COLEÇÃO
DEFESA E
FRONTEIRAS
VIRTUAIS

I

SEGURANÇA E DEFESA CIBERNÉTICA

DA FRONTEIRA FÍSICA AOS MUROS VIRTUAIS

Oscar Medeiros Filho
Walfredo Bento Ferreira Neto
Selma Lúcia de Moura Gonzales

ORGANIZADORES

Editora UFPE

SEGURANÇA E DEFESA CIBERNÉTICA

DA FRONTEIRA FÍSICA AOS MUROS VIRTUAIS

SEGURANÇA E DEFESA CIBERNÉTICA

DA FRONTEIRA FÍSICA AOS MUROS VIRTUAIS

Oscar Medeiros Filho
Walfredo Bento Ferreira Neto
Selma Lúcia de Moura Gonzales
ORGANIZADORES

Editora UFPE
RECIFE | 2014

EDITORA ASSOCIADA À

ASSOCIAÇÃO BRASILEIRA
DAS EDITORAS UNIVERSITÁRIAS

Catalogação na fonte
Bibliotecária Joselly de Barros Gonçalves, CRB4-1748

S456 Segurança e defesa cibernética : da fronteira física aos muros virtuais / organizadores: Oscar Medeiros Filho, Walfredo Bento Ferreira Neto, Selma Lúcia de Moura Gonzales. – Recife : Editora UFPE, 2014.
194 p. : il. – (Coleção Defesa e Fronteiras Virtuais, v.1)

ISBN (broch.)

1. Cibernética – Medidas de segurança. 2. Sistemas de recuperação da informação – Segurança. 3. Segurança pública. I. Medeiros Filho, Oscar (Org.). II. Ferreira Neto, Walfredo Bento (Org.). III. Gonzales, Selma Lúcia de Moura (Org.). IV. Título da coleção.

003.5 CDD (23.ed.) UFPE (BC2014-057)

Agradecimentos

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), que, em parceria com a Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR), lançou o Edital Pró-Estratégia 2012, viabilizando, assim, o Projeto *Vigilância nas Fronteiras e Muros Virtuais: um estudo analítico de políticas públicas e sistemas operacionais de proteção às estruturas estratégicas terrestres*.

Aos colegas que atuam na rede de pesquisa formada pela Universidade Federal de Pernambuco (UFPE), pelo Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército e pela Academia Militar das Agulhas Negras (Aman), todos autores dos diferentes artigos presentes nessa publicação, além dos que integram o Centro de Estudos e Sistemas Avançados de Recife (Cesar).

Aos que trabalharam na edição, revisão, projeto gráfico e divulgação da obra.

Apresentação dos Autores

André Ferreira Alves Machado

Mestre em Engenharia da Computação pelo Programa de Pós-Graduação em Análise Operacional, do Instituto Tecnológico da Aeronáutica (ITA). Membro da Seção de Cibernética do Centro de Instrução de Guerra Eletrônica do Exército Brasileiro.

Flávio Rocha de Oliveira

Doutor em Ciência Política pela USP. Professor do Curso de Relações Internacionais da Universidade Federal de São Paulo (Unifesp) e pesquisador das áreas de Análise de Risco Político, Estudos Estratégicos e Segurança e Defesa Cibernética.

Gills Vilar Lopes

Mestre em Ciência Política na área de RI pela UFPE, tendo realizado pesquisa na Université Laval (Canadá). Doutorando em Ciência Política pela UFPE, bolsista do Pró-Estratégia (Capes & SAE), pesquisador do Nepi/UFPE e professor substituto de Relações Internacionais (RI) da UFPB.

João Gabriel Álvares

Pós-Graduado em Direito e Tecnologia da Informação pelo Centro Universitário UniSEB e Especialista em Guerra Eletrônica. Professor de Direito Digital; assessor de Contratos de Defesa do Centro de Comunicações e Guerra Eletrônica do Exército; Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras.

João Marinonio Enke Carneiro

Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército. Pós-Graduado em Análise de Sistemas (UVA/RJ), MBA em Gerência de Telecomunicações (FGV/RJ), Mestre em Aplicações Militares (EsAO) e Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras.

José Ricardo de Souza Camelo

Mestre em Engenharia Elétrica (UNB), Especialista em Redes de Computadores pelo União Educacional de Brasília e professor coordenador no Centro Universitário Planalto, no Distrito Federal. Supervisiona o Projeto Arcabouço Documental, pertencente ao Projeto Estratégico Defesa Cibernética; chefia a Divisão de Doutrina e Mobilização do Centro de Defesa Cibernética e integra o Grupo Finalístico de Segurança da Informação.

Marcos Aurélio Guedes de Oliveira

PhD em *Government*, pela Universidade de Essex. Chefe do Departamento de Ciência Política da Universidade Federal de Pernambuco (UFPE). Coordenador geral do Projeto *Vigilância nas Fronteiras e Muros Virtuais: um estudo analítico de políticas públicas e sistemas operacionais de proteção às estruturas estratégicas terrestres*. Professor do Programa de Pós-Graduação de Ciência Política da UFPE. Coordenador do Grupo de Estudos Brasil e as Américas (CNPq) e do Núcleo de Estudos Americanos (UFPE).

Oscar Medeiros Filho

Doutor em Ciência Política pela Universidade de São Paulo; Mestre em Geografia Humana. É oficial do Exército Brasileiro (Quadro Complementar) e exerce a função de professor e pesquisador nos Programas de Pesquisa e Pós-Graduação do

Instituto Meira Mattos, da Escola de Comando Estado-Maior do Exército.

Ricardo Borges Gama Neto

Doutor e Mestre em Ciência Política (UFPE). É professor adjunto III da Universidade Federal de Pernambuco (UFPE). Coordena o Programa de Pós-Graduação em Ciência Política da UFPE e é diretor de pesquisa da Associação Brasileira de Ciência Política (ABCP).

Selma Lúcia de Moura Gonzales

Doutora em Geografia Humana (Política) pela Universidade de São Paulo (USP); Mestre em Gestão do Espaço Regional, pela Universidade de Brasília (UnB); e Especialista em Ensino de Geografia pela Universidade Estadual de Londrina (UEL). É oficial do Exército Brasileiro (Quadro Complementar), onde exerce a função de professora e pesquisadora na área de Defesa, nos Programas de Pesquisa e Pós-Graduação do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército.

Walfredo Bento Ferreira Neto

Mestre em Estudos Estratégicos da Defesa e da Segurança, pelo Inest/UFF/RJ; Especialista em Direito Militar e em Direito em Administração Pública. É Bacharel em Direito, pela Universidade Estácio de Sá, e possui licenciatura plena em Geografia, pela Universidade Federal de Pernambuco (UFPE). É oficial do Exército Brasileiro (Quadro Complementar) e professor da Academia Militar das Agulhas Negras e da Associação Educacional Dom Bosco.

Sumário

PARTE 2: DEFESA CIBERNÉTICA: ESTUDOS DE CASO

Prefácio

João Roberto de Oliveira[1]

Os artigos que compõem a obra *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais*, da *Coleção Defesa e Fronteiras Virtuais*, abordam uma temática extremamente atual e importante, que, felizmente, vem merecendo atenção por parte das autoridades e das instituições que lidam com atividades estratégicas em nosso País.

O tratamento desse assunto, no Estado brasileiro, começou a tomar contornos mais visíveis, a partir da edição do Decreto nº 3.505, em 13 de junho de 2000, que instituiu a Política de Segurança da Informação para os órgãos da Administração Pública Federal (APF), cuja implementação foi coordenada pela Secretaria Executiva do Conselho de Defesa Nacional, exercida pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR). A iniciativa conta com o assessoramento do Comitê Gestor de Segurança da Informação, formado por representantes desses órgãos da APF.

1 General-de-Divisão da Reserva, exerce o cargo de assessor especial do Comandante do Exército para o Setor Cibernético e para o Sisfron. É graduado em Administração de Empresas. Na carreira militar, além dos Cursos da Academia Militar das Agulhas Negras, de Aperfeiçoamento de Oficiais e de Comando e Estado-Maior, possui o Curso de Política, Estratégia e Alta Administração do Exército e o Curso de Estado-Maior do Exército Britânico. Desempenhou as seguintes funções: comandante do 4º Batalhão de Comunicações de Exército; oficial de Ligação do Exército Brasileiro junto ao Centro de Armas combinadas nos EUA; diretor de Material de Comunicações, Eletrônica e Informática; comandante da 11ª Região Militar; comandante da 4ª Região Militar e 4ª Divisão de Exército; e secretário executivo do Gabinete de Segurança Institucional da Presidência da República.

Essa medida visou criar os primeiros mecanismos institucionais para lidar com as transformações provocadas pela vertiginosa evolução tecnológica ocorrida nos últimos 20 anos, permitindo o ingresso das Tecnologias da Informação e Comunicações (TIC) em todos os domínios da atividade humana. O emprego intensivo dessas tecnologias modificou a forma de acesso à informação, incorporou inúmeras facilidades trazidas pela *Internet* e provocou uma verdadeira revolução nos processos e meios de gestão das organizações públicas e privadas.

O uso desse ambiente de interação entre pessoas, instituições públicas e privadas e de gestão corporativa, ignorando os limites fronteiriços convencionais entre os Estados e utilizando os recursos proporcionados pelas TIC, atualmente chamado de espaço cibernético, vem sendo alvo de debates de intensidade crescente, em decorrência das inúmeras possibilidades que ele oferece e por trazer imensuráveis benefícios e consideráveis ameaças à sociedade e ao Estado.

No Brasil, a evolução da abordagem sobre segurança da informação e das comunicações para o sentido mais amplo da segurança cibernética, pode ser verificada a partir de 2007, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (Creden), criada em 2003 junto ao Conselho de Governo, e que também funciona vinculada ao GSIPR. A partir daí, aspectos mais significativos como a proteção dos ativos informacionais necessários ao funcionamento seguro das infraestruturas críticas ou estratégicas do País (energia, comunicações, finanças, defesa, dentre outras), foram incorporados à pauta.

Em 2008, esse debate ampliou-se com a aprovação da Estratégia Nacional de Defesa, que indicou, entre suas diretrizes, a necessidade

de fortalecer os setores nuclear, espacial e cibernético nas Forças Armadas e contribuir para a segurança das infraestruturas essenciais à defesa e à segurança nacionais.

O cenário permitiu implantar medidas para preservar o seguro funcionamento das estruturas de defesa e incrementar a capacidade de resposta ante ameaças cibernéticas em tempo de paz ou de crise, no denominado ambiente de Defesa Cibernética, bem como viabilizar o uso de medidas de amplo espectro, quando necessário, mormente em situações de conflito, num ambiente característico de Guerra Cibernética.

Nesse contexto, foi instituído o Centro de Defesa Cibernética, sob liderança do Exército, para coordenar as atividades do setor cibernético, no âmbito da Defesa. A Marinha foi designada para coordenar o setor nuclear, e a Aeronáutica para exercer as mesmas funções no setor espacial.

Outras iniciativas estão em desenvolvimento, a exemplo da conjugação de esforços de vários ministérios, com a academia e com organizações privadas, a fim de dotar o País de estruturas adequadas de gestão, capacitação, inteligência, pesquisa científica e aplicada, independência tecnológica, arcabouço legal e doutrinário, preparo e emprego operacional, além da proteção de ativos informacionais estratégicos. O desafio é fomentar um ambiente altamente desejável de elevada sinergia e colaboração, que permita agir com eficiência e eficácia contra as ameaças cibernéticas que se apresentam à sociedade e ao Estado brasileiro.

No cenário internacional, muitos outros países desenvolvem medidas com esses propósitos há muito mais tempo. Os exemplos de maior expressão são os Estados Unidos, cujas capacidades se tornaram mais visíveis com o episódio das revelações de Snowden;

além da China e de Israel, tidos como detentores de organizações bastante especializadas e atuantes nesse campo; e da Rússia, acusada de motivar ações contra sistemas informatizados da Estônia, em 2007; e da Geórgia, em 2008.

Fazendo um paralelo com os cenários nuclear e espacial, o ambiente cibernético demonstra necessitar também de mecanismos de controle, mas os limites a serem nele estabelecidos parecem mais fluidos e de contornos ainda pouco precisos.

Enquanto nos ambientes nuclear e espacial, em tese, é mais fácil identificar os possíveis atores das ameaças e suas intenções, no ambiente cibernético essa tarefa é bastante complexa. É desafiadora a tarefa de tentar um equilíbrio entre a desejável liberdade e a necessidade de segurança, bem como entre a preservação da privacidade das pessoas e instituições e as ações para detectar possíveis ameaças à sociedade.

E é sobre essa ampla temática que a presente obra se debruça e avalia as consequências desse novo cenário no cotidiano das pessoas e das organizações públicas e privadas, bem como na relação entre Estados.

O artigo de Ricardo Borges Gama Neto e Gills Vilar Lopes, *Armas cibernéticas e segurança internacional*, discute o conceito de "guerra cibernética" conjugado ao uso de "armas cibernéticas". Analisa os diversos contextos em que o termo é utilizado, detendo-se, com maior profundidade, no ambiente das relações entre os Estados, a utilização dos recursos tecnológicos no espaço cibernético para a defesa de interesses estratégicos, chegando até o cenário mais clássico do emprego desses recursos no amplo espectro dos conflitos.

Em *Por uma ordem cibernética internacional*, Oscar Medeiros Filho prossegue esse debate, acrescentando percepções sobre os

conceitos e ações que estariam inseridos nas áreas de segurança, defesa e guerra cibernéticas, envolvendo as relações de interesses individuais, corporativos e de Estados, para, ao final, incitar medidas que visem a um arranjo regulatório internacional sobre o tema.

As relações entre os Estados e o emprego de ações no espaço cibernético como recurso de poder são tratados por Walfredo Bento Ferreira Neto, em *Territorializando o novo e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder*. O autor apresenta um novo conceito, que define de "fronteira-ponto", como forma de atender à necessidade de delimitar o espaço cibernético, não no sentido de separação e, sim, para normatizar responsabilidades frente a essa nova dimensão do poder. O objetivo é evitar o conflito e, até mesmo, a guerra.

Em "*Territorialidade e guerra cibernética: novo paradigma fronteiriço*", João Gabriel Álvares acrescenta questões que envolvem território, segurança e direito, nos âmbitos nacional e internacional, nessa análise das relações entre os Estados quanto ao uso do espaço cibernético. O autor aponta que, se por um lado há necessidade de regulamentar sanções para ilegalidades ou abusos cometidos nesse ambiente (apesar das dificuldades de judicializar essas questões), por outro lado os Estados têm necessidade de atuar de maneira preventiva, a fim de se contrapor às ações cibernéticas que possam afetar a soberania.

O autor conclui seu trabalho com a muito interessante consideração: "Percebe-se, portanto, que a defesa cibernética – cumulada com a possibilidade de responder a ameaças com a mesma forma e intensidade – se mostra como importante instrumento que, em última análise, pode garantir o *status quo* e a paz social de um Estado Democrático de Direito como o Brasil, no ciberespaço".

A análise da questão nos campos da Defesa e Segurança Nacionais, a possibilidade de resposta às incursões que possam degenerar ou interromper o funcionamento de infraestruturas essenciais à sociedade e ao Estado (ambiente de Defesa Cibernética), podendo chegar ao uso de medidas ofensivas nas situações de conflito deliberado (ambiente de Guerra Cibernética), pressupõe a demanda por obter e manter capacidades necessárias para atender a todas as situações que requeiram intervenção no espaço cibernético.

Nas Forças Armadas, por exemplo, teve início a capacitação nesse novo setor de especialização da atividade militar. Nesse contexto, o artigo *Guerra Cibernética e formação militar: contribuições para um perfil do soldado cibernético*, dos autores André Ferreira Alves Machado, Oscar Medeiros Filho e Walfredo Bento Ferreira Neto analisa os requisitos tecnológicos, os atributos pessoais desejáveis e as características desse ambiente de atuação, buscando colaborar na definição do perfil adequado para o "combatente cibernético". Os autores apresentam sugestões para conduzir a capacitação necessária, manifestando a exigência da aproximação entre militares e civis.

Como que corroborando essa última assertiva, os autores José Ricardo de Souza Camelo e João Marinonio Enke Carneiro discorrem com riqueza de detalhes sobre a estrutura montada e o modelo de operação utilizado durante a *Copa das Confederações Fifa/2013*, realizada no Brasil, no contexto das ações cibernéticas necessárias a garantir o funcionamento seguro dos ativos informacionais empregados no evento. Mais uma vez, ficou evidenciada a imperiosa necessidade de sinergia e de elevado nível de colaboração entre todas as instituições públicas e privadas que atuam nesse tipo de atividade.

Por fim, no artigo *Cibersegurança e Ciberguerra: o governo Obama e a política de defesa no espaço cibernético*, o autor Flávio Rocha

analisa o funcionamento das estruturas estabelecidas nos Estados Unidos para lidar com as ações necessárias no espaço cibernético. O foco principal está nos Departamentos de Defesa (DoD) e de Segurança Interna (DHS) e nas suas interações. A análise é bastante oportuna, tendo em vista a elevada capacidade de atuação dos EUA nesse campo.

É importante ressaltar que, embora os modelos de países como os Estados Unidos, Canadá e outros da Comunidade Europeia sejam os mais estudados, devido à facilidade para se obter informações a respeito dos mesmos, não se deve ignorar as capacidades e estruturas de outros países detentores de elevadas competências nessa atividade.

Frente ao exposto, pode-se confirmar a pertinência e a elevada contribuição que a obra *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais* empresta aos estudos e ações que visam dotar o Brasil de estruturas e estratégias adequadas e eficazes para a atuação no espaço cibernético.

Urge acelerar a implementação dessas medidas para que o Brasil não se distancie dos países mais atuantes no setor cibernético e, consequentemente, participe como ator proeminente nesse campo, no cenário internacional. É preciso evitar a defasagem registrada nos setores nuclear e espacial, prejuízos que, atualmente, o País vem lutando arduamente para minimizar.

CAPÍTULO 1

Armas cibernéticas e segurança internacional

ricardo Borges Gama Neto
Gills Vilar Lopes

Introdução

Este trabalho discute o conceito de guerra cibernética (*cyber war*) e uma de suas implicações: o uso estratégico das chamadas armas cibernéticas (*cyber weapons*). Mais especificamente, busca-se situar suas potencialidades e desafios, sob alguns pontos de vistas técnicos e políticos.

Embora a guerra seja um conflito entre dois ou mais Estados soberanos, ela não deixa de ser um fato histórico e social que, assim como o desenvolvimento técnico e cognitivo humano, é aperfeiçoada, conforme é utilizada. Até o início do século XX ela se desenvolve em dois ambientes/topologias/dimensões: terra e mar. Com a utilização dos aviões na Primeira Guerra Mundial, a guerra passa a compreender também o ar. Já sob a insígnia da Cortina de Ferro, um novo tabuleiro do jogo é posto: o espaço (sideral)[1].

1 Durante a Guerra Fria, Estados Unidos e a União Soviética desenvolveram vários sistemas que utilizavam o espaço sideral como local de conflito militar. Por exemplo: satélites do tipo espião e radar, bem como sistemas antissatélite – o míssil ASM-135 ASAT (EUA) ou satélites kamikazes (Istrebitel Sputnikov). Em 1967 foi assinado o Tratado do Espaço disciplinando as atividades militares.

Entre os anos 1990 e 2000, alguns estudos prospectivos[2] já vislumbram possíveis implicações que o uso político e estratégico do ciberespaço poderia gerar para o planejamento e a atuação estratégica das Forças Armadas. Percebe-se que aquilo que era alvo de previsões de outrora se torna algo bem factual: hodiernamente, a guerra ocorre em cinco dimensões: na terra, no mar, no ar, no espaço e no ciberespaço[3]. As quatro primeiras se caracterizam por envolver diretamente a natureza; já a última é um ambiente complexo, totalmente artificial, criado pelo ser humano[4].

Guerra cibernética (*cyber war* ou, ainda, ciberguerra) é um conceito novo e amplamente difundido na mídia mundial, durante este início de século XXI. Tal termo é quase sempre utilizado de forma confusa ou como sinônimo de qualquer ato de invasão *hacker* (intrusão) ou ataque a redes de computadores (*networks*) ou a computadores, por motivações políticas ou econômicas.

Nesse sentido, o objetivo deste texto é situar o fenômeno da guerra cibernética, atrelando-se suas pertinências para a Ciência Política e as Relações Internacionais, no que pese as implicações e os desafios das armas cibernéticas para com os Estudos de Segurança Internacional. Contudo, leva-se em conta que, "considerando as características singulares do ciberespaço e das armas cibernéticas, nenhuma tecnologia ou teoria existente será capaz de proporcionar um entendimento adequado"[5] sobre tal fenômeno.

---

2 John Arquilla e David Ronfeldt, "Cyberwar is coming!", *Comparative Strategy*, 12:2 (1993): 141-165.

3 Arne Schönbohm, *Germany's Security: Cyber Crime and Cyber War* (Verlagshaus: Octopus, 2012), 33-65.

4 Joseph S. Nye Jr., *The future of power*, 1st ed. (New York: PublicAffairs, 2011), 20.

5 Ross M. Rustici, "Armas Cibernéticas: Igualando Condições no Âmbito Internacional", *Military Review Brasil*, 4, jul.-ago. 2012: 61.

O presente texto está divido da seguinte maneira: na primeira parte, discute-se o conceito de guerra cibernética e outros correlatos; na segunda, a política de defesa do Brasil estabelecida na Estratégia Nacional de Defesa (END) e a questão da guerra cibernética; na terceira parte, técnicas e ferramentas utilizadas em ataques; depois, apresentamos alguns casos específicos e, no final, as principais conclusões deste texto serão sumarizadas.

Da guerra cibernética

Guerra eletrônica (*electronic warfare*)[6], infoguerra/*netwar*/*infowar*/desinformação, espionagem cibernética, guerra em rede. Esses são termos cada vez mais encontrados em noticiários e artigos científicos, mundo afora. Eles são comumente designados para imprimir o conceito de um fenômeno novo e complexo e, ainda, podem atuar conjuntamente com aquilo que tentam compreender o crime cibernético. Além disso, outros conceitos – tais como ciberterrorismo, crime cibercrime (*cybercrime*)[7] e hacktivismo – podem ser também confundidos com guerra cibernética, pelo fato de não apenas utilizarem a mesma dimensão – o ciberespaço, mais precisamente a *Internet* – e algumas técnicas, mas também por que aqueles podem ser utilizados como instrumentos governamentais para desviar responsabilidades e consequências de atos contra outras entidades governamentais ou não governamentais.

6 Guerra eletrônica pode ser definida da seguinte forma: utilização de emissões eletromagnéticas e eletro-ópticas com o objetivo de neutralizar ou reduzir a capacidade de combate de um adversário e dificultar ou impedir que o mesmo faça uso eficiente de suas emissões.

7 Para um estudo sobre a aplicabilidade das leis brasileiras e da Convenção de Budapeste aos cibercrimes, *vide*: Gills Vilar Lopes e Dalliana Vilar Pereira, *A Convenção de Budapeste e as leis brasileiras* (2009). http://www.academia.edu/786458/A_CONVENCAO_DE_BUDAPESTE_E_AS_LEIS_BRASILEIRAS, acessado em 2 abr. 2013.

Tanto o conceito clássico de guerra quanto o próprio conceito de cibernética – sendo este desenvolvido no final da década de 1940 – também não ajudam na elucidação do problema[8]. O primeiro é essencialmente percebido como um tipo de conflito envolvendo Estados soberanos onde ocorrem mortes e conquistas de territórios. O segundo é originalmente entendido como um conjunto de processos de comunicação e controle englobando humanos e máquinas[9].

A guerra, enquanto fenômeno característico das sociedades humanas, tem sofrido, ao longo dos anos, fortes transformações – em sua conduta, não em sua natureza – resultantes do avanço de tecnologias. De forma geral, definem-se quatro gerações/tipos de guerra[10]: a primeira é caraterizada pelo uso das armas de fogo, com grandes formações de infantaria estruturadas em linhas e colunas; a segunda, que começa com a Revolução Industrial, caracteriza-se pelo aumento do tamanho dos exércitos, a mecanização em larga escala das forças militares e do uso intenso da artilharia de campanha; a terceira se desenvolve pelo Exército Alemão na Segunda Guerra Mundial (*blitzkrieg*) e é baseada não apenas no poder de fogo, mas também na velocidade e na capacidade de deslocamento de pequenas unidades, e não mais em vultosas companhias. Nesta última geração, não se busca simplesmente destruir o inimigo, mas especialmente causar um colapso em suas forças. Já na guerra de quarta geração "o Estado

8 Como observa Clausewitz, "[...] *every age had its own kind of war, its own limiting conditions, and its own peculiar preconceptions. Each period, therefore, would have held to its own theory of war, even if the urge had always and universally existed to work things out on scientific principles. If follows that the events of every age must be judged in light of its own peculiarities*". Carl von Clausewitz, *On War* (New Jersey: Princeton University Press, 1984), 593.

9 Wiener, Norbert. *Cibernética e sociedade: o uso humano de seres humanos* (São Paulo: Cultrix, 1968).

10 Há autores que não concordam com uma classificação da guerra em gerações, pois, para eles, a natureza da guerra é imutável. Um exemplo dessa posição acadêmica é: Érico Duarte, "As falácias em torno da proposta de guerra de quarta geração". *Anais do IV Encontro Nacional da ABED*, 2010. http://abedef.org/encontrosnacionais2/2010-brasilia, acessado em 8 fev. 2013.

perde o monopólio sobre a guerra. Em todo o mundo, os militares se encontram combatendo oponentes não estatais tais como a al-Qaeda, o Hamas, a Hezbollah e as [Farc][...]. Quase em toda parte, o Estado está perdendo"[11]. Nessa linha de raciocínio, considera-se guerra de quarta geração os conflitos essencialmente assimétricos onde o uso da tecnologia e da propaganda/influência cultural são suas principais armas não letais. Nesses termos, caracteriza-se a guerra cibernética como um elemento definidor da guerra de quarta geração[12].

Atualmente, vive-se numa sociedade hiperconectada, cujos dados produzidos nela são contabilizados em *zettabytes* de informação, *i.e.*, um quatrilhão de *bytes*. Se já não bastasse tal enfoque quantitativo, o uso praticamente ubíquo da *Internet* e das aplicações *web* demonstram que grande parte das atividades humanas está completamente dependente da rede mundial de computadores, a *World Wide Web* (WWW). Imerso nessa mesma acepção, Karpesky afirma que "a infraestrutura de todo o planeta depende da *Internet*"[13]. Embora a citação anterior seja uma espécie de *ode ufanista à Internet* securitizador, por parte do criador russo do maior antivírus que há atualmente no mercado mundial, pode-se dizer que há um tipo de infraestrutura que se torna não só alvo pretendido a ataques cibernéticos, mas também uma das principais questões-chave sobre os estudos de segurança internacional que se debruçam sobre a guerra cibernética: as infraestruturas críticas baseadas em redes de computadores.

---

11 William Lind, "Guerra de Quarta Geração", *Military Review*, jan./fev. 2005: 14.

12 Luis Bonilla e El Troudi Haiman. *Guerra de Cuarta Generación y la Sala Situacional* (Caracas: Ediciones Gato Negro, 2004).

13 Marcelo Ninio, "Guerra ciberespacial", *Folha de São Paulo*, 29 jul. 2012. http://www1.folha.uol.com.br/fsp/ilustrissima/57291-guerra-ciberespacial.shtml, acessado em 21 abr. 2013.

Segundo a Estratégia Nacional de Segurança Cibernética do Canadá[14], infraestruturas críticas são o conjunto de processos, sistemas, instalações, tecnologias, redes, bens e serviços necessários para garantir a saúde, a segurança ou o bem-estar da população, bem como a eficácia do governo. Esse conjunto pode ser tanto infraestruturas autônomas quanto dependentes dentro ou fora das fronteiras de um país. A interrupção desses sistemas pode causar perdas de vidas e fazer com que efeitos econômicos adversos ocorram, além de prejudicar significativamente a confiança do cidadão.

Assim, infraestruturas críticas em redes estão inexoravelmente atreladas ao que se chama de guerra cibernética *lato sensu* (*cyber warfare*) e *stricto sensu* (*cyber war*)[15].

A dificuldade de se conceituar o termo *guerra cibernética* pode ser percebida não apenas pela falta de uma regulamentação internacional, mas também pela descrença de vários pesquisadores sobre a própria existência do conceito. Nenhum dos principais tratados internacionais sobre a regulamentação de conflitos armados e direitos civis assinados depois de 1945 (IV Convenção de Genebra e as Relativas à Proteção de Vítimas em Conflitos Armados Internacionais e Não Internacionais) faz qualquer referência a guerras cibernéticas. Peter Sommer e Ian Brown afirmam que a grande maioria dos acontecimentos descritos

---

14 Sécurité publique Canada, *Stratégie de cybersécurité du Canada*, Ottawa, 2010. http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-fra.pdf, acessado em 24 abr. 2013.

15 Para um estudo ontológico acerca dos principais termos que envolvem o tema guerra cibernética, ver segunda seção de: Gills Vilar Lopes, *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 – Curso de Ciência Política, Universidade Federal de Pernambuco – UFPE, 2013), Orientador: Prof. Dr. Marcelo de Almeida Medeiros. http://www.academia.edu/3418989/Reflexos_da_digitalizacao_da_guerra_na_politica_internacional_do_seculo_XXI_uma_analise_exploratoria_da_securitizacao_do_ciberespaco_nos_Estados_Unidos_Brasil_e_Canada, acessado em 18 mai. 2013.

como guerra cibernética não deve ser classificada com este termo, e que sua designação é exagerada, afirmando ser "*unlikely there will ever be a pure 'cyber war'*"[16]. Howard Schmidt, conselheiro de Barack Obama, defende que não há guerra cibernética: ela é apenas uma metáfora para outras atividades criminosas[17].

Um dos primeiros trabalhos a tentar conceituar estrategicamente o que é guerra cibernética é o artigo de John Arguilla e David Ronfeldt, publicado em 1993. Nele, os autores buscam delimitar o alcance estratégico de tal conceito, ao identificar outras práticas que, embora confundidas com a guerra cibernética, não é ela. O exemplo mais notório é a chamada guerra de informação ou *netwar*, que, segundo esses autores[18], se refere a "[...] *trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it*". Nesse sentido, guerra informacional "[…] *may focus on public or elite opinion, or both*" e não toca, portanto, na seara estratégico-militar.

Os defensores do conceito de guerra cibernética entendem que a *Internet* é uma dimensão de conflito onde o modelo clássico da guerra – ataque e defesa – e sua lógica são reproduzidos[19]. Mesmo que não haja mortes, como em uma guerra convencional, suas consequências são reais, e, desta forma, ela deve ser vista como tal.

O ataque do *worm* Stuxnet às centrífugas de enriquecimento de urânio do Irã é percebido como um exemplo real de como um ataque

16 "Study: unlikely there will ever be a pure 'cyber war'", University of Oxford, 17 jan. 2013. http://www.ox.ac.uk/media/news_stories/2011/111701.html, acessado em 13 abr. 2013.

17 Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar", *Wired*, 4 mar. 2010. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar, acessado em 9 mai. 2013.

18 Arquilla e Ronfeldt, "Cyberwar is coming!", 144.

19 Ver, por exemplo, Soren Olson, "Treino de sombra: a guerra cibernética e o ataque econômico estratégico", *Military Review*, set./out., 2012.

cibernético, com conotações estratégicas, pode ter consequências reais na parte física (*hardware*), da mesma maneira que um ataque real. Como observa Olson, o fato é que "[...] efeitos do Stuxnet no *software* da Siemens permanecem sem reparo, anos depois dos ataques [...]"[20].

Portanto, como se vê, os pesquisadores que não acreditam na existência de guerras cibernéticas, de uma forma geral, têm suas preocupações mais centradas na questão jurídica do direito internacional e veem a guerra a partir de seu conceito clássico. Os que defendem existir realmente a guerra cibernética – e que esta não deve ser confundida com ciberativismo ou cibercrimes, por exemplo – percebem a guerra como um fenômeno histórico dependente das transformações que as tecnologias de informação e comunicação (TIC) trazem como desafio ao Estado. Contudo, este ainda é um conceito em discussão, inclusive para os governos[21]. Independente das divergências, o fato é que centenas de países desenvolvem técnicas e armas cibernéticas, e o número de operações de defesa e ataque cibernéticos tem aumentado fortemente[22].

Reforçando o exemplo do Stuxnet, seus impactos foram tão assombrosos que, não por menos, muitos autores – *e.g.*: o ex-Conselheiro sobre Terrorismo, da Casa Branca, Richard Clarke[23]; o

---

20 Olson, "Treino de sombra", 73.

21 William Jackson, "DOD struggles to define cyber war", *GCN*, May 12, 2010. http://gcn.com/articles/2010/05/12/miller-on-cyberwar-051210.aspx, acessado em 20 mai. 2013.

22 Pierluigi Paganini, "The Rise of Cyber Weapons and Relative Impact on Cyberspace", *INFOSEC Institute*, Oct. 5, 2012. http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace, acessado em 10 mai. 2013.

23 Richard A. Clarke e Robert K. Knake, *Cyber War: the next threat to national security and what to do about it*, 2nd ed. (New York: HarperCollins, 2012).

Ministro das Forças Armadas britânicas, Nick Harvey[24]; Sanger[25] etc. – consideram esse *worm* a primeira arma cibernética já criada.

Mas o que vem a ser uma "arma cibernética"? Na seção seguinte, demonstramos que tal conceito está intrinsecamente ligado a determinadas ferramentas e técnicas usadas para atacar ciberneticamente um inimigo.

Técnicas e ferramentas de guerra cibernética

Ataque cibernético pode ser definido como o conjunto de técnicas que, utilizadas para burlar o sistema de segurança de um computador ou conjunto destes, busca quebrar (*to crack*) a integridade de informações e/ou tirar do ar um determinado serviço virtual. Não é à toa que os indivíduos enquadrados nessa tipologia de crime são conhecidos como *crackers* – outro termo que o senso comum e a grande mídia, comumente, confundem com *hackers*[26].

O arsenal de ataques cibernéticos é deveras vasto: servidores e redes zumbis (*botnets*), scan[27], fraude, *worm*/vírus/*Trojan*/*spyware*, invasão a computadores (força bruta), *man-in-the-middle*, engenharia social[28], *e-mail spoofing*, negação de serviço (DoS, de *Denial of Service*) etc. Porém, o tipo de ataque depende basicamente do objetivo do

24 Nick Hopkins, "UK developing cyber-weapons programme to counter cyber war threat", *The Guardian*, 30 May 2011. http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive, acessado em 20 abr. 2013.

25 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown: 2012).

26 Grosso modo, *hacker* é o indivíduo – geralmente, uma pessoa autodidata e motivada pela curiosidade – que detém conhecimento acima da média acerca de aspectos da tecnologia da informação (TI). Já o *cracker* é o indivíduo – geralmente, um *hacker* – que se utiliza do ambiente cibernético para praticar crimes (*cybercrimes*).

27 Busca de informações em redes de computadores, com o objetivo de identificar vulnerabilidades.

28 Cf. Kevin Mitnick e William L. Simon, *A Arte de Enganar* (São Paulo: Makron Books, 2003).

atacante e pode deixar diferentes tipos de rastros identificáveis. Por exemplo, um ataque que utiliza a técnica de invasão do tipo *força bruta* ou *engenharia social* busca coletar informações no computador invadido e necessariamente demora mais tempo para ser executada, deixando, com isso, mais rastros de como e por quem o ataque foi feito. Outro exemplo: um ataque do tipo negação de serviço[29] que objetiva impedir o funcionamento de um servidor, por meio de uma sobrecarga do sistema, pode utilizar-se de redes de computadores zumbis – cujos utilizadores atacados não têm conhecimento de que estão sendo utilizados para este fim –, deixando menos rastros de sua atuação.

A motivação, o contexto onde ocorre e de onde parte o ataque, bem como o tipo de técnicas utilizadas são variáveis importantes na análise política desse fenômeno técnico.

Por exemplo, no caso da primeira guerra do Iraque, entre 1990 e 1991, o vírus que infectou o sistema de defesa iraquiano tinha o objetivo de inutilizar a defesa antiaérea do país, tendo como cenário a guerra declarada entre os governos de Sadam Hussein e dos Estados Unidos da América (EUA) e seus aliados.

Mais recentemente, no caso do Irã, o objetivo do Stuxnet era inutilizar determinado tipo de centrífuga de enriquecimento de urânio em um ambiente de "guerra fria" entre EUA e Israel, de um lado, e o governo iraniano do outro[30].

Já no que se refere ao caso da Estônia, o ataque de DoS ocorrido em 2007 tinha como objetivo levar o caos ao país, com a motivação clara de puni-lo pela retirada de um símbolo russo estabelecido durante o período soviético – neste caso, uma estátua de bronze do Soldado

29 Há três técnicas de DoS: inundação, amplificação e exploração de protocolos.

30 Sanger, *Confront and Conceal*, 2012.

Morto, que ficava no centro da capital Tallinn e fora removida para um afastado cemitério. Porém, a maioria dos autores sobre guerra cibernética não enquadra o caso Estônia-Rússia como uma guerra cibernética, tendo em vista a falta de provas que a Estônia insistiu em imputar ao Estado russo[31].

Já na guerra da Geórgia contra a Rússia, em 2008, causada pela independência da Ossétia do Sul, *sites* governamentais georgianos também sofreram ataques cibernéticos do tipo DoS[32].

Como se vê, as técnicas de ataques cibernéticos que estão à disposição de *crackers*, hacktivistas, militares e criminosos são as mesmas. A análise dos motivos da ação, do contexto em que os ataques ocorrem e as ferramentas utilizadas permitem delimitar quem ataca e a razão final de tal ataque.

Portanto, técnicas de guerras cibernéticas são instrumentos dentro de um contexto maior de conflito. Elas, *per se*, não ganham guerras, mas tornam a vitória mais provável para o lado que as emprega.

Armas cibernéticas

De todas as novas terminologias e neologismos que emergem com a *guerra cibernética*, certamente *armas cibernéticas* é a que tem crescido mais, nos últimos anos. Porém, ainda são poucos os documentos/autoridades públicos e/ou militares que as citam.

---

31 Cf. Gills Vilar Lopes, "A emergência do tema ciberguerra: contextualizando a criação do Centro de Defesa Cibernética à Luz da Estratégia Nacional de Defesa", *Seminário do Livro Branco de Defesa Nacional*, 2011. http://defesa.gov.br/projetosweb/livrobranco/arquivos/apresentacao-trabalhos/artigo-gills-lopes.pdf, acessado em 21 fev. 2013.

32 Daniel Oppermann, "Virtual Attacks and the Problem of Responsibility: the Cases of China and Russia", *Academia*, set. 2009. http://brasilia.academia.edu/DanielOppermann, acessado em 3 mai. 2013.

Mas, afinal, o que são armas cibernéticas?

Assim como ocorre com o conceito de guerra cibernética, o de arma cibernética ainda está em construção.

Por exemplo, Andress e Winterfeld[33] utilizam o termo "armas lógicas" (*logical weapons*) para designar as armas imaginadas quando se fala em guerra cibernética. Ainda, para tais autores, elas não se diferenciam – tecnicamente falando – daquelas que habitualmente se utilizam para atacar e defender no ambiente cibernético, mas é no escopo do seu uso que elas se distinguem das armas civis, por assim dizer. Nesse sentido, para eles, armas cibernéticas são um conjunto de ferramentas utilizadas para se fazer a guerra cibernética e estão divididas em cinco amplas categorias de ferramentas, a saber: reconhecimento, exploração, infraestrutura, aplicação e sistema operacional[34]. Todavia, é sabido que os sistemas lógicos são totalmente dependentes dos físicos[35]. Justamente por essa relação intrínseca entre *software* e *hardware* – ataques em um meio *pode* ocasionar efeito noutro, como no caso do Stuxnet –, os autores atentam para outros tipos de armas: as físicas. Mas, mais importante do que o vasto leque de possibilidades de armas físicas que se tem disponível, deve-se atentar para a relação em si desses dois reinos: o físico e o lógico. Em outras palavras, no âmbito da guerra cibernética, sabe-se que as infraestruturas físicas em rede são controladas por sistemas de controle industrial (ICS, de *industrial control systems*)[36], então se torna fulcral protegê-las de ataques cibernéticos que podem

33 Jason Andress e Steve Winterfeld, *Cyber Warfare: techniques, tactics and tools for security practitioners* (New York: Syngress, 2011), 83.

34 Andress e Winterfeld, *Cyber Warfare*, 84.

35 Andress e Winterfeld, *Cyber Warfare*, 119.

36 O ICS mais conhecido é o do tipo *Supervisory Control and Data Acquisition* (SCADA), que é o mesmo tipo de sistema lógico que foi alvo do Stuxnet.

tentar implantar algum tipo de arma cibernética. Nesse sentido, faz-se mister o estudo político dessas ferramentas tecnológicas.

Em palestra proferida no II Simpósio de Guerra Cibernética da Academia Militar das Agulhas Negras (Aman), em 2013, na cidade de Resende, Estado do Rio de Janeiro, o perito em segurança digital John Douglas Rowell classifica os tipos de ataques cibernéticos em quatro grandes categorias: espionagem, engenharia reversa, sabotagem e desinformação[37]. É justamente no grupo "sabotagem" que as chamadas armas cibernéticas aqui citadas podem ser alocadas com um grau maior de precisão. Como já mencionado, esse tipo de armamento não difere muito do comumente empregado por *crackers* e *script kids*[38]; o que vai ser, *de facto*, relevante para o âmbito da guerra cibernética é o alvo e a motivação por trás do ataque.

Outro conceito pertinente aos objetivos deste trabalho é o de Ataque a Redes de Computadores (ARC), em contrapartida à simples Exploração de Redes de Computadores (ERC)[39]. Rustici apregoa que, embora existam poucos casos evidentes de um ARC significativo, é possível identificá-lo nos *cases* da Estônia-Rússia, da Geórgia-Rússia e do Irã-Stuxnet.

Além disso, Lior Tabansky[40] informa que as armas cibernéticas são compostas majoritariamente por *software*, mas que, em alguns casos, também podem vir transvestidas de *hardware*. Indo mais além em sua análise, esse autor divide tais armas em três categorias:

---

37 John Douglas Rowell, "Guerra Cibernética: Vetores de Ataques", 27 abr. 2013. http://jdrowell.com/talks/AMAN2013, acessado em 2 mai. 2013.

38 Costuma-se chamar de *script kids* os *hackers* ou *crackers* inexperientes que, por meio do uso de kits de invasão geralmente comprados prontos (com *scripts* já bem desenvolvidos), vangloriam-se de seus atos e/ou apenas buscam praticar algum tipo de crime cibernético.

39 Rustici, *Armas Cibernéticas*, 62.

40 Lior Tabansky, "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs*, 3:1, May 2011: 80.

a) **Armas inequivocamente ofensivas:** diferentes tipos de *malwares*[41], como vírus, *worms*, cavalo de Tróia (*Trojans*) etc.;
b) **Ferramentas de uso dual:** monitoramento de rede, *scanner* de vulnerabilidades, criptografia etc.; e
c) **Ferramentas inequivocamente defensivas:** *firewall* e sistemas de recuperação de desastres.

Conforme se apresenta na Tabela 1, alocam-se as subdivisões de sabotagem cibernética, bem como técnicas, táticas, ferramentas e exemplos em que elas foram empregadas, conforme Rowell, Rustici e Tabansky.

Ainda, de acordo com Rustici, "uma das maiores preocupações de segurança para os Estados Unidos da América atualmente é como minimizar sua vulnerabilidade às armas cibernéticas"[42]. Não é por menos que Kevin Newmeyer[43], professor da National Defense University (NDU) dos EUA, informa que "*Cyber issues are increasingly of a concern in the NDU community at large*", mais especificamente, que "[...] *there is on-going discussion of the policy implications of cyber weapons in the university*". Ainda no que pese aos EUA, Gagnon[44] afirma que, devido ao elevado grau de interconectividade propiciado à sociedade estadunidense, o governo dos EUA está atento às ameaças cibernéticas, fazendo com que, ao se preparar para se defender, os estadunidenses fiquem na dianteira do desenvolvimento de armas cibernéticas altamente sofisticadas.

---

41 *Software* malicioso – daí seu nome derivar de *malicious software* – desenvolvido para, ilicitamente, infiltrar-se em um sistema computacional, visando danificar e/ou roubar informações.

42 Rustici, *Armas Cibernéticas*, 61.

43 Agradecemos ao professor Newmeyer por sua colaboração ao ser entrevistado.

44 Benoît Gagnon, "Cyberwars and cybercrimes", In Stéphane Leman-Langlois, Ed., *Technocrime: technology, crime and social control* (London, UK: Willan Publishing, 2008), 27.

Tabela 1: Tipos de ataques cibernéticos do tipo "sabotagem"

Técnica(s)	Tática	Ferramentas	Exemplo
Vírus, *Worm* (armas inequivocamente ofensivas)	Contaminação de arquivos executáveis	Browser Exploitation Framework (BeEF)	Stuxnet (2010)
DoS, DDoS	Ataques de *Denial of Service* simples ou distribuídos	ping -F, LOIC/ HOIC	Spamhaus vs CyberBunker, 300Gbps (2013)
Invasão	Invasão de máquina e execução de código não autorizado	metasploit, OpenVAS	Anonymous vs Coreia do Norte (2013)
SQL Injection	Alteração de comandos de acesso a bancos de dados	SqlMap, Absinthe	hospital israelense em SP (2011)
Ataque a Redes de Computadores (ARC)	prejudicar, negar, degradar ou destruir redes de computadores, as informações nelas contidas ou os sistemas por elas controlados	ferramentas *hacker* de uso dual	Estônia (2007), Geórgia (2008) e Irã (2010)

Fonte: Elaboração própria, a partir de Rowell (2013), Rustici (2012) e Tabansky (2011), com adaptações.

As preocupações acerca das potencialidades das armas cibernéticas ganham força a partir do ano de 2010, quando o *worm* Stuxnet não só é descoberto, como também suas consequências se tornam públicas. Ao ser perguntado sobre o porquê de o Stuxnet ter sido considerado a primeira arma cibernética, o professor da University of Surrey, na Inglaterra, Alan Woodward[45] rebate, informando que o "*Stuxent was a peculiar hybrid in that it did seek to damage but a very particular type of damage. It sought to render the enrichment facility at Natanz useless by interfering with the control*

45 Esta citação é uma parte de entrevista fornecida pelo prof. Woodward para a Dissertação de Mestrado de Gills Vilar Lopes. Agradecemos a colaboração do entrevistado.

systems used to operate it. The information being fed back to the Natanz operators was modified so that the centrifuges were producing enrichment uranium that was not of sufficiently high quality for use in a fission weapon".

Uma vez vazado na *Internet*, cria-se uma variante do Stuxnet chamada Duqu, que só é descoberta em 2011, quando o *Laboratory of Cryptography and System Security* da *Budapest University of Technology and Economics* (CrySyS) publica um relatório sobre a perícia do seu código-fonte. De acordo com esse documento, os resultados da análise abrem um novo capítulo na história dos ataques cibernéticos cujos alvos não são genéricos, mas bem específicos[46].

Um ano após o relatório do CrySyS, uma segunda variante ainda mais complexa do Stuxnet é descoberta: trata-se do Flame(r) ou sKyWIper[47]. Sua vacina só foi criada em maio daquele ano. Até esse período, nenhum dos 43 antivírus testados pela equipe de respostas a incidentes informáticos (CERT, de *computer emergency response team*) iraniana pôde acusá-lo[48].

A Figura 1 demonstra a linha do tempo do StuxNet e de suas variantes, entre os anos de 2010 e 2012.

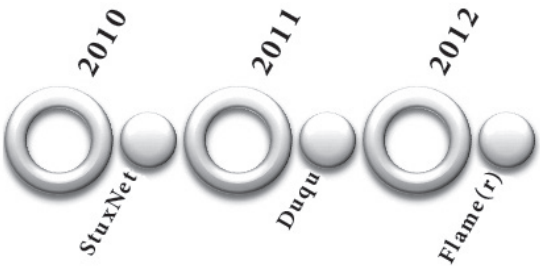
Portanto, é com base no potencial destrutivo de uma arma cibernética que reside o temor de, um dia, uma sabotagem desse tipo auferir danos incalculáveis a uma infraestrutura crítica de uma dada sociedade. Mais que isso: pelo fato de praticamente todos os dispositivos informacionais e telecomunicacionais estarem ligados

46 Boldizsár Bencsáth et al. *Duqu: a Stuxnet-like malware found in the wild* (Budapeste: Laboratory of Cryptography and System Security (CrySyS) at the Budapest University of Technology and Economics, 2011), 2.

47 Lopes, *Reflexos da Digitalização da Guerra*, 49.

48 República Islâmica do Irã, "Identification of a new targeted cyber-attack", *Iranian Computer Security Incident Response Teams – CSIRT*, 28 maio 2012. http://www.certcc.ir/ index.php?name=news&file=article&sid=1894, acessado em 2 de jan. 2013.

Figura 1: Linha do tempo do StuxNet e de suas variantes



Fonte: Lopes, "Reflexos da Digitalização da Guerra", 49 (com adaptações).

em redes, um ataque cibernético a tal tipo de infraestrutura pode promover um efeito dominó, dinamizando ainda mais o ataque. É nesse mesmo sentido que Rustici apregoa que a sofisticação e a capacidade dos ataques cibernéticos crescem em proporções diretas ao grau de conectividade da sociedade[49]. Vale lembrar que essa correlação é um dos três índices (*cyber offense*, *cyber dependence* e *cyber defense*) que Clarke e Knake[50] levam em conta para criar o famoso *framework* chamado *Overall Cyber War Strength*. Nele, além desse índice – que apregoa que quanto menos uma nação está conectada, maior também é o seu escore no *ranking* –, outras três variáveis são analisadas, conforme a Tabela 2.

A dependência para com a Rede Mundial de Computadores (*cyber dependence*) tem tornado-se cada vez mais latente, para a enorme maioria dos países, com o passar dos anos. De acordo com a Consultoria McKinsey[51] (dados de 2010), a *Internet* é essencial

49 Rustici, *Armas Cibernéticas* 61.

50 Clarke e Knake, *Cyber war*, 148.

51 Matthieu Pélissié du Rausas et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity", May 2011. http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters, acessado em 23 abr. 2013.

Tabela 2: *Overall Cyber War Strength*

Nation	Cyber Offense	Cyber Dependence	Cyber Defense	Total
U.S.	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

Fonte: Clarke e Knake, Cyber war, 148 (com adaptações).

para a economia mundial, pois possui dois bilhões de usuários, é responsável por 3,4% do PIB de um conjunto de treze países analisados (incluindo Brasil, EUA, Inglaterra, Japão e Rússia), é grande geradora de empregos (por exemplo, a França criou 700 mil vagas, desde 1995), representa 21% do crescimento do PIB de 2005 a 2010 nos países desenvolvidos, 8 trilhões de dólares mudam de mãos por ano através do *e-commerce*, em torno de dois terços de todas as empresas do mundo possuem presença na *Internet*, dentre outros fatores. Por essas razões, a defesa econômica dos interesses estatais – e sob a alegação de proteção aos interesses privados de seus cidadãos – parece ser o tom de algumas estratégias nacionais de defesa, como é o caso da *National Security Strategy*, lançada pela Administração Obama, em 2010[52]. Esse tom também está estampado nas palavras do próprio Presidente dos EUA, quando, da Casa Branca, ele profere que "[...] *it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation*"[53].

52 The White House, *National Security Strategy*, Washington DC, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, acessado em 14 abr. 2013.

53 Presidente Barack Obama, *Remarks by the president on securing our nation's cyber infrastructure*, Washington, DC: The White House's Office of the Press Secretary, 29 maio 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure, acessado em 13 abr. 2013.

Voltando à Tabela 2, como pode ser visto, a Coreia do Norte é a de melhor escore no índice *Cyber Dependence*, uma vez que o acesso à *Internet* é totalmente controlado pelo Estado. Assim, a implantação de armas cibernéticas em países como Coreia do Norte, Irã e China, por exemplo, tende a ser mais um resultado de implantação *in loco* da arma cibernética do que uma contaminação via *Internet*. O caso do Stuxnet é, mais uma vez, trazido, aqui, à tona, pois ele exemplifica, de maneira análoga, a frase anterior. Segundo um professor de Harvard[54], o *worm* foi implantado no sistema SCADA das centrífugas de enriquecimento de urânio do Irã por intermédio da atuação de agentes secretos que o implantaram num *notebook* de um dos técnicos que davam suporte ao sistema. O *worm* ficou "incubado", esperando o *notebook* ser conectado ao sistema iraniano. O exemplo iraniano é tão emblemático por, basicamente, duas razões: a primeira é que, de maneira pragmática, o *software* conseguiu causar danos à infraestrutura crítica baseada em sistema SCADA de enriquecimento de urânio; e o segundo motivo se refere ao fato de que não foi preciso o sistema está conectado à *Internet* para ser infectado. Depois deste episódio de 2010, muitos países – praticamente todas as principais economias do mundo – lançaram suas políticas/estratégias nacionais de segurança/defesa cibernética e/ou criaram organismos militares voltados especificamente para a defesa cibernética[55].

Num estudo sobre nove documentos oficiais militares de sete países, Gills Vilar Lopes[56] busca elencar quais deles, ao tentar securitizar militarmente as ameaças ciberexistenciais, tratam

54 Sanger, *Confront and Conceal*, *passim*.

55 Lopes, *Reflexos da digitalização da guerra*, 64-65.

56 Gills Vilar Lopes, "Securitizando o ciberespaço: um estudo comparativo sobre a defesa cibernética em sete países", *4º Encontro Nacional da ABRI*, 2013, http://www.encontronacional2013.abri.org.br/download/download?ID_DOWNLOAD=300.

explicitamente da questão das armas cibernéticas. Primeiramente, ele faz um *scanning* em todos os documentos – por meio do *software* ATLAS.Ti[57] – para encontrar o termo "Stuxnet". Apenas dois deles citam o *worm: The National Cyber Security Strategy* holandesa e *Cyber Security Strategy for Germany*, da Alemanha.

O caso brasileiro, mais especificamente, por meio de sua enxuta Política Cibernética de Defesa (PCD), lançada em 2012, não cita nem o Stuxnet nem se refere aos famosos casos da Estônia e da Geórgia (a política nacional de segurança cibernética do Canadá o faz, por exemplo), mas menciona o fato de poder "atuar no reconhecimento de *artefatos e desenvolvimento de ferramentas cibernéticas*, em conjunto com a [...]" Presidência da República[58]. Embora tal medida descrita na PCD possa ser encarada como ousada, a mesma é justificada – e a própria PCD se encarrega de explicitar isso – pelo fato de o Brasil sediar grandes eventos (Copa das Confederações 2013, Copa do Mundo 2014 e Olimpíadas 2016) e, portanto, necessitar de uma estrutura de defesa ainda mais complexa e robusta que a atual.

A Tabela 3 apresenta um resumo do que é exposto no supracitado estudo de Gills Vilar Lopes.

Tabela 3: Análise de nove estratégias nacionais de defesa ou de segurança cibernética

Estado	Documento(s)	Ano
Alemanha	Cyber Security Strategy for Germany	2011
Brasil	Estratégia Nacional de Defesa	2008
	Política Cibernética de Defesa	2012

→

57 ATLAS.ti: The Qualitative Data Analysis & Research Software, http://www.atlasti.com/index.html.

58 Brasil, "Portaria Nº 3.389/MD, de 21 de dezembro de 2012". Edição: Ministério da Defesa do Brasil. *Diário Oficial [da] República Federativa do Brasil* (Poder Executivo) I (12 2012): 11-12.

Estado	Documento(s)	Ano
Canadá	Canada's Cyber Security Strategy	2010
EUA	National Security Strategy	2010
	Strategy for Operating in Cyberspace	2011
França	Information systems defense and security France's strategy	2011
Países Baixos	The National Cyber Security Strategy	2011
Reino Unido	The National Security Strategy	2010
	The UK Cyber Security Strategy	2011

Fonte: Lopes, 2013 (com adaptações).

Considerações finais

Como Nye sugere, "*until now, the issue of cyber security has largely been the domain of computer experts and specialists*"[59]. Nesse sentido, este trabalho buscou situar algumas oportunidades (e desafios) em que tanto cientistas políticos quanto internacionalistas podem encontrar bastante material para inferir sobre um dos fenômenos-mãe de Relações Internacionais em sua acepção mais nova: a guerra cibernética, no que pese o uso estratégico das armas cibernéticas.

A utilização de técnicas de guerra cibernética *num contexto de conflito militar declarado* entre dois ou mais Estados nunca ocorreu. A falta de legislação internacional[60] – ao contrário do que ocorre na seara da segurança cibernética (*cyber security*), com a Convenção de Budapeste sobre Cibercrimes, assinada em 2011 – faz com que os Estados busquem unilateralmente medidas para sanar tal

59 Nye, *The future of power*, 18.

60 Talvez, o que mais se aproxime de um remédio jurídico do tipo Convenção Internacional é o recém-lançado *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, pelo *NATO Cooperative Cyber Defence Centre of Excellence* (CCD-COE).

"*vacum legis* cibernético". Exemplo disso é visto em 2011 quando o Departamento de Defesa estadunidense (DoD, de *Department of Defense* ou simplesmente Pentágono) cogita poder responder a ataques cibernéticos com o uso da força bélica/militar/convencional[61].

Sua utilização tem sido esporádica e de comprovação complexa e nunca oficialmente admitida[62], como ocorreu com o caso estoniano. Corroborando com essa linha de raciocínio, de acordo com uma reportagem veiculada no jornal *Diario de Pernambuco*, "até hoje já foram oficialmente registrada três guerras cibernéticas no mundo: na Estônia (2007), na Geórgia (2008) e entre as Coréias do Norte e do Sul (2009)"[63]. Contudo, mesmo que não tenha havido uma guerra cibernética, *de facto*, entre dois atores estatais (houve por parte de apenas um dos lados), os alvos principais de um ataque cibernético, num contexto de conflito de larga escala, são claramente reconhecidos: infraestruturas críticas civis – *e.g.* redes de eletricidade, telefones, *Internet*, água, gás, transporte, metrô, finanças etc. –, *sites* governamentais e sistemas de defesa do tipo comando, controle, comunicações, computadores, inteligência, vigilância e reconhecimento (C4ISR).

Outro elemento a ser considerado nos estudos de segurança internacional sobre guerra cibernética é a utilização de organizações não militares como "testas de ferro" de ações políticas de ataque cibernético. O ataque à Estônia em 2007, por exemplo, foi originário

61 Siobhan Gorman e Julian E. Barnes, "Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force", *The Wall Street Journal*, 30 maio 2011. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html, acessado em 20 abr. 2013.

62 Rustici, "Armas Cibernéticas", 61.

63 "Ciberguerras e ciberterrorismo fazem surgir novo profissional na área de TI", Diario de Pernambuco. http://www.old.diariodepernambuco.com.br/nota.asp?materia=20100719215545, acessado em 20 abr. 2013.

da Letônia[64]. Porém, o governo estoniano acusou o da Rússia pelo ataque. No entanto, há possibilidade de o governo russo ter utilizado atores não estatais no evento[65]. A China tem sido outro país acusado de utilizar o ciberativismo político com propósitos governamentais[66].

Se, ainda em 1993, quando se asseverava que a revolução da informação iria mudar tanto a forma como as sociedades entrariam em conflito quanto como suas forças armadas poderiam fazer a guerra[67], o século XXI vê surgir não só um campo de análise técnica quanto a esse fenômeno, mas também político.

64 Diário de Pernambuco, 2010.

65 Bill Brenner, "Experts doubt Russian government launched DDoS attacks", *SearchSecurity*, 18 maio 2007. http://searchsecurity.techtarget.com/news/1255548/Experts-doubt-Russian-government-launched-DDoS-attacks, acessado em 20 abr. 2013.

66 Alexander Klimburg, "Mobilising Cyber Power", *Suvirval*, 53:1 (2011): 44.

67 Arquilla e Ronfeldt, "Cyberwar is coming!", 144.

CAPÍTULO 2

Em busca de uma ordem cibernética internacional

Oscar Medeiros Filho

Introdução

Com o advento das redes de computadores e o surgimento de infovias (sistemas interligados de informação) temas como segurança, defesa e guerra cibernética passam a fazer parte da agenda estratégica dos Estados. Ataques cibernéticos como os ocorridos na Estônia (2007), Geórgia (2008) e Irã (2010) têm chamado a atenção dos governos para esse novo tipo de ameaça: a guerra cibernética. Mais recentemente, as denúncias envolvendo espionagem da *National Security Agency* (NSA) trouxeram o debate do tema para as agendas de segurança nacional em todo o mundo. Nesse tipo de guerra, os alvos não são mais somente instalações militares, mas envolvem estruturas de governo, empresas, sistemas de transporte e logística, entre outros. O presente artigo visa a analisar aspectos teóricos relacionados à segurança, à defesa e à guerra cibernética. Parte-se da hipótese de que o tema *cibernética* encerra diferentes questões que variam de aspectos mais ligados à segurança pública (*cybercrime*) a outros mais afeitos a conflitos típicos da relação de poder entre Estados (*cyberwar*). Do ponto de vista das ferramentas, técnicas e conhecimentos utilizados não há praticamente diferenças

entre os dois campos. A principal diferença reside na origem e intenção do autor: enquanto a primeira sugere conflitos no campo privado, a segunda envolve necessariamente relações de poder entre Estados. Até que ponto as ações oriundas de um indivíduo com motivações pessoais não podem ser consideradas como sendo guerra cibernética? Em termos militares, guerra cibernética deve ser entendida como uma combinação de ataques e defesas a sistemas computacionais envolvendo operações de proteção da informação e das infraestruturas críticas de um Estado. Na guerra, toda política, toda estratégia e, consequentemente, todo emprego das Forças Armadas possuem como objetivo último o interesse nacional, representado pela ampliação do poder nacional e defesa de sua soberania. Entretanto, as ameaças de caráter transnacional, como é o caso das ameaças cibernéticas, afetam de forma conjunta a segurança internacional e, por consequência, a segurança nacional de cada um dos países de forma isolada. Tais ameaças constituem fenômenos que se impõem muito além das fronteiras nacionais e possuem consequências globais. O aumento de fluxos, a proliferação de redes e a velocidade com que transitam mercadorias, pessoas e informações entre diferentes países geram teias de interesses que se interpenetram e criam múltiplos canais de contato entre diferentes sociedades, colocando em xeque a capacidade dos Estados de agirem sozinhos como sujeitos controladores dos próprios destinos. Com maior fluidez, superando as fronteiras territoriais rígidas, os fenômenos transnacionais tendem a impor a necessidade de uma governança global. O processo crescente dessas redes de interdependência aponta para a necessidade de maior regulação, através do estabelecimento de redes de governança como forma de gestão além das fronteiras nacionais. Trata-se aqui da necessidade criação de um regime que,

de alguma forma, limite as ações de ciberguerra entre Estados. Tal quadro pode levar os governos nacionais a sacrificar parte da própria liberdade de ação a fim de restringir e tornar mais previsíveis as ações dos outros na sua direção[1]. Nesse sentido, há um vínculo estreito entre governança e ordem e, consequentemente, entre governança e segurança. Tal vínculo sugere um interessante debate teórico acerca da guerra cibernética em meio à necessidade de construção de uma sociedade internacional. Tal debate é o objetivo principal da presente proposta.

Para tanto, o artigo está dividido em três seções. A primeira abordará a cibernética como um dos setores da segurança multidimensional, utilizando-se de autores da chamada Escola de Copenhagen. A segunda seção procurará distinguir os conceitos de "*cybercrime*" e de "*ciberwar*". O terceiro retomará o conceito de ordem e de sociedade internacional desenvolvido especialmente por Heddley Bull para discutir os dilemas apresentados pela cibernética para a segurança internacional.

Cibernética como setor da segurança multidimencional

As transformações geopolíticas ocorridas nas últimas décadas do século XX impactaram profundamente o campo de estudo da segurança internacional. Em um contexto mundial marcado pela violência estrutural e por carência de governança global, novos temas foram introduzido, como mudanças climáticas e cibernética, por exemplo.

1 Joseph S. Nye, *O paradoxo do poder americano* (São Paulo: Unesp, 2002), 175.

Desde que Barry Buzan[2] apresentou, nas últimas décadas do século passado, a sua proposta de ampliação do conceito de segurança para além das dimensões político e militar, nenhuma ameaça se apresentou tão impactante quanto aquelas oriundas do grande desenvolvimento tecnológico observado nos últimos tempos. As "novas" dimensões propostas por Buzan (econômico, ambiental e societal) parecem não dar conta das novas demandas oriundas do chamado "espaço cibernético".

As preocupações em torno dessa nova ameaça são tantas que já há autores que consideram a "cyber security" um setor particular no campo dos estudos de segurança[3].

A seguir, serão apresentados alguns elementos que, em nossa opinião, justificam a relevância da cibernética como setor específico dentre os temas de segurança internacional.

Origens da cibernética

O termo *cibernética* deriva do grego *kybernetidé,* que significava a arte de pilotar uma embarcação. Ao longo dos tempos, o termo foi ganhando novas conotações. Em Platão, referia-se à "arte de governar". Já em meados do século XX, o matemático Norbert Wiener[4] definia cibernética como "o estudo do que em contexto humano é às vezes

2 Barry Buzan, People, States and Fear: An Agenda for International Security Studies in Post Cold War Era (Londres: Lynne Rienner, 1991).

3 Lene Hansen e Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", International Studies Quarterly, Vol 53, Nº 4, (2009): 1155-1175.

4 O interesse de Wiener por esse tema parece ter origem em um projeto de pesquisa iniciado nos primeiros anos da década de 1940, quando, como parte do esforço de guerra norte-americano, ele recebeu a incumbência de desenvolver um "sistema de controle de baterias anti-aéreas que fosse capaz de acompanhar a trajetória em que se movia um avião, predizer sua posição futura e disparar fogo levando em conta, senão só os hiatos humanos do canhão e do avião envolvidos." (Moreira, 1980, 32).

descrito genericamente como o ato de pensar e o que em engenharia é conhecido como controle e comunicação"[5].

A percepção de cibernética como ameaça à segurança surge no final do século XX, relacionada a vulnerabilidades de redes de computadores. Inicialmente, as preocupações possuíam natureza meramente técnica. O conceito de "cyber security" ganhou força no pós-Guerra Fria em um contexto marcado pelas inovações tecnológicas e por mudanças geopolíticas globais[6].

Com o advento das redes de computadores (especialmente a *Internet*), a conotação da cibernética se aproximou cada vez mais da ideia de infovias (sistemas interligados de informação, comunicação e controle).

Nesse contexto, a percepção de que sistemas interligados a estruturas críticas são vulneráveis a ataques de agentes intencionais dá início a um processo de securitização da cibernética. O que antes envolvia "*computer security*" evolui para "*cyber security*". Neste caso, como afirmam Hansen e Nissenbaum[7], em pouca palavras, "*cyber security*" pode ser entendido como um cálculo simples resultante da soma: "*computer security*" + "securitização"[8].

A prática de ataques virtuais em sistemas informatizados surge mesmo antes dos debates sobre cibernética como ameaça percebida.

---

5 Marílio Marques Moreira, "Karl Deutsch, a Política e a Cibernética", in Deutsch na UNB: conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980 (Brasília: Editora da UNB, 1980), 33.

6 Lene Hansen e Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol 53, Nº 4, (2009): 1155.

7 Ibidem: 1160.

8 Securitização é aqui entendida como o uso da retórica para transpor uma questão de política pública para uma esfera elevada forma extremada de politização (BUZAN, 1998, p. 26), deixando-a no mesmo nível de prioridade de outros temas tradicionais de defesa externa, como soberania e integridade territorial, por exemplo, que, em última instância, implicam o emprego da força.

Segundo Oppermann[9], os primeiros ataques cibernéticos remontam aos anos 1980, quando os EUA usaram *hackers* para se infiltrar em redes de computadores da União Soviética, com a intenção primeira de espionagem. A aplicação de ações cibernéticas na guerra, entretanto, teve início com o desenvolvimento das redes nos anos 1990, sendo a guerra do Kosovo, em 1999, o primeiro cenário. Desde então, os ataques virtuais tem se multiplicado. Em termos quantitativos e qualitativos, envolvendo cada vez mais questões políticas e econômicas em diversos países.

Alguns casos tiveram bastante repercussão. Em abril de 2007, foram divulgados ataques maciços a instituições públicas e privadas da Estônia; em agosto de 2008, ocorreram atuações cibernéticas no setor estratégico da Geórgia; foram noticiadas ações nos complexos industriais do Irã, e, mais recentemente, tornou-se público o caso *WikiLeaks,* que divulgou cerca de 250.000 mensagens confidenciais dos Estados Unidos da América, e o caso Prism (suposta parceria da Agência de Segurança Nacional com empresas de informática – *Google, Yahoo, Facebook, Microsoft* e outras – em ações de espionagem virtual).

A natureza das ameaças cibernéticas

Ameaças cibernéticas se relacionam a um grande espectro de temas envolvendo sensoriamento, monitoramento e atuação em diferentes campos: eletromagnético (telecomunicações), redes de computadores (infovias) e controle da informação (sistema

9 Daniel Oppermann, *Virtual attacks and the problem of fresponsibility: the case of China and Russia*, *Carta Internacional* 2 (2010): 13.

de informação). De qualquer forma, a *Internet*, e as redes a ela interligadas, é o *locus* central onde as ameaças ganham maior destaque no espaço cibernético.

Atualmente, a maioria dos sistemas de informação, necessários para o funcionamento de infraestruturas básicas da sociedade moderna, encontra-se interligada por meio de redes de computadores. Nesse contexto:

> Os alvos não são mais somente pessoal e instalações militares. Agora, bancos, usinas elétricas, empresas de telefonia e de telecomunicações, sistemas de transporte e logística, serviços de emergência e segurança pública, entre outros são alvos em potencial, uma vez que a indisponibilidade continuada de quaisquer destes serviços certamente levaria uma nação ao colapso[10].

De fato, a relação entre sistemas virtuais e controle de infraestruturas essenciais é a chave para se entender a magnitude das ameaças cibernéticas. Além de possíveis ataques virtuais a sistemas de controle de infraestruturas críticas como estações de energia, transportes, distribuição de água etc., que, se atingidas, podem causar sérios danos à sociedade em geral, as ameaças cibernéticas se relacionam a ataques virtuais à segurança da informação em três diferentes níveis: o individual (uso de informações pessoais), o grupal (espionagem comercial/industrial) e o estatal (acesso a assuntos estratégico-militares e segredos de Estado).

10 André Melo Carvalhais Dutra, "Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto!". http://161.24.2.250/sige_old/IXSIGE/Artigos/GE_39.pdf, acessado em 08 out. 2011.

Cybercrime ou *cyber war*: entre o crime e a guerra

As ameaças cibernéticas se colocam entre o público e o privado e entre o econômico e o político. Esse caráter dual da cibernética a torna uma ameaça difusa, na qual o conceito de defesa parece fundir-se ao de segurança pública.

Considerando-se os objetivos do presente artigo, torna-se interessante desde já diferenciar a dimensão cibernética de defesa (ligado à noção de guerra) da dimensão de segurança pública (ligado mais a noção de ilícitos). Para tanto, usaremos as tipologias "*cybercrime*" para designar o tipo de violência cibernética aplicado notadamente no campo da segurança pública e "*cyberwar*" para designar a violência exclusiva às relações entre unidades políticas, típicas da guerra clássica.

Do ponto de vista das ferramentas, técnicas e conhecimentos utilizados não há praticamente diferenças: "é seguro afirmar que grande parte das pesquisas desenvolvidas, voltadas para a Segurança da Informação, possui aplicações em Guerra Cibernética"[11]. O que vai de fato diferenciar os campos é a origem e a intenção do autor: enquanto a primeira sugere conflitos no campo privado, a segunda envolve necessariamente relações de poder entre Estados. Ações oriundas de motivações privadas não podem ser consideradas como sendo guerra cibernética. Para que esta ocorra, portanto, faz-se necessária a "existência de patrocínio estatal"[12]. Nesse sentido, vale a pena retomar a ideia de Heddley Bull segundo a qual a "violência só é guerra quando exercida em nome de uma unidade política"[13].

11 André Melo Carvalhais Dutra, Ibidem.

12 Ibidem.

13 Heddley Bull, *A Sociedade Anárquica* (Brasília: UNB, 2002).

Em termos teóricos, torna-se possível estabelecer a diferença entre os dois tipos de violências aqui apresentados. Em termos práticos, entretanto, essa diferença torna-se mais complexa. Uma razões para isso é o fato do surgimento das questões cibernética serem contemporâneas das demandas de emancipação na agenda de segurança internacional.

Entre a soberanía dos Estados e a liberdade dos indivíduos

Para a discussão do presente tópico, torna interesante analisar a resposta da presidente Dilma Rousseff à denúncia apresentada por um jornal brasileiro de que os Estados Unidos mantiveram uma base de espionagem em Brasília mantida pela Agência de Segurança Nacional dos Estados Unidos e da CIA. Para a Presidente, o episódio de espionagem no país representaria "violação de soberania e de direitos humanos"[14]. Soberania e direitos humanos representam dois objetivos que, em termos de segurança cibernética, não são de fácil resolução.

O advento das ameaças cibernéticas é contemporâneo da ampliação da luta pelos direitos civis e de conquista de maior liberdade pelos indivíduos. De acordo com a lógica da segurança humana, desenvolvido pela ONU,

> O objeto de referência mudou dos Estados-nação para 'pessoas', nesse sentido, ser 'pessoacêntrico' significa 'preocupar-se com a maneira como as pessoas vivem e respiram em uma sociedade, quão livremente elas exercem suas várias escolhas, quanto acesso elas têm

14 "Dilma considera caso de espionagem 'violação de soberania e de direitos humanos'", *Folha de São Paulo*, 08/07/2013

> às oportunidades sociais e de mercado – e se elas vivem em conflito ou em paz[15].

Enquanto os Estados se sentem ameaçados pelas diferentes formas de violência cibernética, o conceito de emancipação aponta para a segurança individual, na qual a liberdade das pessoas (como indivíduos ou grupos), livres de constrangimentos, é objetivo fundamental. Nesse sentido, parece atual a ideia de Bull, segundo a qual, em termos extremos, "a doutrina dos direitos humanos e responsabilidades diante do direito internacional é subversiva com relação ao princípio de que a humanidade deve ser organizada como sociedade de estados soberanos"[16].

Nesse novo contexto, o Estado se vê, ao mesmo tempo, ameaçado por outros Estados, mas também pela pressão de sua própria população que, em muitos casos, sente insegura em relação às intenções de seus governos.

Se de um lado o Estado vê questionada a sua legitimidade de manter estruturas oficiais de informação (espionagem) e guerra cibernética (daí a expressão "defesa" cibernética, o que parece sugerir a negação de estruturas de ataque), por outro lado, como vimos na seção anterior, o Estado se sente inseguro em relação ao recrutamento de recursos humanos para ocupar cargos de agente de informação, uma vez que as ferramentas de network estão cada vez mais concentradas entre as empresas privadas.

Há hoje um grande debate, especialmente nos Estados Unidos, em torno da invasão de privacidade em troca de maior segurança pública. A esse respeito, o artigo de Richard Aldrich, professor de

15 Barry Buzan e Lene Hansen, *A evolução dos estudos de segurança internacional* (São Paulo: Unesp, 2012), 308.

16 Heddley Bull, *A Sociedade Anárquica* (Brasília: UNB, 2002), 176.

Segurança Internacional da University of Warwich, publicado recentemente por um jornal brasileiro[17] parece bastante provocador. Para o autor,

> A privacidade acabou. Não por conta das agências de espionagem, mas sim da tecnologia" (...). Ok, nós dois estamos sendo vigiados. Mas as agências de inteligência também estão sendo! (...) Acabou a privacidade para indivíduos, mas também acabou para empresas e agências de espionagem. Tudo vai ser transparente. (…) Daqui a cinco anos, vou ter um *chip* no meu braço para monitorar minha saúde. Se eu tiver um ataque cardíaco, o aparelho vai enviar informações para o médico. A informação dentro do meu corpo é a mais privada que tenho, mas estarei contente de ser monitorado se isso salvar minha vida.

O que Aldrich procura mostrar é que, não obstante o interesse dos indivíduos pela manutenção de suas privacidades, muitas vezes tendemos a abrir mão da privacidade e, em consequência, da segurança em troca de conveniências.

A reflexão de Aldrich nos leva a refletir sobre o paradoxo gerado pela ideia de um mundo sem fronteiras: se de um lado, a vida sem barreiras nos remete ao mundo da liberdade, por outro, nos expõe em demasia. Se por um lado queremos quebrar barreiras, por outro, faz-se necessário construir muros de proteção. Quando trazido para o debate de segurança internacional, a tensão entre segurança nacional e segurança humana (individual) será um complicador a mais na análise da segurança cibernética.

17 Richard Aldrich, "As agências são espionadas", *O Globo*, p. 33, 16 de junho de 2013.

Agentes cibernéticos

O espaço cibernético é dominado por diferentes agentes (*harckers, Insiders* etc), com ou sem patrocínio estatal, possuidores de notáveis conhecimentos técnicos, e engajados em diferentes atividades, tais como: espionagem industrial, propaganda, vigilância, censura e sabotagem.

Eles utilizam diferentes tipos de ferramentas empregadas em ataques virtuais, como por exemplo: programas *scanners* (mapeiam redes), *sniffers* (monitoram dados); *cracker programs* ("quebram" senha), *trojan horses* (camuflam informações), dentre outros.

A facilidade e diversidade de acessos aos espaços cibernéticos multiplica o número de agentes virtuais. A *Internet*, resultado do caráter dual da tecnologia militar, aproximou os civis do sentido *lato* de guerra. As "guerras cibernéticas" tendem a ser diferentes daquelas as quais estamos acostumados a ver. Nelas, certamente, o componente militar continuará a ser fundamental, mas a participação de agentes civis será cada vez mais necessária. Além disso, os melhores "guerreiros cibernéticos" não serão necessariamente aqueles alistados em exércitos formais. Em geral, o que se percebe em países mais desenvolvidos é que o setor privado está bem melhor equipado e estruturado para responder a uma ameaça cibernética[18].

Esse é um dado novo para se pensar a cibernética como um setor da segurança internacional: a partir do espaço cibernético, políticas de defesa e segurança adotadas pelos Estados dependerão cada vez mais da participação decisiva de empresas privadas. O recente escândalo provocado pelas denúncias de um funcionário de um empresa terceirizada sobre espionagens realizadas pela Agência Nacional de

18 Lene Hansen e Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol 53, Nº 4, (2009): 1162.

Segurança dos EUA revela o quanto as informações privilegiadas, que tradicionalmente eram exclusivas a agências de inteligência dos Estados, são hoje armazenadas por empresas privadas. Segundo Richard Aldrich[19], quem mais coleta dados sobre as pessoas são bancos, companhias aéreas, supermercados, provedores de *Internet*. Para ele, estas novas máquinas de vigilância acabam por enfraquecer as tradicionais agências de espionagem. O caso *Wikileaks* seria um exemplo disso.

Recrutar agentes para o "combate cibernético", entretanto, não será tarefa fácil para os Estados. O caso "*Edward Snowden*", que revelou detalhes da vigilância eletrônica desenvolvida pela Agência de Segurança Nacional (NSA), mostra o quão vulneráveis são essas agências. Machado et alli (2012) procuram estabelecer o perfil desses novos "guerreiros cibernéticos". Citando Samuel Huntington[20], os autores procuram mostrar que, sob o ponto de vista tradicional da ética militar, a obediência era observada como a maior das virtudes, atualmente, aspectos como flexibilidade de raciocínio, iniciativa, criatividade parecem ser fundamentais para o perfil dos novos agentes da guerra. Características comuns a quem lida com *Internet* – compartilhar informações e soluções – parece, à primeira vista, destoar da discrição tradicionalmente exigida dos militares, marcada pelo alto grau de discrição (cultura do sigilo) e lealdade. Além disso, é interessante destacar a dificuldade que os Estados, em geral, e as Forças Armadas, em particular, possuem atualmente em reter talentos na engenharia da computação e áreas afins, o que torna um desafio selecionar seus agentes cibernéticos.

19 Richard Aldrich, "As agências são espionadas", *O Globo*, p. 33, 16 de junho de 2013.

20 Samuel P. Huntington, *O Soldado e o Estado: Teoria e Política das Relações entre Civis e Militares*. (Rio de Janeiro: Bibliex, 1996).

Por uma ordem cibernética internacional

Na década de 1970, o Secretário de Estado norte-americano Henry Kissinger cunhou uma interessante frase: "*O mundo diminuiu*, *mas as nações* ainda *não se aproximaram*". O advento da rede mundial de computadores e a ampliação dos sistemas de controle a ela interligados, deu relevância à frase de Kissinger. O fato é que, a pesar da interdependencia crescente, as relações de poder e os intereses nacionais acabam sobressaíndo no sistema internacional. E nesse aspecto, "a vulnerabilidade parece ser um traço comum a todos os países"[21]. Como afirma o atual ministro da Defesa, Celso Amorim, "as fronteiras entre a guerra cibernética e as atividades de monitoramento de dados não são claramente demarcadas. A distinção é sutil e difícil de determinar."[22]

As recentes revelações de espionagem corroboram esse fato. Em depoimento, James Clapper, diretor de agência nacional de inteligência dos EUA, declarou que "conhecer as intenções dos líderes é uma espécie de princípio básico do que nós coletamos e analisamos". Para ele, países aliados, incluindo integrantes da UE (União Europeia), também espionaram os EUA[23].

Em recente artigo, Richard D. Mahoney[24] afirma que a Presidente Dilma, em seu último discurso na Assembleia Geral da ONU, conseguiu chamar a atenção do mundo para uma prática perigosa

---

21 Celso Amorim, "Brasil, um país provedor de paz", *Revista Estudos Internacionais*, v. 1, nr. 2 (2013). http://periodicos.pucminas.br/index.php/estudosinternacionais/article/view/6309 134, acessado em 30 nov. 2013.

22 Ibidem.

23 Joana Cunha, "Espionar líderes é preciso, diz diretor de inteligência dos EUA", *Folha de S. Paulo*, 30 de outubro de 2013.

24 Richard D. Mahoney, "Meu melhor inimigo: EUA e Brasil na ciberguerra global", *Folha de S. Paulo*, 20 de outubro de 2013.

– o *hacking* de Estado contra Estado. Segundo Mahoney, o Brasil se mostraria realmente inovador se seu governo conclamasse à criação de um Tratado de Limitação de Ciberguerra (*Cyber War Limitation Treaty*). Para ele, um tratado desse tipo poderia estabelecer a proibição de todas as formas de *hacking* de um Estado contra outro, delimitar padrões internacionais de responsabilidade nacional e protocolos de inspeção, e, com o tempo, poderia fazer o que fez o Tratado de Não Proliferação Nuclear: isolar os Estados irresponsáveis.

Não se pode ser ingênuo a ponto de acreditar que os Estados renunciariam voluntariamente às suas soberanias em prol de uma governança global. O que pode ser defensável é o fato de que, não obstante a manutenção de um sistema internacional de Estados soberanos, a conjuntura atual demanda novos arranjos de governança global, dentre os quais a discussão sobre um regime internacional para regulação do tema. Parafrasendo Hedlley Bull (2002), a existência de uma rede global, compartilhada mundialmente, com capacidade de atravessar fronteiras nacionais, parece ser subversiva com relação ao princípio de que a humanidade deve ser organizada como sociedade de estados soberanos.

Tal contexto sugere a ampliação da esfera pública para além das fronteiras nacionais e dá relevância ao conceito de sociedade internacional desenvolvido por autores da chamada escola inglesa de Relações Internacionais[25].

25 A ideia de Sociedade Internacional nas relações internacionais surge em meados do século passado com Martin Wight (*A política do poder,* Brasília: UNB, 1985). Wight declarava-se um realista, acreditava que a causa fundamental das guerras é a ausência de um governo internacional e a falta de uma autoridade comum gera um sistema internacional anárquico e que, como consequência, "a política internacional ainda é a política do poder" (p. 238). Para Wight, entretanto, "se anarquia significa a desordem completa, então esta não é uma descrição verdadeira das relações internacionais" (p. 85). Heddley Bull, discípulo de Wight, aprofundou os estudos relativos à Sociedade Internacional, dando ênfase ao conceito de ordem e à "arena social" que caracterizaria a relação entre os Estados.

Partindo de uma visão estatocêntrica, esses autores sugerem que os elementos de uma sociedade sempre estiveram presentes no sistema internacional moderno. Heddley Bull, por exemplo, define a sociedade internacional como um grupo de Estados, conscientes de certos valores e interesses comuns, que se considerarem ligados, no seu relacionamento, por um conjunto de regras e instituições comuns[26].

Outro conceito central da Escola Inglesa que merece ser resgatado para a discussão das ameaças cibernéticas no sistema internacional é o conceito de ordem. Bull define ordem como o padrão de convivência entre coletividades que permite o desenvolvimento de propósitos básicos sociais: proteção contra qualquer forma de violência, a garantia de que as leis sejam cumpridas e a garantia da propriedade:

> Em primeiro lugar, todas as sociedades procuram garantir que a vida seja protegida de alguma forma contra a violência que leve os indivíduos à morte ou produza danos corporais. Em segundo lugar, todas as sociedades procuram a garantia de que as promessas feitas sejam cumpridas, e que os acordos ajustados sejam implementados. Em terceiro lugar, todas as sociedades perseguem a meta de garantir que a posse das coisas seja em certa medida estável, sem estar sujeita a desafios constantes e ilimitados[27].

Para ele, a preservação e o fortalecimento da Sociedade de Estados depende, em primeiro lugar, da manutenção e ampliação do consenso sobre os interesse e valores comuns que fundamentam suas

26 Heddley Bull, *A Sociedade Anárquica* (Brasília: UNB, 2002), 19.

27 Ibidem: 9.

regras e instituições coletivas[28]. Uma atualização desse pensamento deve considerar, necessariamente, o avanço dos direitos civis observado nos últimos tempos.

Bull reconhece os limites dessa "ordem internacional", mas não nega o valor das normas entre os membros da sociedade internacional. Ao discutir a eficácia do direito internacional, por exemplo, Bull defende que a sua importância "não repousa sobre a disposição dos Estados de seguir esses princípios em detrimento dos seus próprios interesses, mas no fato de que eles, com muita frequência, consideram do seu interesse comportar-se de acordo com as normas do direito internacional"[29].

As diferentes "violências cibernéticas" a que os Estados e as populações estão sujeitos poderiam ser um fator contribuinte para a construção de uma ordem cibernética internacional. Afinal, "a vulnerabilidade humana à violência e a inclinação a recorrer a ações violentas levam os homens à noção de que há um interesse comum na limitação da violência"[30].

---

28 Um dos capítulos de sua obra, Bull intitula "Como Reformar o Sistema de Estados". Bull questiona de que modo se poderia reformar ou reajustar o Sistema de Estados de forma que ele pudesse promover mais efetivamente a ordem mundial. O autor discute algumas modalidades imaginadas, mostrando cético em relação a todas elas. Uma delas diz repeito a ideia de "centralismo global", pela qual o planeta é visto como uma espécie de "nave espacial" (Bull , 2002, p.338) regida por uma autoridade mundial centralizada. Neste caso, a saída seria o "o fortalecimento das instituições centrais já existentes, como as Nações Unidas e a Corte Internacional de Justiça" (Idem, p.339). Entretanto, para o autor, "o mais provável é que uma autoridade mundial centralizada refletirá os valores das grandes potências de hoje, pois só elas teriam condições de transformá-la em realidade" (Idem, p.341). Bull, complementa: "Há uma certa ingenuidade nos seus planos para conscientizar as pessoas, como se isto nunca tivesse sido tentado, e também uma certa presunção quando dizem falar em nome da "nave espacial Terra" (Idem, p.342).

29 Heddley Bull, *A Sociedade Anárquica* (Brasília: UNB, 2002), 161.

30 Ibidem: 65.

Até que ponto, entretanto, os Estados estariam dispostos a se submeterem a regras internacionais? "Há, nos sistemas de Estados, uma tensão inevitável entre o desejo de ordem e o desejo de independência. A ordem promove a paz e a prosperidade, que são grandes dádivas. Há, entretanto, um preço. Toda ordem limita a liberdade de ação das comunidades"[31].

No contexto de um mundo marcado pela insegurança cibernética, entretanto, é interessante destacar que elevados níveis de independência tendem a gerar insegurança. Neste caso, torna-se plausível imaginar que governos nacionais poderiam sacrificar parte da própria liberdade de ação a fim de restringir e tornar mais previsíveis as ações dos outros na sua direção[32].

O fato é que a natureza das ameaças cibernéticas demandam espaços de governança globais. O mundo está condenado a se conectar cada vez mais. Neste quadro, ganha relevância o papel do diálogo e da diplomacia entre os povos. Para Khanna[33]:

> A diplomacia nunca foi tão importante como agora. Numa época em que os Estados Unidos não podem impor sua vontade ao mundo e precisam, em vez disso, negociar com todos os países, em que o poder militar ganha batalhas, mas não guerras, e em que o tamanho dos desafios globais ultrapassa a capacidade de ação

31 Adam Watson, *A evolução da sociedade internacional: uma análise. histórica comparativa* (Brasília: UNB, 2004): 28.

32 Joseph S. Nye, *O paradoxo do poder americano* (São Paulo: Unesp, 2002).

33 Em *Como governar o mundo*, Parag Khanna (2011) apresenta interessantes ideias sobre o desafio de governança global. Cético em relção ao papel desempenhado pela ONU, Khanna questiona: "como pode uma organização que toma conte de países com fronteira resolver os problemas de um mundo sem fronteiras?" (Idem, p. 20). Para o autor, "A ONU não é uma superestrutura definitiva que paira sobre a Terra – é, na melhor das hipóteses, um conjunto de pequenos seixos tentando manter o mundo no lugar, ou impedir que ele role para o abismo"(Idem, p. 20). Na sua opinião, " melhorar nosso desenho diplomático global é a chave para melhor governarmos o mundo" (Idem, p. 17).

> de nossas instituições, devemos nos concentrar, acima de tudo, na diplomacia[34].

Para Khanna[35], com os sistemas de tradução universais desenvolvidos pela *Google*, todo mundo tornou-se diplomata em potencial:

> A tecnologia, o capitalismo e as agendas morais, como os direitos humanos, multiplicaram drasticamente o número de participantes no jogo diplomático. A diplomacia hoje se exerce em qualquer grupo de pessoas de alguma relevância. Há cerca de duzentos países no mundo que mantêm constantemente com governos e entre si, e pelo menos 50 mil ONGs transnacionais que trocam ideias sobre leis e tratados internacionais e intervêm em zonas de conflitos para dar assistência a regimes e povos necessitados. Todos esses atores conquistaram autoridade – seja com dinheiro, expertise ou status – para se tornarem influentes.

A construção de uma ordem cibernética internacional depende, em boa medida, de um equilíbrio entre demandas individuais, cujos objetivos estão ligados à conveniência e à privacidade, e as demandas dos Estados, que obedecem ao primado da segurança. Essas questões estão sempre ligadas:

> Concepções de segurança individual e coletiva/estatal estão, portanto, inextricavelmente ligadas: a segurança estatal pressupõe uma resolução específica do problema da segurança individual, (...), e a segurança individual deve – já que o indivíduo sempre

34 Parag Khanna, *Como governar o mundo* (Rio de Janeiro: Intrínseca, 2011): 18.

35 Ibidem: 19.

> se encontra em relação a outros indivíduos – assumir uma autoridade coletiva[36].

As sociedades democráticas sabem que o sucesso de políticas públicas depende muito do grau de transparências das ações dos agentes. Pensado em escala internacional, entretanto, justo pela ausência de um "comunidade política", a ideia de ações políticas transparentes encontra maiores resistências, em um ambiente notadamente marcado por relações de poder.

Desta forma, torna-se plenamente plausível a seguinte observação feita por Celso Amorim:

> "Pensando na eventualidade desses ataques de uma nação contra outra, ocorre-me que um tratado internacional que proscrevesse o 'primeiro uso' dessas armas, ou seja, um *no first use* cibernético, poderia quiçá contribuir para a segurança internacional. É tempo de pensar nisso, antes que alguém pense em um 'TNP cibernético', que consolide e amplie os desequilíbrios e as assimetrias que já existem"[37].

Conclusão

O presente artigo buscou discutir o impacto das ameaças cibernéticas no campo da segurança internacional, considerando as características próprias dessas ameaças. O que se percebe é que, enquanto persistem no sistema internacional políticas de poder, onde os Estados buscam se estruturar para possíveis "guerras cibernéticas", há, por outro lado, sinais de ampliação da esfera pública para além

36 Barry Buzan e Lene Hansen, *A evolução dos estudos de segurança internacional* (São Paulo: Unesp, 2012): 56.

37 Celso Amorim, Ibidem, 137.

das fronteiras nacionais e de constituição de uma sociedade civil transnacional em busca de regulação do espaço cibernético global, que possibilite, ao mesmo tempo, transparência e segurança dos fluxos internacionais que tenderão, naturalmente, a se ampliar cada vez mais.

Se considerarmos que as redes transnacionais tendem a gerar cada vez maiores níveis de interdependência, torna-se lícito imaginar que a sociedade internacional avançará em busca de uma ordem internacional que contemple a segurança cibernética; ou estará condenada a retornar aos tempos das velhas máquinas de escrever. Conciliar: segurança, conveniência e privacidade: eis o grande desafio das sociedades internacionais futuras!

CAPÍTULO 3

Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder[1]

Walfredo Bento Ferreira Neto

Instigações iniciais e marcos teórico-metodológicos

Nos últimos anos tem-se verificado um aumento na quantidade de fatos, de documentos oficiais, de bibliografia e de pesquisas cuja temática é a cibernética empregada na relação entre Estados. Expressões como defesa e segurança, comando e centro militar cibernéticos e guerra cibernética ganham projeção e espaço nas agendas políticas.

Isso se justifica porque no interior dessa "nova" palavra se encontra um dos tradicionais recursos de (e do) poder: a informação. A novidade é que, dependendo da capacidade de cada ator, ciberneticamente falando, há a possibilidade de um ganho real de

1 Artigo vencedor do IV Prêmio Marechal-do-Ar Casimiro Montenegro Filho, tema cibernética, organizado pela Secretaria de Assuntos Estratégicos da Presidência da República, e elaborado a partir da dissertação de Mestrado *Por uma Geopolítica Cibernética: apontamentos da Grande Estratégia brasileira para a nova dimensão da guerra* apresentada, defendida e aprovada pelo PPGEST/UFF, em 27 de junho de 2013.

tempo e, a partir de então, de uma maior consciência situacional.[2] A partir do uso da cibernética, o tomador de decisão aumenta a probabilidade de influenciar outrem e, por conseguinte, aumenta sua chance de êxito na consecução do objetivo.

Desse modo, de timoneiro ou de governo, pelo sentido empregado na Grécia Antiga[3], passando pelo estudo que visava à substituição das funções humanas de controle por sistemas mecânicos e eletrônicos[4], a cibernética alcança, hoje, uma conotação que compreende as ideias mestras de informação e de comunicação, daí o termo infovias, utilizado para representar os meios pelos quais as informações digitalizadas circulam.

Como uma consequência, hipoteticamente falando, em face das possibilidades a partir do uso da cibernética, a segurança das infovias – estas constituídas por ferramentas de Tecnologia da Informação e das Comunicações – passou a ser mais uma meta perseguida pelo Estado, a fim de garantir o fluxo de suas mensagens e impedir ou negar acesso não autorizado ao conteúdo que por essas vias transitam.

Ainda como hipótese, esses mesmos noticiários, agendas e discursos sobre a cibernética tratam-na: 1) ora como um recurso à disposição da política, materializado na informação, portanto um recurso clássico, que, de "novo", possui apenas seu processamento

---

2 Cf. Fernando Malburg da Silveira: "Uma robusta rede integrando forças geograficamente esparsas e de natureza difusa, todas providas por um mesmo nível de informações (táticas e estratégicas) de modo a tirar partido de um mais amplo conhecimento da situação (*situation awareness*) nos diversos níveis de comando, a permitir melhor sincronização de ações e acelerar decisões, aumentando a eficácia das missões dessas forças integradas por redes digitais de alta velocidade", in "Cyberwarfare: a nova dimensão da guerra", *Revista do Clube Naval,* ano 119, n. 360, out./nov./dez. (2011): 33.

3 Marcílio Marques Moreira, MOREIRA, "Karl Deutsch, a Política e a Cibernética", in *Deutsch na UNB*: conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980. (Brasília: Editora da UNB, 1980).

4 Norbert Wiener, *Cibernética e sociedade: o uso humano de sêres humanos. 4. ed. (São Paulo: Cultrix, 1973[1954]).*

por um computador; 2) ora como mais uma dimensão espacial, o ciberespaço, um domínio espacial autônomo, da mesma forma que o terrestre, o marítimo e o aeroespacial.

Quanto a esta última ótica, apesar de formalmente considerado um espaço de uso comum, ou um *global common*[5], esse espaço tem seu controle, logo seu empoderamento, realizado por apenas alguns atores: os mais aptos.

Assim, a cibernética passa a ser tratada como um território, *locus* em que o poder é exercido e confrontado de forma constante, eis que é objeto inerente a uma relação. O que acontece é que, diferentemente dos espaços tradicionais, o ciberespaço é bastante artificial, fruto do atual estágio de desenvolvimento da sociedade e de suas ferramentas tecnológicas. Esse espaço, logo, possui características que desafiam a apreensão e, por conseguinte, a compreensão imediata acerca de sua realidade. Todavia, ao que tudo indica, ele existe.

Por conseguinte, tratando a cibernética como um espaço, verifica-se um processo que os estudos geográficos e geopolíticos denominam *territorialização*, definido por Robert Sack como uma "tentativa de um indivíduo ou um grupo de atingir, influenciar ou controlar pessoas, fenômenos e relacionamentos, através de delimitação e afirmação do controle sobre uma área geográfica"[6]. Esse processo enfatiza, portanto, "o controle de acessibilidade, o território definido,

5 Barry R. Posen, "*Command of the commons: The Military Foundation of U.S. Hegemony*". *International Security*, v. 28, n. 1, p. 5-46, summer 2003. http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf, acessado em 20 set. 2012. Alexandre Reis Rodrigues, "Portugal e o espaço estratégico de interesse", *Jornal de Defesa e Relações Internacionais. Revista Segurança e Defesa*, Loures, Diário de Bordo Editores, 2012. http://database.jornaldefesa.pt/politicas_de_defesa/portugal/JDRI%20009%20221112%20Portugal%20e%20o%20espa%C3%A7o%20estrat%C3%A9gico%20de%20interesse.pdf, acessado em 27 nov. 2012. Kelly de Souza Ferreira, *China e a Ásia Central*: petróleo, segurança e os Estados Unidos (Dissertação de Mestrado, USP, 2012).

6 Cf. Rogério Hasbaert, *Territórios Alternativos* (Niterói: EdUFF; São Paulo: Contexto, 2002), 119.

sobretudo através de um de seus componentes, a fronteira, forma por excelência de controlar acesso".[7]

Dessa forma, para dar o primeiro passo na direção de uma apreensão desse fenômeno aplicado a essa dimensão, é necessário entender que a delimitação da fronteira do "território cibernético", um território originalmente na forma de rede ("*território-rede*"), não pode ser pensada no formato de *zona* ou de *faixa*, como ocorreu com o espaço terrestre até a Idade Média, nem no de *linha*, como passou a ser tratada a epiderme do Estado moderno[8], aproveitando-se de uma maior capacidade de centralizar informações e de produzir tecnologia, como foi o caso da representação por meio de mapas cartográficos.

A fronteira do "*ciberterritório*", coexistindo com as formas pretéritas de delimitação de poder no espaço, deve ser vista na forma de *ponto*, que pode ser ao mesmo tempo uma informação em seu "pacote", ou um "nó" de uma infovia, ou, ainda, uma estrutura estratégica ou infraestrutura crítica selecionada graças, mais uma vez, ao aprimoramento dos recursos disponíveis ao principal ator do sistema internacional: o Estado.

Além disso, ao se abordar a cibernética como mais um recurso de (e do) poder, percebe-se que esse instrumento vem servindo também para uma *(re)territorialização* dos espaços tradicionais, que se encontram expostos ao que se convencionou chamar de globalização, e que, por consequência, estariam submetidos a um processo de *(des)territorialização*.

---

7 Rogério Hasbaert, *Territórios Alternativos* (Niterói: EdUFF; São Paulo: Contexto, 2002), 119.

8 Carlos de Meira Mattos, *Geopolítica e teoria de fronteiras*: fronteiras do Brasil (Rio de Janeiro: Biblioteca do Exército, 1990). Claude Raffestin, *Por uma geografia do poder* (São Paulo: Ática, 1993). Anthony Giddens, *O Estado-nação e a violência* (São Paulo: Edusp, 2001). Barry Buzan; Lense Hansen, *A Evolução dos Estudos de Segurança Internacional* (São Paulo: Editora Unesp, 2012).

Esse é o fenômeno apontado por Claude Raffestin pela sigla T–D–R, correspondendo à territorialização, à (des)territorialização e à (re)territorialização, respectivamente[9]. Essa, portanto, é uma das linhas mestras e premissas deste trabalho, em que os conceitos (des)territorialização, por um lado, e territorialização e (re)territorialização, por outro, de forma ampliada, pela qual alcançam o espaço cibernético, estarão, pelo menos aparentemente, confrontando-se de forma constante, como na lei da ação e reação, mas nem sempre, historicamente, atingindo uma síntese, como nos mostram os imponderáveis *clausewtzianos*. É na permanência desse confronto que surgem os conflitos e a demanda por uma normatização, a fim de se evitar a guerra.

Essa relação de causalidade pode ser assim evidenciada: quanto maior a territorialização do ciberespaço, maior é a capacidade de (re) territorializar, isto é, controlar as demais dimensões espaciais.

Ainda, em virtude da atualidade e da complexidade do tema – que, por si, envolve várias áreas do pensamento científico, tanto exatas quanto naturais, sociais e humanas –, faz-se mister o registro do que não se pretende realizar.

Primeiramente, ressalta-se que, como se está tratando de relações entre Estados, o trabalho não aborda a perspectiva entre Estado-indivíduo em seu ordenamento jurídico, como, por exemplo, as regras de uso e controle da *Internet* e de redes sociais;[10] de crimes comuns via meios eletrônicos ou informatizados, de prostituição ou

9 Cf. Marcos Aurelio Saquet, *Abordagens e concepções sobre território* (São Paulo: Expressão Popular, 2007).

10 Como ocorreu com o debate sobre o *Stop Online Piracy Act* (SOPA) e o *Protect IP Act* (PIPA), ambos no Congresso Norte-Americano, e o próprio Marco Civil Regulatório no Brasil.

pedofilia "virtual".[11] Apesar disso, tem-se ciência dessa possibilidade, que, na visão do geógrafo suíço Claude Raffestin[12], caracterizaria a utilização do aparelho estatal para o controle de sua população ou, para Marcos Kaplan[13], serviria como mais um recurso que o Estado passa a possuir para garantir algumas de suas principais funções, como a institucionalização; a legitimidade e o consenso; a legalidade; a coação social; a educação e a propaganda; e a organização coletiva.

Também não se abordam profundamente as operações e os termos técnicos a respeito da cibernética ou do uso da segurança das informações, como no caso de modelos matemáticos ou chaves logarítmicas, sistemas criptográficos e *malwares* (vírus, antivírus, *trojan horses* e *worms*) no interior de um *software*.

O estudo e a aplicação da cibernética no campo da neurociência também não são levados em consideração, embora se tenha plena certeza que é de grande valia para o desenvolvimento científico por envolver o "comando e o controle" do próprio organismo humano, tal qual um sistema aberto idealizado por Wiener[14] em sua teoria.

O CIBERESPAÇO E SEU USO PELO E PARA O PODER

Para Pierre Lévy, o ciberespaço corresponde a um espaço de comunicação aberto pela interconexão de computadores e das memórias dos computadores, incluindo os sistemas de comunicação tanto por meio de ondas *hertz* quanto pela telefonia clássica, a partir

11 Como foi o caso, no Brasil, da aprovação, em 03/12/2012, da lei que prevê prisão para quem cometer crime na *Internet*: "Invadir computadores alheios ou outro dispositivo de informática com a finalidade de adulterar, destruir ou obter informações sem autorização do titular", ficando conhecida como lei Carolina Dieckmann.

12 Claude Raffestin, *Por uma geografia do poder* (São Paulo: Ática, 1993).

13 Marcos Kaplan, *Formação do Estado nacional na América Latina* (Rio de Janeiro: Eldorado, 1974).

14 Norbet Wiener. Ibiden.

do momento em que essas participarem do processo de transmissão de informações digitalizadas[15].

Mandarino Júnior[16], do Gabinete de Segurança Institucional da Presidência da República do Brasil (GSI/PR), acredita que o espaço cibernético compreende também as pessoas, as empresas e os equipamentos que porventura estejam interconectados, participando, de alguma maneira, do tráfego de informações digitalizadas.

Richard Clarke e Robert Knake debruçaram-se sobre esse tema em um dos capítulos do *Cyber war: The Next Threat to National Security and What to Do About It*[17]. Os autores iniciaram investigando o que seria o ciberespaço e indicando que o termo mais parecia, em um exercício de imaginação, outra dimensão, com iluminação verde e coluna de números e símbolos piscando no ar como no filme *Matrix*. Mas, logo em seguida, atestam que esse novo espaço é realmente bem mundano, no qual está inserido o *laptop* que nós conduzimos ou o que as crianças levam para a escola ou, ainda, um computador de nosso local de trabalho ou uma tubulação instalada sob uma rua. Para Clarke e Knake[18], hoje o ciberespaço está em toda parte, em todo lugar em que encontramos um computador, ou um processador, ou um cabo de ligação.

Esses autores norte-americanos trazem como conceito que o ciberespaço corresponde a todas as redes de computadores em todo o mundo, e tudo que conecte ou controle. Ciberespaço inclui outras

15 Pierre Lévy, *Cibercultura (São Paulo: Ed. 34, 1999).*

16 Raphael Madarino Júnior, "Reflexões sobre segurança e defesa cibernética", i*n* Otávio S. R. Barros; Ulisses M. G. Gomes; Whitney L. de Freitas (Org.). *Desafios estratégicos para a segurança e defesa cibernética*. (Brasília: Secretaria de Assuntos Estratégicos, 2011), 105-128.

17 *Richard Clarke; Robert Knake, Cyber war:* the next threat to national security and what to do about it (*New York: CCCO, 2010). E-book.*

18 Ibidem.

redes de computadores além da *Internet*, que, supostamente, não são acessíveis a partir desta.

Nesse sentido segue Derek Reveron[19], baseando-se na definição de ciberespaço do Departamento de Defesa dos Estados Unidos da América (EUA), informando que esse espaço é "um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a *Internet*, redes de telecomunicações, sistemas de computador e processadores embarcados e controladores".

Prossegue esse autor afirmando que o ciberespaço, assim como o ambiente físico, é muito abrangente, incluindo o *hardware*, como redes e máquinas; as *informações*, como dados e mídia; o *cognitivo*, como o processo mental das pessoas; e o *virtual*, no qual as pessoas se conectam socialmente.

Daniel Ventre[20], pesquisador do Centro de Investigações Científicas e secretário geral do Grupo Europeu de Pesquisa de Normas (GERN), ambos de Paris, elaborou uma proposta quanto aos componentes do ciberespaço. Para Ventre, esse espaço é composto por três "capas", assim denominada cada parte desse domínio. A Tabela 1 ilustra a proposta de Ventre.

A visão do pesquisador do GERN-Paris se coaduna com a tríade formulada por especialistas das áreas de análise de sistemas e de informática, que entendem o *hardware* como a parte rígida ou os componentes do sistema; o *software*, o que diz respeito à programação; e o *peopleware*, referindo-se às pessoas que atuam nesse setor por

19 Derek Reveron, *Cyberspace and national security*: threats, opportunities and power in a virtual world (Washington D. C.: Georgetown University Press, 2012). E-book.

20 Daniel Ventre, "Ciberguerra", in XIX Curso Internacional de Defensa, 2011. *Seguridad global y potências emergentes em un mundo multipolar* (Zaragoza: Imprenta Ministerio de Defensa, 2012), 32-45.

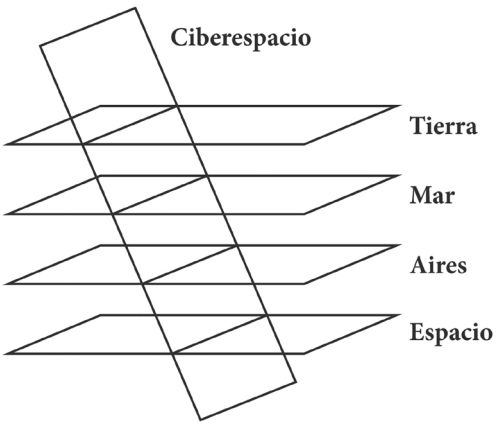
Tabela 1: Espaço cibernético – "capas" e respectiva composição

"CAPA"	COMPONENTES
Inferior	física, material, condizente com a infraestrutura (hardware, redes, ...)
Intermediária	softwares de aplicações
Superior	cognitiva

meio do conhecimento. Além disso, representando graficamente, Ventre expõe o domínio cibernético em face das outras dimensões espaciais, conforme Figura 1, afirmando que uma das características mais marcantes desse novo domínio é a sua transversalidade.

Essa transversalidade torna-se uma característica bem significativa do ciberespaço, uma vez que permite a projeção de poder e seus reflexos nos demais domínios espaciais ou, como é tratado até aqui, o fenômeno da *(re)territorialização*. Ainda se atendo ao ciberespaço, sobretudo quanto às suas características e composição,

Figura 1: Ciberespaço e relação com outras dimensões espaciais



Fonte: Ventre (2012, p. 35).

Joseph Nye enxergou essa dimensão espacial dividida em duas partes principais: o "*intraespaço*" e o "*extraespaço*" cibernético. [21]

Ao se analisar essa forma de simplificação, chega-se à conclusão que muito condiz com a visão do chefe do Comando Cibernético dos Estados Unidos, general Keith Alexander, que vê o ciberespaço "sendo usado por militares no futuro operando de dentro (ou através dele) para atacar pessoal, instalações ou equipamentos [...]".[22]

Dessa forma, ambos mencionam a possibilidade de operações ocorrerem *dentro* (no *intraespaço*) e *através* (no *extraespaço*) do ciberespaço. Nye chega a comparar o poder advindo da cibernética com o poder marítimo, no qual também se distingue o *poder naval sobre os oceanos* – o que, por sua teorização, corresponderia ao *intraespaço marítimo* – do *poder naval sobre outros domínios*, isto é, o poder projetado do ambiente marítimo para outro domínio espacial, no caso o *extraespaço* cibernético.

No intraespaço de Nye, na "capa" inferior e intermediária de Ventre, ou no que se denominou ao longo do trabalho *espaço cibernético considerado em si mesmo*, algumas ações são efetuadas a partir do, e com reflexos no, próprio espaço, como nos exemplos dos ataques de negação de serviço (*Distributed Denial of Service – DDoS*[23]), ou do controle de companhias e empresas, no caso da estrutura física do ambiente cibernético, ambas caracterizando formas de utilização *hard* do poder.

Ao mesmo tempo, a relação política e seus conflitos nesse espaço podem ocasionar reflexos externos, diga-se no mundo

21 Joseph S. Nye, *O futuro do poder (São Paulo: Benvirá, 2012).*

22 Cf. Derek Reveron, ibidem.

23 Ou *DoS Attack*, que ocorre a partir da sobrecarga do sistema e não de uma invasão. Geralmente, um computador mestre comanda milhares de computadores denominados *zumbis*, que passam a funcionar como máquinas escravizadas.

sensorial humano, como no ataque ao sistema SCADA, em 2010, nas usinas nucleares iranianas ou na possibilidade de rupturas de serviços essenciais à população, como no caso de danos às estruturas estratégicas de um Estado: energia elétrica, distribuição de água, serviço de telecomunicações, sistema financeiro, etc.

Dessa forma, e por suas várias interpretações e possibilidades, o espaço cibernético, apesar de considerado virtual e um *global common*, já há algum tempo o deixou de ser. Alguns atores empoderam-se desse espaço, delimitando-o unilateralmente e dispondo de seu controle. É nesse sentido que se enxerga o espaço cibernético não mais como um espaço comum, e sim como um território. Tentar entendê-lo e teorizá-lo, para saber "jogar", e defini-lo, delimitá-lo e demarcá-lo, com as respectivas responsabilidades advindas, torna-se um pressuposto a ser considerado na formulação de políticas sobre esse tema e sob essa abordagem.

O território cibernético e sua fronteira

Compreensão exige teorização. Teoria exige abstração, que, por sua vez, exige simplificação e ordenamento da realidade[24]. Esse entendimento é necessário para a compreensão do *constructo* que se fez até aqui. As percepções sobre a confluência da aplicação do conceito de território e da Teoria das Fronteiras no ambiente cibernético se, no início da pesquisa, se deu de forma dedutiva, ao longo desta investigação foi-se confirmando, tanto pela bibliografia consultada quanto pelas notícias e pelos documentos de órgãos públicos, corroborado em entrevistas de agentes, militares e civis.

24 Samuel P. Huntington, *O soldado e o Estado*: teoria e política das relações entre civis e militares (Rio de Janeiro: Biblioteca do Exército, 1996).

Além disso, as ações planejadas e já implementadas para esse domínio seguem esse sentido. A resposta do Estado para essa possibilidade de ação no ambiente cibernético acompanha o fio condutor da territorialização ocorrida outrora com os demais domínios: o terrestre, o marítimo, o aéreo e o cósmico.

Na abertura do III Seminário de Defesa Cibernética, o ministro da Defesa do Brasil, Celso Amorim, argumentou:

> A internet alterou os parâmetros de ação humana. O próprio conceito de realidade foi expandido pelo espaço digital. A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, à terra, ao ar e ao espaço. Aberto à ação humana, o domínio cibernético abre-se também ao conflito.[25]

A revista *The Economist*[26] de certo modo referiu-se aos estudos de Clarke e Knake sobre a guerra cibernética no artigo Guerra no quinto domínio: o *mouse* e o teclado são as novas armas do conflito?

O general João Roberto de Oliveira[27], pioneiro na implantação do setor cibernético no Exército Brasileiro e hoje à frente do Sistema de Monitoramento de Fronteiras (SisFron) assim se expressou:

> […] No campo militar e mesmo no político, considera-se que existem cinco dimensões no conflito moderno: o terrestre, o aéreo, o marítimo, o espacial e o cibernético. Para os três primeiros é possível estabelecer-se limites ou fronteiras físicas. Na

25 Celso Amorim, "Aspectos da defesa cibernética", in SEMINÁRIO DE DEFESA CIBERNÉTICA, 3., Brasília, 2012. *Palavras do ministro da Defesa*... Brasília: MD, 2012. https://www.defesa.gov.br/arquivos/2012/Pronunciamentos/Ministro_defesa/discurso_seminario_defesa_cibernetica_out_2012.pdf, acessado em 20 nov. 2012.

26 The Economist, "*Cyberwar: war in the fifty domain*". 1 jul. 2010. http://www.economist.com/node/16478792, acessado em 20 jun. 2011.

27 *Fronteira cibernética.* [mensagem pessoal]. Mensagem recebida por <wbfneto@bol.com.br> em 02/10/2012.

> dimensão espacial já há dificuldade de se estabelecer limites ou fronteiras, pois o espaço sideral não é regido, ainda, por regras de utilização bem delimitadas. Temos discussões em alguns órgãos internacionais sobre situações focais, como por exemplo, o uso do espaço para a localização de satélites geoestacionários e outros temas de interesse comum (por sinal, o Brasil está muito atrás nessa discussão, pois até agora o País não tem nenhum satélite próprio).

Inúmeros países e outros atores do sistema internacional, dos diversos tabuleiros e posições do jogo do poder, participam dessa reação, tentando ora delimitar unilateralmente esse novo espaço, ora elaborar normas para a garantia de seu funcionamento:

- Os Estados Unidos, por meio do Departament of Defense (DoD), da Defense Information Systems Agency, da National Security Agency (NSA), do Departament of Homeland Security, da Defense Intelligence Agency e de um Comando específico criado em 2010 para a cibernética (o USCYBERCOM)[28] (Quadro 1):
- O Reino Unido, com a primeira estratégia nacional de segurança cibernética (*Cyber Security Strategy of the United Kingdon: safety, security and resilience in cyber space*), lançada em 2009, com a previsão do Office Cyber Security (OCS), órgão responsável pela macrocoordenação, o Cyber Security Operations Center (CSOC), para monitorar o espaço cibernético e coordenar respostas aos incidentes[29];

28 Cf. João Roberto de Oliveira, "Sistema de segurança e defesa cibernética nacional: abordagem com foco nas atividades relacionadas à defesa nacional", *in* Otávio S. R. Barros; Ulisses M. G. Gomes; Whitney L. de Freitas (Org.). *Desafios estratégicos para a segurança e defesa cibernética* (Brasília: Secretaria de Assuntos Estratégicos, 2011), 116-117.

29 Cf. Claudia Canongia; Raphael Mandarino Júnior, "Segurança cibernética: o desafio da nova

- A China, anunciando a criação de uma unidade específica de segurança e defesa na Província de Cantão[30], no que segue Clarke e Knake (2010), e até mesmo de uma Força Armada específica, "guerreiros cibernéticos", com a Coreia do Norte também seguindo essa mesma linha[31];
- O Canadá, com a Canada's 2010 Cyber Security Strategy (CCSS-CAN), pela qual foram enfatizados três pilares: 1) sistemas de segurança de governo; 2) parceria com o setor privado; e 3) segurança aos canadenses no acesso *on-line* por meio de medidas de sensibilização. A estratégia canadense para o ciberespaço também atribuiu inúmeras responsabilidades entre os ógãos da administração pública, civis e militares daquele país[32];
- Na Europa, além da Inglaterra, destaca-se a Alemanha, por meio da Cyber Security Strategy for Germany (CSSG-ALE), e a França, pela *Défense et sécurité des systèmes d'information: stratégie de la France*;
- Com relação aos organismos internacionais, a atenção é para a reação da Otan, com o Cooperative Cyber Defence Centre of Excellence (Nato CCD COE), e da ONU, conforme relatado

---

sociedade da informação", *Parcerias Estratégicas* – Revista do Centro de Gestão e Estudos Estratégicos do Ministério da Ciência e da Tecnologia, Brasília, v. 14, n. 29 (2009): 21-46.

30 Daniel Ventre, ibidem, p. 43.

31 José Carlos dos Santos, "Podemos recrutar *hackers*". *Revista Época*, 15 jul. 2011. Entrevista concedida a Leandro Loyola, acessada em 20 de julho de 2011, http://revistaepoca.globo.com/Revista/Epoca/0,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

32 Ron Deibert, "*Distributed security as cyber strategy: outlining a comprehensive approach for Canada in cyberspace*", Calgary: Canadian Defense & Foreign Affairs Institute, August, 2012. http://ebookbrowse.com/distributed-security-as-cyber-strategy-pdf-d380969236, acessado em 10 dez. 2012,

em momento anterior, que realizou, inclusive, exercícios reais entre países da região do sudeste asiático próximos ao gigante chinês.

Quadro 1: Estrutura de segurança e defesa cibernética dos EUA

Órgão	Funções de interação com o comando cibernético
National Secutity Council	Planejar e coordenar as atividades gerais ligadas à segurança cibernética (natureza política);
Departament of Defense	Providenciar a capacitação e o adestramento profissional em Segurança e Defesa Cibernética em ligação com o Homeland Secutity e o Director of National Intelligence;
Defense Information Systems Agency	Planejar, instalar, operar e manter, com segurança, a estrutura de TIC necessária para apoiar as operações conjuntas das Forças Armadas, líderes nacionais e outras missões envolvendo parcerias internacionais (coalizões) em todo o espectro de ações militares;
National Security Agency	Assegurar as atividades de inteligência do sinal* nos EUA, as quais enquadram a inteligência da área cibernética;
Departament of Homeland Security	Providenciar um estado de prontidão nacional em face das ameaças cibernéticas às infraestruturas críticas do país;
Departament of Education e Office of Science and Technology Policy	Providenciar ações relativas à educação formal do cidadão a respeito da ameaça cibernética em todos os níveis e em diferentes graus de intensidade;
Office of Personnel Menagement	Conscientizar os servidores públicos federais no que se refere ao seu papel no combate às ameaças cibernéticas.

Fonte: elaborado com base em Oliveira (2011).

* **Inteligência de sinais:** resulta da coleta, da avaliação, da integração e da interpretação dos dados relativos às emissões eletromagnéticas, compreendendo as inteligências de comunicações e eletrônica (BRASIL, 2007).

O fato é que esse "novo" domínio traz consigo uma série de questionamentos e, por consequência, incertezas.

Para o general José Carlos dos Santos, comandante do Centro de Defesa Cibernética do Exército Brasileiro (CDCiber/EB), em entrevista à revista *Época*, de 18 de julho de 2011: "No espaço cibernético a fronteira não existe [...]. O inimigo é difícil de identificar". Para Mandarino Júnior, diretor do Departamento de Segurança da Informação e Comunicações do GSI/PR: "Aqui (no espaço cibernético), a exemplo do espaço real, também são estabelecidas relações sociais e políticas, no tempo e no espaço"[33]. Essas duas afirmativas demonstram bem os pontos de vista e as discussões a respeito do ambiente que envolve a cibernética, sobretudo no tocante à delimitação do poder nesse espaço, por ora desafiador.

A primeira afirmativa, feita pelo comandante do CDCiber/EB, é propensa a declarar a inexistência de uma fronteira no espaço cibernético atualmente. Contudo, *in fine*, o mesmo militar admite que há um inimigo, porém de difícil identificação. Na verdade, como uma inferência, o que o general quis indicar, mesmo ciente da existência de um poder contrário – um oponente – nesse tipo de espaço, foi a impossibilidade de um encaixe do *constructo* voltado para a fronteira terrestre, uma fronteira tradicional, no ambiente cibernético.

Isso ocorre, também, em face da dificuldade de se detectar a origem, a autoria e a materialidade do ataque. Essas são, sem dúvida, algumas questões postas. De antemão, é preciso ter em conta que o espaço nesse ambiente não é natural nem pertence a uma geografia clássica. Esse espaço é específico, obedece a outras regras, e não a que considera o território mero substrato físico. O território do

33 Raphael Mandarino Júnior, ibidem.

domínio cibernético é artificial, produto do homem e fruto do nível tecnológico atual, e é, originariamente, um "território-rede", ou melhor, uma "rede-território".

Da segunda afirmação, de Mandarino Júnior, diretor do DSIC/GSI/PR, apreende-se uma intenção de delimitar esse espaço em face das relações sociais e das políticas existentes, isto é, de poder, tal como acontece no espaço natural. O que ocorre, então, é que esse inimigo, relembrando a afirmativa do general, é um oponente que consegue se valer das características desse ambiente para não ser detectado ou, pelo menos, dificultar ao máximo sua detecção. Todavia, ele está lá, atuando e jogando com o poder, ocupando assim um espaço, interagindo e exercendo influência.

Ao contrário, portanto, do que se possa pensar inadvertidamente, parece haver um território cibernético, havendo desse modo uma delimitação política espacial – uma fronteira – no denominado ciberespaço, ainda que por ora não regulamentada, ou não tendo todas as suas fases de regulamentação percorridas formalmente.[34]

No ambiente cibernético do globo, os Estados definem seus territórios "nitidamente", isto é, apropriam-se de um espaço comum (*global common*) por meio do poder. Como exemplos imediatos, mas não únicos, tem-se os domínios dos sítios ".br"; ".us"; ".uk"; ".it";..., que indicam perfeitamente os respectivos territórios.

Ainda nesse sentido, os Estados Unidos delimitaram não só o território de atuação do seu poder, como, internamente, distribuíram

34 *Definição*, *delimitação* e, por fim, *demarcação* são as fases formais exigidas pelo Direito Internacional Público para o estabelecimento de uma fronteira. "A linha fronteiriça só é de fato estabelecida quando a demarcação se processa. 'De fato estabelecida' significa não estar mais sujeita à contestação por parte de um dos Estados que tivessem essa fronteira em comum. Pela demarcação, elimina-se não um conflito geral, mas um conflito do qual a fronteira pudesse ser o pretexto" (RAFFESTIN, 1993; MAGNOLI, 1997, p. 240).

competências e atribuições acerca de cada domínio: o ".mil" ficou sob o encargo do comando combatente (USCYBERCOM), enquanto os ".gov" e ".com" foram atribuídos ao Departament of Homeland Security e às empresas privadas, respectivamente[35], ao que também segue Oliveira[36] quanto às atribuições dos órgãos e das agências norte-americanos. A estrutura montada e que funciona nesse ambiente também sofre influência do poder. A segurança dos *backbones*, dos *data centers*, dos *firewalls*[37] e demais elementos de filtragem e da hospedagem de sítios são alguns dos exemplos de que há "nitidamente" um exercício de poder no espaço cibernético, portanto há um território e, por conseguinte, sua respectiva fronteira.

Ocorre que, diferentemente das fronteiras delimitadas até então (terrestre, marítima, aérea), todas perceptíveis, incluindo-se, de certo modo, o limite extra-atmosférico, uma nova fronteira desafia homens e Estados devido à sua virtualidade, velocidade, versatilidade, flexibilidade, ambiguidade e, porque não dizer, "volatilidade".

O fluxo que "navega" por essa fronteira não é tão perceptível – pelo menos a olho nu e nem por equipamentos como luneta, binóculo, radar, etc. –, eis que o que flui nessa rede são, sobretudo, informações por meio de caracteres simbólicos dentro de pacotes[38]

---

35 Richard Clarke; Robert Knake, ibidem. Paulo Martino Zuccaro, "Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço", in Otávio S. R. Barros; Ulisses M. G. Gomes; Whitney L. de Freitas (Org.). *Desafios estratégicos para a segurança e defesa cibernética*. (Brasília: Secretaria de Assuntos Estratégicos, 2011), 64.

36 João Roberto de Oliveira, ibidem, p. 116-118.

37 Em uma rede de computadores, *backbone* designa o esquema de ligações/conexões centrais de um sistema mais amplo, tipicamente de elevado desempenho. Dentro de um sistema de capilaridade global, como a *Internet*, há uma hierarquia, uma escala dessas ligações/conexões: a intercontinental, a internacional e a nacional, alcançando as empresas de telecomunicações, que representam, apenas, a periferia do *backbone* nacional. *Data centers* – centros de processamento e de armazenamento de dados. *Firewalls* – filtros de "pacotes" de informações.

38 Termo que nessa área científica indica um grupo de informações sendo transportado unitariamente.

que, muitas vezes, fogem da imediata apreensão e compreensão. A delimitação de poder e de responsabilidades no espaço cibernético torna-se, doravante, a meta perseguida visando à garantia, sobretudo, da segurança, da harmonia e da paz, seja no ambiente interno seja no internacional.

Nesse novo cenário, os conceitos geográficos de rede, de ponto e de "nós", outrora estudados nos espaços terrestre, marítimo e aéreo, serão de suma importância. Sua aplicação guiará os Estados e os Organismos Internacionais reguladores do Direito na formulação dos limites do espaço cibernético, ou melhor, do seu território. Se antes já existiam formas de controle e de monitoramento para as fronteiras tradicionais, nessa "nova" os contornos não se mostram muito claros nem precisos. Entretanto, é certo que essa "nova fronteira" não existe de hoje.

Da "fronteira-zona" à "fronteira-ponto"

Como um dos fatores que provocaram a corrida por esse "novo" espaço encontra-se a *Internet*: a instalação e a operação da rede mundial de computadores na escala global. Outro fator como consequência desse anterior é caracterizado pelo exponencial aumento do número de pessoas que passaram a ter acesso a esse meio e que vem, portanto, ocasionando uma "pressão" nesse espaço. Meira Mattos[39] já apontava para esse fenômeno e seus possíveis reflexos ainda nos idos da década de 1970, denominando-o "*cibernetização*":

> O grau de cibernetização indica, atualmente, o padrão tecnológico da sociedade. As atividades dos grandes complexos empresariais ou educacionais

39 Carlos de Meira Mattos, "A geopolítica e as projeções de poder", in *Geopolítica*. Vol. I (Rio de Janeiro: Editora FGV, 2011[1977]), 305-312.

> estão relacionadas, hoje, com os computadores, cujas memórias realizam cálculos […]. Os números – 70 mil computadores nos EUA e 1.500 no Brasil – revelam o profundo gap, em termos de avanço tecnológico entre ambos os países.

Esse processo de pressionamento assemelha-se bastante ao que deu origem à construção das fronteiras do espaço terrestre. Para ilustrá-la, também é Meira Mattos[40] quem faz um resumo histórico sobre a Teoria das Fronteiras, no qual agora pode ser acrescentado mais um estágio, buscando representar o que se entende como uma nova fase dessa teoria, aplicada também ao ciberespaço, simultaneamente uma rede e um território, desde sua origem (Quadro 2).

Se se observar mais atentamente, além da *pressão demográfica*[41] e da *centralização do poder pelo Estado*[42], outro fator é responsável pela evolução das fases ou estágios das fronteiras: *o fator tecnológico*. À medida que se desenvolveram instrumentos que capacitaram um maior poder de monitoramento dos espaços, por meio do controle e do armazenamento das informações, mais nítida tornava-se sua delimitação, passando-se de uma forma de zona para a de faixa até chegar à de uma linha.

Acredita-se que, no atual estágio tecnológico, os Estados são capazes de delimitar seus interesses à escala de um "ponto", alcançando-se, assim, a fase ou o estágio da "*fronteira-ponto*", como um reflexo da trajetória histórica da capacidade de monitoramento e controle do sistema de Estados, caracterizando-se, dessa forma, a 5ª fase ou estágio da evolução das fronteiras.

---

40 Carlos de Meira Mattos, 1990, ibidem.

41 Carlos de Meira Mattos, 1990, op. cit.

42 Anthony Giddens, 2001, ibidem.

Quadro 2: Resumo histórico – evolução das fronteiras e proposta[43]

Fases/estágios		Descrição
1º	Vazios de ecúmene	Característico do mundo antigo, pouco povoado, quando os núcleos geo-históricos eram separados por enormes vazios demográficos;
2º	Largas zonas inocupadas ou fracamente ocupadas	Estas zonas não abrigavam nenhum poder político capaz de perturbar os interesses dos núcleos geo-históricos de que eram separadores;
3º	Faixas relativamente estreitas, chamadas *fronteiras-faixa*	Nas áreas em que o povoamento dos países limítrofes não chega a pressionar um sobre o outro;
4º	*Fronteira-linha*, estabelecida sob critérios vários (natural, artificial, astronômica, étnica)	Nas áreas em que a densidade populacional colocou em contato permanente o interesse das partes;
5º	*Fronteira-ponto*, acompanhando o atual estágio tecnológico	No ciberespaço, em sua estrutura física e/ou na imaterial, onde os interesses, por meio do fluxo de informações, podem colidir e causar danos a "pontos" escolhidos no território ou fora deste. Selecionam-se "nós" da rede e "pacotes" de informação que por esta trafegam.

A *fronteira*, nessa visada, passa a ser *ponto* (*fronteira-ponto*) não simplesmente pelo objeto a ser defendido, pois isso já ocorria nas outras dimensões que não a cibernética, como no caso dos castelos, das fortalezas, dos fortes, de cidades, portos, estreitos e ilhas, ainda na Idade Média[44] ou pelos Estados tradicionais[45]. Nem também se

43 O 5º estágio está sendo proposto por nós.

44 Carlos de Meira Mattos, *Geopolítica e teoria de fronteiras*: fronteiras do Brasil (Rio de Janeiro: Biblioteca do Exército, 1990). Claude Raffestin, *Por uma geografia do poder* (São Paulo: Ática, 1993). Anthony Giddens, *O Estado-nação e a violência* (São Paulo: Edusp, 2001). Joseph S. Nye, *O futuro do poder (São Paulo: Benvirá, 2012).* Barry Buzan; Lense Hansen, *A Evolução dos Estudos de Segurança Internacional* (São Paulo: Editora Unesp, 2012).

45 Anthony Giddens, op. cit., p. 67-86.

está referindo à fronteira cibernética (*cyber boundary*) indicada por Clarke e Knake[46] em seu glossário; nem ao *ponto* que esses autores indicam dentro dessa fronteira. Para eles, *fronteira cibernética* é empregada no sentido do limite entre o mundo *cyber* e o cinético, e o *ponto* diz respeito ao momento em que o comandante deverá decidir se (e como) passar de uma guerra puramente cibernética para uma envolvendo forças convencionais ou com armas cinéticas.

Como um dos resultados desta investigação científica, tem-se o *ponto*, ou melhor, a "*fronteira-ponto*", como reflexo de uma maior capacidade de controle das informações e de monitoramento, de maior precisão e velocidade de tomada de decisão entre o sensoriamento (detecção, vigilância), o processamento e a atuação (D-P-A), os quais correspondem à (ao): *detecção* – obtenção de informação sobre possíveis ameaças; *processamento* – trabalho da informação com vistas à tomada de decisão e implementação; e *atuação* – implementação da decisão e neutralização da ameaça[47].

Esses pontos, a título de exemplo, significam: 1) as informações digitalizadas em seus "pacotes" transitando por uma rede, localizada dentro ou fora do território terrestre (pelos *backbones* e cabos, pelas ondas *hertz* e fibra ótica), sendo processadas ou armazenadas em um computador (*datacenter*) (ativos da informação[48]); 2) os "nós", isto é, os pontos de conexão da rede pelos quais trafegam esses fluxos ("pacotes"); e 3) as estruturas estratégicas (infraestruturas

46 Ibidem.

47 José Carlos Albano do Amarante, "A batalha automatizada: um sonho exequível?", in *Cadernos de Estudos Estratégicos*, Rio de Janeiro, n. 9, Centro de Estudos Estratégicos da Escola Superior de Guerra, jul. 2010.

48 Ativos de informação – meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2010).

críticas) com interesses vitais para o Estado. Este último caracteriza o "*extraespaço*", enquanto os dois primeiros correspondem ao "*intraespaço*" ou ao "*ciberespaço considerado em si mesmo*".

No caso das informações e de seus "pacotes", a abstração contida no princípio do direito sobre a extraterritorialidade diz respeito, por exemplo, a hipóteses em que, mesmo não estando situadas no território terrestre, no mar territorial ou no espaço aéreo do país, pessoas ou coisas são salvaguardadas. Como origem desse postulado, pode ser citada a obra de Hans Kelsen[49], a partir do momento em que esse autor desvincula o objeto de interesse do Estado do seu *locus* de atuação de poder – seu território. Assim sendo, em alguns casos a personalidade jurídica do Estado fica assegurada juridicamente para o "além terra": o "*território-competência*".

O resultado dessa construção teórica pode ser visto, de forma exemplificativa e sintetizada, no artigo 7º do Código Penal Brasileiro, quando ficam submetidos à legislação brasileira, embora cometidos no estrangeiro, crimes contra o presidente da República, o patrimônio ou a fé pública da União e demais entes federativos. Além disso, encontram-se sob essa proteção as empresas públicas, as sociedades de economia mista, as autarquias ou as fundações instituídas pelo poder público e a própria administração pública. Em todos esses, a finalidade perseguida é a salvaguarda da personalidade jurídica estatal e seus interesses, isto é, a proteção da instituição, mesmo fora de seu território físico.

No mais, objetos ou coisas também são colocados sob essa condição, embora com algumas nuanças (extraterritorialidade

49 Cf. Dalmo de Abreu Dallari, *Elementos de teoria geral do Estado*. 19. ed. Atual (São Paulo: Saraiva, 1995), 74-76.

condicionada), como é o caso de aeronaves e de embarcações brasileiras, mercantes ou privadas, quando em território estrangeiro. Essa é uma das soluções que o sistema de Estados pode adotar a fim de determinar fronteiras no espaço cibernético.

É dessa forma que se pode concluir que no espaço cibernético, considerado em si – em muitas ocasiões imperceptível, com estrutura micro ou nano –, vem ocorrendo uma territorialização, uma vez que a disputa pelo controle de informações e da possibilidade de seu fluxo vem sendo objeto de poder. Ao mesmo tempo, também se infere que há uma (re)territorialização ocorrendo nos demais domínios espaciais, fruto das possibilidades advindas desse recurso.

Como exemplos localizados no domínio terrestre, as usinas hidrelétricas e as centrais de distribuição de energia, as estações de tratamento de água e o setor financeiro, considerados essenciais para o Estado e para seu sistema, são selecionados a fim de uma atenção maior no que tange à segurança e à defesa.

Mais uma vez, portanto, a delimitação dessa fronteira, de forma clara e precisa, torna-se crucial para a manutenção da harmonia, da segurança e da paz. Com as pressões exercidas nessa nova dimensão e a busca pelo seu empoderamento, há a transformação do conceito *espaço* para o de *território*, vez que, intrinsecamente, circula e se confronta poder.

Como mais um aspecto, a informação, em si, não tem valor caso não se tenha capacidade de processá-la ou de torná-la inteligível, em certo tempo, para determinados fins. Assim, o conhecimento mais detalhado das características dessa fronteira torna-se primordial, pois proporciona condições de defender tanto as informações quanto alguns pontos de uma rede e de um país.

Fronteira cibernética: classificação, realidade e representação

De forma semelhante aos estágios registrados, a teoria de Meira Mattos, com base no estudo de alguns dos principais pensadores geopolíticos, permitiu a classificação das fronteiras segundo vários critérios. Partindo dessa classificação, essa "nova" fronteira, objeto deste estudo, pode ser tida como *artificial*, *ocupada*, *esboçada*, *planejada ou de construção* e *antropogeográfica*.

Quanto a ser *artificial*, esta se refere à natureza da fronteira e ao ambiente criado e manipulado pelo homem; *ocupada*, devido ao grau de ocupação, dado pelo fluxo material ou imaterial, mas com reflexos no mundo físico que a perpassa; *esboçada*, quanto ao grau de evolução[50], pois ainda não se impõe uma demarcação clara. No entanto, aqui cabe um destaque: pelo que se constata ao longo da pesquisa, devido às pressões exercidas ultimamente nesse espaço, podemos enquadrar essa fronteira na transição entre a forma esboçada e a de fronteira *viva* ou *de tensão* em face do confronto real e constante de interesses.

Com relação à fronteira *planejada ou de construção*, consoante Rudolf Kjéllen[51], isso se dá devido ao sentido de obedecer à finalidade e ao traçado dado pelo homem. É classificada como *antropogeográfica* porque obedece ao critério realístico ou existente, na concepção de Whitemore e Boggs[52], devido às características do fluxo (linguístico, cultural, estratégico ou militar). É por possuir qualidades intrínsecas à fronteira do tipo *antropogeográfica* que a delimitação da fronteira cibernética, em si, torna-se muito complexa e altamente conflitante.

50 Brunhes, Vallaux, cf. Meira Mattos, 1990, p. 31, ibidem.

51 Cf. Meira Mattos, op. cit., p. 32.

52 Cf. Meira Mattos, op. cit., p. 33.

Meira Mattos afirma que fisicamente é até mesmo impossível o estabelecimento de fronteira quando esta é do tipo antropogeográfica. Todavia, ressalva esse autor que as fronteiras, mesmo as naturais – que até hoje são as mais claramente delimitadas –, nem sempre o são fisicamente. Grande parte, por sinal, ocorre por convenção ou acordo entre as partes (convencionalidade). É como afirma Lacoste: as fronteiras são delimitações políticas[53]. Foi o que ocorreu inicialmente com a terrestre, a marítima e a aérea.

Em relação à marítima, este tipo de fronteira foi inicialmente considerado por F. Ratzel[54] "a fronteira ideal", pois separaria, protegeria, isolaria ou uniria de acordo com a conveniência do Estado. Quanto à aérea, elaborada após o desenvolvimento da aviação (pós-I GM), o escritor francês Victor Hugo chegou a escrever para seu conterrâneo, o balonista Félix Nadar, afirmando que, além do fim das guerras, o uso do espaço aéreo pelo avião ocasionaria a "imediata, instantânea, universal e perpétua abolição das fronteiras"[55]. Em ambos os casos, contudo, isso parece que não se concretizou.

O desafio, então, no que diz respeito à fronteira cibernética passa a ser a compreensão de que essa fronteira não é em forma de zona ("*fronteira-zona*"), nem de faixa ("*fronteira-faixa*"), nem de linha ("*fronteira-linha*"), como ocorre com o espaço geográfico tradicional, natural. A delimitação de um território cibernético se dá sob outra lógica, por sinal obedecendo às próprias características

53 Yves Lacoste, *A geografia: isso serve, em primeiro lugar, para fazer a guerra* 3. ed. (Campinas: Papirus, 1989). http://www.geoideias.com.br/geo/images/livros/a%20geografiaIves%, acessado em 23 jul. 2012.

54 Cf. Meira Mattos, op. cit., p. 37.

55 David M. Isaac, "Vozes do azul: teóricos do poder aéreo", in Peter Paret, *Construtores da estratégia moderna*: de Maquiavel à era nuclear. v. 2 (Rio de Janeiro: Biblioteca do Exército, 2001), 214.

desse ambiente, em que território e rede perfazem originalmente um binômio de coexistência.

A fronteira cibernética, por conseguinte, obedece à forma de "pontos" ("nós") ou "pacotes" de informações eleitos pelos Estados devido ao seu grau de interesse – sistemas de defesa, infraestruturas críticas ou estruturas estratégicas e a informação em si são alguns dos exemplos. Com isso, nesse ambiente, a fronteira apresenta-se sob a forma de "*fronteira-ponto*", um prosseguimento contínuo, embora com certas interrupções, que acompanha o contexto histórico da formação do sistema internacional pautado no princípio da territorialidade estatal: da "*fronteira-zona*" (faixa) dos Estados tradicionais às "*linhas*" do Estado moderno e em grande parte do atual sistema de Estados-Nação, alcançando no (e com o) espaço cibernético a meticulosidade da "*fronteira-ponto*" em face da capacidade inovadora das ferramentas de TIC à disposição, que foge ao visível, que é aparentemente virtual, mas de grande reflexo no mundo real.

Esse território cibernético existe e coexiste com os demais domínios tradicionais, e já é, inclusive, mapeado, isto é, objeto de representação e, por conseguinte, de projeção de poder. Dessa forma, esse território é transformado materialmente em objeto de apreensão pela mente humana, ultrapassando a ideia de mera metafísica ou de coisa intangível. Esse território é real e também palco de intensas disputas de (e pelo) poder, com fulcro no seu controle, no seu domínio. É desse modo que enxerga também Vesentini, ao apresentar a obra de Yves Lacoste que aborda a relação de uma representação (um mapa) com o poder:

> Assim como o grande pensador de Iena proclamava que tudo que é real é racional e tudo que é racional

> é real, pode-se dizer que para Lacoste o "real", o espaço geográfico, é tão-somente aquilo que pode ser mapeado, colocado sobre a carta, delimitado portanto com precisão sobre o terreno e definido em termos de escala cartográfica.[56]

Para garantir o funcionamento desse sistema à sombra do conflito, Clarke e Knake[57] apontam para a necessidade, em face dessa composição do domínio cibernético, de se estabelecer prioritariamente a defesa com base em uma tríade – *Defensive Triad Strategy* – que focaria três setores bem definidos:

1) O que envolve os *backbones*, e pelo qual o governo e algumas empresas estipulariam uma atenção especial à segurança. Dentre as empresas, no caso norte-americano destacam-se a AT&T, a Verizon, a Level 3, a Qwest e a Sprint, responsáveis por grande parte da estrutura de fibra ótica usada pela *Internet* no interior dos EUA e no ambiente submarino ao longo do globo;
2) O que corresponde à garantia de uma rede de energia segura, tendo em vista a dependência de energia elétrica para ocorrer o fluxo de informações no (e pelo) ciberespaço; e
3) O que diz respeito à própria defesa, constituindo-se na elaboração de medidas de defesa e de ataque a partir do Departamento de Defesa (*DoD*) daquele Estado. Envolve, entre outros, as redes do próprio *DoD* e os sistemas de controle de efetivos e de armas.

56 José William Vesentini, 1988, in Yves Lacoste, op. cit., apresentação.
57 Ibidem.

Quanto a este último setor, pode ser vista a preocupação do Brasil com o funcionamento de seu Sistema Militar de Comando e Controle (SISMC²), materializada em projetos como o CDCiber, o SisFron, o Sistema de Gerenciamento da Amazônia Azul (SisGAAz) e o Sistema de Defesa Aeroespacial (Sisdabra) e as novas atribuições do Centro Integrado de Telemática do Exército (Citex).

No tocante aos outros dois setores dessa tríade proposta por Clarke e Knake, visualiza-se exatamente a preocupação do domínio cibernético, ora tido como *espaço em si mesmo* (*backbone*, por exemplo), ora como recurso do poder, quando os autores citados demonstram a preocupação com uma estrutura estratégica para o Estado: a estrutura energética.

Ainda quanto à importância desses dois setores – informação e energia e sua interligação –, parece que esses autores estão em consonância com o que expôs Raffestin[58] com relação ao poder e a suas fontes: "Sendo toda relação um lugar de poder, isso significa que o poder está ligado muito intimamente à manipulação dos fluxos que atravessam e desligam a relação, a saber: a energia e a informação".

A preocupação dos Estados não só com o setor cibernético em si mesmo, mas, e principalmente, com a interligação e a dependência dos outros setores a partir deste é bem plausível, pois os danos causados a partir do ciberespaço podem transbordar para outros, como no caso das estruturas estratégicas, o que inclui a energética.

Concretamente, embora não seja especificamente voltada para questões de defesa (relação entre Estados), temos em vigor, desde 2004, a Convenção de Budapeste ou a Convenção sobre o Cibercrime, que conta com 43 signatários, sendo apenas 12 o número de Estados que a ratificaram. Contudo, em síntese, essa tentativa de

58 Ibidem, p. 53-54.

normatização não possui mecanismos de coação bem definidos, isto é, não possui "dentes" (*tothless*). Como exemplo, em face das características inerentes a esse domínio, a Convenção não menciona nada a respeito da perseguição de um criminoso nem sobre sua punição. Isso, portanto, termina por esvaziar muito sua finalidade.

Entretanto, em face dos últimos acontecimentos que envolveram o ciberespaço e as possibilidades que a cibernética vem proporcionando, a normatização do sistema internacional cada vez mais se torna imprescindível, pois em muitos desses casos a utilização desse novo domínio vem ocorrendo realmente na (e para) a guerra.

Considerações finais

A *Internet* realmente mudou os parâmetros da ação humana, como afirmou o ministro Celso Amorim. Espaço virtual e real intercambiam-se constantemente. Assim, a necessidade de se pensar essa nova dimensão espacial como recurso de poder se torna essencial.

É a partir dessa forma de "saber pensar", envolvendo categorias de análise e conceitos da geopolítica, que as políticas públicas poderão ser formuladas, implantadas, monitoradas e avaliadas com maior probabilidade de êxito.

Como consequência dessa percepção é que se tem hoje projetos que tratam do ciberespaço considerado ora em si mesmo, como os programas, os *softwares*, os antivírus, etc., quanto como projetos que se utilizam da cibernética como mais um recurso à disposição do poder. É nessa visada que vêm surgindo pelo globo, por exemplo, sistemas de monitoramento do espaço terrestre, do marítimo, do aeroespacial.

Derivada dessas possibilidades é que surge a demanda por delimitação, não com o sentido de separação ou de isolamento, e sim pelo contrário, para normatizar responsabilidades no uso dessa "nova" dimensão espacial a fim de se evitar o conflito e até mesmo a guerra.

A delimitação do ciberespaço, em face de suas características, não obedecerá à forma de linha, nem de faixa, nem de zona, mas sim de um ponto, a "*fronteira-ponto*", tendo em vista a atual capacidade do sistema de Estados.

Considerando o ciberespaço em si, esse ponto materializa-se na informação ou no "pacote" de informações e pelos "nós" de uma rede. Ao ser tratada como recurso, a cibernética é capaz de selecionar pontos em outras dimensões do espaço para uma *(re)territorialização*.

Saber pensar o espaço, como disse Yves Lacoste, para melhor se organizar, para melhor combater, agora pode ser aplicado ao domínio cibernético em um arcabouço geopolítico e jurídico.

CAPÍTULO 4

Territorialidade e guerra cibernética: novo paradigma fronteiriço

João Gabriel Álvares

Introdução

O Estado contemporâneo apresenta ainda hoje os mesmos elementos essenciais elencados por teóricos e juristas ao longo dos séculos. Porém, aos Estados do novo milênio colocam-se novos desafios, indissociáveis da realidade atual, marcada por profundas transformações sociais e tecnológicas.

A *Internet* foi e continua sendo um dos principais elementos propulsores da chamada "era da informação"[1]. A despeito dos diversos benefícios proporcionados pela sociedade em rede, as infovias passam a ser novos veículos para a prática de condutas, inclusive as ilícitas. Em se tratando de condutas implementadas no Brasil ou em condições previstas no ordenamento pátrio, o poder judiciário tem legitimidade e competência para julgar os autores, impondo penas sempre que um ato, comprovadamente, se enquadra em um tipo penal pré-estabelecido.

Contudo, os modernos meios tecnológicos podem quebrar barreiras territoriais, mitigando os conceitos de soberania e de Estado, dificultando a eficácia de alguns processos judiciais que

1 Marcelo X. F. Crespo, *Crimes digitais.* (São Paulo: Saraiva, 2011), 25-33.

culminariam com a criminalização dos agentes. Essa constatação revela uma face de um novo paradigma fronteiriço, que conflita com o conceito tradicional de fronteira como o limite do território de um Estado.

Nesse novo contexto, a Guerra Cibernética surge como uma poderosa arma de alcance transnacional. A possibilidade de se perpetrarem ataques com elevado poder destrutivo sem adentrar fisicamente o território de outro país leva a uma reconsideração não somente das estratégias para que sejam defendidas as fronteiras, mas também de que sejam compreendidas a existência e os limites de soberania entre os Estados.

Frente a essa nova realidade, torna-se necessária a cooperação entre os diversos atores do Direito Internacional. O estabelecimento de tratados e acordos internacionais pode ser uma importante ferramenta a fim de se coibir e punir condutas danosas ao patrimônio público e privado, em especial o bem jurídico tutelado pelo Direito Penal.

Diante da dificuldade ou da insipiência para que sejam propostas tais medidas transnacionais, faz-se mister que aqueles Estados que dispõem de meios para tanto se capacitem no sentido de oferecer defesa e mesmo contra-resposta a possíveis ataques perpetrados por meio do *ciberespaço*.

Ameaças cibernéticas e o contexto atual

A globalização, como a entendem alguns autores, não é um fenômeno recente, remontando aos primórdios da atividade de comércio entre regiões de culturas distintas. Porém, as novas

dimensões da globalização são inéditas e têm repercussões sobre boa parte da comunidade internacional.

O fenômeno que se verifica no contexto atual tem como principal causa o surgimento e a popularização da *Internet*. Para que se tenha uma noção do alcance da rede mundial de computadores, o número de usuários já no ano 2000 passava dos 360 milhões[2]. Passados apenas 12 anos, o número de usuários é mais que o quíntuplo do que fora registrado, chegando a 2,4 bilhões. Os números são expressivos, especialmente quando se observa que, a despeito de tantos que vivem abaixo da linha da miséria, cerca de 34,3% de toda a população mundial possuía acesso à *Internet* em junho de 2012[3].

O aumento de usuários da rede mundial foi acompanhado pelo surgimento de uma multiplicidade de novos usos da *Internet*. Inúmeros sistemas passaram a ser informatizados, desde os mais antigos – como o sistema de transporte ou de distribuição de água – até os mais modernos. Dentre as novas funcionalidades, a rede mundial começou a ser utilizada para a realização de condutas prejudiciais ao patrimônio de entes públicos e privados.

Em virtude da quantidade de sistemas estratégicos controlados por computadores ligados em rede, percebeu-se o quanto os governos passaram a depender dos meios de informática para manter o funcionamento do Estado. Da intenção de tirar proveito das vulnerabilidades dos sistemas informáticos alheios surgiu a Guerra Cibernética. Esse novo ramo bélico, ainda que sem fazer uso de pólvora e conhecimentos de balística, é capaz de causar grande

2 "*Internet Usage Statistics, Internet World Stats*". http://www.internetworldstats.com/stats.htm, acessado em 2 out. 2013.

3 Ibid.

destruição no objeto de seus ataques. Imagine-se o impacto se ataques cibernéticos tiverem alvos tais como: redes de energia elétrica e gás, abastecimento de água, serviços de transporte, de saúde, ou financeiros, entre outros.

Eventos recentes mostraram como a Guerra Cibernética pode ser nociva a países inteiros. Em 2007, a Estônia foi vítima de ataques que, segundo os estonianos, tiveram origem na Rússia[4]. A causa teria sido a retirada de um monumento em homenagem aos soldados soviéticos mortos na segunda guerra mundial que ficava em Tallin. Os ataques duraram algumas semanas e incluíram a negação de serviço de diversos sítios eletrônicos do governo estoniano e de partidos políticos, bem como sistemas de grandes companhias e bancos, que pararam de responder devido aos ataques[5].

Outra ocorrência paradigmática foram os ataques à Geórgia em 2008, também atribuídos aos Russos. Foi a primeira vez em que se verificou uma coordenação entre ataques cibernéticos e forças convencionais[6]. Os ataques às redes de computadores antecederam a ação das forças armadas russas e tiveram como resultado isolar a Geórgia do restante do mundo, mediante sobretudo diversos ataques de negação de serviço.

O Irã também foi vítima de um poderoso ataque cibernético. Neste caso, uma sucessão de versões de um vírus chamado *Stuxnet*, supostamente desenvolvido em conjunto pelos Estados Unidos da América e Israel, teriam sido utilizadas para afetar usinas nucleares

---

4 Richard A. Clarke e Robert K. Knake. *Cyber war: the next threat to national security and what to do about it* (New York: ECCO, 2010), 18.

5 Luiz F. D. Moura e Castro, *"Estônia sofre ataque virtual"*, PUC Minas (2007), 2-4.

6 Paulo Shakarian, *"Análise da campanha cibernética da Rússia contra a Geórgia em 2008"*, Military Review, novembro-dezembro de 2011. http://usacac.army.mil/CAC2/MilitaryReview/Archives/Portuguese/MilitaryReview_20111231_art011POR.pdf, acessado em 5 out. 2013.

iranianas. O ataque supostamente resultou na interrupção do funcionamento de milhares de centrífugas de enriquecimento de urânio. Porém, em virtude da permeabilidade das redes de computadores, o vírus acabou se espalhando pela rede e infectou máquinas por todo o mundo, causando prejuízos incalculáveis[7].

A fim de compreender a dimensão dos ataques a sistemas de interesse público no Brasil, até junho 2012 a Polícia Federal já havia identificado e monitorava 250 *hackers*. Ainda de acordo com esse órgão, as redes informatizadas do Governo Federal sofrem, a cada hora, cerca de dois mil ataques cibernéticos[8]. Os dados apontam para a necessidade de que sejam evitadas tais ameaças e, na medida em que se conhecem seus autores, de o Estado se utilizar de sua competência punitiva exclusiva.

A insegurança relacionada a bens jurídicos tutelados pelo Direito é tão relevante que os próprios *softwares* antivírus materializam como a solução técnica pode suplantar uma solução jurídica face a ameaças cibernéticas, muitas vezes.

Noções de territorialidade

Dos diversos autores que teorizam o Estado, é recorrente o entendimento que existem três elementos essenciais do Estado moderno: o povo, o território e a soberania. A despeito de considerações acerca da possibilidade de sobrevivência do Estado sem um desses elementos de forma temporária, é quase unânime

7 "Stuxnet – Obama ordenou os ataques ao Irã", Defesanet. http://www.defesanet.com.br/cyberwar/noticia/6262/stuxnet---obama-ordenou-os-ataques-ao-ira, acessado em 20 set. 2013.

8 "Polícia Federal inaugura centro contra ataques cibernéticos", *G1 Brasil*. http://g1.globo.com/brasil/noticia/2012/06/policia-federal-inaugura-centro-contra-ataques-ciberneticos.html, acessado em 2 out. 2013.

a opinião de que ambos são condições *sine qua non* para o Estado como se entende ainda hodiernamente.

De maneira geral, entende-se que o povo é o elemento humano que compõe o Estado. Diversos são os autores que se dedicam a diferenciar o conceito de povo com as noções de população e de nação. Para uma reflexão jurídica, torna-se satisfatória a consideração de que o povo é o conjunto daqueles sobre quem o Estado pode exercer seu poder, o que correspondia a todos aqueles situados em sua área de abrangência.

A soberania é a expressão do poder do Estado. Esse poder apresenta diferentes repercussões e formas de expressão conforme se analisa a partir do aspecto político ou do aspecto jurídico. Porém, consoante o surgimento do Estado de Direito e a constante judicialização das relações internas e externas ao Estado, esses dois aspectos tendem a se fundir em um mesmo conjunto de manifestações: independência em relação a outros Estados, capacidade de auto-organização, legitimidade para usar a violência como medida coercitiva dentro do seu território, possibilidade de ter sempre a última palavra (última instância) sobre toda e qualquer questão interna, dentre outros.

O território é a porção física do globo que um determinado Estado ocupa. Em regra, o povo habita o território e somente dentro dos limites de seu território o Estado pode exercer a soberania. Segundo Bonavides[9] fazem parte do território de um Estado, além da terra firme: as águas compreendidas no limite terrestre, o subsolo, a plataforma continental e o espaço aéreo. Segundo esse mesmo autor, o território possui uma concepção política e outra jurídica. A fim de explicar a natureza jurídica do território, destacam-se quatro

9 Paulo Bonavides, *Ciência Política* (São Paulo: Malheiros, 2000), 93-94.

teorias: território-patrimônio, território-objeto, território-espaço e território-competência[10].

A partir dessas teorizações acerca do território, permite-se ver a estreita ligação entre território e soberania: o primeiro limita o alcance do segundo. De acordo com a Teoria Geral do Estado, a soberania se realiza com o total domínio do território por parte do Estado, impedindo que outros atores se sobreponham ao seu poder. Quanto ao aspecto jurídico dessa relação, parece ser suficiente para demonstrar a soberania do Estado que ele consiga exercer jurisdição sobre todos os pontos de seu território, mantendo o povo sob domínio exclusivo.

Todavia, a importância do território para o desenvolvimento de Estados – e mesmo muito antes da criação do Estado moderno – resultou em diversos conflitos de interesse. A fim de não se pensar que essa afirmação se situa num passado longínquo, basta observar as dissidências internacionais que ainda hoje existem entre países vizinhos em virtude de questões territoriais. Tais conflitos de interesse podem culminar em guerras, que historicamente ocasionaram perda de território para os derrotados, dentre outras tantas consequências prejudiciais.

Direito penal e territorialidade

A partir da noção de territorialidade, passa-se à análise da interseção desta com o Direito, entendido aqui como o ordenamento jurídico próprio de cada Estado[11]. As diversas incompatibilidades

10 Ibid., 107-115.

11 Sobre as diversas acepções da palavra "Direito", verificar a obra de Tércio Sampaio Ferraz Júnior *Introdução ao Estudo do Direito*.

entre o Direito tradicional e as condutas criminosas envolvendo a informática podem ser sintetizadas em três enunciados. Inicialmente, existe grande dificuldade em se determinar o juízo competente para julgar condutas, especialmente quando elas acontecem de maneira fragmentada em territórios de diferentes países. Em segundo lugar, a dificuldade de se imputarem as condutas ao agente. Uma terceira dificuldade é a insipiência – ou mesmo a inexistência – de leis que visem à punição de tais agentes. Nesse ínterim, já restou comprovado que a *Internet* torna imperiosa a adoção de novas medidas para que as normas jurídicas tenham eficácia.

Os limites da competência penal dos Estados

O tema ora apresentado relaciona-se, de forma mais relevante, com o Direito Penal Internacional, o qual tem ligações com o Direito Penal de cada Estado. Assim sendo, uma corte internacional pode se considerar competente para julgar crimes cometidos internamente em um Estado associado.

Nas hipóteses em que um bem jurídico tutelado é afetado por crimes considerados de maior gravidade e repercussão, como os crimes contra a humanidade e os crimes universais, o Tribunal Penal Internacional, em alguns casos, declara-se competente para julgar a conduta.

Exemplos de condutas, quase sempre gravíssimas, as quais o Tribunal Penal Internacional se afirma competente para julgar podem ser exemplificadas pelos crimes de: genocídio, guerra, tráfico de mulheres, dentre outros. Percebe-se, assim, que o Direito Penal Internacional compreende também um conjunto de princípios e normas que disciplinam conflitos de leis no espaço.

Para bem se aplicar a Lei Penal no espaço, é conveniente que se tenha noções do conceito de território – já que o conceito de territorialidade compõe o que se conhece por soberania.

Sobre o tema, destaca-se a obra de Bastos:

> No território de cada Estado vige, tão-somente, a sua ordem jurídica. Em outros termos, a nenhum país estrangeiro é lícito praticar atos coativos dentro do território nacional. A esse fenômeno dá-se o nome de impenetrabilidade da ordem jurídica estatal. Daí a importância assumida pelo território na configuração do Estado. É precisamente a circunstância de dispor ele de uma porção de terra sobre a qual apenas o seu poder é reconhecido, o que permite ao Estado ser soberano. [12]

Por certo tais definições, clássicas, quedam hoje questionadas, visto que na prática não atendem mais muitas das necessidades, se consideradas as novas tecnologias, a globalização e os delitos transfronteiriços. O cerne do problema neste questionamento está no fato de ser o território elemento essencial do Estado, sem o qual um Estado não existe. Em outras palavras, se alguém admite a inexistência de território, admitirá a ausência de Estado.

Se território é o espaço físico onde um Estado exerce sua soberania, equipara-se ao território, que seria o solo e tudo o que ele compõe, o mar territorial[13] e o espaço aéreo.

---

12 Celso Ribeiro Bastos, *Curso de teoria do estado e ciência política* (São Paulo: Saraiva, 1995), 12-13.

13 Dispõem sobre o assunto: a Lei 7.565/86, em seu art.11, combinada com a Convenção de Paris de 1919, e a Lei 8.617/93, em seu art. 1º. Ressalte-se que a adoção de determinada quantidade de milhas a partir da costa como mar territorial é instituto polêmico em sua extensão. Hoje o Brasil adota mar territorial como todo aquele a até 12 milhas da costa. Nem todos os Estados adotam esta mesma distância. O Brasil já adotou esta distância como 200 milhas. O antigo conceito cedeu ao novo por pressão internacional, em especial dos Estados Unidos. Hoje uma Convenção das Nações Unidas – a CNUDM, de 1982 – considera o espaço compreendido, em regra, entre 12 e 200 milhas da costa como Zona Econômica Exclusiva, região onde o Estado tem prioridade para exploração econômica na região considerada.

Nenhum Estado exerce sua soberania de maneira exclusiva sobre o alto-mar ou o espaço que existe depois da atmosfera. Tais bens são considerados bens de domínio público internacional.

Em alguns casos, o Brasil se considera competente para julgar uma conduta criminosa ocorrida em qualquer lugar do mundo: hipóteses de extraterritorialidade atinentes ao Direito Penal. A Lei n. 9.455, dispõe sobre os crimes de tortura, e prevê em seu art. 2º a aplicação da norma brasileira, ainda que o crime não tenha sido cometido em território nacional, desde que a vítima seja brasileira ou encontre-se o agente em local sob jurisdição brasileira. O problema é que algumas vezes, na prática, tipos penais como o ora apresentado, não apresentam efetividade/eficácia.

O art. 5º, § 1º do Código Penal trata do chamado território por extensão, equiparação ou ficção e do § 2º também interessa o conteúdo:

> art. 5º, § 1º: Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
>
> § 2º É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.

Normalmente os países aceitam os termos de um tratado que sugere que, em caso de crimes cometidos em aeronaves ou

embarcações, a jurisdição competente seria a do país cuja bandeira é hasteada na embarcação ou da matrícula da aeronave. Observe-se que, mesmo aceitando os termos de tal acordo internacional, o Brasil toma pra si uma responsabilidade extra, um *plus* somado à regra geral. E, com um pouco de reflexão, conclui-se razoável a legislação pátria sobre o assunto. Nem todos os Estados atendem ao pé da letra o Tratado Internacional e acabam por tentar expandir sua competência jurisdicional.

O tráfego rápido de informações proporcionado pela *Internet* faz com que frequentemente uma conduta nela realizada desconheça os limites impostos por fronteiras.

É difícil a identificação do instituto do território no *ciberespaço*. O *ciberespaço* dispõe de normas ou técnicas, que regulam sistemas de acesso e que não pertencem ao mundo jurídico tradicional. Desta forma, não vigora o conceito de soberania nem de competência territorial.

Um agente pode, do México, invadir um sistema de computadores em Londres se utilizando de um provedor asiático, causando prejuízos na África do Sul. O local do crime é um dos questionamentos de resposta polêmica. Outro seria qual o país competente para processar e julgar o sujeito da conduta. Um dos grandes desafios consiste em determinar se um país prejudicado por uma conduta praticada na *Internet* deve usar o poder de coerção de um ordenamento jurídico próprio para deter um indivíduo que está fora de seus limites de soberania. Some-se a este questionamento a hipótese de o país onde se encontra o agente da conduta prejudicial não punir a aludida atividade virtual.

Valin opina a respeito deste tipo de questionamento:

> O grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na *Internet*, reside no caráter internacional da rede. Na *Internet* não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?[14]

Os fatos elencados sobre a rede de computadores forçam ao entendimento de que está em curso uma mitigação da soberania nacional em favor de uma jurisdição, e portanto de uma soberania internacional, onde haveria a participação dos Estados na resolução de conflitos extraterritoriais. Efetivamente, quando se fala em efetivação do Direito Penal, percebe-se a relativa ineficácia do Direito Penal Internacional devido a seu caráter notadamente subsidiário em relação à jurisdição interna dos Estados. Conclui-se ser este um problema que carece de grandes esforços para se encontrar uma solução razoável.

O Código Penal brasileiro considera praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado, consoante a teoria da ubiquidade. Qualquer fragmento de conduta que tenha tocado o solo nacional, sugere a aplicação da lei penal brasileira. A Teoria da Ubiquidade é aplicada pela maioria dos Estados do mundo e leva em conta tanto o momento executivo, quanto o momento consumativo do crime.

Considerar como local do crime somente aquele em que está localizado o agente, não se apresenta como entendimento pacífico,

14 Celso Valin, *A questão da jurisdição e da territorialidade nos crimes praticados pela Internet*, in *Direito, sociedade e informática: limites e perspectivas da vida digital* (Florianópolis: Fundação Boiteux, 2000), 115.

mais que isso, tem sido objeto de recusa internacional: os Estados desejam tutelar os bens jurídicos que lhe são caros.

Doutrinadores brasileiros muitas vezes posicionam-se no sentido de que deve ser aplicada a regra geral do art. 6º do Código Penal, seguindo a Teoria da Ubiquidade, sem prejuízo de convenções, tratados e regras de Direito Internacional. Desta forma, os delitos cometidos fora do território nacional, poderiam receber, no Brasil, punição; desde que previstos em Convenções ou Acordos internacionais os quais o Brasil subscreva.

Quando se trata da necessidade de firmar um documento internacional que aponte parâmetros transnacionais a serem tomados com o escopo de que seja evitado o posicionamento de que nenhum país se considere apto a julgar crimes cibernéticos, a doutrina é uníssona no sentido de que é uma necessidade premente.

Dificuldades para a imputação de condutas a seus agentes

Ressalte-se que, muitas vezes, o que dificulta a punição de crimes é a realização fragmentária dos mesmos. Isso pode ser constatado a partir de uma análise da norma legal pátria: como não são puníveis os atos preparatórios de um crime, não são puníveis as condutas de agentes que planejam ou reúnem meios para cometer um crime no estrangeiro. Percebe-se que a realização fragmentada do *iter criminis*[15] em diferentes países pode dificultar – ou, na maioria dos casos, impedir – a punição de um agente por conduta criminosa praticada pela *Internet*.

15 O *iter criminis* é a trajetória para que um crime se consume. A doutrina comumente divide esse percurso da prática criminosa em quatro diferentes fases: cogitação, preparação, execução e consumação. No caso dos crimes cibernéticos, identificar que um agente praticou todos os atos que compõem o *iter criminis* é tarefa muito complicada, especialmente ao se considerar que tais atos podem ser praticados em diferentes países, dadas as características próprias da *Internet*.

Além disso, na maioria dos casos não é simples a identificação do autor responsável por um determinado dano. Existem inúmeras formas de ataques cibernéticos[16], e sua quantidade e variedade aumentam na proporção do número de sistemas que se deseja atacar e do número de computadores e de *hackers*. Porém, algumas dessas formas de ataque são realizadas utilizando-se outras máquinas. Isso é comum em ataques de negação de serviço, nos quais diversas máquinas são utilizadas com zumbis simultaneamente. Neste caso, identificar os proprietários de todos os computadores dos quais os acessos foram realizados não indicaria o agente a ser responsabilizado pelo dano causado ao alvo do ataque.

Os crimes digitais no ordenamento jurídico brasileiro

Na falta de hipótese mais efetiva, frise-se a possibilidade da aplicação da lei penal brasileira em crimes cometidos fora do território brasileiro, quando em conformidade com o que dispõe o art. 7º do Código Penal. De acordo com esse dispositivo legal, sujeitam-se ao ordenamento brasileiro algumas condutas criminosas cometida no exterior. Para algumas dessas condutas, tem relevância o contexto externo (punibilidade da conduta no local em que foi praticada, dentre outros fatores previstos no art. 7º, §2º). Para outras condutas – previstas no inciso I do mesmo artigo – prevalece sempre a legislação brasileira[17], no entender da norma pátria.

16 Segundo Marcelo X. F. Crespo, os principais crimes digitais próprios são: acesso não autorizado, obtenção e transferência ilegal de dados, dano informático, disseminação de vírus, divulgação ou utilização indevida de informações, embaraçamento ao funcionamento de sistemas, engenharia social e phishing, interceptação ilegal de dados. Marcelo X. F. Crespo, *Crimes Digitais* (São Paulo: Saraiva, 2011), 63-87.

17 "Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:

I - Os crimes: a) contra a vida ou a liberdade do Presidente da República; b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa

Apesar das tentativas teóricas de que sejam criminalizadas condutas com base na extraterritorialidade, a aplicação prática da lei penal sobre uma conduta criminosa praticada fora do território brasileiro torna-se um problema cientificamente insuperável sem a cooperação entre os atores internacionais. Como resultado dessa limitação, é comum que condutas criminosas praticadas pela *Internet*, se assim tipificadas por um Estado isoladamente, permaneçam impunes.

No contexto interno, entrou em vigor em 2012 a lei 12.737[18], que resultou na tipificação de delitos informáticos, dentre outras alterações no Código Penal. Em virtude daquela lei, as seguintes condutas passaram a ser consideradas criminosas:

> invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim

pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; c) contra a administração pública, por quem está a seu serviço; d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil;

II - Os crimes: a) que, por tratado ou convenção, o Brasil se obrigou a reprimir; b) praticados por brasileiro; c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.

§ 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.

§ 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições: a) entrar o agente no território nacional; b) ser o fato punível também no país em que foi praticado; c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

§ 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: a) não foi pedida ou foi negada a extradição; b) houve requisição do Ministro da Justiça."

18 A Lei 12.737/12 também ficou conhecida como "Lei Carolina Dieckman" em virtude dos eventos ocorridos com essa atriz pouco antes da aprovação do projeto de lei: fotos íntimas da atriz teriam sido supostamente copiadas de seu computador e divulgadas na *Internet*, em uma violação clara à sua privacidade.

> de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.[19]

Todavia, esta lei tem aplicabilidade consoante o limite da jurisdição brasileira, ressalvadas as circunstâncias já destacadas de extraterritorialidade. Assim sendo, uma série de hipóteses não são abrangidas por esse dispositivo de maneira efetiva em virtude das circunstâncias em que ocorre uma conduta criminosa, como por exemplo um ato praticado parcialmente no Brasil e parcialmente em outro Estado.

A despeito das diversas críticas feitas à lei 12.737, há que se destacar que esse já foi um grande passo para romper a longa inércia do Poder Legislativo brasileiro em aprovar um projeto de lei sobre o assunto. Em 1999, já tramitava no Congresso Brasileiro um projeto de lei que visava à criminalização de condutas praticadas com o uso de meios informáticos[20].

Extrapolando os limites da jurisdição interna na tentativa de contornar a impunidade dos crimes cibernéticos, algumas iniciativas já foram tomadas com base na cooperação entre países. Um exemplo de mecanismo que tenta viabilizar a internacionalização do combate a delitos que transcendem os limites fronteiriços é a Convenção de Budapeste.

---

19 Presidência da República, Lei 12.737, de 30 de novembro de 2012. www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm, acessado em 12 nov. 2013.

20 Projeto de Lei 84, de 1999, de autoria de Carlos Affonso Pereira de Souza, Thiago Bottino, Ronaldo Lemos, Luiz Fernando Moncau, Pedro Paranaguá, Sérgio Vieira branco Jr., Bruno Magrani, e Pedro Nicoletti Mizukami.

Convenção de Budapeste

A Convenção sobre o Cibercrime (ETS 185) – também conhecida como Convenção de Budapeste – é um importante marco no Direito Internacional no sentido de harmonizar o Direito Penal Material dos Estados que a subscrevem no que tange a delitos informáticos. Assinada no ano de 2001, ela define poderes e ações que podem facilitar na tutela dos bens jurídicos protegidos pelo Direito Penal e na celeridade e eficácia de cooperação entre os signatários.

A Convenção, ao contrário do que se pode pensar num primeiro momento, não exige cópia literal de suas definições para os ordenamentos internos dos países, mas apenas coerência com relação ao previsto em seus quatro capítulos. Nesse sentido, é bastante esclarecedor o artigo 22[21], que trata das competências.

---

21 Convenção de Budapeste, art. 22:

"1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer à competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infração seja cometida:

a) no seu território;

b) a bordo de um navio;

c) a bordo de aeronave matriculada nessa parte e segundo as suas leis; ou

d) por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for de competência territorial de nenhum Estado.

2. Cada parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou condições específicas as regras de competência definidas no nº 1, alínea b à d do presente artigo ou em qualquer parte dessas alienas;

3. Cada parte adotará medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infração referida no artigo 24, nº1 da presente convenção, quando o presumível autor da infração se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição.

4. A presente convenção não exclui qualquer competência penal exercida por uma Parte sem conformidade com seu direito interno.

5. Quando mais de uma Parte reivindique a competência em relação a uma presumível infração prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal."

A Convenção de Budapeste é baseada na Recomendação R(89) 9 do Conselho da Europa – a qual sugere a elaboração de uma política criminal uniforme – e em trabalhos patrocinados por outros organismos internacionais, tais como a Organização das Nações Unidas (ONU), a Associação Internacional de Direito Penal (AIDP) e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

As condutas a serem combatidas, segundo o texto do documento, englobam, por exemplo: acesso ilícito de dados, interceptação ilícita, interferência nos dados ou nos sistemas, utilização indevida de equipamentos, pornografia infantil, infrações a direitos autorais, falsificação ou fraude cometidos com o uso de computadores.

Além das inovações no Direito Penal material, a convenção aborda também questões relativas a Direito Processual, versando, dentre outras coisas, sobre salvaguarda de provas, interceptação e apreensão de dados informáticos, e ações de cooperação internacional, inclusive quanto a hipóteses de extradição.

A Convenção acima citada representou um grande passo no sentido de se intensificar uma cooperação internacional com escopo no combate aos crimes cibernéticos. Todavia, há que se reconhecer que seu alcance ainda é deveras limitado, se comparado com a extensão e frequência das condutas que visa a coibir. Atualmente, segundo o Conselho da Europa[22], 43 países assinaram a Convenção, mas, destes, somente 12 foram ratificados[23]. A participação de países na Convenção depende do convite e aprovação por parte dos

22 Council of Europe, "Convention on cybercrime". http://conventionscoe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF+9/2/2006&CL=ENG, acessado em 12 nov. 2013.

23 Países signatários da Convenção de Budapeste ratificados: Albânia, Bulgária, Croácia, Chipre, Dinamarca, Estônia, França, Hungria, Lituânia, Romênia, Eslovênia e Macedônia.

membros do Conselho. O Brasil, que já soma mais de 83 milhões de internautas, não assinou a Convenção. Uma vez que o Brasil não fez parte do Conselho em que a Convenção foi criada, não lhe é facultado a simples aderência ao acordo. Segundo o Secretário do Ministro das Relações Exteriores, Samuel Pinheiros Guimarães, o Brasil teria que ser convidado pelo Comitê de Ministros do Conselho da Europa para assinar a Convenção[24]. Há que se destacar, nesse contexto, que pesa contra o Brasil o fato de somente em novembro de 2012 ter sido aprovada a primeira lei incriminando crimes cibernéticos.

Conclusão

Diante desses fatos, observa-se que a tutela a bens jurídicos até então realizada pelos ordenamentos nacionais apresenta novas questões que suscitam respostas rápidas, sob pena de reduzirem de maneira expressiva a eficácia do Direito e, consequentemente, do poder e da soberania dos Estados, mitigando a paz social.

Contudo, sabe-se que um dos grandes desafios ao se tratar do conceito de jurisdição a partir da territorialidade frente à *Internet* é a transnacionalidade da rede. Dessa forma, demonstrou-se que o alcance da jurisdição é significativamente prejudicado devido a três condicionantes principais: i) a dificuldade de se determinar o juízo competente; ii) a dificuldade de se imputarem as condutas ao agente; iii) a insipiência, ou mesmo a inexistência de leis que visem à punição de tais agentes.

---

24 Gills Vilar Lopes e Dalliana Vilar Pereira, A *convenção de Budapeste e as leis brasileiras*. www.academia.edu/786458/A_CONVENCAO_DE_BUDAPESTE_E_AS_LEIS_BRASILEIRAS, acessado em 12 nov. 2013.

No que diz respeito à punibilidade de crimes perpetrados por meio da rede mundial de computadores, porém, não basta a existência de leis nacionais, sendo imperiosa a cooperação internacional. Tal iniciativa já existe, porém ainda com grandes restrições para aumentar seu alcance. A Convenção de Budapeste sobre *cibercrimes* é um exemplo de tentativa de proteger interesses legítimos relacionados às novas tecnologias. Porém, para ter efetividade, seria indispensável adesão geral, com a finalidade de que não sejam mantidos locais de onde as ações de *hackers* podem ter início sem que haja consequência na esfera penal ou cível. A título de exemplo, o Brasil não é signatário dessa convenção.

Em razão da dificuldade de juridicizar as relações estabelecidas no *ciberespaço*, especialmente no que tange a ataques cibernéticos, evidencia-se a importância de o Estado atuar de maneira preventiva quanto a possíveis ataques desse tipo. Uma vez que a norma não é capaz de tutelar, por si só, um bem jurídico de forma satisfatória, a capacidade de combater o ilícito por outros meios – como a força ou a técnica – podem ser cogitados. De fato, no caso de um ataque cibernético transnacional, talvez a prevenção e a capacidade de contra-atacar sejam os únicos meios eficazes de defender os sistemas informáticos críticos, visando a tutelar, por fim, a paz social.

Frente a um contexto de ataques cibernéticos, percebe-se a dificuldade de se prover a tutela jurisdicional dos bens jurídicos afetados. Ao se verificar a mitigação do conceito tradicional de fronteira devido ao ambiente virtual proporcionado principalmente pela *Internet*, punir condutas praticadas por meio da *Internet* é tarefa que pode ultrapassar os limites do atual paradigma do Poder Judiciário, não somente no contexto nacional. Percebe-se, portanto,

que a defesa cibernética – cumulada com a possibilidade de responder a ameaças com a mesma forma e intensidade – se mostra como importante instrumento que, em última análise, pode garantir o *status quo* e a paz social típicos de um Estado Democrático de Direito como o Brasil.

CAPÍTULO 5

Guerra cibernética e formação militar: contribuições para um perfil do soldado cibernético

André Ferreira Alves Machado
Oscar Medeiros Filho
Walfredo Bento Ferreira Neto

Introdução

O presente trabalho visa discutir o perfil necessário à formação de militares para a chamada "guerra cibernética". Em termos militares, esta faz parte do conjunto de novas ameaças. Em 2008, a Estratégia Nacional de Defesa estabeleceu o tema como prioridade para o Exército Brasileiro. Apesar de possuir uma etimologia aparentemente clara, o termo *cibernética* passou a referir-se, a partir dos trabalhos de Norbert Wiener, à área do conhecimento que aborda o campo de comunicação e controle entre máquinas e homens. Buscar-se-á descrever a natureza desse novo tipo de combate que, aparentemente, sugere um novo campo de batalha, para além dos tradicionais ambientes operacionais. Tendo como objetivo específico discorrer sobre o perfil do militar nesse novo desafio, o trabalho se propõe a apresentar três alternativas às Forças Armadas: a) Inserir disciplinas "cibernéticas" na formação de todos os militares; b) Criar núcleos de

formação, dentro de cada Força; c) Criar uma quarta Força Armada. Sem a pretensão de oferecer respostas, o trabalho apresenta soluções adotadas por algumas forças militares. Pretendemos chamar a atenção para a possibilidade de mutação no perfil do soldado, que, provavelmente, deixará de ter menos características atléticas, aproximando-se do perfil de um "*nerd*". O texto divide-se em três seções. Na primeira, serão tratados aspectos relativos ao significado do termo "cibernética". Na segunda, serão discutidas as características que envolvem esta dimensão da guerra. Na última, discutiremos o perfil do "combatente cibernético".

Origem e significado do termo "cibernética"

A palavra cibernética deriva do termo grego *kybernetidé,* que significava a arte de pilotar uma embarcação. Platão relaciona o termo à arte de governar[1]. O significado moderno da palavra cibernética, entretanto, relaciona-se ao uso do termo *governator* (do inglês) em Mecânica. Em 1790, James Watt usou a expressão ao designar um mecanismo para estabilizar a velocidade de rotação do motor a vapor. Em 1868, o físico escocês James Clerk Maxwell descreveu certo tipo de mecanismo de controle no ensaio *The Theory of Governors*. Foi nesse ensaio de Maxwell, que o matemático Norbert Wiener diz ter-se inspirado para, em 1948, escrever a obra *Cybernetics, or Control and Communcation in the Animal and the Machine*. O interesse de Wiener por esse tema parece ter origem em um projeto de pesquisa iniciado nos primeiros anos da década de 1940, quando, como parte do esforço de guerra norte-americano, ele recebeu a incumbência

1 Marcílio Marques Moreira, "Karl Deutsch, a Política e a Cibernética", in: Deutsch na UNB: conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980 (Brasília: Editora da UNB, 1980), 31.

de desenvolver um "sistema de controle de baterias anti-aéreas que fosse capaz de acompanhar a trajetória em que se movia um avião, predizer sua posição futura e disparar fogo levando em conta, senão só os hiatos humanos do canhão e do avião envolvidos"[2]. Segundo o próprio Wiener, a cibernética envolveria "o estudo do que, em contexto humano, é, às vezes, descrito genericamente como o ato de pensar, e o que, em engenharia, é conhecido como controle e comunicação"[3].

Assim, os primeiros projetos "cibernéticos" tratavam do desenvolvimento de mecanismos destinados a regular automaticamente determinados artefatos industriais e bélicos, capazes de substituir o homem na tarefa de corrigir desvios dos sistemas projetados, por dispositivos reguladores programados especificamente para esta finalidade[4]. De forma geral, o termo *cibernética* no século XX passou a sugerir "o estudo das funções humanas de controle e dos sistemas mecânicos e eletrônicos que se destinam a substituí-los"[5].

Com o advento das redes de computadores (especialmente da *Internet*), a conotação da cibernética se aproxima cada vez mais da ideia de *infovias* (sistemas interligados de informação). O controle dos sistemas de comunicação passa a dominar a "agenda cibernética", onde temas como segurança, defesa e guerra cibernética fazem parte do dia a dia. Os exemplos proliferam-se. Em abril de 2007, aconteceram ataques maciços a instituições públicas e privadas da

2 Idem, p. 32.

3 Idem, p. 33.

4 Norbert Wiener, "*Cybernetics, or control and communication in the animal and the machine*", *apud* Isaac Epstein, *Cibernética* (São Paulo: Ática, 1986), 13-14.

5 Roque Theophilo, "A História da Cibernética", http://www.psicologia.org.br/internacional/ap10.htm, acessado em 3 out. 2011.

Estônia; em agosto de 2008, ocorreram atuações cibernéticas no setor estratégico da Geórgia.

Em 2010, foram noticiadas ações nos complexos industriais do Irã, China e Indonésia; e, recentemente, tornou-se público o caso *WikiLeaks* que divulgou cerca de 250.000 mensagens confidenciais dos Estados Unidos da América, e, em 2011, empresas nacionais como a Petrobras e até a Presidência da República têm sofrido "ataques cibernéticos"[6], além do caso de espionagem norte-americana divulgado pelo ex-técnico da *Central of Inteligence Agency* (CIA), Edward Snowden.

Esses são alguns exemplos do emprego da cibernética utilizada tanto a partir do uso das redes físicas, quanto pelo poder advindo do uso das informações digitalizadas, o que se tem denominado de "poder cibernético".

Dimensão cibernética da guerra: medidas de ataque e de defesa

Do ponto de vista militar, ameaças cibernéticas se relacionam a um grande espectro de temas que envolvem tópicos de guerra eletrônica até segurança de sistemas de informação (Quadro abaixo). O envolvimento militar, tanto defensivo quanto ofensivo, em uma guerra cibernética, sugere sensoriamento (detecção),

6 Em tom alarmante, um recente artigo publicado na Revista *Info Exame* sugere que qualquer computador pessoal pode estar sendo utilizado, por hackers, em ações criminosas. Ele apresenta uma tabela contendo a cotação de trabalhos no mercado negro das fraudes: com aproximadamente US$ 1 podemos adquirir dados pessoais roubados para abrirmos uma conta bancária; com o valor de US$ 150 compramos o envio de spams para 1 milhão de e-mails; e que com um pouco mais de investimento, aproximadamente US$ 300, podemos infectar uma centena de máquinas. Cf. Luiz Cruz Carlos Machado e Aline Monteiro, "Guerra Anônima", *Revista Info Exame*, agosto de 2011.

monitoramento e atuação[7]. Assim, faz-se necessário diferenciar os campos: eletromagnético (telecomunicações), redes de computadores (*infovias*) e controle da informação (sistema de informação).

Quadro 1: Temas relacionados à Cibernética

Guerra eletrônica: Conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas.
Guerra centrada em redes: Guerra que reúne em rede os mais diversos elementos das forças armadas de um país, permitindo-lhe administrar diversas tarefas que vão desde a coleta até a distribuição de informações críticas entre esses muitos elementos. Outorga-lhe maior capacidade de combate ao ligar em rede os elementos de sensoriamento, de combate e de comando. Visa obter melhor sincronismo entre aqueles elementos e os efeitos que podem proporcionar, assim como o incremento na velocidade das operações bélicas e do processo decisório de comando.
Guerra de informação: Conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos.

Fonte: Glossário das Forças Armadas, 2007.

De todo modo, cibernética envolve muito mais temas do que o simples controle de sistemas computacionais de informação, como sugere o senso comum. Entretanto, considerando os objetivos do presente artigo, estabeleceremos um recorte na abrangência que o termo sugere e discutiremos o perfil do soldado cibernético,

7 José Carlos A. do Amarante, "A batalha automatizada: um sonho exequível?" *Cadernos de Estudos Estratégicos*, Rio de Janeiro, n. 9, p. 3-18, Centro de Estudos Estratégicos da Escola Superior de Guerra, jul. 2010.

levando em consideração apenas os aspectos que dizem respeito à comunicação e ao controle de sistemas de informação, na sua forma digitalizada.

Essa parece ser a definição adotada pelo Exército Brasileiro (EB). Segundo Paulo Carvalho[8], oficial general do Exército, oriundo da Arma de Comunicações, *cibernética* é um

> termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC), bem como os sistemas de armas e vigilância.

Oliveira[9] prefere não definir o termo, por considerar um tanto quanto prematura a apresentação de conceito, sobretudo de uma área extremamente dinâmica, apenas falando em entendimento acerca de um "ambiente ou espaço cibernético, que contém a interação de pessoas, empresas e instituições públicas e privadas, nacionais e internacionais, utilizando modernos recursos de Tecnologia da Informação e das Comunicações (TIC)."

Para Oliveira considerando esses enfoques é que, utilizando-se dos recursos de TIC, as Forças Armadas devem buscar o aperfeiçoamento de sua capacidade de C4I (Comando, Controle, Comunicações, Computação e Inteligência), de modo a atenderem o

8 Paulo Sergio Melo de Carvalho, "O Setor Cibernético nas Forças Armadas Brasileiras", in *Desafios Estratégicos para a Segurança e Defesa Cibernética.*. In: BARROS, Otávio S. R Barros et al. (Brasília: Secretaria de Assuntos Estratégicos, 2011), 17.

9 *João Roberto de Oliveira, "Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional", in* Desafios *Estratégicos para a Segurança e Defesa Cibernética,* ed Otávio S. R. Barros et al. (Brasília: Secretaria de Assuntos Estratégicos, 2011), 108.

imperativo de atuação em rede, como preconiza a Estratégia Nacional de Defesa (END) de 2008 e na proposta de 2012.

Segundo o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, do Departamento de Segurança da Informação e Comunicação, S*egurança Cibernética* é a: "arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas."[10].

Em todos esses estudos há um ponto de contato – a *informação processada por computador* –, o seu uso ou negação de uso. Dessa forma, levaremos em consideração os aspectos que dizem respeito à comunicação e ao controle de sistemas de informação pautados em rede de computadores. Essa é a definição adotada pelo Exército Brasileiro (EB), por meio da utilização da sigla *C^4I*, que engloba Comando, Controle, Comunicações, Computação e Inteligência[11].

Apesar de discordarmos da ideia de que cibernética envolve exclusivamente "espaços virtuais", tomaremos emprestado a definição de guerra cibernética elaborada por Parks e Dugan:

> Guerra Cibernética é um sub-grupo da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existe uma diversidade de espaços cibernéticos, mas o mais relevante para a Guerra Cibernética é a *Internet* e as redes a ela

10 Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. v. 01. Brasília: Gabinete de Segurança Institucional da Presidência da República, 2010. http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf, acessado em 8 ago. 2011.

11 Internacionalmente emprega-se, hoje, a sigla C4ISR (Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento). Na Argentina, C4IVR (EISSAR et. al., 2012, p. 9).

> interligadas. Em termos militares, guerra cibernética deve ser entendida como uma combinação de ataque e defesas a redes de computadores envolvendo operações especiais de informação[12].

Para os fins propostos nesse artigo, torna-se interessante, desde já, distinguir "segurança da informação" de "guerra cibernética". De fato, não existem muitas diferenças do ponto de vista das ferramentas, técnicas e conhecimentos utilizados. A principal distinção reside na origem e intenção do autor: enquanto a primeira sugere conflitos no campo privado, a segunda envolve, necessariamente, relações de poder entre Estados. Ações oriundas de um indivíduo, com motivações pessoais, não podem ser consideradas como sendo guerra cibernética. Para que esta ocorra, portanto, faz-se necessária a "existência de patrocínio estatal"[13]. Essa abordagem, portanto, serve para sistematizar as ações de segurança pública e as de Defesa propriamente dita.

O fato é que a guerra cibernética impõe uma nova realidade para os teatros de operações militares, na medida em que o "espaço cibernético" constitui-se como outro tipo de "território" (espaço de poder). Atualmente, a maioria dos sistemas de informação, necessários para o funcionamento da sociedade moderna, encontram-se interligados por meio de redes de computadores. Nesse contexto:

> Os alvos não são mais somente pessoal e instalações militares. Agora, bancos, usinas elétricas, empresas de telefonia e de telecomunicações, sistemas de transporte

12 Raymon C Parks et al., "Principles of Cyber-warfare". Paper apresentado no *Workshop on Information Assurance and Security* realizado pela Academia Militar de West Point em junho de 2001. http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf, acessado em 4 out. 2011.

13 André Melo Carvalhais Dutra, Ibidem.

> e logística, serviços de emergência e segurança pública, entre outros são alvos em potencial, uma vez que a indisponibilidade continuada de quaisquer destes serviços certamente levaria uma nação ao colapso.[14]

Outro aspecto interessante é que a guerra cibernética aponta para uma questão paradoxal: quanto mais desenvolvida tecnologicamente uma sociedade, maior será sua vulnerabilidade aos ataques cibernéticos. Ou seja, quanto mais dependemos de redes de computadores, maior será o medo de que adversários ataquem essas redes. Esse paradoxo também é verificado e quantificado por Clarke e Knake[15] (2010). Os dados obtidos por esses autores encontram-se condensados na Tabela 1.

Na tentativa de mensuração do poder cibernético de alguns países (EUA, Rússia, China, Irã e Coreia do Norte), Clarke e Knake montam uma tabela, conforme gráfico abaixo, a partir da avaliação de três

Tabela 1: Capacidade geral de guerra cibernética

Estado	Capacidade ofensiva	Capacidade defensiva	Grau de dependência	Score total
Estados Unidos	8	1	2	11
Rússia	7	4	5	16
China	5	6	4	15
Irã	4	3	5	12
Coreia do Norte	2	7	9	18

Fonte: adaptado de Clarke e Knake (2010).

14 Idem.

15 *Richard Clarke e Robert Knake, Cyber war:* the next threat to national security and what to do about it. (*New York: CCCO, 2010).* Obra consultada em formato e-book (kindle), portanto sem como precisar a página.

variáveis: *cyber offensive*; *cyber dependence* e *cyber defense*, na qual: *ofensiva* refere-se à capacidade de atacar outra nação; *dependência* significa medida que a nação é interligada por redes e sistemas que podem ser vulneráveis a um ataque cibernético no caso de guerra; e *defesa* diz respeito à capacidade de um país tomar medidas para bloquear ou mitigar um ataque cibernético. A variação do escore é de 0 (zero) a 10 (dez).

Para Clarke e Knake, os Estados Unidos seguidos de perto pela Rússia são os países com maior capacidade de realizar ações ofensivas no ambiente cibernético. Em seguida, formando uma espécie de segundo time, vem a China e, talvez, a França. Além desses, cerca de 20 países, entre esses o Irã e a Coreia do Norte, formam outro bloco.

Alvos, vulnerabilidades e medidas de guerra cibernética

De início, deve-se destacar que qualquer sistema computadorizado que possa aceitar entrada de dados constitui-se alvo em potencial. André Dutra[16] atenta para os dois meios de entrada de dados:

> A entrada desses dados pode ocorrer através de dois meios: meios físicos e meios de transmissão de dados. Meios físicos compreendem os dispositivos agregados à estrutura do equipamento: teclados e disquetes para computadores, ou manetes e botões para o computador de bordo de uma aeronave, por exemplo. Meios de transmissão de dados são aqueles que permitem a entrada de dados sempre que uma conexão direta, ou indireta for estabelecida ao sistema, por exemplo, através de redes sem fio, ou controle de

16 André Melo Carvalhais Dutra, "Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto!". http://161.24.2.250/sige_old/IXSIGE/Artigos/GE_39.pdf. Artigo sem numeração de página. Acessado em 08 out. 2011.

> um satélite através do qual passe as comunicações do sistema alvo.

Considerando as ideias de Lionel Alforde (2000), André Dutra[17] destaca:

> [...] o principal meio de proteção de sistemas cibernéticos é a sua segurança física. Essa afirmação ganha importância quando são consideradas as medidas passivas de defesa: isolar todos os sistemas críticos, colocar sobre controle manual as operações críticas (não podem ser realizadas por software, ou automatizadas), reduzir o nível de integração dos sistemas (o que reduz o número de entradas nos mesmos), e onde essa redução não for possível, manter o elemento humano no ciclo (embora o ser humano seja o elo fraco da segurança, é o único elemento capaz de tomar decisões baseadas em sua capacidade de discernimento e de realizar inferências) e ater-se às potenciais brechas de segurança (as conexões de comunicação são sempre a porta de entrada esperada para os intrusos).

Para o autor, a segurança física das entradas e saídas dos sistemas de informação computadorizados constitui a primeira linha de defesa. Neste caso, torna-se de suma importância pensar o ser humano como o elo fraco na manutenção da segurança da informação.

Em termos estritamente militares, a preocupação principal recai sobre sistemas de Comando e Controle e sistemas de armas. Citando a obra *Strategic Information Warfare: An Introduction*, de Gian Piero Siroli, Oliveira[18] destaca alguns tipos de ferramentas empregadas em

17 André Melo Carvalhais Dutra, "Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto!". http://161.24.2.250/sige_old/IXSIGE/Artigos/GE_39.pdf, acessado em 08 out. 2011.

18 João Roberto de Oliveira. *Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional*. 2011, p. 17.

ataques virtuais, como por exemplo: programas *scanners*, usados para mapear a topologia de redes; *sniffers*, que monitoram pacotes de dados; *cracker programs*, que podem "quebrar" senhas de acessos a sistemas; *trojan horses*, códigos que se camuflam em aplicadores com intenções pouco amistosas; dentre outros.

Essas ferramentas e respectivas possibilidades são alertadas por Almeida[19] e por Brein[20] (2012). O primeiro, militar da Força Aérea Brasileira, participante de fóruns de discussões na ONU, no sentido de normatização do ciberespaço, nos anos de 2005 e de 2010. O segundo, perito em segurança da informação, integrante do Centro Brasileiro de Perícia Forense, em palestra no I Seminário de Guerra Cibernética na Academia Militar das Agulhas Negras, no ano de 2012.

De acordo com Almeida[21]:

> Em quase todos os computadores vendidos ao redor do mundo, o sistema operacional já instalado pela fábrica é o Windows. Somente a NSA[22], nem mesmo a Microsoft, possui o algoritmo de *backdoor* do Windows. Segundo os russos, isso permite que a NSA acesse qualquer computador ligado à *Internet*, direta ou indiretamente, o que traz grande segurança às forças dos EUA, no caso de uma ação cibernética.

---

19 José Eduardo P. Almeida, "A Tendência Mundial para a Defesa Cibernética*", in Desafios Estratégicos para a Segurança e Defesa Cibernética*, ed. Otávio S. R. Barros et al. (Brasília: Secretaria de Assuntos Estratégicos, 2011), 79-102.

20 Paulo Cesar Brein., "Fronteira Cibernética" [mensagem pessoal]. Mensagem recebida por <wbfneto@bol.com.br> em 3 de outubro de. 2012.

21 José Eduardo P. Almeida, Ibidem, 86-87.

22 Agência de Segurança Nacional dos EUA.

E segundo Paulo Brein[23], os Estados Unidos:

> possui um controle "branco" nas comunicações e em muitos softwares. Há informações que o governo americano possuiria senha de acesso a roteadores que estão espalhados no mundo. […] ninguém pode garantir que o governo americano não tenha uma senha que permita que ele acesse esse roteador, e a partir daí "sniffar"[24] tudo o que passa por ele. Há também informações que sistemas operacionais como Windows, por exemplo, quando vendidos para países inimigos, são fornecidos com algumas funcionalidades adicionais, que permitem o controle remoto de servidores.

Diante de um ataque cibernético[25], Dutra[26], sugere um conjunto de medidas ativas:

> [...] o uso de senhas e autenticação, medidas antropomórficas (ou segurança baseada em biometria), uso de *tokens*, esquemas de autenticação multicamadas (autenticações distintas para níveis de acesso distintos), autenticação por múltiplas conexões (a autenticação em um sistema, por exemplo, ativa o funcionamento de uma linha telefônica, que será utilizada durante a comunicação de dados, e para a

23 Paulo Cesar Brein., Ibidem.

24 *"Sniffar"*, no sentido empregado em redes de computadores, é um procedimento que ocorre a partir do uso de uma ferramenta denominada *sniffer*, que permite a interceptação e o registro de tráfego de dados. A partir disso, há possibilidades, como a captura de pacote, a decodificação e a análise do conteúdo, em tempo real.

25 Como medidas de ataque, Dutra (2011) destaca: programas de quebra de senha, programas de observação, obtenção de informação, disfarçadores de endereço e de identificação do alvo; programas de ataque (direcionados para um sistema específico); programas de marcação de alvos; programas de comportamento virulento, cavalos de tróia; programas de sobrecarga do sistema; manipulação direta de dados; e, por fim, bombas lógicas (sequências de código específicas em arquivos de dados, que manipulam os programas que acessam estes arquivos ou o BIOS do sistema).

26 André Melo Carvalhais Dutra, Ibdem.

qual é exigida uma outra autenticação), autenticação por múltiplos endereços (a autenticação só é reconhecida se originar-se de mais de um endereço válido) e uso de software de monitoramento.

O PERFIL DO SOLDADO CIBERNÉTICO

Chegamos, agora, no cerne de nossa proposta para o presente texto: discutir o perfil do "combatente cibernético". Como veremos, já há uma série de iniciativas que visam qualificar militares para o combate cibernético. Alguns países tomaram a dianteira dessa tarefa. Países como China e Taiwan já estão investindo na formação de novas unidades militares devotadas ao assunto[27]. A pergunta que devemos fazer de início é: que habilidades devemos desenvolver no guerreiro cibernético? Essas habilidades devem ser desenvolvidas por todos os militares, ou devem ser restritas a um grupo especializado? E, principalmente: qual o perfil esperado desse guerreiro cibernético?

Um ponto de partida parece ser os próprios atores que lidam no espaço cibernético. Citando a obra *Strategic Information Warfare: An Introduction*, de Gian Piero Siroli, Oliveira[28] aponta alguns potenciais atores cibernéticos: *hackers,* levados por desafios pessoais; *insiders*, em busca de recompensas financeiras; criminosos, envolvidos em espionagem industrial, por exemplo; e atores estatais e não-estatais, engajados em atividades de coleta de dados, propaganda, vigilância, censura e sabotagem. Para esse autor, estes últimos atores precisam, além de competência técnica e capacidade de produzir inteligência, de uma grande disponibilidade de recursos.

27 André Melo Carvalhais Dutra, Ibdem.

28 João Roberto de Oliveira, Ibdem, 19.

Fernandes[29] sugere um leque de temas que envolvem a relação entre cibernética e emprego militar e que poderiam ser ministrados nas instituições militares de ensino:

> [...] por exemplo, na tomada de decisão por parte dos comandantes, com base na informação disponível; na concepção de dispositivos automáticos e semi-automáticos de monitoramento e vigilância; no desenvolvimento de instrumentos eletrônicos e de comunicação; na análise matemática dos fenômenos aleatórios, perturbativos ou sujeitos a imprecisões de medida; na análise e correção de desvios e ruídos em redes de transmissão de sinais; na teoria formal dos autômatos; no estabelecimento das bases neurofisiológicas do comportamento humano e animal; nas pesquisas sobre equilíbrio em organismos e em comunidades, inclusive humanas; no projeto de máquinas de calcular ultra-rápidas (computadores), simuladores, radares, dispositivos de inteligência artificial, jogos virtuais, sistemas de busca-de-alvos, veículos não tripulados, nanotecnologia, órteses-próteses.

Sobre o perfil esperado do combatente cibernético, há que se atentar para as novas características que envolvem a guerra em espaços cibernéticos: "A *Internet* viabiliza a ação isolada do indivíduo, que passa a ter condições técnicas de realizar ataques pontuais independentemente de pertencer a um exército organizado"[30]. (Segundo Oliveira, "o engajamento pessoal em batalhas, mesmo que virtuais, é um aspecto importante do futuro da guerra que merece

29 Clístenes Guella Fernandes, "A educação do oficial para um mundo cibernético". Trabalho apresentado no II EPESM, realizado na Academia Militar das Agulhas Negras, Resende-RJ, em setembro de 2010, p. 5.

30 João Roberto de Oliveira, Ibdem, 50.

aprofundamento em futuros estudos". O autor destaca o fato de que, se há uma tendência a multiplicação de "guerreiros solitários" (virtuais), ao mesmo tempo "já não é tão simples alistar jovens para o serviço militar. A ideia de morrer em combate perdeu o charme que a propaganda ideológica vendeu durante as Grandes Guerras". Para o autor, "os interesses militares e econômicos enxertados no moderno combate, a privatização das forças que combatem em campo e as implicações da existência de novos mercenários são os temas em voga nos dias de hoje."[31]

Com um modelo de guerra coordenado à distância por sistemas de Comando e Controle e combatido cada vez mais por máquinas robotizadas, a luta em campo de batalha deixa de ser uma questão de honra para o guerreiro humano, sugerindo alterações na própria ética militar: "com o uso de robôs, muda o perfil da batalha e mudam também os soldados, o que levou à necessidade de recrutamento e seleção baseada em novas competências: adolescentes vêm sendo o alvo de campanhas publicitárias pelas Forças Armadas dos EUA"[32].

Citando o artigo Guerra das Máquinas, de P. W. Singer (*Scientific American Brasil*, 2010), Oliveira[33] destaca algumas mudanças que as novas características da guerra estariam provocando no perfil do combatente:

> A nova característica da guerra, a capacidade de ser executada à distância, é um dos fatores mais surpreendentes para a atual geração, provavelmente assim como o foram o avião para quem lutava em terra ou o espaço sideral para quem combatia no ar. [...]. De pronto, mudam as características do soldado,

31 Ibdem,

32 Ibdem, 51.

33 João Roberto de Oliveira, Ibdem, 53-54.

> que passa a ter um perfil mais técnico do que força para o combate homem a homem. Jovens recrutas muito rapidamente passam a ter acesso a atribuições e comandos anteriormente restritos ao oficialato mais graduado.

O perfil autônomo e criativo do "guerreiro cibernético" parece ir de encontro ao perfil tradicionalmente imaginado para o militar. Em um interessante trabalho, Giuliana Leal[34] discute a tensão entre autonomia versus homogeneização na formação dos oficiais da Aeronáutica. Partindo da ideia de mortificação de Erving Goffman, Leal[35] sugere:

> Em vista desses processos ocorridos na formação dos oficiais da aeronáutica, temos uma contradição entre, de um lado, a mortificação do eu típica das instituições totais (processada no sentido da homogeneização do grupo) e, de outro, a valorização da individualidade, como parte das exigências de perfil do oficial que se pretende formar.

Para Leal, a socialização baseada na homogeneização se deve a fatores ligados ao preparo para as situações de guerra, que exigem rusticidade e tolerância ao estresse, além da criação de um espírito de corpo, compreendido pela instituição como um dos valores a ser cultuados. O problema apresentado por Leal é que a consequência principal da "mortificação do eu" é o desincentivo à autonomia dos indivíduos. Para a autora, porém, as constantes transformações por que tem passado o mundo, especialmente a partir da segunda

34 Giuliana Franco Leal, "Autonomia *versus* homogeneização na formação dos oficiais da Força Aérea Brasileira: hipóteses preliminares". Artigo apresentado no II EPESM realizado na Aman em outubro de 2010. http://www.aman.ensino.eb.br, acessado em 26 mai. 2011.

35 Giuliana Franco Leal, Ibdem, 9.

metade do século XX, exigem cada vez mais do oficial a "capacidade de questionamento e interpretação da realidade, na medida em que os conhecimentos se tornam também mais passíveis de mudanças"[36].

Assim, "o prejuízo à autonomia dos internos, típico das instituições totais, não pode ser mantido durante toda a formação do oficial, sem prejuízo do exercício de suas funções"[37]. Para ela, então, torna-se necessário ao futuro oficial o desenvolvimento de habilidades como "espírito crítico, para compreender as grandes questões estratégicas do mundo, e a capacidade de iniciativa, para agir de modo pró-ativo. Tudo isso exige um certo grau de autonomia, no sentido da liberdade intelectual"[38].

Por outro lado, pensar em um perfil marcado pela autonomia e criatividade tende a ferir o *ethos* consagrado do militar, segundo o qual o sucesso em qualquer atividade exige a subordinação da vontade individual à vontade do grupo[39]. Do ponto de vista sociológico, portanto, a "intensificação das individualidades tende a ser acompanhada pelo enfraquecimento da consciência coletiva"[40].

Outro aspecto destacado por Huntington e que deve ser considerado é o da disciplina. Para Huntington[41], a ética militar enfatiza a obediência como a maior das virtudes do soldado.

Aparentemente não é bem esse o perfil que se espera de um soldado cibernético. Aspectos como flexibilidade de raciocínio, iniciativa e criatividade parecem ser fundamentais para o perfil

36 Ibdem, 7.

37 Ibdem, 6.

38 Ibdem, 8.

39 Samuel P. Huntington, "O Soldado e o Estado: Teoria e Política das Relações entre Civis e Militares" (Biblioteca do Exército. Rio de Janeiro, 1996).

40 Giuliana Franco Leal, Ibdem, 9.

41 Samuel P. Huntington, Ibidem, 97.

do guerreiro cibernético. Características comuns a quem lida com *Internet* – compartilhar informações e soluções – parecem, à primeira vista, destoar da discrição tradicionalmente exigida dos militares (cultura do sigilo). Ao mesmo tempo, cabe aqui lembrar que, sendo o ser humano o elo principal entre as redes de computadores, com capacidade de decisão e discernimento, este torna-se um potencial alvo de "ataque", exigindo do "combatente cibernético" alto grau de discrição e lealdade.

Em um esforço de simplificação, apresentaremos no Quadro 2 uma tipologia do perfil militar em relação ao modelo tradicional e cibernético.

O futuro das guerras cibernéticas parece sugerir uma parceria cada vez mais aproximada entre "combatentes" civis e militares. Como vimos anteriormente, a distinção entre "guerra cibernética" (lutas de poder envolvendo Estados) e "segurança da informação" (ambiente privado) reside na origem e intenção do autor, e não nas ferramentas, técnicas e conhecimentos utilizados. Desta forma, é seguro afirmar que grande parte das pesquisas desenvolvidas voltadas para a "segurança da informação" possuem aplicações em "guerra cibernética"[42]. Essa visão é importante, na medida em que interfere diretamente no recrutamento desses "soldados".

Quadro 2: Tipologia do perfil do militar tradicional e do cibernético

Aspecto	**Perfil Tradicional**	**Perfil Cibernético**
Iniciativa	Obediente	Criativo
Sigilo	Discreto	Curioso
Habilidade esperada	Rusticidade	Raciocínio lógico
Pertença ao Grupo	Pelotão	Rede Social

42 André Melo Carvalhais Dutra, Ibidem.

Citando a obra *Information Warfare and the Laws of War* (2003), de Geoffrey Darnton, Oliveira[43] discute a convergência das atividades civis e militares, o que o autor denomina de *civilinização* da guerra e dos assuntos militares, que teria como um dos fatores impulsionadores o aspecto dual da tecnologia militar: o GPS e a *Internet* seriam exemplos disso. Essa fusão civil-militar encontra paralelo também na fusão atores estatais e não-estatais: os últimos já estão engajados nos esforços de guerra e os primeiros vêm se envolvendo em operações de escopo mais abrangente do que as meras operações militares.

Além disso, é interessante destacar a dificuldade que as forças armadas possuem, atualmente, de reter talentos na área de engenharia da computação, como bem destaca Eliot Cohen, em *Technology and Warfare*[44]:

> Na era da informação, as semelhanças entre as organizações militares e civis foram rompidas. Organizações militares permanecem mais hierárquicas do que muitos de seus congêneres civis, e o mais importante, eles vem achando mais dificuldade em obter recursos humanos que necessitam. Um engenheiro de *software* no setor civil é muito bem pago, e bastante autônomo, trabalhando com pouca supervisão, relativamente. Tornou-se agudamente difícil para as forças armadas recrutar (e mais difícil ainda reter) homens e mulheres qualificados nestes domínios. Da mesma forma, jovens oficiais talentosos e agressivos são muito mais conscientes do que nunca das possibilidades abertas para eles fora do

43 João Roberto de Oliveira, Ibdem, 26.

44 Eliot Cohen, "Technology and Warfare", in *Strategy in the contemporary world,* ed. John Baylis et al (New York, Oxford. University Press, 2002), 141-160.

> âmbito militar. Reter os seus serviços em uma época de oportunidade econômica é difícil não apenas por causa de desigualdades de remuneração – que sempre existiu – mas também porque o setor civil muitas vezes pode oferecer muito mais oportunidade para mudança, autonomia e responsabilidade ilimitada. (tradução nossa)

Formação cibernética no Exército Brasileiro

Em 2008, o Ministério da Defesa brasileiro, por meio da Estratégia Nacional de Defesa (END), reconheceu o setor cibernético como de grande interesse para as Forças Armadas, cabendo ao Exército desenvolvê-lo para futura implantação nas demais Forças.

Para atender a essa demanda, o Exército Brasileiro está implantando o Centro de Guerra Cibernética visando qualificar os futuros guerreiros cibernéticos. Considerando a necessidade de capacitação de militares para operações conjuntas e em rede, o Departamento de Educação e Cultura do Exército, expediu uma portaria versando sobre a implantação do assunto cibernética nos cursos de formação de oficias e de sargentos da Linha de Ensino Militar Bélico, de todas as armas, quadro e serviços, com foco no processo de decisão em ambiente cibernético.

Como consequência, a partir de 2012 é ministrada na Escola Preparatória de Cadetes do Exército (EsPCEx), em parceria com a Universidade de Campinas, a disciplina Tecnologia da Informação e Comunicação (TIC), com uma carga de 60 a 75 horas. A partir deste ano, a Academia Militar das Agulhas Negras (Aman) iniciou, para todos os cadetes, de todas as armas, quadro e serviços, a disciplina de Segurança da Informação e Comunicação (SIC). Desta forma, ao

final dos cinco anos de formação, os cadetes terão aproximadamente 120 horas/aula de disciplinas vocacionadas à cibernética. Os cadetes da Arma de Comunicações, especificamente, terão uma carga horária maior, de aproximadamente 345 horas/aula. Além disso, todos os cadetes do 5º ano participarão de um Exercício de Atuação em Rede, com uma carga horária de aproximadamente 45 horas e, como disciplina eletiva, 25 cadetes poderão realizar o Estágio de Guerra Cibernética, no Centro de Instrução de Guerra Eletrônica (Cige)[45].

O Perfil Profissiográfico (Portaria Nº 89 do Estado-Maior do Exército, de 26 de julho de 2006) é o documento que estabelece os atributos desejáveis do Oficial Combatente do Exército Brasileiro, destacando, dentre outros, os seguintes requisitos comuns: crença em valores e culto às tradições, capacidade física, disciplina, respeito às leis, equilíbrio emocional, tato, capacidade de se integrar à vida social e capacidade de gerência pessoal. Considerando o cenário traçado ao longo do presente texto, caberia perguntar: os atributos acima listados figurariam entre os requisitos considerados primordiais para o combatente cibernético?

O novo Perfil Profissiográfico proposto (baseado no ensino por competências) sugere aspectos bem mais próximos daquilo que se imagina para o perfil de um guerreiro cibernético, dentre os quais

45 O Centro de Instrução de Guerra eletrônica (Cige) foi a primeira unidade de treinamento de Guerra Eletrônica da América Latina, criado em 1984. O Cige é a unidade do Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx), sediado em Brasília, que abriga o Núcleo Experimental de Cibernética. O núcleo possui a missão de aplicar e desenvolver o assunto Guerra Cibernética no âmbito da força. Atualmente realiza estágios de Guerra Cibernética para os cadetes da Aman e para militares das demais forças (Marinha e Aeronáutica). Para 2015, a missão é iniciar o Curso Básico de Guerra Cibernética, para Oficiais do Exército, com duração de 24 semanas, já com a utilização de um simulador de Guerra Cibernética, que está sendo desenvolvido pela empresa israelense ELBIT SYSTEM, especialmente, para as necessidades brasileiras. Futuramente, a intenção do CComGEx é envolver também a Escola de Comunicações (EsCom), unidade recentemente integrada ao centro, com a missão de desenvolver o setor de Defesa Cibernética.

destacamos: aplicar as tecnologias; utilizar equipamentos modernos; atuar em operações conjuntas; atuar em ambiente de rede; operar frente ao grau de imprevisibilidade; ser proficiente em dois idiomas, além do português; realizar pesquisas; trabalhar de forma integrada; adaptar-se a mudanças; produzir novos dados em busca de soluções eficazes; ter habilidade numérica e raciocínio lógico; raciocínio abstrato; raciocínio espacial; e resolver problemas.

Quanto ao aspecto afetivo destacado na tipologia acima, há que se pensar uma estratégia de formação que combine as qualidades típicas de um perfil cibernético com aquelas tradicionalmente exigidas dos militares, como obediência, lealdade e discrição.

Considerações finais

Sem pretender concluir o perfil do futuro "soldado cibernético", o artigo que se encerra buscou abrir uma discussão a respeito das possibilidades de formação do combatente desejável diante da iminência de eclosão dos chamados "conflitos cibernéticos".

Ao que tudo indica, vem ocorrendo um processo que, aparentemente, exigirá alteração do perfil do soldado voltado para a guerra cibernética. Sob tal conotação, o termo nos remete à ideia de descoloração, pois os tons que colorem o guerreiro cibernético ainda não estão nítidos.

O perfil desejável do soldado da guerra cibernética ainda não está claro. Tal indefinição gera um dilema a respeito da melhor estratégia para a sua formação: ou se investe na formação de um núcleo extremamente especializado, ou se prepara o contingente como um todo, capacitando o combatente clássico para os novos desafios da guerra.

Um aspecto, porém, parece verdadeiro: as novas características do campo de combate cibernético exigirão o trabalho coordenado das diferentes agências do Estado, aproximando, ainda mais, civis e militares no campo de batalha cibernético.

CAPÍTULO 6

A atuação do Centro de Defesa Cibernética na Copa das Confederações Fifa/2013

José Ricardo de Souza Camelo
João Marinonio Enke Carneiro

Introdução

A Defesa Cibernética vem se tornando uma atividade fundamental para o êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle (C2), por meio da proteção dos ativos de informação. Na condição de atividade especializada, sua execução se baseia em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares.

Em dezembro de 2008, a Estratégia Nacional de Defesa (END) reconheceu três setores estratégicos para a Defesa Nacional: Nuclear, Cibernético e Espacial. Ao Exército, coube a responsabilidade pela coordenação e integração do Setor Cibernético[1]. Em decorrência dessa atribuição, foi ativado, em 2 de agosto de 2010, o Núcleo do Centro de Defesa Cibernética (NuCDCiber).

1 A Diretriz Ministerial nº 14/2009 do Ministério da Defesa, de 9 de novembro de 2009, definiu providências para o cumprimento da END nos setores estratégicos da defesa, estabelecendo as responsabilidades para cada Força Armada.

Foi somente dois anos depois, em 20 de setembro de 2012, que o Decreto Presidencial nº 7.809, entre outras medidas, incluiu na Estrutura Regimental do Comando do Exército, o Centro de Defesa Cibernética (CDCiber), ativando o Centro propriamente dito. Posteriormente, o Ministério da Defesa (MD), por intermédio da Portaria nº 3.405/MD, de 21 de dezembro de 2012, atribuiu ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa.

Desta forma, o Centro de Defesa Cibernética passou a atuar em prol do MD e das demais Forças Armadas, passando ao controle operacional[2] daquele Ministério por ocasião das operações conjuntas.

A seguir, veremos como se desenrolou a atuação do CDCiber na Copa das Confederações.

A missão do CDCiber

A atuação do CDCiber materializou o "vetor" Segurança e Defesa Cibernética do planejamento das ações de segurança previstas para a Copa das Confederações. Esse planejamento foi elaborado pelo MD em coordenação com a Secretaria Especial para Grandes Eventos (Sesge), vinculada ao Ministério da Justiça, contando com as Forças Armadas, com a Polícia Federal e as Polícias Estaduais e Municipais, além de uma miríade de agências governamentais. Foi, portanto, uma Operação Interagências, com todas as diferenças de cultura e nível de complexidade em segurança cibernética entre as organizações

2 Poder atribuído a um comandante para empregar e controlar forças, em missões ou tarefas específicas e limitadas, de modo a capacitá-lo ao cumprimento de sua missão. Ministério da Defesa, MD35-G-01, *Glossário das Forças Armadas*, 2007.

envolvidas e uma necessidade intrínseca de grande coordenação de esforços.

Assim, a missão do CDCiber no evento, como definida na Ordem de Operações do Destacamento Defesa Cibernética (Dst Def Ciber), pode ser descrita pela seguinte frase: A fim de colaborar com as medidas de segurança durante a Copa das Confederações Fifa/2013, coordenar e integrar os planos de segurança e defesa cibernéticas contra ações cibernéticas hostis.

A missão de coordenar consistiu em conjugar harmonicamente os esforços para a consecução da segurança e defesa cibernéticas da Copa das Confederações, otimizando os resultados e aumentando a eficácia da ação conjunta de todas as entidades governamentais de segurança e defesa cibernéticas envolvidas no evento.

A missão de integrar consistiu em contribuir para os processos de segurança e defesa cibernéticas da Copa das Confederações, por meio da coordenação dos parceiros; análise de riscos de ativos críticos para o evento; gestão de incidentes de rede; inteligência cibernética; e segurança e defesa da própria rede, inserida no ambiente cibernético do evento.

Como a missão era por demais abrangente, foi necessária a delimitação de um escopo capaz de atender com a infraestrutura e recursos disponíveis. O escopo abrangido por essa missão e as medidas de proteção voltaram-se, prioritariamente, para os ativos informacionais e infraestruturas de tecnologia da informação dos seguintes centros e organizações:

- Centro de Coordenação de Defesa de Área (CCDA).
- Centro Integrado de Comando e Controle Regionais (CICCR).
- Centro de Defesa Cibernética (CDCiber).

- Rede Operacional de Defesa (ROD), abrangendo parte das redes do Ministério da Defesa (MD) e Forças Singulares (Marinha, Exército e Aeronáutica).

Também integraram os ativos a serem protegidos os domínios (*URLs*), os blocos de endereços, os sistemas e os serviços informados pelas organizações parceiras e colaboradores que, se comprometidos, poderiam afetar a segurança ou o desenvolvimento do evento.

Modelos anteriores: Jogos Olímpicos de Inverno em Vancouver, Rio + 20 e Jogos Olímpicos de Londres

As ações planejadas buscaram inspiração em modelos anteriores de proteção cibernética empregados em grandes eventos, iniciando com os Jogos Olímpicos de Inverno de 2010, oficialmente conhecidos como Jogos da XXI Olimpíada de Inverno, realizados entre 12 e 28 de fevereiro 2010, em Vancouver, Canadá.

Este estudo permitiu modelar a concepção da segurança e defesa cibernética montada pelo CDCiber para fazer face aos desafios impostos pela Conferência das Nações Unidas sobre Desenvolvimento Sustentável (CNUDS), conhecida como Rio + 20, e que foi realizada entre os dias 13 e 22 de junho de 2012. Esta atuação marcou o início das Operações conduzidas pelo CDCiber. As lições aprendidas na ocasião permitiram amadurecer em muito o modelo, os procedimentos e as ferramentas necessárias para as operações seguintes, além de fornecer subsídios para formular a primeira versão da Doutrina Militar de Defesa Cibernética, que foi enviada ao MD para apreciação no final de julho de 2013.

Em outubro de 2012, o CDCiber sediou o III Seminário de Defesa Cibernética do Ministério da Defesa. Na ocasião, o Centro recebeu, como palestrante convidado para o seminário o diretor do Quartel General de Comunicações do Governo do Reino Unido[3] (GCHQ), o Sr. Martin Howard, órgão que foi responsável pela coordenação da segurança e defesa cibernética nos Jogos Olímpicos de Londres. Essa participação também resultou em troca de lições aprendidas entre o CDCiber e o GCHQ.

Desenho da atuação

Para a atuação no evento, o CDCiber estabeleceu um Destacamento de Defesa Cibernética (Dst Def Ciber), cujo comandante foi o Coordenador Executivo de Segurança e Defesa Cibernética da Copa das Confederações (Cesd Ciber). Foi também estabelecido que todas as ações de segurança e defesa cibernética que envolvessem duas ou mais organizações relacionadas com o evento estariam sob a coordenação do Cesd Ciber.

O Destacamento de Defesa Cibernética foi composto por um Dst Def Ciber Central, localizado em Brasília, e mais seis Dst Def Ciber Remotos (RMTO), situados em cada uma das sedes da Copa das Confederações, a saber Belo Horizonte, Brasília, Fortaleza, Recife, Rio de Janeiro e Salvador. A cidade de Brasília abrigou, portanto, o Dst Def Ciber Central e um Dst Def Ciber Rmto.

Todos os Dst Def Ciber Remotos foram conjuntos, ou seja, compostos por militares das três Forças Armadas. O Dst Def Ciber Central também foi conjunto, além de ser integrado por parceiros institucionais e empresas contratadas.

3 GCHQ Website. http://www.gchq.gov.uk, acessado em 03 set. 2013.

Assim, o Dst Def Ciber coordenou e integrou, a partir do seu Destacamento Central, no período de 10 a 30 da junho de 2013, as ações de segurança cibernética nos âmbitos nacional e regional (em cada sede), visando contribuir para a proteção do ambiente cibernético relacionado à Copa das Confederações.

Coordenação e integração

O Dst Def Ciber desempenhou as seguintes atribuições de coordenação:

- Estabelecimento de parcerias com organizações brasileiras que atuam em segurança e defesa cibernéticas de modo a perceber, obter, registrar, processar e disseminar informações que permitam mitigar ou evitar incidentes de segurança cibernética que ameacem a Copa das Confederações.
- Definição da estratégia geral entre os parceiros para cumprimento da missão de segurança e defesa cibernéticas para a Copa das Confederações.
- Construção, de modo conjunto, das estratégias específicas com cada parceiro.
- Organização e treinamento da equipe que compôs o Destacamento de Defesa Cibernética, com membros das Forças Armadas, Ministério da Justiça e empresas civis, recebendo o pessoal especializado de cada órgão.
- Regeu o trabalho conjunto, verificando a efetividade das estratégias geral e específicas e viabilizando a harmonização e adequação dos esforços empregados.

- Manteve integrantes do destacamento nas sedes (Dst Def Ciber Rmto) e no Ministério da Defesa, por intermédio de um oficial de ligação, para facilitar a gerência do trabalho conjunto.
- Organizou e compartilhou as lições aprendidas entre os parceiros após a ação.

O Dst Def Ciber desempenhou as seguintes atribuições de integração:

- Montagem de um "sistema de consciência situacional", por meio de um conjunto de mecanismos para obter e concentrar informações sobre:
  - sistemas de Tecnologia da Informação e Comunicações (TIC) e ativos críticos para a Copa das Confederações;
  - diagnósticos de riscos dos ativos analisados, no que foi considerado pertinente;
  - inteligência cibernética;
  - incidentes nas redes envolvidas;
  - eventos de segurança da informação de interesse;
  - gerência de redes de interesse;
  - lições aprendidas;
  - outros.
- Gestão das informações de inteligência sobre ameaças à Copa das Confederações, detectadas no espaço cibernético.
- Identificação dos principais ativos informacionais relacionados ao Evento, no âmbito dos Centros de Coordenação de Defesa de Área.

- Monitoramento do espaço cibernético de interesse para avaliação do nível de risco dos sistemas envolvidos.
- Comunicação aos envolvidos das informações de relevância para segurança dos sistemas de TIC envolvidos no Evento (incidentes de segurança, ameaças aos sistemas, vulnerabilidades detectadas, alertas e outras).
- Gestão dos incidentes que ocorreram nos ativos de informação e sistemas de TIC críticos para o Evento (detecção, triagem, análise, comunicação e acompanhamento da evolução e solução).
- Acompanhamento e verificação do tratamento realizado pelos proprietários, custodiantes ou gestores dos ativos de informação atingidos em incidentes detectados pelo destacamento e coordenação da participação de atores adicionais para efetivação da solução, quando necessário.
- Efetivação da segurança cibernética do próprio destacamento.
- Comunicação aos CCDA, por intermédio dos seus Oficiais de Comando e Controle (D6), da necessidade de mudança no Nível de Alerta Cibernético no início e fim das atividades da Copa das Confederações, assim como as demais mudanças que se fizeram necessárias durante o evento.

Os Destacamentos de Defesa Cibernética Remotos foram organizados em duas equipes de dois integrantes para cada cidade-sede, totalizando quatro elementos em cada localidade. A primeira equipe ligou-se diretamente ao CCDA e, a segunda, ao CICCR de cada local atendido.

Os Dst Def Ciber RMTO desempenharam as seguintes atribuições:

- Recomendação de ações para corrigir as vulnerabilidades encontradas.
- Acompanhamento e documentação da efetivação ou não da correção das vulnerabilidades encontradas nas análises de risco realizadas nos CCDA e CICCR, mantendo o Dst Def Ciber Central informado sobre o assunto.
- Notificação imediata ao Dst Def Ciber Central da ocorrência de eventos de segurança que necessitassem de acompanhamento centralizado.
- Acompanhamento e documentação das providências tomadas pelos responsáveis pela proteção cibernética nos CCDA e CICCR em face aos incidentes de segurança que viessem a ocorrer, relatando ao Dst Def Ciber Central o mais rápido possível.
- Identificação dos contatos e estabelecimento claro do relacionamento técnico e gerencial com os responsáveis por ativos de informação nos CICCR e CCDA (equipes de tratamento de incidentes de rede [Etir], gerentes de rede, equipe de segurança da informação, pessoal de inteligência e demais contatos que se fizessem necessários).
- Manutenção de ligação permanente com o Dst Def Ciber Central.
- Recebimento dos Informativos de Inteligência e Notificações Técnicas do Dst Def Ciber Central e disseminação do conhecimento para os responsáveis pelos ativos em risco.

- Avaliação preliminar (a ser estendida na Copa do Mundo) das vulnerabilidades dos ativos de TIC dos CCDA envolvidos na Copa das Confederações, valendo-se de empresa civil contratada pelo CDCiber.
- Avaliação preliminar (a ser estendida na Copa do Mundo) das vulnerabilidades dos ativos de TIC dos CICCR, conforme a disponibilidade de meios dos Dst Def Ciber Rmto, desde que cada CICCR disponibilizasse, oportunamente, os ativos de TIC a serem considerados.

Ações cibernéticas

As ações de segurança e defesa cibernéticas buscaram proteger os ativos de informação relevantes para a Copa das Confederações, bem como os sistemas de TIC que sustentavam as estruturas organizadas contra ameaças cibernéticas advindas dos ambientes interno e externo ao País. O adequado funcionamento das estruturas de TIC e a continuidade da prestação de serviços específicos relacionados à Copa das Confederações foram garantidos mediante ampla coordenação com os órgãos e entidades parceiras ligadas ao setor cibernético.

As ações de segurança e defesa cibernéticas foram executadas em apoio às operações conduzidas pelo Ministério da Defesa e pelo Ministério da Justiça (MJ), por intermédio da Secretaria Extraordinária de Segurança para Grandes Eventos, vinculada a esse Ministério.

A proteção cibernética é uma atividade de caráter permanente, que abrange as ações para neutralizar ou mitigar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes

de computadores e de comunicações, incrementando as ações de Segurança e Defesa Cibernética.

O escopo de proteção cibernética abrangeu, prioritariamente, os principais sistemas ou ativos de informação identificados como críticos para a realização da Copa das Confederações, pertencentes às infraestruturas de TIC dos CCDA, CICCR e MD.

As ações de exploração cibernética estiveram voltadas, prioritariamente, para a obtenção de informações no espaço cibernético acerca de possíveis movimentações de pessoas, grupos e organizações, ou ainda, ocorrências que demonstrem uma tendência à concretização de violações da segurança da Copa das Confederações. Cabe ressaltar, no que diz respeito a informações que permitiram o acompanhamento de indivíduos e grupos, foram somente utilizadas informações disponíveis publicamente, que puderam ser obtidas sem a necessidade de autorizações judiciais.

As ações de segurança cibernética específicas para correção de vulnerabilidades, configurações, correção de falhas, recuperação de desastres e manutenções diversas realizadas diretamente nos ativos, nos sistemas ou nas infraestruturas de TIC utilizadas pelas diversas organizações envolvidas no evento foram executadas pelos proprietários, custodiantes ou gestores desses ativos e sistemas. O Dst Def Ciber apoiou esse processo, por meio de orientações técnicas e gerenciais, e não por intervenção nos ativos e sistemas.

Serviços para proteção cibernética

O Dst Def Ciber orientou a atuação como prestador de serviços, ou seja, procedimentos e atividades desenvolvidos e disponibilizados

pelo Destacamento de Defesa Cibernética, durante a coordenação e integração das ações de segurança e defesa cibernética na Copa das Confederações.

Como premissa, considerou-se Incidente de Segurança qualquer fato adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Dentre os diversos tipos de incidentes de segurança possíveis de serem analisados e tratados pelo Dst Def Ciber, destacaram-se:

1. Abuso de sítios (desfiguração, injeção de links/código - *spamdexing*, erros de código, *cross site scripting*, abuso de fórum ou livros de visita etc.).
2. Páginas falsas.
3. Inclusão remota de arquivos (*remote file inclusion* – RFI) em servidores *web*.
4. Uso abusivo de servidores de *e-mail*.
5. Hospedagem ou redirecionamento de artefatos ou código malicioso.
6. Ataques de negação de serviço ou indisponibilidade de domínio.
7. Uso ou acesso não autorizado a sistemas ou dados.
8. Varredura de portas.
9. Comprometimento de computadores ou redes.
10. Desrespeito à política de segurança ou uso inadequado dos recursos de Tecnologia da Informação (TI).
11. Ataques de engenharia social (*phishing*).
12. Cópia e distribuição não autorizada de material protegido por direitos autorais.

13. Uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

As ações do destacamento foram balizadas pela RFC 2350[4] (*Expectation for Computer Security Incident Response*), que é um guia de boas práticas no qual se recomendam requisitos gerais e o comportamento que uma equipe deve seguir quando está sendo estabelecida ou encontra-se em operação. Esse documento se concentra nos métodos para informar a comunidade sobre os serviços e processos que serão desenvolvidos.

Abaixo estão descritos os serviços que foram disponibilizados pelo Dst Def Ciber, durante a Copa das Confederações Fifa/2013:

Detecção automática de incidentes: por meio de mecanismos de detecção implementados pelo destacamento ou por parceiros, o Dst Def Ciber foi capaz de detectar incidentes de segurança ocorridos na infraestrutura que estava sendo monitorada. Como exemplo de mecanismos automatizados de detecção podemos destacar: indisponibilidade de sítios web, desfigurações de sítios, *spamdexing*, erros de código, computadores pertencentes a *botnets* e postagens em canais variados e redes sociais.

Inteligência cibernética: esta atividade consistiu em gerar prognósticos de ataques aos principais ativos relacionados à Copa das Confederações, previamente mapeados pelos CCDA e informados ao CDCiber. Visou, também, atuar em parceira com entidades do Ministério da Justiça, na dissuasão das atividades dos principais grupos *hackers* no Brasil.

4 Brownlee N. e E. Guttman. RFC 2350. "Expectations for Computer Security Incident Response". http://www.ietf.org/rfc/rfc2350.txt, acessado em 28 ago. 2013.

Esta atividade permitiu ao CDCiber, de forma proativa, identificar antecipadamente possíveis ações hostis em planejamento. Os dados gerados foram tempestivamente repassados aos detentores dos ativos em risco, por alertas e notificações de eventos de segurança.

Notificação de eventos de segurança: todo evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos dos CCDA deveria ser enviado para o Dst Def Ciber, conforme o protocolo de comunicação previamente definido. O recebimento das notificações permitiu ao destacamento atuar como ponto focal para coordenação de possíveis soluções para os problemas verificados, por meio da coleta de atividades e incidentes reportados, análise das informações e correlação destas no âmbito da organização informante ou da comunidade atendida durante a Copa das Confederações.

A compilação das informações enviadas por meio de notificações foi utilizada para proporcionar, ao Dst Def Ciber, consciência situacional durante a Copa das Confederações, verificar tendências e padrões de atividades hostis e para recomendar estratégias de prevenção adequadas para toda a comunidade atendida.

Análise de incidentes: esta atividade consistiu em examinar todas as informações disponíveis sobre os incidentes, recebidos pelas notificações, incluindo artefatos e outras evidências relacionadas. O propósito da análise foi identificar o escopo do incidente, a extensão, a natureza e quais os prejuízos causados, repassando aos parceiros para análises mais aprofundadas, quando necessário. Essa atividade foi desenvolvida no âmbito do Dst Def Ciber.

Suporte à recuperação de incidentes: o destacamento esteve preparado para auxiliar no processo de recuperação, sob demanda do CCDA. Esse auxílio poderia ser prestado pelos integrantes do Dst Def Ciber Remoto, por telefone, *e-mail*, fax ou pela indicação de documentos que pudessem auxiliar no processo de recuperação. Essa atividade também poderia envolver o auxílio na interpretação dos dados coletados e na recomendação de estratégias de contenção e recuperação.

Coordenação na resposta a incidentes: nesta atividade o destacamento coordenou as ações entre os envolvidos em um incidente, o que poderia incluir redes e outros centros de tratamento externos ao seu âmbito de atuação. O processo de coordenação envolveu a coleta de informações de contato, a notificação dos responsáveis pelas redes, computadores ou sistemas que pudessem estar envolvidos ou comprometidos e a geração de indicadores e estatísticas relativas aos incidentes. O Dst Def Ciber agiu como facilitador no processo de recuperação dos incidentes e na troca de informações entre as partes envolvidas. A ação foi desenvolvida no âmbito do Dst Def Ciber.

O CDCiber, por meio do Dst Def Ciber, atuou na coordenação e cooperação com outras Equipes de Tratamento de Incidente, bem como com outros times de resposta a incidentes de segurança computacionais (*Computer Security Incident Response Team* – CSIRT), públicos e privados, nacionais e internacionais, visando a cooperação técnica, a capacitação e a ajuda mútua no tratamento dos incidentes de segurança detectados durante a Copa das Confederações.

Distribuição de alertas, recomendações e estatísticas: esta atividade consistiu em disseminar informações relativas a novos

ataques ou tendências de ataques observadas pelo destacamento durante a operação ou capitaneadas pelo CDCiber, por outros centros de tratamento ou por empresas parceiras especializadas. Esses alertas, em geral, foram produzidos pelo próprio destacamento, baseados nas notificações recebidas ou em incidentes tratados, ou representaram redistribuições de alertas emitidos por outros Centros com responsabilidade nacional. O destacamento, ao redistribuir alertas, tinha também a prerrogativa de acrescentar recomendações específicas para seu público e atribuir diferentes graus de severidade.

Análise de Risco: o processo de análise e avaliação de riscos realizado pelo Dst Def Ciber, sob demanda dos CCDA e priorização dos recursos, envolveu o mapeamento dos ativos de informação, a identificação, análise e avaliação dos riscos, tudo visando subsidiar os responsáveis pelos ativos das melhores práticas do mercado.

Como resultado das análises de risco realizadas nos ativos críticos informados ao CDCiber, foram entregues relatórios de risco aos responsáveis pelos ativos, visando oferecer subsídios acerca das melhores práticas disponíveis no mercado de TIC para mitigar ou neutralizar as vulnerabilidades encontradas. No relatório, constavam não só os riscos identificados, como também a forma como os detentores dos ativos deveriam conduzir a aplicação de controles de segurança, visando corrigir os problemas mapeados, com a consequente redução dos riscos a um nível aceitável. O papel da gestão de riscos era de facilitar o equilíbrio entre os riscos avaliados e a mitigação viável dos mesmos.

Esta atividade foi desenvolvida por representantes do Dst Def Ciber em parceria com empresas contratadas.

Estabelecimento das parcerias

Para a consecução da missão formulada, o CDCiber precisou estabelecer uma série de parcerias, uma vez que o modelo de segurança e defesa cibernética adotado foi eminentemente colaborativo e necessitava que informações fossem trocadas com grande agilidade entre os parceiros, visando aumentar a efetividade das ações.

Desta forma, foram estabelecidas as parcerias a seguir, com as suas atribuições específicas:

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por intermédio do Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov), apoiou as ações do Dst Def Ciber, por meio de troca de informações sobre a detecção de incidentes, correlação de eventos e determinação de tendências de ataques nos sítios da Administração Pública Federal (APF), que pudessem estar relacionados à Copa das Confederações; análise, dentro de suas possibilidades, de artefatos e *malwares* potencialmente perigosos e utilizados em ataques voltados para a Copa das Confederações; e a notificação ao destacamento de outras informações de relevância para a segurança do Evento.

O Comitê Gestor da *Internet* no Brasil (CGI.br), por intermédio do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br), estabeleceu um trabalho colaborativo com o Dst Def Ciber, por meio da troca de informações sobre a

detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço cibernético, com potencial para comprometer a realização da Copa das Confederações e afetar a imagem do País.

A Agência Brasileira de Inteligência (Abin) integrou a segurança cibernética da Copa das Confederações, realizando a coordenação das ações inerentes ao Sistema Brasileiro de Inteligência (Sisbin) relacionadas ao Setor Cibernético.

A Agência apoiou as ações do Dst Def Ciber, por meio de troca de informações, por canal técnico adequado, sobre indícios de mobilização de forças adversas com motivação para realizar ações cibernéticas que pudessem vir a comprometer a segurança do Evento, em especial aquelas que tivessem potencial para afetar a imagem do País e sobre condições anômalas potencialmente críticas para segurança de redes relacionadas ao Evento e que estavam sob a proteção ou supervisão da Abin.

A Secretaria Extraordinária de Segurança para Grandes Eventos (Sesge) apoiou as ações de coordenação e integração do Dst Def Ciber, por meio da orientação e articulação das entidades locais dos estados-sede da Copa das Confederações, ligadas à Segurança Pública, Defesa Civil e à segurança cibernética do evento, conforme ações conjuntas com o CDCiber e conduziu a orientação das oficinas temáticas de cada cidade-sede.

O Serviço Federal de Processamento de Dados (Serpro), por intermédio do seu Grupo de Respostas a Ataques (GRA), integrou a segurança cibernética da Copa das Confederações, realizando a segurança dos sítios de governo sob sua gestão, tais como as páginas do Ministério dos Esportes. Além disso, estabeleceu trabalho colaborativo com o Dst Def Ciber, por meio da troca de informações

sobre a detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço cibernético voltados para os sítios relacionados à Copa das Confederações sob sua proteção, além de notificar o destacamento de outras informações de relevância.

O Departamento de Polícia Federal (DPF) integrou a Segurança Cibernética, por meio da atuação do Centro de Segurança Cibernética do DPF e das Delegacias Especializadas em Repressão a Crimes Cibernéticos instaladas nas cidades-sede da Copa das Confederações.

Apoiou as ações do Dst Def Ciber, por meio da integração ao destacamento, por intermédio do Serviço de Repressão a Crimes Cibernéticos (SRCC); realizando troca de informações, por canal técnico adequado, sobre ações ilegais detectadas no espaço cibernético e que pudessem estar relacionadas à segurança cibernética da Copa das Confederações e eventos de segurança com potencial para comprometer a realização do Evento, em especial aqueles que pudessem afetar a imagem do País;

Atuou também realizando a (o):

- Notificação ao destacamento acerca de condução de investigação criminal sobre crimes com potenciais desdobramentos relevantes para a segurança e defesa cibernéticas da Copa das Confederações.
- Monitoramento de ameaças contra os ativos de informação relacionados ao evento, por meio de buscas na *Internet*, realizadas pelo Centro de Monitoração/SRCC/DPF.
- Apuração de infrações penais contra o funcionamento e segurança de ativos de informação, tais como invasão de sistemas ou dispositivos, destruição, alteração ou obtenção

não autorizada de dados e a interrupção do funcionamento dos sistemas ou serviços, nos Grupos de Repressão a Crimes Cibernéticos (GRCC).

- Triagem e levantamentos preliminares, para encaminhamento de informações quanto aos crimes cuja investigação seja atribuição das Polícias Civis, desde que não relacionados a ativos de informação críticos.
- Cessão de elementos especializados para compor o Dst Def Ciber Central.
- Articulação das ações de combate aos crimes cibernéticos, no âmbito das forças de Segurança Pública, durante o planejamento e realização da Copa das Confederações.

A Agência Nacional de Telecomunicações integrou a segurança cibernética do evento, por meio do monitoramento do espectro de radiofrequências, nas faixas relativas à transmissão de dados de dispositivos móveis no padrão 802.11, em todas as variantes, assim como 802.16 ou outros padrões identificados como de interesse.

Apoiou as ações do Dst Def Ciber, por meio da notificação de tráfego anômalo que indicasse a tendência para saturação da banda de redes nos padrões de frequências de interesse para a segurança cibernética e da notificação a respeito de indisponibilidade na transmissão de dados nos padrões de frequências de interesse para a segurança cibernética.

Especial prioridade foi atribuída aos jogos de abertura e final da Copa das Confederações e para aqueles que o CDCiber ou o Dst Def Ciber indicou como tendo se tornado prioritários, em razão de fatos novos que foram surgindo antes ou durante o torneio.

Foram também contratadas empresas de TIC pelo CDCiber que cumpriram suas obrigações contratuais, mantendo funcionários especializados junto aos Dst Def Ciber Central e Remotos.

Desenrolar da operação

Praticamente toda a estrutura voltada para defesa cibernética estava operacional em 10 de junho de 2013, com a programação do jogo de abertura somente para o dia 15 de junho, faltando apenas pequenos ajustes e configurações. Nos dias que se seguiram, houve um aumento progressivo de incidentes de segurança, com o pico alcançado no dia 16 de junho, domingo, um dia após o início dos jogos. Seguiu-se, então, um período de incidentes decrescentes, que voltaram a subir com a proximidade do jogo de encerramento, no dia 30 de junho de 2013.

De forma não prevista, os protestos ocorridos durante o período dos jogos demandaram o ajuste das ferramentas de coleta de informações públicas na *Internet* para atender às demandas que chegavam ao CDCiber sobre o acompanhamento da mobilização das manifestações. A grande maioria dessas manifestações era convocada abertamente nas redes sociais por diversos grupos ativistas, sem uma organização centralizada e sem uma pauta única de reivindicações, normalmente exigindo do governo mais transparência na aplicação dos impostos e mais austeridade no combate à corrupção.

Os processos de comunicação e integração com os parceiros foram sendo aprimorados, demostrando que a estratégia de trabalho cooperativo com o estabelecimento de parcerias havia sido uma decisão acertada.

Os tipos de incidentes foram caracterizados de forma a refletir o seu tratamento, ou seja, para cada tipo de incidente foi criada uma série de procedimentos que deveria ser seguida. A expertise inicial no tratamento de incidentes de rede veio de ensinamentos consagrados internacionalmente e adotados pelo Cert.br e CTIR Gov.

Os tipos mais comuns de incidentes tratados incluíam abusos de sítios, alertas, tentativas de execução de engenharia social, hospedagem de artefatos maliciosos, indisponibilidade ou desfiguração de sítios, varredura de portas, vazamento de informações e vulnerabilidades detectadas em *software*.

Esses eventos de segurança foram originados por informações inseridas no sistema de gerenciamento de incidentes do CDCiber pelos Destacamentos Remotos localizados nos Centros de Coordenação de Defesa de Área e nos Centros Integrados de Comando e Controle Regionais, pelo Destacamento de Defesa Cibernética Central e pelo Oficial de Ligação do CDCiber no Ministério da Defesa.

Os eventos de segurança foram detectados, em sua maioria, por meio de informações obtidas pela Seção de Inteligência do Dst Def Ciber, informações trocadas com os parceiros e informações fornecidas por elementos integrantes da segurança do evento como um todo, sem estar diretamente relacionadas com a parte cibernética.

No total, foram detectados pelo CDCiber pouco mais de 300 registros de segurança no decorrer da operação. Desses, aproximadamente 120 foram identificados como incidentes de segurança e receberam tratamento específico.

As informações entre os CCDAs e o comando da operação no Estado Maior Conjunto das Forças Armadas, no Ministério da Defesa, eram consolidadas diariamente em um relatório enviado ao Centro de Operações Conjuntas do MD e discutidas, caso necessário,

em uma reunião realizada diariamente por videoconferência, por vezes com a presença do próprio ministro da Defesa.

Lições aprendidas

Mais de 200 aspectos relevantes foram identificados para aperfeiçoar processos de coordenação e integração. Isso gerou aproximadamente 100 lições aprendidas que estão sendo implementadas no preparo para os próximos grandes eventos.

Houve substancial incremento no nível de maturidade do modelo de ações de proteção baseado na metodologia de tratamento de incidentes de rede do que àquele empregado na Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio+20). Isso permitiu uma gestão mais ampla dos incidentes que estavam ocorrendo, além de uma operação mais automatizada, baseada em ferramentas de gerenciamento de risco, apoio à decisão e "inteligência de negócios". Essas ferramentas foram customizadas especialmente para a utilização pelo CDCiber, com modelagens próprias que refletem a evolução das técnicas, táticas e procedimentos adotados pelo centro.

Mereceu destaque também o trabalho colaborativo e integrado entre: as Equipes de Segurança de Redes das Forças Armadas e MD; principais Equipes de Tratamento de Incidentes de Redes Brasileiras (CTIR Gov e Cert.br); e órgãos da administração pública federal ligados à segurança cibernética do evento (GSI, Serpro, DPF). Esse trabalho colaborativo ocorreu tanto na parceria externa quanto na composição do Destacamento de Defesa Cibernética.

A forma de atuação da Inteligência do destacamento como vetor de coleta de dados da fonte cibernética (fontes abertas) e disseminação

desses dados para o canal de inteligência ou de tratamento técnico, sempre priorizando os princípios da oportunidade e legalidade, pode ser aprimorada e ganhou agilidade na reconfiguração das ferramentas que suportavam a atividade. Os analistas que trabalhavam com esse conjunto de ferramentas puderam amadurecer o modelo de trabalho e aprimorar a forma de atuação.

Houve também a geração de requisitos que, na maioria, puderam ser implementados para personalização, segurança e otimização das ferramentas de tecnologia da informação utilizadas nos processos de operações e inteligência do destacamento, proporcionando um legado de grande valor para a missão do CDCiber no contexto do Setor Cibernético Brasileiro.

Novos desafios: Copa do Mundo de 2014

A Operação Copa das Confederações serviu de base para avaliar a dificuldade que estará presente para a proteção cibernética da Copa do Mundo de 2014, que contará com 12 cidades-sede, em vez de as seis que fizeram parte do torneio anterior.

Engana-se quem inferir que, por haver o dobro de cidades-sede em 2014, o esforço será dobrado. Na verdade, a expectativa é que o empenho necessário supere isso.

Tendo em vista o ainda reduzido efetivo do CDCiber, o esforço de coordenação e integração de atividades necessitará ser ampliado, com o reforço das parcerias e do quantitativo de pessoas especializadas em todos os níveis.

A popularidade de um acontecimento como a Copa do Mundo, com a participação de 32 países, representando todos os continentes do planeta e televisionada em tempo real para bilhões de pessoas

durante um mês, apresenta-se como cenário ideal para os que desejem de trazer notoriedade e visibilidade para alguma causa, seja ela de qual natureza for.

Cabe à sociedade brasileira fazer frente a este grande desafio de proteger os jogos e manter um ambiente seguro para todos, inclusive no espaço cibernético.

Conclusão

O presente artigo teve por objetivo mostrar como foi, em linhas gerais, a atuação do CDCiber na Copa das Confederações da Fifa em 2013.

A relevância da atividade de defesa cibernética cresceu tanto, nos últimos anos, que já se tornou mais um domínio operacional. Juntamente com os domínios terrestre, marítimo, aéreo e espacial, muitos países incluíram o domínio cibernético na doutrina militar.

O CDCiber busca desenvolver as atividades norteado nos pressupostos básicos e nos objetivos estabelecidos na Política Cibernética de Defesa[5]. Dentre eles, destacam-se a necessidade da atuação colaborativa da sociedade brasileira e os objetivos de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas, além de impedir ou dificultar a sua utilização contra interesses da Defesa Nacional. Trabalha-se, ainda, a necessidade de desenvolver e manter atualizada a doutrina de emprego do setor cibernético.

Todo o trabalho desenvolvido pelo CDCiber na proteção dos grandes eventos, particularmente durante a Copa das Confederações, esteve perfeitamente alinhado com essa política, buscando ganhar

5 Ministério da Defesa. MD31-P-02, Política Cibernética de Defesa. Acessada em 02 de Setembro, 2013. http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf

maturidade e aprimorar o modelo de atuação mais adequado a esse tipo de realização.

A adoção e o aprofundamento de um modelo cooperativo foram extremamente exitosos. Pode-se afirmar que não seria possível enfrentar o desafio proposto sem a adoção desse modelo e sem o efetivo comprometimento dos parceiros institucionais e privados citados anteriormente.

Cabe destacar, entretanto, que esses são os primeiros degraus de uma longa subida que se vislumbra, onde outras capacidades ainda devem ser buscadas, sem perder de vista o aprimoramento e a adequação das qualidades obtidas. Pode-se, mesmo, dizer que é impressionante o quanto se avançou, a despeito do pouco tempo e dos recursos limitados de que dispõe o CDCiber.

O desafio, agora, é manter a caminhada em busca da qualificação das competências e capacidades necessárias ao desenvolvimento e aprimoramento da defesa cibernética do Brasil.

CAPÍTULO 7

Cibersegurança e ciberguerra: o governo Obama e a política de defesa no espaço cibernético

Flávio Rocha de Oliveira

Introdução

Após a Guerra Fria, o fenômeno conhecido como Globalização aconteceu ao mesmo tempo em que se consolidava a hegemonia dos Estados Unidos da América. De fato, a liderança desse país terminou por configurar várias das estruturas que sustentam tanto a Globalização como o sistema internacional contemporâneo: o controle geopolítico dos mares, a aliança militar com os países europeus (OTAN), a construção de parâmetros de trocas comerciais e financeiras e o *estabelecimento dos fundamentos da moderna estrutura de comunicações e informações* (*hardware e software*) que é utilizada por estados, nações e etnias: a *Internet*.

Junto com esse avanço no campo das Tecnologias de Informação e Comunicação (TIC), observou-se que os países mais avançados passaram a depender da rede de computadores para a execução da vida cotidiana, em suas mais diferentes manifestações. Das comunicações telefônicas até o desenvolvimento de produtos industriais, passando pelas mensagens políticas e pela consolidação do mercado global de capitais na sua forma mais dinâmica e incontrolável, o fato é que a

intensidade dos contatos entre grupos sociais só chegou a escala atual por conta do desenvolvimento das ciências da computação.

Tal desenvolvimento não ficou restrito apenas aos EUA. Ainda que os estadunidenses estejam na dianteira global nesse campo, o fato é que um subproduto do próprio desenvolvimento tecnológico foi o barateamento e o acesso a equipamentos, serviços e mão de obra especializada, o que permitiu que outros países – em especial na Ásia e na Europa, mas não exclusivamente nesses continentes – terminassem desenvolvendo conhecimentos no campo das TIC. Com esse avanço, vários estados desenvolveram capacidades relevantes na área, e passaram a competir e cooperar entre si – e a competir e a cooperar com os próprios norte-americanos.

O barateamento e a facilidade de acesso não ficaram restritos, "apenas", aos Estados. Vários grupos passaram a se beneficiar de computadores mais rápidos e de baixo custo e, nos últimos cinco anos, viram sua capacidade de acesso à *Internet* aumentar com a chegada dos *Tablets* e dos *Smartphones*. ONGs, grupos econômicos dos mais variados tamanhos, organizações religiosas de diferentes matizes, organizações políticas e indivíduos que estabelecem contatos entre si de maneira rápida, estão entre os que souberam se aproveitar desse *boom* tecnológico. Ocorre que outras "associações" também mergulharam nessa expansão da rede mundial de computadores: organizações criminosas ("máfias") e grupos terroristas[1]. Do tráfico de armas e seres humanos até o uso da *Internet* com o objetivo de divulgar mensagens políticas *violentas* e extremistas, o que se observou foi uma proliferação de atores não-estatais com capacidade de enfrentar governos e de constituírem uma ameaça real a diferentes

1 Misha Glenny, *McMáfia. Crime Sem Fronteiras* (São Paulo: Ed. Cia das Letras, 2008); Misha Glenny, *Mercado Sombrio: O Cibercrime e Você* (São Paulo: Ed. Cia das Letras, 2012).

setores sociais. Como exemplo, podemos citar os diferentes casos envolvendo o roubo de cartões de créditos (ou melhor, de seus códigos de funcionamento).

Como a maior força geopolítica e econômica, os Estados Unidos tiveram que desenvolver uma série de medidas de modo a se proteger no *ciberespaço*. Ao mesmo tempo, procuraram levar adiante a construção de capacidades ofensivas, devidamente institucionalizadas. Finalmente, ao compreender a natureza global e fluída do espaço cibernético, começaram a se preparar para influenciar o sistema internacional no sentido da adoção de normas de comportamento que facilitassem a governança da *Internet* – sempre, é claro, no benefício de sua liderança hegemônica[2].

Nas páginas seguintes, serão analisadas algumas ações do governo Obama no âmbito do ciberespaço. O objetivo é discutir, ainda que brevemente, a política que esse governo procurou - e procura – implementar para assegurar os interesses dos EUA. Além da discussão de uma literatura específica, haverá uma análise de alguns dos principais documentos oficiais relacionados com esse problema. Ainda que se leve em consideração a questão mais ampla da *Internet*, o foco recairá sobre a *segurança e defesa cibernética.*

Visão dos EUA: o ciberespaço como problema de segurança nacional

Segundo Joyner[3], os EUA tem uma concepção do espaço cibernético como um problema de segurança nacional, e que

2 Ibidem.

3 James Joyner, "Competing Transatlantic Visions of Cybersecurity", in *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World,* ed. Derek S. Reveron. (Washington: Georgetown University Press, 2012, Kindle Edition).

nesse sentido deve ser *defendido e controlado principalmente pelos militares*[4]. Esses, por seu turno, concebem a *Internet* como um quinto domínio da guerra, e, como tal, deve ser objeto de uma ação estratégica que possibilite o seu controle em caso de conflito. Para tornar mais clara essa visão, os outros domínios seriam a *terra, o mar, o ar e o espaço.* Classicamente, a maioria das guerras ocorreu nos dois primeiros ambientes, sendo que o os dois últimos foram efetivamente agregados ao escopo das operações militares com os avanços científicos e tecnológicos do século XX.

O que é importante na questão dos domínios da guerra é a divisão que existe entre os quatro primeiros e o espaço cibernético: no primeiro caso, temos *ambientes* que existem independentemente da ação humana, ainda que sejam fortemente manipulados/ aproveitados para as ações bélicas. Já no segundo caso, o *ciberespaço é uma criação inteiramente humana*.

Obviamente, essa visão não é consensual[5], o que pode ser explicado, em parte, justamente pelo contraste com as outras dimensões. Alguns autores acham exagerada a ideia de que o ciberespaço seja, por si só, uma dimensão análoga ao *mar,* por exemplo. Ainda que possua uma capacidade multiplicadora quando aplicados na utilização de aviões de caça ou de mísseis cruzadores disparados de navios, os computadores operando em rede terminam por alavancar (ou *multiplicar*) a destruição desejada pelos soldados nos *domínios já existente*[6].

---

4 O autor aponta que o Reino Unido (RU) tem uma posição semelhante a americana. Juntos, EUA e RU possuem uma visão distinta dos países da Europa Continental, que veem a *Internet* como um meio majoritariamente civil.

5 No decorrer das pesquisas para a realização desse texto, fica-se com uma forte impressão de que os consensos na questão terminológica são fortemente teorizados, mas que a parte empírica só recentemente começou a ser operacionalizada de modo a tornar as definições mais claras.

6 Thomas Rid, "Cyber War Will Not Take Place" , *Journal of Strategic Studies* (2012): 5-32; Peter Singer,

Um outro problema em relação a questão dos domínios diz respeito à defesa setorial por parte dos diferentes ramos das forças armadas estadunidenses. Joyner relata, citando a revista *The Economist*, que o presidente Barack Obama declarou que a infraestrutura digital americana era um ativo de valor estratégico. Isso ocorreu em 2010, quando ele indicou Howard Schmidt, antigo executivo do setor da Microsoft, como o "Czar" da cibersegurança governamental. Todavia, em 2005 a Força Aérea declarou que o ciberespaço era o quinto domínio da guerra, e que doravante a missão da USAF era "*to fly and fight in air, space, and cyberspace*"[7].

Segundo alguns autores, a Força Aérea acalentava a ideia de que ela seria a grande responsável pela segurança cibernética norte-americana. A Marinha e o Exército trataram de estruturar suas unidades especializadas de defesa cibernética, e o mesmo fez o corpo de fuzileiros navais[8].

Com o aumento da percepção de que a *Internet* abria uma nova frente de oportunidades e de perigos, o governo americano redesenhou a estrutura de comando para lidar com esse problema e criou o *US Cybercommand,* cuja responsabilidade é a coordenação das diferentes unidades cibernéticas das Forças Armadas americanas, com o objetivo principal de garantir a melhor defesa possível das estruturas militares que dependem da *Internet*. Do ponto de vista institucional, a competição burocrática entre os vários setores militares é minimizada com esse arranjo, ainda que as rivalidades persistam.

"Interview with Peter Singer", *International Review of The Red Cross***.** (2012): Volume 94, Issue 886, 467- 481.

7 James Joyner, *Op Cit:* posição 3649.

8 Richard A. Clarke and Robert Knake**,** *Cyber War: The Next Threat to National Security and What To Do About It.* (New York, HarperCollins, 2011)

Apesar das discordâncias conceituais, o fato é que governos e militares em vários países estão, cada vez mais, adotando a ideia de que o espaço cibernético é realmente o quinto domínio da guerra. Nesse sentido, pode-se notar que a posição inicial estadunidense contribuiu para que essa concepção fosse sendo aceita no cenário internacional.

Governo Obama: ciberestratégia em construção

Quando um exame mais detido de alguns dos principais documentos norte-americanos em relação ao ciberespaço é feito, percebe-se que a própria velocidade das transformações tecnológicas leva a um processo de adaptação contínua. Ao mesmo tempo que a mudança tecnológica barateia o acesso a *software* e *hardware*, a dispersão do conhecimento torna vários atores estatais e não-estatais como possíveis concorrentes do governo estadunidense e dos interesses estatais e econômicos desse país. Conforme discutido na seção anterior, isso aguça a percepção de que o espaço cibernético é parte da segurança nacional, e que a adoção de salvaguardas militares deve ser garantida – e implementada rapidamente.

No governo Obama, observa-se a criação de um discurso político que vai sendo encampado por vários veículos de comunicação e que tem por objetivo criar a consciência de que as redes de computadores públicas e privadas são vulneráveis. Ao mesmo tempo, trabalha-se com a ideia de urgência e de perigo imediato, o que, em certa literatura de Segurança Internacional, pode ser entendido como um processo de *Securitização*[9]. Em 2012, o então Secretário de Defesa

9 Ralf Emmers, "Securitization", in *Contemporary Security Studies*, ed. Allan Collins (Oxford: OUP, 2007), 109-125.; Barry BUZAN et al., *Security: A New Framework for Analysis* (London: Lynne Rienner Pub, 1997).

Leon Panetta, num discurso em Nova Iorque, afirmou que os EUA estariam ameaçados pela possibilidade de um "Pearl Harbour cibernético", estando vulneráveis a ação crescente de Hackers estrangeiros que poderiam prejudicar seriamente a infraestrutura energética, os sistemas de transportes e as redes de computadores que faziam funcionar o sistema financeiro e todo o governo americano[10].

Segundo Betz e Stevens, tal discurso tem uma função política do ponto de vista do decisor, que é estimular um "chamado à ação" e adicionar uma urgência através do uso de metáforas[11]. Analisando os diferentes discursos usados no âmbito da *cibersegurança*, e a falta de consensos quanto a esse conceito, os autores chamam a atenção para o fato de que o *recurso discursivo* em parte da literatura especializada, e dentro dos governos, usa constantemente para metáforas e analogias espaciais/geopolíticas e biológicas. No primeiro caso, pode-se apontar para os seguintes exemplos: expressões como *Cyber Pearl Harbour*, o ciberespaço como um domínio exclusivo (e separado dos tradicionais *terra, mar, ar e espaço)* ou como uma *esfera separada da sociedade* (mundo virtual *x* mundo real) são utilizadas para defender dispositivos de segurança operados por governos e agentes especializados (públicos e privados). No segundo caso, a situação fica ainda mais carregada de dramaticidade, pois termos como "vírus", "vermes", "zumbis" e "higiene digital" trazem à mente do público perigos reais, como o de doenças, ou *imaginários* e *amplificados* pela literatura de ficção científica, pelo cinema e pelas minisséries televisivas (como é o caso da onda de livros e filmes de zumbis). Em

10 Elisabeth Bummiller and Tom Shanker, "Planneta Warns of Dire Threat of Cyberattack on US", *New York Times,* 11 de Outubro de 2012. http://goo.gl/vcnFA, acessado em 03 abr. 2013.

11 David J Betz and Tim Stevens, "Analogical Reasoning and Cyber Security", *Security Dialogue.* 44 (2013):147-164.

certo momento, um esforço gigante por parte dos governos no sentido de eliminar vírus é colocado como uma necessidade inescapável[12].

Não obstante o processo de *securitização* em questão, o fato é que alguns eventos contribuíram para a percepção de ameaça crescente por parte de pesquisadores, do próprio governo americano e de empresas que, de alguma maneira, estariam interessadas, atentas ou vulneráveis aos perigos que realmente rondam o ciberespaço[13]. Um desses eventos aconteceu em 2007, quando o governo da Estônia sofreu um forte ataque cibernético e que atribuiu aos Russos. Alguns pesquisadores estadunidenses chegaram a chamar esse ataque de a Primeira Guerra Virtual da Web[14]. Um outro evento ocorreu em 2008, e novamente envolveu a Rússia, que entrou em guerra com a Geórgia. Durante o conflito, que durou aproximadamente uma semana, uma série de ciberataques degradaram quase que completamente as comunicações da Geórgia com o exterior.

O que chamou a atenção foi a negativa do governo russo de que tenha empreendido oficialmente os ataques cibernéticos. Nos dois casos, houve a ação de atores não estatais que, pelo menos oficialmente, não eram ligados ao governo. Já ficava explicitado algo que apareceria constantemente na literatura e em vários documentos estadunidenses sobre o problema da segurança na *Internet*: a dificuldade de se localizar com precisão as fontes dos ataques, algo

12 William Lynn Jr III, "The Pentagon Cyberstrategy, one year later", *Foreign Affairs,* 28 de setembro de 2011. http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later, acessado em 12 set. 2012.

13 Flávio Rocha de Oliveira, "Os Estados Unidos da América e o Desenvolvimento de uma Estratégia para o Espaço Cibernético". (Trabalho apresentado no VI Encontro Nacional da ABED, São Paulo, 2012).

14 Gill L.M. Souza, "Da Ciberguerra: Idiossincrasias do Século XXI e as Instituições Militares de Defesa Cibernética de Brasil, Estados Unidos e União Européia" (Trabalho apresentado no V Encontro Nacional da ABED em Fortaleza, 2011).

bem diferente do que ocorre no âmbito das outras dimensões da guerra.

No ano de 2009, o governo Obama lança o *Cyberspace Policy Review*[15]. Nesse documento, há a seguinte afirmação: *The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.*(…) Igualmente forte é a ênfase do documento no fato de que o governo deve assumir um papel de liderança na construção de uma infraestrutura cibernética resiliente, de modo a coordenar os esforços das diferentes agências públicas, militares e civis, e do setor privado – que é o principal produtor de equipamentos e softwares que fazem com que a *Internet* efetivamente funcione.

Em 2010, o governo publica o *National Security Strategy* (NSS 2010) que estabelece, em linhas gerais, as prioridades americanas sobre a segurança nacional. Esse documento é construído tendo, como um dos princípios norteadores, uma avaliação do cenário internacional e das oportunidades e perigos que ele pode apresentar para os Estados Unidos Em relação ao ciberespaço, afirma-se que "*The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore, is a strategic national*

15 Cyberspace Policy Review. "Assuring a Trusted and Resilient Information and Communications Infrastructure". White House, 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, acessado em 15 jun. 2013.

asset, and protecting it – while safeguarding privacy and civil liberties – is a national security priority. ***We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks*** *(…)* [16]". Uma ênfase forte é colocada sobre a necessidade de cooperação internacional, não só no sentido de construir um sistema de alerta robusto que leve em conta as necessidades estadunidense e de países aliados, mas também num esforço de construção de normas de comportamento e convivência na rede mundial de computadores. Essa é apresentada como um bem público global, que beneficia diferentes grupos, sejam eles estados ricos ou pobres, sociedades e indivíduos.

O *The National Military Strategy of the United States of America*[17], também publicado em 2011 (NMS 2011), trabalha com essa ideia de bem público global. Ele cita como exemplo a ser seguido no ciberespaço, a ideia de liberdade do uso do mar, que beneficia países com diferentes capacidades econômicas e militares. A potência hegemônica do nosso século, os próprios EUA, detém um poder naval não equiparado por outras potências. Mesmo sendo a nação mais forte em termos marítimos, os Estados Unidos não criam obstáculos ao comércio internacional ou ao uso das riquezas oceânicas, segundo o documento.

Apesar da supremacia naval, não é impossível que outros países empreendam ações marítimas para negar aos EUA, ainda que temporariamente, o acesso a algumas regiões. A mesma lógica é aplicada ao ciberespaço. Vários atores, estatais e não estatais, estão

16 National Security Strategy, Maio de 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (27-28), acessado em 16 mai. 2012.

17 The National Military Strategy of The United States of America, "Redefining America's Military Leadership", February 2011, Chairman of the Joint Chiefs of Staff. http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf (08-12), acessado em 13 ago. 2012.

desenvolvendo tecnologia e recursos humanos que podem atacar os interesses estadunidenses e, ao mesmo tempo, negar o acesso à *Internet* por parte do governo e de vários grupos dos EUA que dependem da rede mundial de computadores.

Um ponto interessante do documento é a analogia que é criada com a Guerra Fria. É defendida a ideia de que o conceito de *deterrence* deve ser adaptado para a realidade do século XXI, alcançando o domínio do ciberespaço. A *deterrence* deveria ser garantida através do desenvolvimento de uma capacidade *bélica* de luta em ambientes degradados por ataques cibernéticos, assim como pela construção de uma habilidade de *identificar* os atacantes e derrotá-los no próprio ambiente virtual. O domínio militar do ciberespaço torna-se prioridade das Forças Armadas norte-americanas, pois ele potencializa o uso das outras dimensões da guerra.

No documento emitido pelo Departamento de Defesa, o *Department of Defense Strategy for Operating in Cyberspace*[18], cinco iniciativas estratégicas são colocadas. Dessas, duas chamam a atenção: a primeira, "*Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential*". Enfatiza-se o conceito de domínio operacional da Guerra, já referido em outra seção desse trabalho, mas é colocado que o potencial das diferentes agências e forças militares americanas deve ser maximizado através da coordenação institucional. Para isso, no documento é atribuída a responsabilidade de assegurar o ciberespaço ao *United Strategic Command* (USSTRATCOM), aos comandos combatentes e aos departamentos militares. Ao mesmo tempo, estabelece o *US Cybercommand* (USCYBERCOM) como

18 Departament of Defense Strategy for Operating in Cyberspace, July 2011, US Department of Defense. http://www.defense.gov/news/d20110714cyber.pdf (p. 5), acessado em 15 ago. 2012.

um subcomando unificado do USSTRATCOM. A terceira iniciativa apresenta a seguinte noção: *Partner with other US government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy*. É defendida a necessidade de parceria com o *Department of Homeland Security* (DHS), dentro de um esforço de trabalho interagências. O DHS tem como missão garantir a cibersegurança do governo federal, em âmbito civil. Mas o DoD coloca que os efetivos militares estarão a disposição para partilhar conhecimento e treinar os membros do DHS quando for necessário, operando dentro de regulamentos civis, algo semelhante ao que os militares fazem quando, durante desastres naturais, auxiliam as equipes civis do governo a resgatar e ajudar a população.

No documento *International Strategy for Cyberspace*[19] (ISS 2011), são apresentadas várias prioridades em termos de políticas públicas. Além da necessidade de esforços diplomáticos para minimizar as ameaças aos interesses americanos, estão declarados duas possibilidades de resposta a ações hostis. Num primeiro caso, cibercrimes, o documento defende que os EUA agirão de acordo com a Convenção de Budapeste sobre o Cibercrime. Isso implica numa ação marcada por investigações e pela aplicação da lei. Num outro caso, o de atos hostis que comprometam a segurança estadunidense, o documento estabelece que "*We reserve the right to use all necessary means – diplomatic, informational, military and economic – as appropriate and consistente with applicable international law, in order to defend out Nation, our allies, our partners, and our interests.* ***In so doing, we will exhaust all options before military force whenever we***

19 International Strategy for Cyberspace. "*P*rosperity, Security, and Openness in a Networked World". White House, Maio de 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, pg. 13, acessado em 15 ago. 2012.

can…" Dito de outro modo, a opção do uso de armas convencionais para afastar uma ciberameaça está colocada na mesa – o que alguns autores irão chamar de opção pelas armas cinéticas, em oposição, ou complementação, as armas virtuais do ciberespaço.

Cibersegurança ou ciberguerra?

Os termos cibersegurança e ciberguerra aparecem em diferentes contextos na literatura. A única coisa que é comum a todos os pesquisadores do campo é a existência do espaço cibernético, com sua rede de computadores, seu potencial para o progresso e prejuízos econômicos e políticos dada a ubiquidade de *hardware e software* na sociedade internacional.

Para Samaan, o governo estadunidense tem feito um esforço para institucionalizar o tema da ciberdefesa. Exemplos disso são a indicação de Howard Schmidt como coordenador de cibersegurança do governo Obama, em 2009, a implementação de uma parceria formal entre o DHS e o DoD, com as responsabilidades de cada departamento devidamente estabelecida, e a criação do *US Cybercommand* em 2010, e que inclui os componentes de todos os serviços militares que lidam com a segurança cibernética. Não obstante, "d*espite these bureaucratic efforts in the White House and in the interagency process, (…) remains a lack of consensus in Washington, particularly within the Department of Defense, on threat assessment in cyberspace and its military implications. A stark intellectual rift between "alarmists" and "skeptics" still prevails. As a result, this elementary battle has led to dysfunction in the institutional response to cyber-threatsand jeopardizes the implementation of aneffective*

military posture in cyberspace. Consequently, we need to reassess the relevance of cyberspace as a distinct military domain[20]".

Segundo esse autor, há uma rivalidade de atuação e de concepções entre o DHS e os militares do DoD. Para o primeiro departamento, faz sentido que se fale em cibersegurança, e em especial no tocante ao número de ações ameaçadoras do ciberespaço e que se concentram em atividades criminosas, motivadas por indivíduos, pequenos grupos tecnicamente capacitados ou máfias. A concepção majoritária, aqui, é que a *Internet* é um espaço civil. No Departamento de Defesa, a concepção é outra, e que já foi indicada em outra parte desse trabalho: o ciberespaço é essencial para a segurança nacional, e uma visão militarizada, que empregue recursos bélicos *virtuais* e *reais,* é necessária para garantir que os interesses norte-americanos sejam preservados e defendidos. Ao mesmo tempo, também nessa visão dos militares (em princípio), os mecanismos testados da *deterrence* devem ser combinados com a diplomacia no sentido de assegurar a defesa de países e grupos amigos que sejam vitais para os Estados Unidos.

Para Valeriano e Maness[21], o termo ciberguerra carece, ainda, de um estudo mais empírico para que sua validade seja estabelecida. Não obstante, ele aponta que há todo um jargão que é usado por documentos oficiais e pela literatura especializada, e que provém da ficção científica e do cinema. Assim, o conceito de *ciberguerra* parece

---

20 Jean-Loup Samaan, "Beyond the Rift in Cyber Strategy.A middle ground for the US military posture in cyberspace", *Strategic Insights* (Spring 2011, Volume 10, Issue 1). http://nato.academia.edu/jeanloupsamaan/Papers/843886/Beyond_the_Rift_in_Cyber_Strategy, acessado em 15 mai. 2012.

21 Brandon Valeriano and Ryan Maness, "Persistent Enemies and Cyberwar. Rivalry Relations in an Age of Information Warfare", in *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World,* ed Derek S. Reveron (Washington, Georgetown University Press, 2012, Kindle Edition.), Cap. 09.

indicar uma batalha puramente tecnológica, fora de um contexto de política externa mais amplo.

Segundo os autores, o termo ciberguerra termina sendo usado para designar as capacidades *ofensivas* de um Estado no ciberespaço. Na definição deles, "*cyberwar as the use of computational technologies on the military or diplomatic battlefield of international affairs and interactions* (…). Cibersegurança teria o significado oposto: (…) *cybersecurity is the term used for a state's defensive (and sometimes offensive) capabilities in cyberspace*[22]".

O fato relevante é que a literatura e os documentos refletem posições que derivam das pesquisas (caso dos cientistas sociais e dos estudiosos do tema, em sua diversidade teórica e ideológica) e das diversas agências governamentais que tem que operacionalizar a ciberestratégia num contexto em que as mudanças são rápidas e fluídas.

Conclusão: Problemas de pesquisa, definição e políticas públicas

Algumas conclusões, provisórias, vão se impondo ao final desse texto. A ideia é estabelecer algumas possibilidades de discussão e pesquisa, que possam constituir boas questões de investigação em trabalhos futuros.

Primeiramente, os termos *ciberguerra e cibersegurança* são usados de maneira equivalente, o que pode confundir os pesquisadores e o público em geral. Autores como Rid simplesmente rejeitam que o termo ciberguerra tenha uma validade em si, e que o ciberespaço seja

22 Brandon Valeriano and Ryan Maness, *Op. Cit.,* Posição 3177.

um domínio separado e em pé de igualdade com os outros quatro domínios da guerra. O fato de que o primeiro conceito tem uma forte carga de militarização, enquanto o segundo é mais amplo e maleável é inegável. Todavia, pesquisas baseadas em observação empírica e na evolução futura dos conflitos internacionais são necessárias para o esclarecimento maior dessa questão.

Betz, Samaan e Singer chamam a atenção para o fato de que a inflação do termo ciberguerra pode confundir o público na medida em que é um termo que embute os mais diversos interesses, como o de grupos, empresas e indivíduos que possam ter ganhos com a percepção de que o ciberespaço é uma fonte permanente de perigos. Por outro lado, é inegável que o uso de computadores e *softwares* constituem uma fonte de ameaças, e que a evolução futura pode indicar que eles têm realmente capacidades disruptivas (como parece ser o caso do vírus Stuxnet, ainda que seja classificado por Rid e Samaan como uma arma de um único tiro, pois perde eficácia uma vez que é descoberto, dado que vários países-alvo em potencial tratarão de implementar defesas cibernéticas eficazes contra esse mesmo *malware*).

Uma segunda conclusão está presente no campo do uso do ciberespaço como meio de guerra, mas associado às operações militares em tempo real. Boa parte da literatura, e praticamente todos os documentos emitidos pelo US DoD, aponta para essa possibilidade. O Pentágono, inclusive, estabeleceu ambientes virtuais para o treinamento de conflitos cibernéticos. Mas pouco tem sido escrito, por exemplo, sobre a utilização do ciberespaço em conjunto com os ataques efetuados pelos drones. A programação dessas armas, a operação a distância e o seu uso são, todos, permeados pelo espaço

cibernético, e não é raro que surjam na imprensa especulações de que hackers podem invadir, em algum momento, os sistemas de guiagem e operação dos VANTs.

Finalmente, a tecnologia do ciberespaço, em conjunto com outras tecnologias aplicadas ao setor bélico, tem feito com que a discussão em torno da própria guerra tenha sofrido modificações até então impensáveis. No caso norte-americano, Singer observa que o avanço tecnológico tem sido tão intenso que ataques e intervenções com possibilidades de destruir instalações e países inteiros tem sido possíveis com o emprego de um número reduzido de soldados de carne e osso.

Isso impacta no relacionamento político entre os poderes da República estadunidense. O WPR, *War Powers Resolutions,* estabelece que o Congresso americano tem a última palavra na hora de declarar a guerra. O presidente pode ordenar uma intervenção militar durante, aproximadamente, noventa dias, mas depois disso deve obter o consentimento político e legal dos congressistas. Com o uso dos drones, o poder executivo tem se valido de brechas na legislação americana para não consultar o Congresso. O mesmo tem sido feito pelo Departamento de Defesa, e especialmente no tocante a cibersegurança: a lógica, aqui, é terrivelmente simples – nos ciberataques, vidas norte-americanas não são colocadas em risco, *portanto, não há a necessidade de uma aprovação do congresso por parte de várias operações militares que se apoiam na tecnologia.*

Resta agora a pesquisa e a observação constante do avanço da tecnologia do espaço cibernético e, no caso dos EUA, a avaliação das respostas que eles apresentarão nesse processo. Considerando-se que ainda serão a potência hegemônica do sistema internacional,

não é demais considerarmos que as políticas adotadas pelos Estados Unidos afetarão outros países[23], que deverão segui-las ou enfrentá-las[24].

23 Isso já afeta, diretamente, o Brasil. As revelações feitas em setembro de 2013 pela imprensa internacional sobre a espionagem estadunidense levada a cabo pela NSA, a partir dos documentos vazados por Edward Snowden, colocou em evidência a nossa necessidade de avaliação de tudo o que tem sido feito na área de cibersegurança no país. As interceptações foram feitas em relação a presidência da república e a Petrobrás. Ficou evidente que um esforço que combine governo, universidades, sociedade civil e setor privado deve ser feito de maneira contínua, de modo a gerar capacidades de ciberdefesa/cibersegurança compatíveis com as aspirações brasileiras no cenário internacional.

24 Esse artigo foi escrito, com modificações, a partir de trabalho apresentado durante o 7º Encontro Nacional da ABED, realizado em agosto de 2013 em Belém do Pará.

CAPÍTULO 8

(In) Conclusão: sobre a necessidade de se pensar a defesa a partir do poder cibernético

Marcos Aurélio Guedes de Oliveira

Com o crescente uso de armas cibernéticas e suas técnicas de ataque, a exemplo de programas maliciosos (*malwares*), o meio cibernético se tornou um dos principais espaços disponíveis para medidas, tanto abertas quanto secretas dos Estados, no que se refere à inteligência, à sabotagem e ao apoio a insurreições. Muito se tem falado em ações envolvendo esse recurso com o intuito de (i) destruir *hardware*, como no caso Stuxnet, (ii) provocar irrupção de serviços e redes essenciais – como queda de energia elétrica ou cegamento de meios eletrônicos –, e (iii) atuar em missões de inteligência e contra inteligência.

Alguns dos usos estratégicos atuais dos meios cibernéticos de guerra são tão antigos quanto a própria guerra e foram, no passado, desempenhados por indivíduos, e.g.: agentes ou cientistas especializados, recursos hoje considerados primitivos. Lembremos que a quebra da máquina nazista Enigma foi talvez a mais importante realização de inteligência para a vitória Aliada na Europa da Segunda Guerra.

Nesse sentido, o rápido desenvolvimento tecnológico tem possibilitado a materialização de possibilidades até recentemente existentes apenas no campo da ficção científica. Por exemplo, as declarações de Edward Snowden sobre a montagem do sistema de espionagem norte-americano no pós-11 de setembro indicam a obsolescência do modelo do *Big Brother* imaginado por George Orwell e a emergência de um novo *Big Brother* fundamentado na espionagem tecnológica sutilmente inserida na cultura de massa e nas redes.

Na medida em que a leitura geopolítica encapsulada nas fronteiras físicas passou a ser dependente das fronteiras virtuais, potências emergentes que se beneficiaram no passado de uma leitura geopolítica tradicional não podem mais considerar seus interesses estratégicos e de defesa sem os contemplar nos níveis regional, global e no mundo virtual.

Se a recente utopia de tudo e a todos ouvir é hoje banal realidade, será que um dia a tecnologia dará a alguns de nós o poder de destruir inteiras civilizações, como o faz o protagonista do livro e filme *Enders Game*? Não foi a leitura de que a bomba atômica incorporava tal poder que levou a Guerra do Pacífico ao fim?

A fragilidade em que o processo de globalização coloca as sociedades e nações permite que a ação de um individuo - sentado em frente a um computador ou sequestrando um avião - provoque uma escalada de reações que interrompam sistemas dos quais dependem milhões de pessoas, e que provoquem consequências inimagináveis.

O potencial da guerra cibernética não está totalmente explorado. Áreas de ação em defesa podem ser abertas dependendo dos novos recursos de rede. Um possível novíssimo campo de ação está relacionado com a facilitação de insurreições, manifestações e

mesmo golpes via uso e manipulação de recursos compartilhados pelas redes de telefonia celular. O sucesso em operações com esse formato reduziria em muito os custos de intervenção aberta e militar em países menores e daria às nações dominantes dessa tecnologia um forte argumento em favor da não regulamentação internacional do meio cibernético.

Afinal, em um mundo onde a teoria e a prática realistas do poder de Estado se entrincheiram cada vez mais nas funções consideradas de defesa e de segurança nacional, nada melhor que alimentar a ideia de que, por esse caminho, tanto as potências em declínio quanto as emergentes poderiam ampliar os poderes militar e de defesa em detrimento das nações competidoras. Se essa tese prevalecer, um eventual regime de regulação e cooperação dessa temática poderá ser bem mais frágil que o atual regime nuclear gerido pela Agência Internacional de Energia Atômica.

Os desafios que essa nova fronteira colocam para a área de estudos de defesa e de guerra são semelhantes aos apresentados com a introdução do avião nos combates, há cerca de cem anos. Existe um novo modelo a ser pensado e executado para que esse mecanismo de poder possa ser maximizado, adequadamente utilizado e transformado num recurso positivo a favor da segurança e da paz internacional.

Os valiosos escritos reunidos no primeiro volume da coleção indicam alguns elementos que compõem essa nova relação profissional civil-militar: o perfil do "soldado cibernético, a necessidade de investimentos em tecnologias de ponta, de ir além das leituras geopolíticas tradicionais, de criar um corpo jurídico e institucional internacional de regulamentação e cooperação são alguns exemplos.

Essa publicação, que abre com chave de ouro a coleção de estudos sobre o tema, é prova de que dispomos de recursos intelectuais e institucionais para enfrentarmos as demandas e nos tornarmos participantes influentes nos destinos desse inovador modelo de poder.

Segurança e defesa cibernética: da fronteira física aos muros virtuais

Tipografia
Exo (títulos) e Minion Pro (texto)

Papel
Capa em Triplex 250g/m²
Miolo em Off-set 75g/m²

Montado e impresso na oficina gráfica da

Editora UFPE

Rua Acadêmico Hélio Ramos, 20 | Várzea, Recife - PE | CEP: 50740-530
Fones: (81) 2126.8397 / 2126.8930 | Fax: (81) 2126.8395
www.ufpe.br/edufpe | livraria@edufpe.com.br

André Ferreira Alves Machado

Flávio Rocha de Oliveira

Gills Vilar Lopes

João Gabriel Álvares

João Marinonio Enke Carneiro

José Ricardo de Souza Camelo

Marcos Aurélio Guedes de Oliveira

Oscar Medeiros Filho

Ricardo Borges Gama Neto

Selma Lúcia de Moura Gonzales

Walfredo Bento Ferreira Neto

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CAPES

SAE SECRETARIA DE ASSUNTOS ESTRATÉGICOS PRESIDÊNCIA DA REPÚBLICA

60 anos Editora UFPE

ISBN 978-85-415-0425-6