicações”²⁶⁷ (HEALEY, 2013, p. 27, tradução nossa), foi apenas nos anos 1960 que “os Estados Unidos e outros países começaram a perceber”²⁶⁸ as implicações dos primeiros incidentes ciber para a segurança nacional (HEALEY, 2013, p. 27, tradução nossa). Antes disso, “Incidentes envolvendo espionagem, os primeiros vírus de computador e roubo de senhas ocorreram, mas estes [eram] mais bem compreendidos fazendo-se uso de conceitos existentes, tais como guerra eletrônica, inteligência de sinais ou segurança computacional, ao invés de

²⁵⁵ USCERT – *United States Computer Emergency Readiness Team* (Equipe de Respostas a Incidentes de Emergência dos Estados Unidos).

²⁵⁶ JFCC-NW – *Joint Functional Component Command – Network Warfare* (Comando Conjunto de Componente Funcional – Guerra em Rede).

²⁵⁷ IOTC – *Information Operations Technology Center* (Centro de Tecnologia de Operações de Informação).

²⁵⁸ JTRB – *Joint Telecommunications Resources Board* (Conselho Conjunto de Recursos de Telecomunicação).

²⁵⁹ NIPC – *National Infrastructure Protection Center* (Centro de Proteção da Infraestrutura Nacional).

²⁶⁰ ISAC – *Information Sharing and Analysis Centers* (Centros de Compartilhamento de Informações e Análises).

²⁶¹ NCRCG – *National Cyber Response Coordination Group* (Grupo de Coordenação Nacional de Resposta Ciber).

²⁶² SCC – *IT Sector Coordinating Council* (Conselho Coordenador do Setor de TI).

²⁶³ NSC – *National Security Council* (Conselho de Segurança Nacional).

²⁶⁴ J39 – *Information Operations* (Operações de Informação).

²⁶⁵ PCIPB – *President’s Critical Infrastructure Protection Board* (Conselho para a Proteção da Infraestrutura Crítica do Presidente).

²⁶⁶ “SIGINT – informações obtidas a partir da interceptação e decodificação de comunicações e sinais eletromagnéticos.” (CEPIK, 2003, p. 36).

²⁶⁷ pushed forward the development of programmable electronic computers and communication networks.

²⁶⁸ the United States and other nations began to realize

ciberconflitos.”²⁶⁹ (HEALEY, 2013, p. 27, tradução nossa). De acordo com Michael Warner (2012), historiador do Comando Ciber dos Estados Unidos (*US Cyber Command - USCYBERCOM*), acredita-se que o incidente envolvendo um espião da Alemanha do Leste pego pela polícia da Alemanha do Oeste espionando uma subsidiária da IBM em 1968 “poderia muito bem ter sido o primeiro caso no mundo de espionagem informática.”²⁷⁰ (WARNER, 2012, p. 784, tradução nossa).

Healey (2013, p. 27-29), contudo, considera que a fase de Tomada de Consciência (*Realization*) só teve início em 1986 (HEALEY, 2013, p. 27-29). Antes dessa fase foram elaborados relatórios,²⁷¹ exercícios para descobrir vulnerabilidades foram conduzidos²⁷² e criaram-se sistemas de redes militares,²⁷³ mas foi somente depois dos incidentes conhecidos como *Cuckoo's Egg* (1986) e *Morris Worm* (1988) que o governo dos Estados Unidos e suas Forças Armadas passaram a combater de forma mais efetiva os ciberataques.²⁷⁴

O incidente *Cuckoo's Egg*²⁷⁵ aconteceu em agosto de 1986 e foi descoberto por Cliff Stoll que, com a ajuda de alguns colaboradores, dentre eles, Jim Christy, agente especial do Escritório de Operações Especiais da Força Aérea dos EUA (*US Air Force Office of Special Operations*), conseguiu levar os autores a julgamento (HEALEY, 2013, p. 29-30).

O incidente consistiu em um ataque *hacker* de espionagem contra os Estados Unidos, mais especificamente contra a rede militar MILNET. Os *hackers*, localizados em Hanover, na Alemanha, teriam utilizado os computadores do Laboratório Lawrence Berkeley (*Lawrence Berkeley Laboratory – LBL*), um instituto de pesquisas de caráter não classificado, para se conectar à MILNET e roubar informações que, provavelmente, seriam vendidas à KGB (União Soviética). Os responsáveis pela segurança dos computadores no laboratório, ao

²⁶⁹ Incidents involving espionage, early computer viruses, and stolen passwords occurred, but these are best understood using existing concepts, such as electronic warfare, signals intelligence, or computer security, rather than cyber conflict.

²⁷⁰ could well have been the world's first case of computer espionage

²⁷¹ Por exemplo, o relatório “Controles de Segurança para Sistemas de Computador” (*Security Controls for Computer Systems*), elaborado pelo Conselho Científico de Defesa dos Estados Unidos (*US Defense Science Board*) em 1970 (HEALEY, 2013, p. 27-28).

²⁷² Por exemplo, a condução de exercícios pelas Forças Armadas pelos “times vermelhos” ou “times dos tigres” a partir de 1979 (HEALEY, 2013, p.28)

²⁷³ Por exemplo, a criação da MILNET (*Military Network*), Rede Militar dos Estados Unidos, nos anos 1980, antecessora da NIPRNET (*Non-classified Internet Protocol Router Network*), criada nos anos 1990 (HEALEY, 2013, p. 28).

²⁷⁴ Healey (2013), no prefácio, afirma que, embora o incidente *Cuckoo's Egg* tenha sido um importante ciberconflito, ele não o considera como um alerta ciber (*cyber wake-up call*), pois não instigou os Estados Unidos a fazer grandes mudanças institucionais ou políticas, mas incluiu o evento no livro pelo seu significado e para ajudar o leitor a visualizar as semelhanças dos eventos com o passar do tempo.

²⁷⁵ Para saber mais sobre esse incidente, veja STOLL (2013, p. 89-106).

perceberem a intrusão, optaram por rastreá-la a fim de encontrar o invasor, processo que levou quase um ano (STOLL, 2013, p. 89-106; HEALEY, 2013, p. 29-30).

Esse incidente ofereceu ao governo estadunidense a “primeira oportunidade de criar mecanismos para lidar com questões-chave que guiariam as próximas décadas de ciberconflitos”²⁷⁶ (HEALEY, 2013, p. 30, tradução nossa). Os tomadores de decisão, no entanto, se limitaram a responder as questões, nada tendo feito de realmente concreto, além disso (HEALEY, 2013, p. 30), e é por esse motivo que o segundo incidente desse período, *Morris Worm*, foi considerado o primeiro alerta ciber verdadeiro para a cibersegurança, pois resultou na criação do primeiro CERT (*Computer Emergency Response Team*) que, no Brasil, é conhecido como Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança.²⁷⁷ Criado pela *Carnegie Mellon University*, universidade fundada pelo Departamento de Defesa dos Estados Unidos (DoD), o CERT representou o primeiro passo para coordenar as ações de defesa, que, antes desse incidente, eram feitas *ad hoc* (HEALEY, 2013, p. 32).

O incidente *Morris Worm*²⁷⁸ aconteceu em novembro de 1988 e foi resolvido por empresas do setor privado, que possuíam as ferramentas e o conhecimento necessários na época, ao contrário do governo (EICHEN; ROCHILIS, 1989 apud HEALEY, 2013, p. 31). Consistiu em uma brincadeira de um estudante universitário chamado Robert Tappan Morris, que derrubou mais de 10% da internet em muito pouco tempo.

Esses graves incidentes, somados à recente demanda por novas ideias e conceitos gerada pela Revolução da Informação, impulsionaram ainda mais a produção intelectual voltada aos Estudos de Segurança, Defesa e Estratégicos nos anos 1990²⁷⁹ (HEALEY, 2013, p. 34). Conforme vimos no capítulo anterior, essa literatura levou as Forças Armadas a repensar suas missões, doutrinas, estratégias, operações, organizações e instituições a partir do uso das tecnologias digitais, o que ficou conhecido como Revolução nos Assuntos Militares (*Revolution in Military Affairs – RMA*) (HEALEY, 2013, p. 34).

Assim, no governo e nas Forças Armadas passou-se a falar cada vez mais no uso da superioridade informacional na guerra (HEALEY, 2013, p. 33), a considerar o uso de armas

²⁷⁶ first opportunity to tackle key questions that would guide the next decades of cyber conflict

²⁷⁷ Disponível em: <<http://www.cert.br/>>. Acesso em: 16 dez. 2013.

²⁷⁸ Para saber mais sobre esse incidente, veja uma versão editada do relatório elaborado pelo Escritório de Auditoria do Governo dos Estados Unidos (*Government Accountability Office – GAO*) em junho de 1989, disponibilizada no livro editado por Healey (2013, p. 107-119).

²⁷⁹ Healey (2013, p. 34) refere-se mais especificamente à seguinte literatura: *Information Warfare and Security* (DENNING, 1998), *The First Information War: The Story of Computers and Communications in the Persian Gulf War* (CAMPEN, 1992), *Cyberwar: Security, Strategy and Conflict in the Information Age* (CAMPEN; DEARTH; GOODDEN, 1996), *In Athena's Camp: Preparing for Conflict in the Information Age* (ARQUILLA; RONFELD, 1997), *Networks and Netwars: The Future of Terror, Crime and Militancy* (ARQUILLA; RONFELDT, 2001), dentre outros.

ciber em conjunto com o arsenal cinético já existente (HEALEY, 2013, p. 34), a falar na realização de “projetos altamente secretos e compartimentados”²⁸⁰ para começar o desenvolvimento de armas ciber”²⁸¹ (ARKIN, 1999 apud HEALEY, 2013, p. 35, tradução nossa) e, em 1991, ouviu-se pela primeira vez a expressão “Pearl Harbor eletrônico”, dita por Winn Schwartau, especialista em segurança de computadores, ao testemunhar perante o Congresso estadunidense sobre a total desproteção dos sistemas comerciais e governamentais do país (HEALEY, 2013, p. 33).

Em 1993, o Centro de Guerra Eletrônica da Força Aérea (*Air Force Electronic Warfare Center*) foi transformado em Centro de Guerra de Informações da Força Aérea (*Air Force Information Warfare Center*), “com a missão expandida de ‘explorar, aplicar e migrar capacidades ofensivas e defensivas de guerra de informações para operações, aquisições e testes; e fornecer treinamento avançado em IW’”²⁸² (ESTADOS UNIDOS, 2013 apud HEALEY, 2013, p. 35, tradução nossa). Logo em seguida foram criados o Centro de Atividades de Guerra de Informações da Marinha (*Navy Information Warfare Activity*), em 1994, e o Centro de Atividades de Guerra de Informações do Exército (*Army Land Information Warfare Activity*), em 1995 (FREDERICKS, 1996 apud HEALEY, 2013, p. 35).

Somada a esses centros de excelência (*centers of excellence*), em 1995 foi criada a primeira unidade militar de combate ciber no intuito de tentar integrar “a capacidade ciber com as operações militares tradicionais”²⁸³ (HEALEY, 2013, p. 35, tradução nossa). Denominada 609º Esquadrão de Guerra de Informações (*609th Information Warfare Squadron*) foi a “primeira unidade militar a combinar operações ciber ofensivas e defensivas para auxiliar diretamente um comando de guerra, nesse caso o CENTAF (agora AFCENT), o comando da Força Aérea que estava conduzindo as operações de combate contra o Iraque”²⁸⁴ naquela época (ESTADOS UNIDOS, 2013 apud HEALEY, 2013, p. 35, tradução nossa).

Sob o ponto de vista estratégico, em 1996 o Estado-Maior Conjunto das Forças Armadas (*Joint Chiefs of Staff*) elaborou o documento “Visão Conjunta 2010” (*Joint Vision 2010*), que tinha por objetivo fornecer diretrizes capazes de orientar as Forças Armadas para

²⁸⁰ Em 1998 foi criado o Centro Tecnológico de Operações de Informação (*Information Operations Technology Center*) para congregar “capacidades altamente secretas da Célula P42 de Guerra de Informações da NSA’, a Divisão Tecnológica de Defesa Crítica da CIA [e as] ‘operações especiais de tecnologia’ do Pentágono.” (ARKIN, 1999 apud HEALEY, 2013, p. 35, tradução nossa).

²⁸¹ Highly secretive and compartmented projects to start developing cyber weapons

²⁸² with an expanded mission to ‘explore, apply and migrate offensive and defensive information warfare capabilities for operations, acquisition, and testing; and provide advanced IW training’

²⁸³ cyber power with more traditional military operations

²⁸⁴ the first military unit to combine offensive and defensive cyber operations to directly support a war-fighting commander, in this case CENTAF (now AFCENT), the Air Force command conducting combat operations against Iraq.

uma atuação conjunta no futuro, diante das novas tendências trazidas pela Era da Informação (HEALEY, 2013, p. 37-38).

No mesmo ano a Casa Branca criou a Comissão Presidencial para Proteção da Infraestrutura Crítica (*President's Commission on Critical Infrastructure Protection – PCCIP*), cujo relatório contribuiu para o lançamento da Diretiva Presidencial 63 (*Presidential Decision Directive 63 – PDD-63*) de 1998 que, impulsionada por Richard Clarke, então Coordenador Nacional de Segurança, Proteção de Infraestruturas e Contra-Terrorismo (*National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism*) implementou várias recomendações estabelecidas no relatório (HEALEY, 2013, p. 38, 41), sendo, uma delas, a prerrogativa do governo em atuar de forma mais articulada com o setor privado (HEALEY, 2013, p. 54). Essa diretiva deu início ao segundo período de mudanças institucionais e políticas nos Estados Unidos: a fase de Decolagem (*Takeoff*) (HEALEY, 2013, p. 38).

4.1.2 Decolagem (*Takeoff*) (1998-2003)

O período de Decolagem (*Takeoff*) foi marcado primeiramente pelos alertas ciber (*cyber wake-up calls*) ELIGIBLE RECEIVER e SOLAR SUNRISE.²⁸⁵ Operacionalizado em 1997, o exercício de ciberguerra denominado ELIGIBLE RECEIVER (ER 97) serviu não só como treinamento, mas também como um acelerador de mudanças na estrutura organizacional do Departamento de Defesa estadunidense. Realizado pelo time vermelho (*read team*) da NSA, o exercício ELIGIBLE RECEIVER tinha por objetivo penetrar as redes do Departamento de Defesa (DoD) e verificar suas vulnerabilidades (HEALEY, 2013, p. 42).

Em 1998, o ataque real SOLAR SUNRISE às redes desclassificadas do Departamento de Defesa “demonstrou problemas do mundo real previstos pelo ER 97”²⁸⁶ (POULSEN, 2000 apud HEALEY, 2013, p. 42-43, tradução nossa). “As invasões vieram logo depois do ER 97 e foram inicialmente concebidas como precursoras de uma ciberguerra do Iraque de Saddam Hussein.”²⁸⁷ (HEALEY, 2013, p. 345, tradução nossa). Posteriormente, descobriu-se que se tratava de dois adolescentes na Califórnia orientados por um mentor israelense, mas esse incidente representou um importante alerta ciber para os Estados Unidos, pois, além dos problemas comuns de atribuição do ataque, a liderança do Pentágono se viu diante de um

²⁸⁵ Para saber mais sobre esses incidentes, veja MAURER (2013, p. 121-135).

²⁸⁶ demonstrated real world problems predicted in ER 97

²⁸⁷ The intrusions came soon after ER 97 and were initially thought to be the precursors of a cyber war from Saddam Hussein's Iraq.

problema maior: a inexistência de uma autoridade responsável e com atribuições específicas para coordenar uma resposta a esse tipo de incidente (CAMPBELL, 2012 apud HEALEY, 2013, p. 43). Diante disso, foi criada, em dezembro de 1998, a primeira organização conjunta de ciberguerra denominada Força Tarefa Conjunta para a Defesa de Redes de Computadores (*Joint Task Force for Computer Network Defense – JTF-CND*). “Pela primeira vez, alguém foi capaz de emitir comandos para os defensores de computador em outras partes do DoD, em vez de simplesmente pedir a cooperação ou oferecer sugestões.”²⁸⁸ (HEALEY, 2013, p. 44, tradução nossa).

Criada a JTF-CND, a dificuldade maior, então, foi estabelecer uma relação dessa força tarefa defensiva com as forças-tarefas ofensivas até então existentes: as missões do 609º Esquadrão IW, as missões da NSA que, em março de 1997 havia recebido a tarefa de desenvolver técnicas de Ataque a Redes de Computadores (*Computer Network Attack – CNA*) e as missões do Pentágono, que possuía uma agência chamada J-33 ou STOD Divisão Especial de Operações Técnicas (*Special Technical Operations Division - STOD*) criada durante a Guerra Fria (HEALEY, 2013, p. 45).

Em uma tentativa de resolver esse empasse, em outubro de 2000 a JTF-CND deixou de reportar diretamente ao secretário de defesa e passou a ser governada pelo Comando Espacial dos Estados Unidos (*US Space Command*), que tinha ambas as missões ofensivas e defensivas, embora muitos acreditassem que o Comando de Operações Especiais (*Special Operations Command*) é que deveria ter recebido a missão cyber, já que os ciberconflitos eram tão irregulares quanto aqueles atribuídos a essa instituição (HEALEY, 2013, p. 46-47). Tendo em vista essa missão dupla a que foi designada, a JTF-CND passou, então, a se chamar Força Tarefa Conjunta para Operações em Redes de Computadores (*Joint Task Force for Computer Network Operations – JTF-CNO*) (HEALEY, 2013, p. 47), como veremos mais adiante.

O objetivo central do comando JTF-CND não era estabelecer metas para assegurar as redes, mas principalmente defender os Estados Unidos contra as ações de seus adversários no ciberespaço (HEALEY, 2013, p. 44). Para realizar essa missão, o JTF-CND atuou inicialmente em parceria com a Agência de Defesa de Sistemas de Informação (*Defense Information Systems Agency – DISA*) e com o CERT (HEALEY, 2013, p. 44-45). Posteriormente passou a atuar, também, com o Centro de Proteção à Infraestrutura Nacional (*National Infrastructure Protection Center*) do FBI e outros órgãos do governo federal

²⁸⁸ For the first time, someone was able to issue commands to computer defenders elsewhere in the DoD, rather than merely asking for cooperation or providing suggestions.

(HEALEY, 2013, p. 48) que, em breve, se viram diante de outro ciberconflito: o MOONLIGHT MAZE.

Acredita-se que o incidente MOONLIGHT MAZE²⁸⁹ tenha começado em março de 1998 e que tenha durado, pelo menos, três anos. Na época, foi considerado “o primeiro grande caso de ciberespionagem,”²⁹⁰ resultando em invasões a “centenas de computadores da NASA (*National Aeronautics and Space Administration*), do Pentágono e de outras agências do governo, bem como de universidades privadas e laboratórios de pesquisa”²⁹¹ que, aparentemente, teriam sido feitas pela Rússia (ADAMS, 2001 apud HEALEY, 2013, p. 49, tradução nossa). “Os intrusos levantaram milhares de arquivos contendo informações sobre pesquisas técnicas, contratos, técnicas de criptografia e especificações não classificadas dos sistemas de planejamento de guerra do DoD”²⁹² (ELKUS, 2013, p. 155, tradução nossa) sem utilizar a internet, explorando a então dependência do DoD na estrutura (*backbone*) científica-industrial do país (ELKUS, 2013, p. 156).

Esse incidente acarretou mudanças na forma como as redes desclassificadas eram monitoradas (DROGIN, 1999 apud HEALEY, 2013, p. 49-50) e fez com que o Departamento de Defesa alterasse todas as senhas de seus sistemas desclassificados (VERTON, 1998 apud HEALEY, 2013, p. 50). Foi também nesse período que uma célula de inteligência da JTF-CND “desenvolveu uma escala²⁹³ para determinar quão responsável uma nação [poderia ser] por um ciberincidente em particular”²⁹⁴ (HEALEY, 2013, p. 52, tradução nossa), já que, mais uma vez, a atribuição dos ataques havia sido negada.

4.1.3 Militarização (*Militarization*) (2003-2012)

A criação do Departamento de Segurança Interna (*Department of Homeland Security* – DHS) marcou o início do período denominado Militarização (*Militarization*) (HEALEY, 2013, p. 64). O período recebeu essa designação, segundo Healey (2013, p. 64), devido à crescente tendência de intensificação da participação das Forças Armadas e da Comunidade de Inteligência nos assuntos de Cibersegurança, apoiados por inovações desenvolvidas pelo

²⁸⁹ Para saber mais sobre esse incidente veja ELKUS (2013, p. 152-163).

²⁹⁰ the first major cyber espionage case

²⁹¹ hundreds of computers at NASA, the Pentagon, and other government agencies, as well as private universities and research laboratories.

²⁹² The intruders lifted thousands of files, containing information on technical research, contracts, encryption techniques, and unclassified specifications of DoD war-planning systems.

²⁹³ Para maiores detalhes sobre essa escala, veja Healey (2012).

²⁹⁴ developed a scale to determine how responsible a nation was for any particular cyber incident.

setor privado e por agências de segurança civis (HEALEY, 2013, p. 64), tendência que se verifica até os dias de hoje.

O DHS foi criado em resposta aos ataques de 11 de setembro, quando se constatou a falta de integração das agências de segurança domésticas e de suas respectivas funções (HEALEY, 2013, p. 64). Ao “reunir muitas organizações existentes em uma estrutura unificada”²⁹⁵ e ao receber suporte da Casa Branca com a publicação em 2003 da Diretiva Presidencial de Segurança Interna 7 (*Homeland Security Presidential Directive - HSPD-7*) e da Estratégia Nacional para Proteger o Ciberespaço (*National Strategy to Secure Cyberspace*) (HEALEY, 2013, p. 64, tradução nossa), esperava-se que o DHS alcançasse um papel de liderança nos assuntos ciber, o que não ocorreu. Embora tenha coordenado várias iniciativas basilares de proteção da infraestrutura crítica, como a criação da “rede EINSTEIN de detecção de invasões para proteger os sistemas federais,”²⁹⁶ a produção de “documentos importantes, como o Plano de Proteção à Infraestrutura Nacional (*National Infrastructure Protection Plan*) e o Plano Nacional de Respostas a Incidentes Ciber (*National Cyber Incident Response Plan*),”²⁹⁷ outros departamentos, às vezes, destacaram-se mais no que se refere aos assuntos ciber (HEALEY, 2013, p. 64-65, tradução nossa). Além disso, ao lidar com parceiros internacionais, o DoD e as Comunidades de Inteligência estavam “mais equipados e tinham muitos programas ativos, especialmente para compartilhar informações entre os tradicionais parceiros ‘Cinco Olhos’ (*Five Eyes*) Reino Unido, Canadá, Austrália, Nova Zelândia e os Estados Unidos.”²⁹⁸ (HEALEY, 2013, p. 65, tradução nossa). Sendo assim, com “muitas responsabilidades e poucos recursos, o DHS ficou pra trás.”²⁹⁹ (HEALEY, 2013, p. 65, tradução nossa).

Numa tentativa de aperfeiçoar ainda mais as capacidades ciber ofensivas e defensivas, o DoD decidiu separar as missões da JTF-CNO (HEALEY, 2013, p. 65). Embora a princípio tenha-se concluído que a melhor solução fosse reuni-las, o comandante da JTF-CNO já havia identificado que a missão ofensiva travava um pouco a missão defensiva, devido ao caráter sigiloso e classificado da primeira (BRYAN, 2012 apud HEALEY, 2013, p. 65). Sendo assim, em 2003 a missão ofensiva foi transferida para a NSA, sob controle operativo do Comando Estratégico dos Estados Unidos (*US Strategic Command – USSTRATCOM*) (MADDEN

²⁹⁵ brought together many existing organizations under a unified structure

²⁹⁶ the EINSTEIN intrusion detection network to protect Federal systems

²⁹⁷ Important documents like the National Infrastructure Protection Plan and National Cyber Incident Response Plan.

²⁹⁸ better resourced and had very active programs, especially for sharing information between the traditional “Five Eyes” partners of the United Kingdom, Canada, Australia, New Zealand, and the United States.

²⁹⁹ DHS, fell behind with so many responsibilities and few resources.

apud HEALEY, 2013, p. 65) que, em 2004, a acoplou à missão do Comando Conjunto de Componente Funcional – Guerra em Rede (*Joint Functional Component Command – Network Warfare – JFCC-NW*) (HEALEY, 2013, p. 65). Uma das principais razões da NSA ter recebido a missão ofensiva é “não menos pela profundidade do seu conhecimento em assuntos ciber, mas também devido aos seus ‘acessos’ únicos aos sistemas ciber estrangeiros.”³⁰⁰ (HEALEY, 2013, p. 65, tradução nossa). Além disso, seu diretor é um oficial de inteligência sênior, o que lhe garante acesso à Casa Branca, “um privilégio normalmente não estendido aos generais que coordenavam as redes militares”³⁰¹ (RADUEGE, 2012 apud HEALEY, 2013, p. 65, tradução nossa).

Após a missão ofensiva ter sido enviada à NSA (JFCC-NW), a Força Tarefa Conjunta para a Defesa de Redes de Computadores (*Joint Task Force for Computer Network Defense – JTF-CND*) retomou a missão defensiva e, em 2004, passou a ser denominada Força Tarefa Conjunta para as Operações em Rede Globais (*Joint Task Force for Global Network Operations – JTF-GNO*) (HEALEY, 2013, p. 66).

A atmosfera de guerra advinda das invasões ao Afeganistão e Iraque em resposta ao 11 de setembro deu uma “ênfase especial à missão ofensiva”³⁰² (HEALEY, 2013, p. 66, tradução nossa), que culminou com a revelação da operação encoberta (*covert operation*) do vírus Stuxnet, que foi tida como “a maior revelação sobre as capacidades ciber ofensivas estadunidenses”³⁰³ de que se tem conhecimento (HEALEY, 2013, p. 67, tradução nossa).

A missão defensiva, por sua vez, foi direcionada à proteção dos sistemas governamentais, principalmente os militares e os pertencentes à comunidade de inteligência, com o lançamento da Iniciativa Global Nacional para a Cibersegurança (*Comprehensive National Cybersecurity Initiative – CNCI*) na administração Bush, em janeiro de 2008 (HEALEY, 2013, p. 67).

Mesmo com as missões desdobradas, o DoD optou pela “contínua centralização e elevação das capacidades ciber”³⁰⁴ (HEALEY, 2013, p. 73, tradução nossa) e, em 23 de junho de 2009 criou o Comando Ciber dos Estados Unidos (*US Cyber Command – USCYBERCOM*) (ESTADOS UNIDOS, 2009b) como um comando unificado subordinado ao Comando Estratégico dos Estados Unidos (*US Strategic Command – USSTRATCOM*) (HEALEY, 2013, p. 73), que passou a planejar, coordenar, integrar, sincronizar e conduzir

³⁰⁰ not least because of the depth of their expertise in cyber issues, but also due to their unique “accesses” into foreign cyber systems.

³⁰¹ a privilege not normally extended to generals that ran military networks

³⁰² particular emphasis to the offensive mission

³⁰³ the biggest revelation about US offensive cyber capabilities.

³⁰⁴ the continued centralization and elevation of cyber capabilities

atividades de defesa e ataque no ciberespaço, tendo alcançado sua plena capacidade operacional em 31 de outubro de 2010 (ESTADOS UNIDOS, 2011d, p. 25).

As missões defensiva (JTF-GNO) e ofensiva (JFCC-NW), antes coordenadas pela Força Tarefa Conjunta para as Operações em Rede Globais (*Joint Task Force for Global Network Operations – JTF-GNO*) e pelo Comando Conjunto de Componente Funcional – Guerra em Rede (*Joint Functional Component Command – Network Warfare – JFCC-NW*), respectivamente (ESTADOS UNIDOS, 2011d, p. 25), permaneceram como o núcleo do Comando Ciber dos Estados Unidos (USCYBERCOM), cujo comando, até fevereiro de 2014, ficou nas mãos do General Keith B. Alexander, também diretor da Agência de Segurança Nacional (*National Security Agency – NSA*)³⁰⁵ (ANDRESS; WINTERFELD, 2011, p. 39).

O USCYBERCOM, além de receber as missões defensivas e ofensivas passou a coordenar as atividades ciber desempenhadas pela aeronáutica (24ª Força Aérea – *24th Air Force/AFCYBER*), pelo exército (Comando Ciber do Exército – 2º Exército - *Army Cyber Command – 2nd Army/ ARFORCYBER*), pela frota naval (Comando Ciber da Frota Naval - 10ª Frota – *Navy Fleet Cyber Command – 10th Fleet/FLTCYBERCOM*) e pela marinha (Comando Ciber das Forças Marítimas – *Marine Forces Cyber Command/MARFORCYBER*) (ESTADOS UNIDOS, 2011d, p. 143):

Os esforços do USCYBERCOM também darão suporte à habilidade das Forças Armadas em conduzir de forma segura, em ritmo acelerado, operações eficazes, bem como proteger os sistemas de comando e controle e a infraestrutura do ciberespaço dando apoio às plataformas de sistemas de armas contra interrupções, invasões e ataques.³⁰⁶ (ESTADOS UNIDOS, 2011d, p. 143, tradução nossa).

Essas forças têm como objetivos, dentre outros, “desenvolver e aprimorar a consciência situacional sobre o ciberespaço”³⁰⁷ (AFCYBER), desenvolver a doutrina ciber (ARFORCYBER) e dar ênfase a processos centrados de informação baseados em tecnologias autônomas (FLTCYBERCOM) (ANDRESS; WINTERFELD, 2011, p. 39-41, tradução nossa).

Embora ainda esteja subordinado ao Comando Estratégico dos Estados Unidos (*US Strategic Command – USSTRATCOM*), o USCYBERCOM tem atuado cada vez mais no

³⁰⁵ No dia 30 de janeiro de 2014 o secretário de defesa anunciou Michael S. Rogers, vice-almirante da marinha, como o novo nomeado para comandar o USCYBERCOM, bem como para atuar como diretor da NSA e do Serviço de Segurança Central (*Central Security Service*). Se confirmado pelo senado, ele vai substituir o General Keith Alexander, que foi diretor da NSA desde 2005 e comandante do USCYBERCOM desde 2010. (ESTADOS UNIDOS, 2014a).

³⁰⁶ USCYBERCOM’s efforts will also support the Armed Services’ ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks.

³⁰⁷ developing and improving cyberspace situational awareness

sentido de se tornar um “comando combatente autônomo”³⁰⁸ (HEALEY, 2013, p. 74, tradução nossa).

Healey (2013, p. 74) acredita que o USCYBERCOM tenha sido a maior mudança institucional ciber ocorrida nos Estados Unidos desde a criação do DHS, mas reconhece que várias outras mudanças institucionais também ocorreram durante esse período. A título de exemplo, destaca a criação, em 2009, do Centro Integrado Nacional de Cibersegurança e Comunicações (*National Cybersecurity and Communications Integration Center – NCCIC*), a criação de um Coordenador para Assuntos Ciber dentro da estrutura diplomática e a criação de um novo cargo dentro do Pentágono para lidar especificamente com a política ciber de segurança nacional (HEALEY, 2013, p. 74-75).

Todas essas mudanças vieram como respostas aos vários incidentes ciber que continuavam a acontecer em todo o mundo (HEALEY, 2013, p. 73).

A onda de Espionagem Chinesa³⁰⁹ atingiu agências governamentais, empresas privadas e grupos de pesquisa (*think tanks*) nos Estados Unidos, no Canadá, na Alemanha, no Reino Unido e em vários outros países (HEALEY, 2013, p. 68-69). A invasão TITAN RAIN envolveu o roubo de informações do DoD e do DHS, *GhostNet* foi uma invasão que envolveu espionagem aos escritórios do Dalai Lama, a invasão *Shadows in the Cloud* hackeou embaixadas e alvos de interesse chineses, e a invasão *Night Dragon* espionou companhias energéticas globais. Muitas dessas invasões se deram a partir de dados protegidos pela empresa RSA,³¹⁰ que produz equipamentos de criptografia e segurança para empresas e governos no mundo inteiro (HEALEY, 2013, p. 68-69). Nos Estados Unidos, a RSA “ajuda a defender as redes da Casa Branca, da Agência Central de Inteligência (*Central Intelligence Agency – CIA*), da Agência de Segurança Nacional (*National Security Agency - NSA*), do Pentágono, do Departamento de Segurança Interna e da maioria das empresas top de defesa”³¹¹ no país (SEGAL, 2013, p. 167, tradução nossa).

A Rússia, “embora certamente engajada em ciberespionagem assim como a China, [ficou] mais conhecida por ignorar, encorajar e coordenar seus *hackers* patriotas”³¹² na

³⁰⁸ a stand-alone combatant command

³⁰⁹ Para saber mais sobre esses incidentes veja SEGAL (2013, p. 165-173).

³¹⁰ RSA. Disponível em: <<http://www.emc.com/domains/rsa/index.htm>>. Acesso em: 01 fev. 2014.

³¹¹ helps defend networks at the White House, the Central Intelligence Agency, the National Security Agency, the Pentagon, the Department of Homeland Security, and for most top defense contractors.

³¹² Para saber mais sobre os primeiros *hackers* patriotas veja DIAMOND (2013, p. 136-151).

condução de ciberconflitos contra a Estônia em 2007 e contra a Geórgia, um ano depois.”³¹³ (HEALEY, 2013, p. 69, tradução nossa).

O incidente na Estônia,³¹⁴ como vimos no segundo capítulo, consistiu em ataques DDoS a websites do governo, instituições financeiras e à conectividade nacional de maneira geral, fazendo com que seus sistemas operacionais entrassem em colapso (TIKK; KASHA; VIHUL, 2010 apud HEALEY, 2013, p. 70). De acordo com Healey (2013, p. 70), embora esses ataques tenham sido considerados um desastre ciber (*cyber disaster*), na verdade representaram uma vitória para a Estônia, que conseguiu publicidade bastante para garantir a hospedagem do Centro de Excelência para a Cooperação em Defesa Ciber (*Cooperative Cyber Defence Centre of Excellence – CCDCOE*)³¹⁵ da NATO em seu território (HEALEY, 2013, p. 70).

É interessante notar que, na época, nem o governo da Estônia nem os governos aliados foram capazes de mitigar o impacto do conflito, que só foi possível com a ajuda do setor privado (HEALEY, 2013, p. 71). De acordo com Healey (2013, p. 71, tradução nossa), na falta de uma resposta governamental adequada, “esse tipo de habilidade é necessária e externada todos os dias por defensores do setor privado”³¹⁶ que, embora não disponham da robustez financeira e laboral existentes nas organizações de defesa estatais, têm desempenhado um papel importante no combate aos ciberconflitos da atualidade.

“O ciberconflito contra a Geórgia³¹⁷ coincidiu com a invasão russa do país em agosto de 2008 devido a uma disputa sobre a região separatista da Ossétia do Sul.”³¹⁸ (HEALEY, 2013, p. 71, tradução nossa). O incidente consistiu em ataques DDoS a websites do governo e de empresas privadas, assim como na Estônia, e teve como auge a incapacidade das lideranças da Geórgia de utilizar a internet para se comunicar internamente e internacionalmente³¹⁹ (HEALEY, 2013, p. 71).

Também em 2008 o governo estadunidense se viu diante de outro alerta ciber (*cyber wake-up call*), “um incidente que envolveu redes classificadas e desclassificadas do Comando

³¹³ Russia, though certainly engaged in cyber espionage like China, is better known for ignoring, encouraging or coordinating its patriotic *hackers* to conduct cyber conflicts against Estonia in 2007, and Georgia a year later.

³¹⁴ Para saber mais sobre esse incidente veja SCHMIDT (2013, p. 174-193).

³¹⁵ CCDCOE - Disponível em: <<https://www.ccdcoe.org/>>. Acesso em: 01 fev. 2014.

³¹⁶ this kind of ability is required and displayed everyday by private sector defenders

³¹⁷ Para saber mais sobre esse incidente veja HAGEN (2013, p. 194-204).

³¹⁸ The cyber conflict over Georgia coincided with the Russian invasion of the country in August 2008 over a dispute regarding the breakaway region of South Ossetia.

³¹⁹ Diferentemente da Estônia, que possuía um Ponto de Troca de Tráfego (*Internet Exchange Point – IXP*), o que possibilitou ao país a manutenção da sua comunicação interna, a Geórgia não possuía tal Ponto e foi obrigada a se desconectar não só internacionalmente, mas também nacionalmente, a fim de interromper os ataques (HEALEY, 2013, p. 72).

Central (*Central Command* – CENTCOM)³²⁰ (HEALEY, 2013, p. 72, tradução nossa), mais especificamente a rede SIPRNET, “utilizada para transmitir comandos operacionais”³²¹ e a rede JWICS, “utilizada para o [compartilhamento de] material de inteligência da mais elevada classificação”³²² (HEALEY, 2013, p. 73, tradução nossa), cuja resposta estadunidense resultou na Operação BUCKSHOT YANKEE,³²³ que combateu a ameaça. De acordo com Grindal (2013, p. 205),

No verão de 2008, um pen drive infectado, possivelmente deixado em um estacionamento ou colocado em uma pasta, foi inserido em um laptop militar dos EUA em uma base no Oriente Médio. O vírus tecnicamente avançado armazenado no *pendrive* penetrou o intervalo de interrupção (*air gap*) que separa as redes seguras dos militares a partir da internet como um todo, infectando ambas as redes classificadas e não classificadas. Uma vez fora do intervalo, o *malware* rapidamente se replicou em toda a rede ao infectar *drives* adicionais, levando o pessoal a espalhar o vírus involuntariamente ainda mais.³²⁴ (GRINDAL, 2013, p. 205, tradução nossa).

No ano de 2010, a organização *Wikileaks*,³²⁵ liderada por Julian Assange, desencadeou um processo de vazamento de uma enorme quantidade de documentos confidenciais do governo estadunidense, causando a primeira crise das instituições ciber nos Estados Unidos, com consequências políticas significativas para os EUA e alguns de seus aliados. Embora a natureza inicial do vazamento não tenha tido o caráter de um ciberconflito, evoluiu para tal, uma vez que a organização *Anonymous* “iniciou uma série crescente de ataques prejudiciais em apoio à *Wikileaks*”³²⁶ (HEALEY, 2013, p. 75, tradução nossa).

“Entretanto, foi o vírus Stuxnet,³²⁷ em meados de 2010, que trouxe o alarme mais profundo para os profissionais de cibersegurança”³²⁸ (HEALEY, 2013, p. 75, tradução nossa), materializando a tendência atual de “aparente inclinação das nações para se engajarem em campanhas encobertas umas contra as outras”³²⁹ (HEALEY, 2013, p. 75, tradução nossa):

³²⁰ an incident involving unclassified and classified networks of the war-fighting Central Command.

³²¹ used for passing operational commands

³²² used for the highest classification intelligence material.

³²³ Para saber mais sobre esse incidente veja GRINDAL (2013, p. 205-211).

³²⁴ In the summer of 2008 an infected thumb drive, possibly dropped in a parking lot or slipped into a briefcase, was inserted into a US military laptop on a base in the Middle East. The technically advanced virus stored on the USB stick penetrated the air gap that separates the military's secure networks from the Internet at large, infecting both classified and unclassified networks. Once beyond the gap, the malware rapidly replicated throughout the network by infecting additional thumb drives, leading personnel to unintentionally spread the virus further.

³²⁵ Wikileaks - Disponível em: <<http://wikileaks.org/>>. Acesso em: 01 fev. 2014.

³²⁶ began a series of increasingly damaging attacks in support of *Wikileaks*

³²⁷ Para saber mais sobre esse incidente, bem como sobre os vírus Duqu e Flame, veja MORTON (2013, p. 212-231).

³²⁸ However, it was the Stuxnet virus in mid-2010 that instilled the deepest alarm to cybersecurity professionals.

³²⁹ the apparent willingness of nations to engage in covert campaigns against each other

O Stuxnet surgiu no cenário mundial no verão de 2010 como a peça mais sofisticada de *software* malicioso já encontrada. Projetado para danificar permanentemente centrífugas de gás de enriquecimento de urânio iranianas, o Stuxnet representou um salto quântico em termos de complexidade e audácia em ciberconflitos. O *malware* deixou perplexos não só os pesquisadores, com a sua capacidade de penetrar e mutilar o programa sensível de enriquecimento nuclear de um regime secreto, mas também especialistas em segurança devido à destruição impetuosa de parte da infraestrutura crítica de uma nação. Com o surgimento dos vírus de computador Duqu e Flame³³⁰, a revelação de uma campanha virtual secreta americana (de codinome OLYMPIC GAMES) contra o Irã e o reconhecimento da comunalidade entre essas três peças de *malware*, o Stuxnet se tornou conhecido como a peça central de uma ampla campanha, que pode dar-nos uma ideia de como será o futuro da guerra³³¹ (MORTON, 2013, p. 212, tradução nossa).

Assim, intitulada OLYMPIC GAMES, a operação encoberta que criou e lançou o vírus Stuxnet contra as usinas nucleares iranianas foi atribuída a Israel e Estados Unidos (SANGER, 2012 apud HEALEY, 2013, p. 76), o que abriu um amplo debate sobre as operações ciber ofensivas estadunidenses e colocou em cheque a mais recente estratégia ciber dos Estados Unidos, a Estratégia Internacional para o Ciberespaço (*International Strategy for Cyberspace*) (2011), que sustenta uma postura responsável dos governos em relação ao ciberespaço (HEALEY, 2013, p. 76-77).

Atualmente, as instituições ciber estadunidenses vivenciam mais uma crise. Em junho de 2013, através de informações vazadas por Edward Snowden, ex-consultor da NSA, os jornais *The Washington Post* e *The Guardian*³³² publicaram inúmeras revelações³³³ sobre atividades secretas do governo dos Estados Unidos. Dentre elas, a coleta massiva de metadados telefônicos dos cidadãos americanos, o programa de monitoramento estadunidense em larga escala (recentemente compartilhado com o Reino Unido) denominado PRISM, a espionagem a empresas estrangeiras e a comunicação de alguns chefes de governo (NSA...,

³³⁰ “Duqu é um Trojan de Acesso Remoto (RAT) projetado especificamente para reunir inteligência sobre a infraestrutura industrial e adquirir documentos de design, que poderiam permitir um futuro ciberataque contra os sistemas.” (HEALEY, 2013, p. 219, tradução nossa). “Flame é um tipo de *malware* que copia textos, grava áudios e deleta arquivos de computadores que hackeia.” (VALERIANO; MANESS, 2012).

³³¹ Stuxnet emerged on the world stage in the summer of 2010 as the most sophisticated piece of malicious software ever found. Designed to permanently damage Iranian uranium enrichment gas centrifuges, Stuxnet represented a quantum leap in complexity and audacity in cyber conflict. Not only did the malware astonish researchers with its ability to penetrate and cripple a secretive regime's sensitive nuclear enrichment program, it also concerned security experts due to its brash destruction of part of a nation's critical infrastructure. With the emergence of the Duqu and Flame computer viruses, the revelation of a covert American cyber campaign (code-named OLYMPIC GAMES) against Iran, and the recognition of commonality between the three pieces of malware, Stuxnet became known as the centerpiece of a broader campaign, one that might hint at the future of warfare.

³³² Em novembro de 2013 o jornal *The Guardian* criou uma página denominada “Arquivos da NSA: desclassificados. O que as revelações significam para você” (*NSA Files: Decoded. What the revelations mean for you*) com o objetivo de esclarecer o significado das revelações, apresentar o debate que elas originaram nos Estados Unidos e no mundo, mostrar entrevistas com especialistas, membros e ex-membros do governo estadunidense, além de postar o conteúdo dos arquivos revelados (NSA..., 2013a).

³³³ Para uma linha do tempo sobre as revelações, veja Gidda (2013).

2013a). Essas revelações têm gerado debates³³⁴ sobre o comportamento não responsável do governo estadunidense no ciberespaço, que atenta contra as liberdades civis e o direito de privacidade de milhares de pessoas em todo o mundo, evidenciando, também, o desenvolvimento avançado das capacidades ciber ofensivas pelos Estados Unidos.

4.2 Lições aprendidas e breves reflexões

Para este trabalho, tão ou mais importante que detalhar os ciberconflitos ou a criação e modificação de algumas instituições estadunidenses-chave de ciberguerra, é compartilhar as lições explicitadas por Healey (2013) advindas desse processo, bem como fazer breves reflexões nossas sobre o mesmo, que serão apresentadas nas nossas considerações finais.

A história dos ciberconflitos sob a perspectiva dos Estados Unidos foi marcada, até agora, por disputas institucionais (HEALEY, 2013, p. 30), excesso de sigilo (HEALEY, 2013, p. 30), desconhecimento técnico (HEALEY, 2013, p. 29), inércia burocrática (HEALEY, 2013, p. 30), transformações organizacionais (HEALEY, 2013, p. 35), rigorosa classificação de informações (HEALEY, 2013, p. 36), dúvidas quanto a retaliação (HEALEY, 2013, p. 37), escolhas equivocadas (HEALEY, 2013, p. 41-42), dificuldades na atribuição (HEALEY, 2013, p. 43), disputas e complexidade em interligar comandos (HEALEY, 2013, p. 45-47), contradições no uso de termos e conceitos (HEALEY, 2013, p. 45), mudança de paradigma na contratação de pessoal (HEALEY, 2013, p. 53), falhas em atingir os propósitos das instituições criadas (HEALEY, 2013, p. 64), mudanças operacionais estratégicas (HEALEY, 2013, p. 65-66) e vários alertas ciber que fizeram com que o governo dos Estados Unidos, aos poucos, criasse e modificasse várias de suas instituições e políticas (HEALEY, 2013).

Dessa história surgiram algumas lições que Healey assim sintetiza:

1. Os ciberconflitos mudaram apenas gradualmente ao longo do tempo; assim, lições históricas derivadas de casos passados ainda são relevantes hoje (embora elas sejam frequentemente ignoradas).
2. A probabilidade e consequências dos ciberconflitos destrutivos têm sido muitas vezes exageradas, enquanto os impactos reais das invasões ciber têm sido consistentemente subestimados.
3. Quanto mais estratégico um ciberconflito é, mais ele se assemelha aos conflitos na terra, no ar ou no mar – com uma exceção crítica, [qual seja, a presença significativa do setor privado nas novas dinâmicas do ciberespaço]. (HEALEY, 2013, p. 10, 15, tradução nossa)³³⁵

³³⁴ A título de exemplo, especialistas recentemente discutiram esse assunto no Fórum Econômico Mundial (*World Economic Forum*) que ocorreu em Davos, Suíça, em janeiro de 2014, cujo vídeo do painel intitulado *The Big Brother Problem* pode ser encontrado no website do Fórum. (THE BIG..., 2014)

³³⁵ 1. Cyber conflict has changed only gradually over time; thus, historical lessons derived from past cases are still relevant today (though these are usually ignored). 2. The probability and consequences of disruptive

Essas lições, porém, têm sido frequentemente ignoradas e, de acordo com Healey, isso se deve ao fato de a “A história ciber [ter] sido esquecida, ignorada como irrelevante ou intencionalmente falsificada.”³³⁶ (HEALEY, 2013, p. 10, 14, tradução nossa). Enquanto os treinamentos em outras áreas relacionadas com a segurança nacional, como a diplomacia e Forças Armadas, têm ensinado aos novatos a aprender com os erros passados através de um estudo formal da história, aos novos ciberguerreiros nenhuma história dos ciberconflitos tem sido ensinada, pelo contrário; os treinamentos têm sido direcionados para o futuro (HEALEY, 2013, p. 11, 14). De fato, as dinâmicas no ciberespaço, principalmente as técnicas e as táticas, em grande parte diferem daquelas exercidas na terra, no ar ou no mar,

Mas, em se tratando de segurança internacional, o mantra “esqueça tudo” está simplesmente equivocado. As verdades técnicas tão cruciais para os defensores da rede são muito menos importantes quando separadas daquelas de comandantes e tomadores de decisão encarregados do tratamento de crises de segurança nacional.³³⁷ (HEALEY, 2013, p. 11, tradução nossa).

Segundo Healey (2013, p. 11), é preciso que a história dos ciberconflitos seja ensinada para impedir não só que os esforços desnecessários ou improvisados do passado sejam repetidos, mas para que reflexões sejam feitas acerca desses acontecimentos. Segundo Healey (2013, p. 15), “em grande medida, os problemas enfrentados hoje se refletem em grande parte, ou são exatamente os mesmos que aqueles enfrentados pela geração anterior.”³³⁸ (HEALEY, 2013, p. 15, tradução nossa).

Para Healey (2013, p. 16), “Uma série de fatores têm contribuído para ocultar não apenas as lições importantes da história ciber, mas também o fato de que existe uma história dos ciberconflitos”³³⁹ (HEALEY, 2013, p. 16, tradução nossa): o primeiro deles é a entrada massiva de um grande número de profissionais no campo, o segundo, as divergências de pensamento entre tecnologistas e especialistas em assuntos de segurança nacional e internacional e, o terceiro, os efeitos maléficos do sigilo governamental.

cyber conflicts have often been hyped, while the real impacts of cyber intrusions have been consistently under-appreciated. 3. The more strategically a cyber conflict is, the more similar it is to conflicts on the land, in the air, or on the sea - with one critical exception.

³³⁶ Cyber history has been forgotten, ignored as irrelevant, or intentionally falsified

³³⁷ But at the level of international security, the “forget everything” mantra is simply wrong. The technical truths so crucial to network defenders are far less important when abstracted up to commanders and policymakers in charge of handling national security crises.

³³⁸ to a large degree the issues faced today are largely reflected in, or are exactly the same as, those faced by the previous generation.

³³⁹ A number of factors have contributed to hide not just the important lessons of cyber history, but also the fact that there is a history of cyber conflict.

A entrada massiva de um grande número de operadores no campo e o fato de a eles não ser ensinada a história dos ciberconflitos faz com que se sintam pioneiros na área; “muitos não conseguem distinguir entre o que é realmente novo *versus* o que é novo apenas para eles.”³⁴⁰ (HEALEY, 2013, p. 16, tradução nossa). Ademais, também pelo relativo despontar do campo, para muitos tomadores de decisão as características inerentes ao ciberespaço aparentam estar em constante mudança, o que os direciona a esquecer a história e “olhar para frente, em direção ao futuro e às novas tecnologias.”³⁴¹ (HEALEY, 2013, p. 16, tradução nossa).

Divergências de pensamento entre tecnologistas e especialistas em assuntos de segurança internacional também têm feito com que as lições da história sejam esquecidas. Os tecnologistas têm visto os ciberconflitos como desafios técnicos, ignorando as dinâmicas relacionadas à segurança internacional inerentes a esses conflitos. Os especialistas em assuntos de segurança internacional, por outro lado, têm visto o ciberespaço como algo totalmente novo e diferente, onde “suas teorias e abordagens existentes não podem ser colocadas em prática.”³⁴² (HEALEY, 2013, p. 16, tradução nossa).

Para Healey, é preciso haver um equilíbrio de pensamentos: os profissionais envolvidos com a segurança nacional devem entender de ciberconflitos, mas, da mesma forma que “Os generais não precisam entender detalhes de balística do armamento naval para planejar uma campanha naval, generais ciber não precisam conhecer os detalhes íntimos de pacotes TCP/IP.” (HEALEY, 2013, p. 14, tradução nossa).³⁴³ Também os especialistas ciber devem entender das dinâmicas do ciberespaço e dos ciberconflitos, mas precisam conhecer, de certa forma, o contexto de segurança nacional em que estão inseridos (HEALEY, 2013, p. 14).

Healey (2013, p. 16) também aponta os efeitos maléficos do sigilo governamental como umas das razões para que a história dos ciberconflitos tenha sido deixada de lado: muitos profissionais, quando consultados, argumentam que grande parte dessa história encontra-se classificada, ou seja, impossível de ser adequadamente contada, e alguns ainda acham que muitas dessas histórias talvez não deveriam ser recontadas.

Para Healey (2013, p. 17), é necessário que algumas informações sejam desclassificadas para que se possa aprender com elas. Da mesma forma, uma história

³⁴⁰ many fail to distinguish between what is actually new versus what is just new to them.

³⁴¹ to look forward, toward the future and to new technologies.

³⁴² their existing theories and approaches do not apply.

³⁴³ Admirals don't need to understand details of the ballistics of naval weaponry to plan a naval campaign, cyber generals do not need to know the intimate details of TCP/IP packets.

classificada desses conflitos deve ser desenvolvida e ensinada àqueles que necessitam conhecê-la.

Por todas essas razões, nos Estados Unidos, cada alerta ciber “chocou e surpreendeu os defensores e os tomadores de decisão que passaram por eles, mas suas lições foram logo esquecidas, até que uma nova onda de líderes ciber foi novamente ‘despertada’ por um choque similar.”³⁴⁴ (HEALEY, 2013, p. 14, tradução nossa).

Apesar de terem sido frequentemente ignoradas, essas três lições representam as tendências atuais não só dos ciberconflitos, mas também, em grande parte, do que os governos estão fazendo no que concerne às capacidades operativas no ciberespaço. Essas lições, de certa forma, desmistificam a noção de que “ciberataques são como guerras destrutivas massivas relâmpago desencadeadas por adolescentes em seus porões ou por nações que utilizam ataques surpresa totalmente alheios às atuais tensões geopolíticas.”³⁴⁵ (HEALEY, 2013, p. 22, tradução nossa). A história comprova que “As nações, em geral, mostram-se relutantes em conduzir ataques nocivos em larga escala umas contra as outras fora dos conflitos geopolíticos tradicionais.”³⁴⁶ (HEALEY, 2013, p. 21-22, tradução nossa).

Por muito tempo, representantes governamentais vêm sustentando a ideia de que “para alguém com bons recursos intelectuais e boas habilidades ciber, um *laptop* barato e uma conexão com a internet é tudo o que se precisa para se tornar um grande jogador no domínio”³⁴⁷ (SHELTON apud HEALEY, 2013, p. 24, tradução nossa), mas as tendências demonstram que esses recursos são úteis para espionar, acessar dados e até mesmo conduzir ataques mais intrusivos, mas, do ponto de vista estratégico, “é preciso uma grande dose a mais de recursos, esforço e conhecimento”³⁴⁸ (ANDRESS; WINTERFELD, 2011, p. 178) para tornar-se um operador legítimo no ciberespaço. A comunidade de segurança deve saber que “é difícil obter um efeito estratégico prolongado, mesmo no ciberespaço.”³⁴⁹ (HEALEY, 2013, p. 24, tradução nossa).

Por muitos anos se fala em “Pearl Harbor eletrônico” e “Ciber 9/11”, mas até o momento não se tem conhecimento de nenhum ciberataque que tenha sido “concebido para

³⁴⁴ shocked and surprised the defenders and decision-makers that suffered through them, but their lessons were soon forgotten, until a new wave of cyber leaders were again “awakened” to a similar shock.

³⁴⁵ cyber attacks are like massive disruptive, lightning wars unleashed either by kids in their basements or by nations using surprise attacks which are wholly unrelated to current geopolitical tensions.

³⁴⁶ Nations seem generally reluctant to conduct large-scale damaging attacks on one another, outside of traditional geo-political conflicts.

³⁴⁷ for someone with the right brain power and the right cyber abilities, a cheap laptop and Internet connection is all it takes to be a major player in the domain.

³⁴⁸ requires a great deal more resources, effort, and knowledge

³⁴⁹ it is difficult to have a prolonged strategic effect, even in cyberspace.

causar morte, destruição e terror.”³⁵⁰ (HEALEY, 2013, p. 21-22, tradução nossa). A tendência histórica tem demonstrado que, ao contrário, os governos têm utilizado as capacidades ciber para espionar e realizar operações encobertas uns contra os outros (HEALEY, 2013, p. 11): “os ciberconflitos mais importantes não têm envolvido guerra ou terror, mas sim espionagem.”³⁵¹ (HEALEY, 2013, p. 20, tradução nossa).

No que se refere às dinâmicas estratégicas, Healey (2013, p. 15) aponta que, de maneira geral, as dinâmicas tradicionais dos conflitos se assemelham, em grande parte, às novas dinâmicas dos ciberconflitos.³⁵²

essas lições mostram a continuidade subjacente dos ciberconflitos com as relações internacionais tradicionais, a segurança nacional e as operações militares. Embora certamente existam diferenças, até o momento os ciberconflitos não foram fundamentalmente diferentes dos conflitos na terra, no ar ou no mar.³⁵³ (HEALEY, 2013, p. 22, tradução nossa).

Existe apenas uma exceção a essas dinâmicas: o papel central do setor privado na defesa do ciberespaço (HEALEY, 2013, p. 15):

Talvez a maior diferença entre os ciberconflitos e seus equivalentes tradicionais seja a mais frequentemente esquecida: em se tratando de defesa contra os ciberconflitos, são atores não estatais, e não os governos, que geralmente são decisivos na defesa ciber. Empresas e grupos voluntários têm usado repetidamente sua agilidade e conhecimento no assunto para mitigar e triunfar na maioria dos conflitos [...], enquanto os governos ficam ao seu lado. Apenas raramente os governos são capazes de reunir os recursos superiores de suas burocracias onerosas para conseguir, em tempo suficiente, se defender decisivamente contra ataques.³⁵⁴ (HEALEY, 2013, p. 22, tradução nossa).

³⁵⁰ designed to cause death, destruction, and terror.

³⁵¹ the most important cyber conflicts have not involved war or terror, but rather espionage.

³⁵² Healey (2013, p. 25) sustenta sua argumentação no trabalho desenvolvido por Brandon Valeriano e Ryan Maness (VALERIANO; MANESS, 2012b). Esses pesquisadores “utilizaram métodos tradicionais das ciências políticas” (HEALEY, 2013, p. 25, tradução nossa) e descobriram que “Apenas 20 de 124 rivais ativos – definidos como a maioria dos pares de Estados propensos a conflitos no sistema – se envolveram em ciberconflitos entre 2001 e 2011. E houve apenas um total de 95 ciberataques entre estes 20 rivais. [...] Foi utilizada uma escala de gravidade que varia de cinco, que é o mínimo de danos, a um, em que a morte ocorre como resultado direto da ciberguerra. De todos os 95 ciberataques de nossa análise, a pontuação mais alta – a do Stuxnet e do Flame – foi apenas três.” (VALERIANO; MANESS, 2012b). Diante desse estudo, Healey (2013, p. 25) conclui que, ao contrário do que muitos dizem, os conflitos no ciberespaço não acontecem aleatoriamente, mas seguem um padrão que se iguala aos conflitos geopolíticos tradicionais. Para o estudo completo realizado por Valeriano e Maness, veja (VALERIANO; MANESS, 2012a).

³⁵³ these lessons show the underlying continuity of cyber conflict with traditional international relations, national security, and military operations. While there are certainly differences, to date cyber conflicts have not been fundamentally different from conflicts on the land, in the air, or on the sea.

³⁵⁴ Perhaps the biggest difference between cyber conflicts and their traditional equivalents is the one most often overlooked: when defending against cyber conflicts, it is non-state actors, not governments, which typically are decisive in cyber defense. Companies and volunteer groups have repeatedly used their agility and subject matter knowledge to mitigate and prevail in most of the conflicts in this book, while governments are on the side. Only uncommonly are governments able to bring the superior resources of their unwieldy bureaucracies to bear in enough time to decisively defend against attacks.

Para Healey (2013, p. 24) os mitos têm muitas implicações críticas para os Estados Unidos, implicações essas que também se aplicam à realidade de muitos países:

1. A comunidade ciber dos EUA provavelmente investirá excessivamente em capacidades e doutrina para contra-atacar, automaticamente, ataques surpresa.
2. Regras de engajamento permitirão que os níveis cada vez mais baixos de autoridade militar “disparem em contra-ataque” sem solicitar autorização – um relaxamento das regras que pode não ser propício aos interesses econômicos ou militares de longo prazo dos EUA.
3. Planos de resposta recairão sobre os incidentes de hoje, com pouca reflexão sobre a forma com que se pode aumentar e sustentar um esforço ao longo de semanas e meses, o que fez com que os conflitos anteriores ocorressem.
4. Ações defensivas que fazem sentido em campanhas mais longas (como a instalação de novos recursos de rede e de Pontos de Troca de internet) serão ignoradas.
5. Os militares dos EUA irão treinar seus novos quadros profissionais ciber com doutrinas e estratégias que estão focadas apenas no combate imediato, com pouca concepção da verdadeira natureza do todo estratégico.³⁵⁵ (HEALEY, 2013, p. 24, tradução nossa).

Healey (2013, p. 85), embasado nas lições oferecidas pela história dos ciberconflitos, apresenta o seguinte cenário prospectivo sobre os ciberconflitos e as operações no ciberespaço:

1. Os ciberconflitos se tornarão mais destrutivos
2. O papel do setor privado nos ciberconflitos aumentará
3. Haverá mais ataques disruptivos praticados pelos Estados
4. Haverá mais ciberconflitos encobertos praticados pelos Estados
5. Haverá mais operações ciber ofensivas estadunidenses³⁵⁶ (HEALEY, 2013, p. 86, tradução nossa).

Healey (2013, p. 85) acredita que, apesar de a história confirmar que os ciberconflitos foram bastante amenos até o momento (com exceção do Stuxnet), as tendências atuais comprovam que, no futuro, haverá mais ataques disruptivos, como ocorreu nos ciberconflitos entre a Rússia, a Geórgia e a Estônia, e os ataques trarão consequências mais destrutivas, “especialmente aqueles vindos de conflitos encobertos entre Estados-nação”³⁵⁷ (HEALEY, 2013, p. 85, tradução nossa), como foi o Stuxnet, e os governos, aos poucos, identificarão “as

³⁵⁵ 1. The US cyber community will likely over-invest in capabilities and doctrine to automatically counterattack against surprise attacks. 2. Rules of engagement will allow ever-lower levels of military authority to “shoot back” without seeking authorization – a relaxation of the rules which may not be conducive to long-term US economic or military interests. 3. Response plans will focus on today’s incident, with little thought on how to surge and sustain an effort over the weeks and months that it has previously taken conflicts to occur. 4. Defensive actions which make sense in longer campaigns (such as installing new networking capabilities and Internet Exchange Points) will be ignored. 5. The US military will train their new cyber cadres with doctrines and strategies that are focused only on the immediate fight, with little conception of the true nature of the strategic whole.

³⁵⁶ 1. Cyber conflicts will become more destructive. 2. Increasing private-sector role in cyber conflicts. 3. More disruptive attacks by states. 4. More covert cyber conflicts by states. 5. More US offensive cyber operations.

³⁵⁷ especially from more covert nation-state conflicts.

próprias vantagens de perturbar seus adversários online.”³⁵⁸ (HEALEY, 2013, p. 86, tradução nossa). Além disso, as empresas do setor privado começarão a expandir ainda mais seus esforços para desenvolver capacidades defensivas no ciberespaço (HEALEY, 2013, p. 85), enquanto os Estados aperfeiçoarão suas capacidades ofensivas, “encorajando, dirigindo e conduzindo ataques disruptivos.”³⁵⁹ (HEALEY, 2013, p. 86, tradução nossa).

No que concerne especificamente aos Estados Unidos, Healey (2013, p. 86-87) acredita que mais operações ciber ofensivas ocorrerão, devido a quatro principais fatores: 1. A crença de que uma defesa passiva já não é suficiente, sendo necessária uma defesa ativa, o que pode fazer com que as formas de retaliação ultrapassem as fronteiras rígidas “das redes de computadores militares, para tentar combater ciberataques em computadores particulares.”³⁶⁰ (HEALEY, 2013, p. 86, tradução nossa); 2. O interesse crescente do setor privado em atuar em operações ofensivas para combater ameaças de caráter geral, “em vez de [atuarem apenas em] uma resposta técnica específica a um incidente em particular.”³⁶¹ (NAKASHIMA apud HEALEY, 2013, p. 86, tradução nossa); 3. As opções atrativas e de baixo custo oferecidas pelas capacidades ciber ofensivas relacionadas às missões tradicionais de segurança nacional, como a coleta de inteligência e a realização de operações encobertas ou de difícil imputação (HEALEY, 2013, p. 87); 4. A ambição que cada comandante possui, ao “enfrentar adversários tradicionais no campo de batalha”³⁶² de querer “utilizar todos os recursos possíveis a seu favor, incluindo as capacidades ciber.”³⁶³ (HEALEY, 2013, p. 87, tradução nossa). Como vimos, as atividades relacionadas ao programa de monitoramento PRISM da Agência de Segurança Nacional estadunidense, reveladas recentemente, comprovam essas prospecções.

Para Healey, “Quanto mais cedo começarmos a ensinar as lições do passado, mais cedo poderemos, esperançosamente, romper o ciclo de repetidos ‘alertas ciber’ e começar a criar novas tendências para o futuro.”³⁶⁴ (HEALEY, 2013, p. 87, tradução nossa).

³⁵⁸ its own advantages in disrupting adversaries online.

³⁵⁹ encouraging, directing, and conducting disruptive attacks.

³⁶⁰ military-related computer networks to try to combat cyberattacks on private computers.

³⁶¹ rather than a specific technical response to a particular incident.

³⁶² to face traditional adversaries on the battlefield

³⁶³ want to use every arrow in their quiver, including cyber capabilities.

³⁶⁴ The sooner we begin teaching these lessons from the past, the sooner we can hopefully break out of the cycle of repeated “wake-up calls” and start creating new trends for the future.

5 CONSIDERAÇÕES FINAIS

A partir da observação das doutrinas, estratégias, operações e instituições de ciber guerra estadunidenses, percebe-se que a obtenção de um controle satisfatório dos aspectos fundamentais que envolvem o ciberespaço tem se tornado, cada vez mais, um objetivo estratégico nacional dos Estados Unidos. Assim como este país, muitos outros também já projetam o ciberespaço, hoje, como uma ferramenta estratégica, um meio para obter vantagens e conduzir eventos de âmbito nacional e internacional.

Ao longo deste trabalho verificamos, sob a perspectiva estadunidense, que capacidades ciber defensivas e ofensivas no ciberespaço têm sido desenvolvidas por vários países, no âmbito da segurança nacional.

Vários governos têm direcionado seus esforços, principalmente, para a proteção de informações, sistemas e redes governamentais e privadas que armazenam ou controlam as infraestruturas críticas da nação. Isso tem sido feito, especialmente, através do aumento da conscientização nacional e internacional sobre cibersegurança; do desenvolvimento de sistemas mais robustos e de práticas mais coordenadas de resposta a incidentes; da realização de parcerias com o setor privado no combate às ameaças; do incentivo ao aprimoramento constante das tecnologias de informação e comunicação; da coordenação de políticas públicas voltadas para os assuntos ligados ao ciberespaço; do incentivo à cooperação nacional e internacional na área ciber e na criação de instituições capazes de implantar essas diretrizes e iniciativas.

Além disso, sob a ótica estadunidense, constatamos que existe uma atual tendência, por parte de alguns governos, de inserção das Forças Armadas nos assuntos ciber, caracterizada, sobretudo, pela criação e reestruturação das instituições e funções militares, pela especialização do pessoal nos assuntos ciber, pela tentativa de integração das capacidades tradicionais com as novas capacidades ciber em suas operações no ciberespaço, pela elaboração de doutrinas e estratégias que fundamentem essas operações, pelo aprimoramento da resiliência, do gerenciamento de risco e das práticas de dissuasão no ciberespaço, pelo desenvolvimento de armas ciber e pela realização de operações cada vez mais ofensivas no ciberespaço. Operacionalizar essas ações governamentais, contudo, tem sido um grande desafio.

Acredita-se, porém, que as principais dificuldades de operacionalização dos esforços pelos Estados não estejam apenas ligadas à forma de conectividade e natureza única do ciberespaço. De fato, devido à rápida e contínua evolução das tecnologias de informação e

comunicação, à constante convergência das redes que compõem o ciberespaço para plataformas digitais e às dinâmicas de conectividade intrínsecas do ciberespaço, a rapidez de comunicação e liberdade de realização, em nível global, dos mais diversos tipos de atividades no ciberespaço, muitas vezes anônimas, para além das fronteiras físicas e políticas controladas pelos Estados, trazem inúmeras vulnerabilidades que podem ser exploradas tanto por indivíduos, quanto por organizações e Estados, maximizando a presença de ameaças de natureza bastante variadas no ambiente internacional. Contudo, as inconsistências conceituais, midiáticas, teóricas e governamentais que permeiam o debate ciber têm mistificado e, muitas vezes, ocultado o real impacto que as atividades no ciberespaço têm trazido e podem trazer, conduzindo o planejamento estratégico de muitos governos para direções contrárias às reais necessidades estatais.

Supõe-se, portanto, que as ações governamentais devam se pautar tanto no desenvolvimento de tecnologias capazes de direcionar as atuais dinâmicas de conectividade do ciberespaço para seus interesses nacionais, quanto no estímulo de um aprofundamento do debate ciber. Assim, pesquisas nas áreas de ciência da computação, engenharia de rede, tecnologia da informação, segurança da informação, investigação digital forense e afins devem ser fomentadas. Além disso, o debate ciber no campo dos estudos de segurança, defesa, estratégicos, de política internacional, relações internacionais, direito e outros, dentro dos âmbitos acadêmico, das instituições governamentais e organizações não governamentais, militares ou civis, também deve ser instigado, promovendo, sempre que for vantajoso, uma interatividade e interdisciplinaridade entre essas duas grandes áreas da ciência. Dessa forma, os Estados serão capazes de aperfeiçoar as suas capacidades ciber e, com isso, dar-lhes melhor utilidade, colocando ao seu dispor ferramentas para melhor aprimorar o uso dos seus instrumentos de poder, sejam eles políticos, diplomáticos, econômicos, militares ou informacionais.

REFERÊNCIAS

- ACÁCIO, Igor Daniel P.; SOUZA, Gills Lopes M. Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço? **36º Encontro Anual da Anpocs (Associação Nacional de Pós-Graduação e Pesquisa em Ciências Sociais)**. Águas de Lindóia, São Paulo, 21 a 25 de outubro de 2012. Disponível em: <http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_details&gid=8169&Itemid=76>. Acesso em: 16 fev. 2014.
- ALEXANDER, Keith B. Warfighting in Cyberspace. **JFQ NDU Press**. Issue 46, 3rd quarter, 2007. Disponível em: <<http://www.carlisle.army.mil/DIME/documents/Alexander.pdf>>. Acesso em: 20 jan. 2014.
- ANDERSON, Chris; WOLFF, Michael. The Web is Dead. Long Live the Internet. **Wired**. Sept. 2010. Disponível em: <http://www.wired.com/magazine/2010/08/ff_webrip/>. Acesso em: 19 fev. 2014.
- ANDRESS, Jason; WINTERFELD, Steve. **Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners**. Waltham, USA: Syngress, 2011.
- ARQUILLA, John; RONFELDT, David. Cyberwar is coming! **Comparative Strategy**, Vol. 12, N. 2, Spring 1993, p. 141-165. Taylor & Francis, Inc., 1993. Disponível em: <<http://www.tandfonline.com/toc/ucst20/12/2#.UILcdlBwpqV>>. Acesso em: 07 out. 2013.
- ARQUILLA, John; RONFELDT, David. Cyberwar is coming! In: ARQUILLA, John; RONFELDT, David (Ed). **In Athena's Camp: Preparing for Conflict in the Information Age**. Santa Monica, CA: Rand Publishing, 1997. Disponível em: <http://www.rand.org/pubs/monograph_reports/MR880>. Acesso em: 07 out. 2013.
- ARQUILLA, John; RONFELDT, David. **Networks and Netwars: The Future of Terror, Crime and Militancy**. Santa Monica, CA: RAND Corporation, 2001. Disponível em: <http://www.rand.org/pubs/monograph_reports/MR1382>. Acesso em: 12 fev. 2014.
- BETZ, David J.; STEVENS, Tim. **Cyberspace and the State: Toward a Strategy for Cyberpower**. The International Institute for Strategic Studies (IISS). London, UK: Routledge, 2011.
- BETZ, David J.; STEVENS, Tim. Analogical reasoning and cyber security. **Security Dialogue**. London, UK: Sage Publications, 2013. Disponível em: <<http://sdi.sagepub.com/content/44/2/147>>. Acesso em: 14 jan. 2014.
- BRENNER, Joel F. Eyes wide shut: The growing threat of cyber attacks on industrial control systems. **Bulletin of the Atomic Scientists**. Vol. 69, Issue 5, Sept. 2013. Disponível em: <<http://www.thebulletin.org/2013/september/eyes-wide-shut-growing-threat-cyber-attacks-industrial-control-systems>>. Acesso em: 09 fev. 2014.
- BRITO, Jerry. WATKINS, Tate. Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. **Social Science Research Network**. May, 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1830625>. Acesso em: 19 fev. 2014.

BUZAN, B.; WÆVER, O.; e WILDE, J. de. **Security: A New Framework for Analysis**. Boulder-CO: Lynne Rienner Publishers, 1998.

CAMPEN, Alan D. **The First Information War: The Story of Computers and Communications in the Persian Gulf War**. Afcea International Press, 1992.

CAMPEN, Alan D.; DEARTH, Douglas; GOODDEN, R. Thomas. (Ed.) **Cyberwar: Security, Strategy and Conflict in the Information Age**. Afcea International Press, 1996.

CANABARRO, Diego Rafael; BORNE, Thiago. Ciberespaço e Internet: Implicações Conceituais para os Estudos de Segurança. **Mundorama: divulgação científica em Relações Internacionais**. 2013a. Disponível em: <<http://mundorama.net/2013/05/19/ciberespaco-e-internet-implicacoes-conceituais-para-os-estudos-de-seguranca-por-diego-rafael-canabarro-e-thiago-borne/>>. Acesso em: 29 maio 2013.

CANABARRO, Diego Rafael; BORNE, Thiago. Reflections on The Fog of (Cyber)War. **National Center for Digital Government (NCDG) Policy Working Paper N. 13-001**. Mar. 2013b. Disponível em: <http://www.umass.edu/digitalcenter/research/working_papers/13_001_Canabarro-Borne_FogofCyberWar.pdf>. Acesso em: 07 out. 2013.

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro**. Tese apresentada à Escola de Comando e Estado-Maior do Exército. Escola Marechal Castelo Branco. Rio de Janeiro, 2012. Disponível em: <<http://redebie.decex.ensino.eb.br/vinculos/000004/00000457.pdf>>. Acesso em: 20 jan. 2014.

CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. **Bulletin of the Atomic Scientists**. Vol. 69, Issue 5, Sept. 2013. Disponível em: <<http://www.thebulletin.org/2013/september/misunderstood-acronym-why-cyber-weapons-arent-wmd>>. Acesso em: 09 fev. 2014.

CASTELLS, Manuel. **The Rise of the Network Society, The Information Age: Economy, Society and Culture**. Vol. I. Cambridge, MA: Blackwell Publishing, 1996.

CAVELTY, Myriam Dunn. The militarisation of cyber security as a source of global tension. In: MÖCKLI, Daniel (Ed). **Strategic Trends 2012: Key Developments in Global Affairs**. Zurich, Switzerland: Center for Security Studies (CSS), 2012. Disponível em: <http://www.css.ethz.ch/publications/DetailansichtPubDB_EN?rec_id=2027>. Acesso em: 24 jan. 2014.

CEBROWSKI, ARTHUR K. ; GARSTKA, John J. Network-Centric Warfare: Its Origin and Future. **Proceedings**, Vol. 124/I/I, 139. Jan. 1998. Disponível em: <<http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future>>. Acesso em: 07 out. 2013.

CEPIK, Marco A. C. **Espionagem e democracia**. Rio de Janeiro: FGV, 2003.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: CEPIK, Marco (Org.). **Do 11 de**

Setembro de 2001 à “Guerra Contra o Terror”: reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014. No prelo.

CHAPMAN, Gary. **An Introduction to the Revolution in Military Affairs**. In: XV AMALDI CONFERENCE ON PROBLEMS IN GLOBAL SECURITY. Helsinki, Finland. Sept. 2003. Disponível em: <<http://www.lincci.it/rapporti/amaldi/papers/XV-Chapman.pdf>>. Acesso em: 20 jan. 2014.

CHEN, Thomas M. **An Assessment of the Department of Defense Strategy for Operating in Cyberspace**. The Letort Papers. Strategic Studies Institute (SSI) & U.S. Army War College. Carlisle, PA: United States Army War College Press, Sept. 2013. Disponível em: <<http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1170>>. Acesso em: 11 fev. 2014.

CLARKE, R.; KNAKE, R. **Cyber War: The Next Threat to National Security and What to Do About It**. New York: Ecco, 2010.

COMMISSION on Cybersecurity for the 44th Presidency. **Center for Strategic and International Studies (CSIS)**. Disponível em: <<http://csis.org/program/commission-cybersecurity-44th-presidency>>. Acesso em: 22 jan. 2014.

CREVELD, Martin van. War and Technology. **The Newsletter of FPRI's Wachman Center**. Foreign Policy Research Institute. Vol. 12, N. 25. Oct. 2007. Disponível em: <<http://www.fpri.org/footnotes/1225.200710.vancreveld.wartechology.html>>. Acesso em: 24 jan. 2014.

CRISPIN, Mirian Cristina Generoso Ribeiro. **Doutrina Nacional: Crimes praticados pela internet e crimes de informática**. BuscaLegis.ccj.ufsc.br. Disponível em: <<http://www.buscalegis.ufsc.br/revistas/files/anexos/6025-6017-1-PB.pdf>>. Acesso em: 10 mar. 2010.

DATA Mining: Conceitos, Técnicas, Ferramentas e Aplicações. Departamento de Informática. Coordenação Central de Extensão. Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ). Disponível em: <http://www.cce.puc-rio.br/sitecce/website/website.dll/folder_curso?nCurso=data-mining>. Acesso em: 17 fev. 2014.

DAVIDOFF, Sherri; HAM, Jonathan. **Network Forensics: tracking hackers through cyberspace**. New Jersey, USA: Pearson Education, Inc., 2012.

DENNING, Dorothy E. **Information Warfare and Security**. Addison-Wesley, Dec. 1998. Disponível em: <<http://vxheaven.org/lib/pdf/Information%20warfare%20and%20security.pdf>>. Acesso em: 12 fev. 2014.

DENNING, Doroty E. **Cyberterrorism**. Testimony before the Special Oversight Panel on Terrorism. Committee on Armed Services. U.S. House of Representatives. May 2000. Disponível em: <<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>>. Acesso em: 19 fev. 2014.

DIAMOND, Jonathan. Early Patriotic Hacking. In: HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

DIAS, João Cândido Marques. A Guerra Centrada na Rede - NWC. **Passadiço** - CAAML, p. 44-47, 2006. Disponível em: <<http://www.mar.mil.br/caaml/passadico/2006/15aguerra.pdf>>. Acesso em: 07 out. 2013.

ELKUS, Adam. Moonlight Maze. In: HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

ERIKSSON, Johan; GIACOMELLO, Giampiero. **International Relations and Security in the Digital Age**. London, UK: Routledge, 2007.

ESTADOS UNIDOS. Air Force. **Cyberspace Operations**. Air Force Doctrine Document 3-12 (Incorporating Change 1, 30 November 2011). July 2010a. Disponível em: <<http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf>>. Acesso em: 20 jan. 2013.

ESTADOS UNIDOS. Congressional Research Service. **Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations**. CRS Report for Congress. Mar. 2009a. Disponível em: <<https://www.fas.org/sgp/crs/natsec/R40427.pdf>>. Acesso em: 22 jan. 2014.

ESTADOS UNIDOS. Department of Defense. **Department of Defense Directive 3600.01**. Information Operations (IO). May 2013a. Disponível em: <<http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf>>. Acesso em: 11 jan. 2013.

ESTADOS UNIDOS. Department of Defense. **Department of Defense Strategy for Operating in Cyberspace**. July 2011a. Disponível em: <<http://www.defense.gov/news/d20110714cyber.pdf>>. Acesso em: 14 jan. 2014.

ESTADOS UNIDOS. Department of Defense. **DoD Announces Nomination of Cyber Command Commander/NSA Director**. Release No: NR-058-14. Jan. 2014a. Disponível em: <<http://www.defense.gov/Releases/Release.aspx?ReleaseID=16514>>. Acesso em: 12 fev. 2014.

ESTADOS UNIDOS. Department of Defense. **Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations**. Memorandum for Secretaries of The Military Departments. June 2009b. Disponível em: <<http://online.wsj.com/public/resources/documents/OSD05914.pdf>>. Acesso em: 24 fev. 2014.

ESTADOS UNIDOS. Department of Defense. **Information Operations Roadmap**. Oct. 2003a. Disponível em: <http://www.information-retrieval.info/docs/info_ops_roadmap.pdf>. Acesso em: 18 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **Compendium of Key Doctrine Publications**. Compiled by Deputy Directorate, Joint Staff, J-7; Joint Education and Doctrine; Joint Doctrine Analysis Division. June 2013b. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/compendium.pdf>. Acesso em: 20 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **Department of Defense Dictionary of Military and Associated Terms** – JP 1-02. (As Amended Through 15 December 2013). Nov. 2010b. Disponível em: <http://www.dtic.mil/doctrine/dod_dictionary/>. Acesso em: 13 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **Information Operations**. Joint Publication 3-13. Feb. 2006a. Disponível em: <http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf>. Acesso em: 18 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **Information Operations**. Joint Publication 3-13. Nov. 2012a. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf>. Acesso em: 18 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **Joint Doctrine for Information Operations**. Joint Publication 3-13. Oct. 1998. Disponível em: <http://www.c4i.org/jp3_13.pdf>. Acesso em: 09 fev. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **Joint Terminology for Cyberspace Operations**. Nov. 2010c. Disponível em: <<http://www.nsc.gov/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>>. Acesso em: 18 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **National Military Strategy for Cyberspace Operations - NMS-CO**. Dec. 2006b. Disponível em: <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>. Acesso em: 12 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow**. 2004. Disponível em: <<http://www.defense.gov/news/mar2005/d20050318nms.pdf>>. Acesso em: 14 jan. 2014.

ESTADOS UNIDOS. Department of Defense. Joint Chiefs of Staff. **The National Military Strategy of the United States of America: Redefining America's Military Leadership**. Feb. 2011b. Disponível em: <<http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf>>. Acesso em: 22 jan. 2014.

ESTADOS UNIDOS. Department of Defense. **Strategic Communication and Information Operations in the DoD**. Memorandum for Secretaries of the Military Departments. Jan. 2011c. Disponível em: <<http://www.carlisle.army.mil/dime/documents/Strategic%20Communication%20&%20IO%20Memo%2025%20Jan2011.pdf>>. Acesso em: 19 jan. 2014.

ESTADOS UNIDOS. Department of Homeland Security. **National Infrastructure Protection Plan: Partnering to enhance protection and resiliency**. 2009c. Disponível em: <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>. Acesso em: 07 maio 2013.

ESTADOS UNIDOS. Department of the Army. Army Capabilities Integration Center. **Cyberspace Operations Concept Capability Plan 2016-2028**. TRADOC Pamphlet 525-7-8.

Feb. 2010d. Disponível em: <<http://www.fas.org/irp/doddir/army/pam525-7-8.pdf>>. Acesso em: 24 jan. 2014.

ESTADOS UNIDOS. Department of the Army. Army War College. Department of Military Strategy, Planning, and Operations & Center for Strategic Leadership. **Information Operations Primer: Fundamentals of Information Operations**. AY12 Edition. Nov. 2011d. Disponível em: <<http://www.carlisle.army.mil/dime/documents/AY12%20IO%20Primer%20FINAL%20CD.pdf>>. Acesso em: 19 jan. 2014.

ESTADOS UNIDOS. Executive Branch of the United States Government. **National Security Strategy Archive (NSSA)**. Disponível em: <<http://nssarchive.us/>>. Acesso em: 22 jan. 2014b.

ESTADOS UNIDOS. Executive Office of the President. National Science and Technology Council. **Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program**. Dec. 2011e. Disponível em: <http://www.nitrd.gov/fileupload/files/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf>. Acesso em: 07 maio 2013.

ESTADOS UNIDOS. Government Accountability Office. **Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented**. Report to Congressional Addressees. GAO-13-187. Feb. 2013c. Disponível em: <<http://www.gao.gov/assets/660/652170.pdf>>. Acesso em: 22 jan. 2014.

ESTADOS UNIDOS. National Security Agency. Central Security Service. **2013 National Centers of Academic Excellence in Information Assurance Designees Announced**. Fort George G. Meade, Maryland: NSA Press Release, Dec. 2013d. Disponível em: <http://www.nsa.gov/public_info/press_room/2013/academic_excellence_designees.shtml>. Acesso em: 01 fev. 2014.

ESTADOS UNIDOS. Senate. **Cyber Security Public Awareness Act of 2011**. 112th Congress, 2011–2013. Apr. 2011f. Disponível em: <<http://www.govtrack.us/congress/bills/112/s813/text>>. Acesso em: 07 maio 2013.

ESTADOS UNIDOS. The White House. **Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure**. May 2009d. Disponível em: <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em: 23 jan. 2014.

ESTADOS UNIDOS. The White House. **Cyberspace Policy Review supporting documents**. 2009e. Disponível em: <<http://www.whitehouse.gov/cyberreview/documents>>. Acesso em: 07 maio 2013.

ESTADOS UNIDOS. The White House. Executive Office of the President of the United States. **The Comprehensive National Cybersecurity Initiative**. Mar. 2010e. Disponível em: <<http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>>. Acesso em: 22 jan. 2014.

ESTADOS UNIDOS. The White House. **International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World**. May 2011g. Disponível em:

<http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf>. Acesso em: 23 jan. 2014.

ESTADOS UNIDOS. The White House. **National Plan for Information Systems Protection**. Version 1.0. 2000. Disponível em: <<https://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf>>. Acesso em: 22 jan. 2014.

ESTADOS UNIDOS. The White House. **National Strategy for Trusted Identities in Cyberspace**. Draft. June 2010f. Disponível em: <http://www.dhs.gov/xlibrary/assets/ns_tic.pdf>. Acesso em: 07 maio 2013.

ESTADOS UNIDOS. The White House. **Presidential Policy Directive/PPD-20**. U.S. Cyber Operations Policy. Oct. 2012b. Disponível em: <<http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text>>. Acesso em: 15 jan. 2014.

ESTADOS UNIDOS. The White House. **Presidential Policy Directive/PPD-28**. Signals Intelligence Activities. Jan. 2014c. Disponível em: <<http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>>. Acesso em: 11 fev. 2014.

ESTADOS UNIDOS. The White House. **The Comprehensive National Cybersecurity Initiative (CNCI)**. Disponível em: <<http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>>. Acesso em: 22 jan. 2014d.

ESTADOS UNIDOS. The White House. **The National Initiative for Cybersecurity Education**. Apr. 2010g. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/cybersecurity_niceeducation.pdf>. Acesso em: 07 maio 2013.

ESTADOS UNIDOS. The White House. **The National Strategy to Secure Cyberspace**. Feb. 2003b. Disponível em: <http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em: 07 maio 2013.

FITZGERALD, Mary C. **Marshal Ogarkov and The New Revolution in Soviet Military Affairs**. Center for Naval Analyses (CNA). Jan. 1987. Disponível em: <<http://www.cna.org/sites/default/files/research/2787000200.pdf>>. Acesso em: 09 fev. 2014.

FOIA (Freedom of Information Act). Disponível em: <<http://www.foia.gov/about.html>>. Acesso em: 12 fev. 2014.

GENERAL DYNAMICS C4 Systems. Secure Voice over IP (SVoip) vs. Voice over Secure IP (VoSIP) Installations. FAQ. 2014. Disponível em: <http://www.gdc4s.com/Documents/Products/SecureVoiceData/GD-SVOIP_FAQ-w.pdf>. Acesso em: 31 jan. 2014.

GIBSON, William. **Neuromancer**. New York: Ace Books, 1984. Disponível em: <http://www.ebooksbeus.com/uploads/6/3/0/8/6308108/neuromancer_-_william_gibson.pdf>. Acesso em: 03 abr. 2013.

GIDDA, Mirren. Edward Snowden and the NSA files – timeline. **The Guardian**, July 2013. Disponível em: <<http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>>. Acesso em: 18 fev. 2014.

GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata**. Niterói: Impetus, 2009.

GREENWALD, Glenn; MACASKILL, Ewen. Obama orders US to draw up overseas target list for cyber-attacks. **The Guardian**. 7 June 2013a. Disponível em: <<http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>>. Acesso em: 19 jan. 2014.

GREENWALD, Glenn; MACASKILL, Ewen. Obama tells intelligence chiefs to draw up cyber target list – full document text. **The Guardian**. 7 June 2013b. Disponível em: <<http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text>>. Acesso em: 19 jan. 2014.

GRINDAL, Karl. Operation BUCKSHOT YANKEE. In: HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

GUIMARÃES JR, Mário J.L. O Ciberespaço como Cenário para as Ciências Sociais. In: IX CONGRESSO BRASILEIRO DE SOCIOLOGIA. Set. 1999, Porto Alegre. Trabalho apresentado no Grupo Temático “**A sociedade da informação e a transformação da sociologia**”. Disponível em: <http://www.cfh.ufsc.br/~guima/papers/ciber_cenario.html>. Acesso em: 03 abr. 2013.

GVOSDEV, Nikolas K. The Bear Goes Digital: Russia and Its Cyber Capabilities. In: REVERON, Derek S. (Ed.). **Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World**. Georgetown University Press, 2012.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, 53, 1155-1175. 2009. Disponível em: <<http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>>. Acesso em: 21 jan. 2014.

HEALEY, Jason. **Beyond Attribution: Seeking National Responsibility for Cyber Attacks**. Cyber Statecraft Initiative. Atlantic Council. Jan. 2012. Disponível em: <http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF>. Acesso em: 11 fev. 2014.

HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

INKSTER, Nigel. China in Cyberspace. In: REVERON, Derek S. (Ed.). **Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World**. Georgetown University Press, 2012.

JAVA. O que é um servidor proxy? Como obter informações sobre o servidor proxy? Disponível em: <http://www.java.com/pt_BR/download/help/proxy_server.xml>. Acesso em: 23 fev. 2014.

KRAMER, Franklin D; STARR, Stuart H.; WENTZ, Larry K. (Ed.) **Cyberpower and National Security**. Washington, DC, USA: National Defense University Press, 2009.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin D; STARR, Stuart H.; WENTZ, Larry K. (Ed.) **Cyberpower and National Security**. Washington, DC, USA: National Defense University Press, 2009.

KUROSE, James F.; ROSS, Keith W. **Computer Networking: A Top-Down Approach** Featuring the Internet, 4th Edition. Solutions to Review Questions and Problems. June 2007. Disponível em: <<http://university.reckless.ir/download/other/Kruse%20answers.pdf>>. Acesso em: 19 fev. 2014.

LESSONS from Our Cyber Past: The First Cyber Cops. **Atlantic Council**. Mar. 2012a. Disponível em: <<http://www.atlanticcouncil.org/events/past-events/lessons-from-our-cyber-past-the-first-cyber-cops>>. Acesso em: 31 jan. 2014.

LESSONS from Our Cyber Past: The First Military Cyber Units. **Atlantic Council**. Mar. 2012b. Disponível em: <<http://www.atlanticcouncil.org/events/past-events/lessons-from-our-cyber-past-the-first-military-cyber-units>>. Acesso em: 31 jan. 2014.

LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

LEWIS, James Andrew; NEUNECK, Götz. **The Cyber Index: International Security Trends and Realities**. Geneva, Switzerland: United Nations Institute for Disarmament Research (UNIDIR), 2013. Disponível em: <<http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>>. Acesso em: 10 fev. 2014.

LIBICKI, Martin C. **What is Information Warfare?** Strategic Forum Number 28. Institute for National Strategic Studies. National Defense University: May 1995a. Disponível em: <http://www.dodccrp.org/files/Libicki_What_Is.pdf>. Acesso em: 07 out. 2013.

LIBICKI, Martin C. **What is Information Warfare?** Washington D. C.: United States Government Printing, Aug. 1995b. Disponível em: <<http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA367662>>. Acesso em: 07 out. 2013.

LIBICKI, Martin C. **Defending Cyberspace and Other Metaphors**. The Center for Advanced Concepts and Technology (ACT). Washington, DC: National Defense University, 1997.

LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**. RAND Corporation, 2009. Disponível em: <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf>. Acesso em: 11 fev. 2014.

LIBICKI, Martin C. Cyberspace Is Not a Warfighting Domain. **I/S: A journal of law and Policy for the Information Society**. Vol. 8:2, 2012. Disponível em: <<http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf>>. Acesso em: 19 fev. 2014.

LIN, Herbert. Operational Considerations in Cyber Attack and Cyber Exploitation. In: REVERON, Derek S. (Ed.). **Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World**. Georgetown University Press, 2012.

LUTZ, Brenda; LUTZ, James. Terrorism. In: COLLINS, Alan. **Contemporary Security Studies**. Oxford: Oxford University Press, 2007.

MACHADO, Jussara de Oliveira. **Inteligência e ciberespaço: desafios do século XXI**. Monografia apresentada Curso de Pós-Graduação Lato Sensu de Especialização em Inteligência de Estado e Inteligência de Segurança Pública da Escola Superior do Ministério Público de Minas Gerais em parceria com o Centro Universitário Newton Paiva. Maio 2010. Disponível em: <http://issuu.com/fesmpmg_inteligencia/docs/inteligencia_ciberespaco>. Acesso em: 09 fev. 2014.

MACHADO, Jussara de Oliveira. Inteligência e ciberespaço: desafios do século XXI. In: CEPIK, Marco (Org). **Inteligência Governamental: contextos nacionais e desafios contemporâneos**. Niterói: Impetus, 2011.

MATHERS, Russel F. **Cyberspace Coercion in phase 0/I: How to deter armed conflict**. Newport, R. I.: Naval War College, 2007. Disponível em: <<http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA476693>>. Acesso em: 03 abr. 2013.

MAURER, Tim. SOLAR SUNRISE: Cyber Attack from Iraq? In: HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

MITCHELL, Paul T. **Network Centric Warfare: Coalition operations in the age of US military primacy**. Adelphi Paper 385. The International Institute for Strategic Studies (IISS). London: Routledge, 2006.

MOFFAT, James. **Complexity Theory and Network Centric Warfare**. DoD Command and Control Research Program (CCRP), 2003.

MOLANDER, ROGER C.; RIDDILE, ANDREW S.; WILSON, Peter A. **Strategic Information Warfare: A New Face of War**. Santa Monica, CA: National Defense Research Institute - RAND, 1996. Disponível em: <http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf>. Acesso em: 07 out. 2013.

MORTON, Chris. Stuxnet, Flame, and Duqu – the OLYMPIC GAMES. In: HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

NISSENBAUM, Helen. Where computer security meets national security. **Ethics and Information Technology**. Issue 7, p. 61-73. New York University: Springer, 2005. Disponível em: <<http://www.nyu.edu/projects/nissenbaum/papers/ETINsecurity.pdf>>. Acesso em: 19 fev. 2014.

NSA files: Decoded. What the revelations mean for you. **The Guardian**, Nov. 2013a. Disponível em: <<http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>>. Acesso em: 18 fev. 2014.

NSA slides explain the PRISM data-collection program. **Washington Post**, June, 2013b (Updated July, 2013). Disponível em: <<http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>>. Acesso em: 27 jan. 2014.

NYE Jr., Joseph S. **O futuro do poder**. Tradução de Magda Lopes. São Paulo: Benvirá, 2012.

NYE Jr., Joseph S. From bombs to bytes: Can our nuclear history inform our cyber future? **Bulletin of the Atomic Scientists**. Vol. 69, Issue 5, Sept. 2013. Disponível em: <<http://www.thebulletin.org/2013/september/bombs-bytes-can-our-nuclear-history-inform-our-cyber-future>>. Acesso em: 09 fev. 2014.

PALERI, Prabhakaran. **National Security: Imperatives and Challenges**. New Delhi, India: Tata McGraw-Hill Publishing Company Limited, 2008.

PATTERN MATCHING (F#). Microsoft Developer Network Library (MSDN Library). Visual Studio 2013. Disponível em: <<http://msdn.microsoft.com/en-us/library/dd547125.aspx>>. Acesso em: 17 fev. 2014.

PEER-TO-PEER. Cartilha de Segurança para Internet. Glossário. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (cert.br)**. Disponível em: <<http://cartilha.cert.br/glossario/>>. Acesso em: 31 jan. 2014.

PRESIDENTIAL Directives and Executive Orders. **Federation of American Scientists (FAS)**. Disponível em: <<https://www.fas.org/irp/offdocs/direct.htm>>. Acesso em: 22 jan. 2014.

RATTRAY, George J. An Environmental Approach to Understanding Cyberpower. In: KRAMER, Franklin D; STARR, Stuart H.; WENTZ, Larry K. (Ed.) **Cyberpower and National Security**. Washington, DC, USA: National Defense University Press, 2009.

RAUSCHER, Karl Frederick; YASCHENKO, Valery. The Russia-U.S. Bilateral on Cybersecurity - Critical Terminology Foundations. **EastWest Institute and the Information Security Institute of Moscow State University**. Issue 1, 2011. Disponível em: <<http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=130080>>. Acesso em: 09 fev. 2014.

REVERON, Derek S. An Introduction to National Security and Cyberspace. In: REVERON, Derek S. (Ed.). **Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World**. Georgetown University Press, 2012.

RID, Thomas. Cyber War Will Not Take Place. **Journal of Strategic Studies**, Vol. 35, N. 1, 5-32. London: Routledge, 2012. Disponível em: <<http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939#.UvgQLPldVJd>>. Acesso em: 21 jan. 2014.

RID, Thomas. **Cyber War Will Not Take Place**. New York: Oxford University Press, 2013.

RYAN, Johnny. A History of the Internet and the Digital Future. London: Reaktion Books, 2010.

SECURING Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. **Center for Strategic and International Studies**. Dec. 2008. Disponível em: <http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf>. Acesso em: 23 jan. 2014.

SHACHTMAN, Noah; SINGER, Peter W. The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive. **Brookings**. Government Executive. Aug. 2011. Disponível em: <<http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman>>. Acesso em: 19 fev. 2014.

SAMPAIO, Fernando G. **Ciberguerra, guerra eletrônica e informacional**: um novo desafio estratégico. Escola Superior de Geopolítica e Estratégia (ESGE). 2001. Disponível em: <<http://www.defesanet.com.br/esge/ciberguerra.pdf>>. Acesso em: 07 out. 2013.

SCHMIDT, Andreas. The Estonian Cyberattacks. In: HEALEY, Jason (Ed.). **A Fierce Domain**: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association (CCSA). June 2013.

SCHMITT, Michael N. Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework. **The Columbia Journal of Transnational Law**, v. 37, 1999. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800>. Acesso em: 07 out. 2013.

SEGAL, Adam. From TITAN RAIN to BYZANTINE HADES: Chinese Cyber Espionage. In: HEALEY, Jason (Ed.). **A Fierce Domain**: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association (CCSA). June 2013.

SHELDON, John B. Toward a Theory of Cyber Power: Strategic Purpose in Peace and War. In: REVERON, Derek S. (Ed.). **Cyberspace and National Security**: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, 2012.

SIGNIFICANT Cyber Incidents Since 2006. **Center for Strategic and International Studies (CSIS)**. Disponível em: <http://csis.org/files/publication/131010_Significant_Cyber_Incidents_Since_2006_0.pdf>. Acesso em: 11 fev. 2014.

SOUZA, Gills Lopes Macêdo. **Reflexos da digitalização da guerra na política internacional do século XXI**: Uma análise exploratória da Securitização do Ciberespaço nos

Estados Unidos, Brasil e Canadá. Dissertação de Mestrado Acadêmico do Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco. Recife, 2013.

STARR, Stuart H. Toward a Preliminary Theory of Cyberpower. In: KRAMER, Franklin D; STARR, Stuart H.; WENTZ, Larry K. (Ed.) **Cyberpower and National Security**. Washington, DC, USA: National Defense University Press, 2009.

STOLL, Clifford. Cuckoo's Egg: Stalking the Wily Hacker. In: HEALEY, Jason (Ed.). **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA). June 2013.

THE BIG Brother Problem. **World Economic Forum**, Jan. 2014. Disponível em: <<http://www.weforum.org/events/world-economic-forum-annual-meeting-2014>>. Acesso em: 18 fev. 2014.

VALERIANO, Brandon; MANESS, Ryan. Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare. In: REVERON, Derek S. (Ed.). **Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World**. Georgetown University Press, 2012a.

VALERIANO, Brandon; MANESS, Ryan. The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype. **Foreign Affairs**. Council on Foreign Relations. Nov. 2012b. Disponível em: <<http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar>>. Acesso em: 17 fev. 2014.

ZIMET, Elihu; BARRY, Charles L. Military Service Overview. In: KRAMER, Franklin D; STARR, Stuart H.; WENTZ, Larry K. (Ed.) **Cyberpower and National Security**. Washington, DC, USA: National Defense University Press, 2009.

ZITTRAIN, Jonathan L. **The Future of the Internet and How to Stop it**. New Haven & London: Yale University Press, 2008. Disponível em: <<http://pt.scribd.com/doc/9642447/the-Future-of-the-Internet>>. Acesso em: 19 fev. 2014.

WARNER, Michael. Cybersecurity: A Pre-history. **Intelligence and National Security**. London: Routledge, 2012, Vol. 27, Issue 5, p. 781-799.

WEIMANN, Gabriel. Cyberterrorism: How Real is the Threat? Special Report 119. **United States Institute of Peace**. Dec. 2004. Disponível em: <<http://www.usip.org/sites/default/files/sr119.pdf>>. Acesso em: 19 fev. 2014.

WIENER, Norbert. **Cibernética**; ou, controle e comunicação no animal e na máquina. São Paulo: Ed. da USP: Polígono, 1970.

WILSON, Clay. Cyber Crime. In: KRAMER, Franklin D; STARR, Stuart H.; WENTZ, Larry K. (Ed.) **Cyberpower and National Security**. Washington, DC, USA: National Defense University Press, 2009.