UNIVERSIDADE DE BRSÍLIA
Instituto de Relações Internacionais
Programa de Pós-Graduação em Relações Internacionais
XVII Curso de Especialização em Relações Internacionais

A Evolução dos Conflitos Assimétricos e suas Consequências no Preparo e Emprego das Forças Armadas: os projetos estratégicos do Exército Brasileiro e a implementação da defesa cibernética

Rafael Siqueira Marques

Artigo apresentado como requisito parcial para a obtenção do título de Especialista em Relações Internacionais pela Universidade de Brasília.

Orientador: Prof. Dr. Alcides Costa Vaz.

Brasília

2015

A Evolução dos Conflitos Assimétricos e suas Consequências no Preparo e Emprego das Forças Armadas: os projetos estratégicos do Exército Brasileiro e a implementação da defesa cibernética

RESUMO

Os marcos históricos que pontuaram modificações nos processos industriais ocasionaram, e continuam a fazê-lo, mudanças nos fenômenos de guerra e paz. Como um estudo no campo das Relações Internacionais, tem-se que os mecanismos de defesa dos Estados vêm se adaptando de tempos em tempos para melhor adequação aos interesses de cada país de acordo com a conjuntura em que ele esteja inserido. O conflito denominado assimétrico ganhou evidência a partir do final da década de 90 e inseriu diversos novos fatores aos processos de tomada de decisão, sejam elas táticas ou estratégicas, para melhor adequação das capacidades militares. No Brasil, impulsionado pela Estratégia Nacional de Defesa, o Exército Brasileiro implementou diversos projetos estratégicos para transformação da Força Terrestre, dentre eles a estruturação da defesa cibernética e a consequente proteção dos domínios virtuais de interesse.

Palavras-chave: conflitos assimétricos, exército, defesa cibernética.

ABSTRACT

The landmarks that pointed modifications in industrial processes have caused, and continue to do so, changes in war and peace phenomena. As a study in the field of International Relations, it seems the defense mechanisms of the States are adapting from time to time to better match the interests of each country according to the conjuncture in which it is inserted. The denominated asymmetric conflict gained credible evidence from the late 90s and insert several new factors to the decision-making processes, whether tactical or strategic, to better adapt military capabilities. In Brazil, driven by the National Defense Strategy, the Brazilian Army has implemented several strategic projects for transformation of the Land Force, among then the structuring of cyber defense and the consequent protection of virtual domains of interest.

Keywords: asymmetric conflict, army, cyber defense.

INTRODUÇÃO

A evolução do modo como ocorrem os conflitos bélicos pode ser organizada em diferentes gerações de guerra, as quais coincidem com as revoluções tecnológicas de suas épocas e significativas mudanças nas relações internacionais. A seguir, e em sequência cronológica, uma breve síntese dessas evoluções.

Estabelecida após a revolução da pólvora, a guerra de primeira geração era aquela ocorrida com surpreendente ordem para os parâmetros atuais. Tratava-se de um conflito com local previamente estabelecido, grupamentos lineares na disposição das tropas e enfrentamentos em bloco.

Na guerra de segunda geração, a automatização de armamentos, a qual foi consequência direta do desenvolvimento advindo da revolução industrial, ceifava largas frentes do campo de batalha, obrigando as tropas a fazerem uso de abrigos e batalharem por cada metro do terreno, configurando o que ficou conhecido como "guerra de trincheiras".

A terceira geração surgiu da necessidade de superar as limitações da "guerra de trincheiras", valendo-se, para isso, do combate em vetores simultâneos, valorizando a manobra e a velocidade, por vezes combinando meios aéreos e veículos blindados naquilo que os alemães resumiram em um único termo: *"blitzkrieg"* – ou guerra relâmpago.

É a partir do conceito de guerra de quarta geração, ou *fourth generation warfere* (4GW), que a guerra se aproxima da realidade contemporânea dos conflitos e do tema proposto pelo presente artigo. Nesse tipo de conflito, o enfrentamento entre Estados, principalmente por questões territoriais, deixa de ser o padrão dando lugar a questões culturais, políticas e econômicas que passaram a figurar com mais frequência nas definições de "inimigo".

Os avançados meios de tecnologia da informação, aliados a armamentos cada vez mais eficientes dos Estados considerados desenvolvidos, em contraposição aos Estados ou facções com baixas capacidades político-econômico-militares, fazem com que esses acabem por adotar o confronto não-linear, a insurgência e o combate de guerrilha como doutrina, configurando um tipo de enfrentamento que hoje é chamado de "guerra assimétrica" (METZ, 2001).

No campo teórico das Relações Internacionais, uma abordagem por meio da teoria construtivista seria a mais indicada para análise da consolidação e da mutação dos interesses dos Estados, os quais, principalmente no paradigma da segurança internacional, variam conforme os constrangimentos internacionais de cada momento.

Entretanto, é na abordagem sistêmica das distribuições de capacidades do realismo estrutural (WALTZ, 2002) que mais facilmente se compreende o desenrolar prático dos conflitos assimétricos contemporâneos. Portanto, pode-se dizer que em conflitos assimétricos tem-se as características político-sociais e econômico-militares como as grandes condicionantes do modo de combate adotado por cada grupo ou país beligerante.

Tomando Westphalia como primeira referência, o gráfico abaixo ilustra uma conjugação de fatores em uma linha do tempo, evidenciando também a predominância atual da 4GW sem que para isso ocorresse a extinção das demais modalidades, mas sim uma significante diminuição de sua incidência.

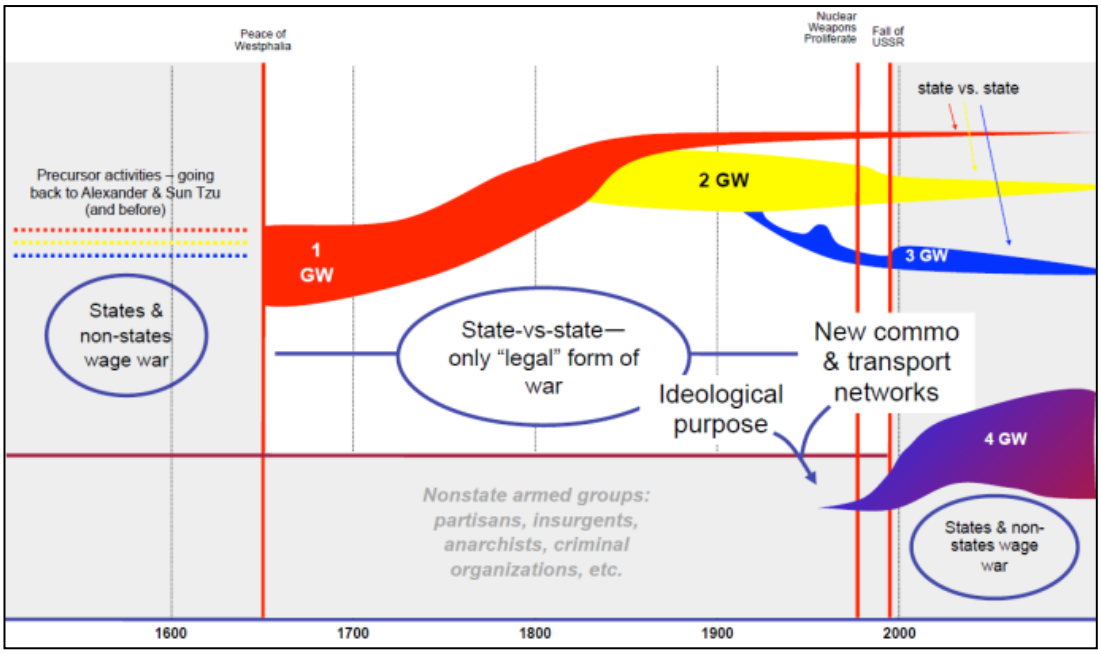

Figura 01 – Linha do tempo e evolução dos conflitos

(Fonte: https://geopolicraticus.wordpress.com/2010/10/26/the-generational-warfare-model)

1. O CONFLITO ASSIMÉTRICO E AS NOVAS AMEAÇAS À SEGURANÇA INTERNACIONAL

A definição de conflito assimétrico remete a um processo comparativo de forças que decorre em desigualdades nos diversos níveis, lembrando que não só no nível das capacidades bélicas das partes em litígio, mas também nos recursos econômicos, político-sociais e diplomáticos.

Em um conflito assimétrico, a diferença de capacidades entre as partes ocasiona mudanças nos processos de uso da força, o qual ocorre de modo distinto do enfrentamento direto em frentes de combate facilmente delimitadas e de fácil identificação. Ao contrário disso, tem-se que as insurgências, ações táticas especializadas, o terrorismo e o amplo uso da propaganda e contrapropaganda em frentes de combate não definidas e/ou multidimensionais, são as reais características do conflito assimétrico.

Esse tipo de conflito costuma ainda desenvolver-se em áreas urbanas com larga presença de civis. Suas principais motivações são os objetivos político-econômicos, sendo os efeitos psicológicos do conflito amplamente utilizados para atingi-los, gerando uma espécie de conflito híbrido onde destaca-se o emprego de ações de operações psicológicas e de combate irregular (HAMMES, 2007).

Desde o fim da União da Repúblicas Socialistas Soviéticas (URSS), na verdade até mesmo durante o período da Guerra Fria, a possibilidade de grandes conflitos com declarações de guerra entre Estados foi tornando-se cada vez menos provável. No entanto, alguns focos de tensão e instabilidade ainda existem nos níveis subnacionais e supranacionais, dando origem a fenômenos tais como as guerras preventivas e as intervenções militares.

No início da década de noventa, houve o surgimento de uma agenda internacional um tanto quanto mais liberal e que passou a contar com a presença de temas como direitos humanos, meio ambiente e desenvolvimentismo (MESSARI, 2005). No entanto, tomando a participação dos Estados Unidos nos recentes conflitos ocorridos no Oriente Médio como exemplo evidente do que se quer demonstrar, observa-se que as agendas “menos realistas” só tiveram sua importância até o

momento em que os interesses de poder e *high politics* fossem confrontados, tornando aquele caso um claro exemplo de conflito no qual um país fez uso de suas capacidades superiores e discrepantes em relação aos demais atores para satisfazer ambições de sua política de poder naquela região. Naquele caso, pode-se ainda dizer que há referência no realismo clássico, pois o envolvimento de um país em um confronto bélico com a intenção de aumento, manutenção, ou demonstração de poder, remete à primeira formulação da teoria realista (MORGENTHAU, 2003).

Seguindo o entendimento sobre o modo de conflito de quarta geração, destaca-se que, ainda no ano de 1999, dois oficiais de estado-maior das forças armadas chinesas já haviam publicado uma obra denominada *"Unrestricted Warfare"*[1] – ou *A Guerra Além dos Limites* (tradução em publicações nacionais do livro) – na qual apontavam para o fato de que, devido às modificações no cenário geopolítico ocorridas até o final da década de 90, não mais seriam adequadas as antigas estratégias militares convencionais e sim um novo modo de emprego militar em um cenário onde governos, organizações não-governamentais e as corporações nacionais e transnacionais atuariam de modo cada vez mais interdependentes. Destaca-se a temporização da obra "*Unrestricted Warfare"* que foi publicada antes mesmo do atendado terrorista de 2001 aos Estados Unidos da América (EUA), o qual pode ser considerado um dos marcos para os conflitos de quarta geração e o início da consequente "Guerra Global ao Terror" empreendida pelos EUA.

No que se refere à guerra ao terror, ela parte do princípio de que a estratégia de dissuasão, na qual o objetivo principal se resume a desestimular as contra si, não mais seria eficiente contra um adversário ideologicamente motivado e estruturado como uma organização terrorista transnacional. A reação ao atentado de 11 de setembro de 2001 veio em forma de intervenção militar, no caso do Afeganistão, e fomentou argumentos para a decisão pela guerra preemptiva no Iraque em 2003 (WESTER, 2005).

Antes de avançar com as características assimétricas dos conflitos contemporâneos, destaca-se que a atividade terrorista transnacional, motivada pelo fanatismo religioso, é um dos principais temas da atual agenda de segurança

[1]LIANG, Qiao; XIANGSUI, Liang. Beijing, 1999. Disponível em: https://www.egn.mar.mil.br/arquivos/cepe/GUERRAALEMLIMITES.pdf. Acesso em: 12 de novembro de 2015.

internacional decorrendo em medidas de securitização em curso em diversos países. Por securitização, adota-se aqui os pressupostos da Escola de Copenhague e suas definições sobre o processo de securitizar algo, ou seja, diante de um fato interpretado como ameaça, adotar medidas extraordinárias que não seriam adequadas a um cenário de normalidade, as quais seriam justificadas pelo suposto dano potencial e iminente que a ameaça poderia gerar caso nenhuma medida fosse tomada para debelá-la (BUZAN, 1998)

No caso da empreitada norte-americana a partir de 2001, tem-se que ela resultou em mudança de regime em dois Estados do Oriente Médio e há discussões sobre outras motivações que teriam orientado as ações naquela região, a qual abriga algumas das poucas culturas que não adotaram o modelo de capitalismo de consumo tão caro aos norte-americanos, mas tudo isso seria tema suficiente para um outro artigo.

Retomando o entendimento da 4GW, cabe lembrar que, quando de seu surgimento, o conceito de guerra assimétrica foi pouco absorvido pelos estrategistas e estudiosos militares (HAMMES, 2007). A ideia de supremacia da força, superior em números e em tecnologia, vinha prevalecendo mesmo nos primeiros anos após o atentado de 11 de setembro de 2001, isso devido a rápida derrota das forças iraquianas, em 2003, em uma operação com manobras semelhantes às da 3GW combinando manobra e poder de combate. A modificação do pensamento veio com a continuidade daqueles conflitos, que acabaram por migrar para uma realidade de insurgência no Iraque e no Afeganistão, e com as debilidades da multidimensionalidade da guerra global contra o terrorismo fora daqueles países.

Percebe-se que a assimetria provoca consequências de combate não tão lógicas e que podem, até mesmo, favorecer o lado dito mais fraco do conflito (HAMMES, 2007). O amplo espectro dos conflitos assimétricos passou a caracterizar-se pela combinação de restrições econômicas, tecnologia militar, fatores étnicos e ideológicos, combate de guerrilha e presença de companhias militares privadas.

Contando com a presença de boa parte desses fatores, o conflito em curso no território sírio é o exemplo mais atual de conflito assimétrico, sendo ainda alvo de

intervenções e de financiamentos seletivos de atores externos apoiadores das diferentes forças em conflito dentro da Síria.

Já em relação às intervenções militares, elas podem ser entendidas como o resultado da deterioração ou ineficiência de mecanismos de controle e instituições sólidas, as quais, em uma visão mais liberal, seriam o caminho para a paz. Atualmente, as intervenções têm ocorrido sob justificativas humanitárias, todavia nota-se que sua ocorrência está sob a tutela de organismos como o Conselho de Segurança da Organização das Nações Unidas (ONU) que, por sua vez, acaba por refletir interesses de seus membros em suas escolhas, como exemplificado na seguinte problematização hipotética: por que intervir no país A, e não país o B, quando os dois possuem os mesmos "pré-requisitos" humanitários que legitimam a intervenção?

A hipótese acima indica uma brecha para o Conselho condicionar os próprios mecanismos do sistema internacional, dito sem hierarquia e sem parcialidade, de acordo com seus próprios interesses, os quais também podem variar de acordo com as circunstancias e constrangimentos que afrontam os objetivos dessas mesmas potências que compõe o Conselho. O que se conclui é que esse tipo de jogo de poder corrói a credibilidade dessas instituições criando, ironicamente, cenários mais suscetíveis ainda à deflagração de conflitos.

O que se quer dizer é que, apesar dos dispositivos internacionais de controle, da interdependência cada vez maior entre os atores internacionais e das ferramentas de análise construtivistas, tem-se que, na deflagração e condução dos embates bélicos, os pressupostos realistas dos jogos de poder negociados de acordo com as diferentes capacidades dos Estados ainda são as principais condicionantes em tela, valendo-se, inclusive, de prerrogativas tipicamente liberais como justificativas para a consecução de seus objetivos de poder político-estratégico. Como exemplo, pode ser citado o uso seletivo de termos como "levar a democracia e a liberdade" em justificativas de ações militares.

Sobre esse tipo de uso das capacidades, Waltz (2002) escreveu que "os Estados usam meios econômicos para fins militares e políticos; e meios militares e políticos para alcançar interesses econômicos". Até mesmo o destacado neoliberal,

Joseph Nye, pontuou que mesmo com a importância das organizações e do direito internacional, a política internacional realista é a que melhor explica os conflitos no Oriente Médio (NYE, 2002).

2. A POLÍTICA DE DEFESA BRASILEIRA E OS PROJETOS ESTRATÉGICOS DO EXÉRCITO PARA ADEQUAÇÃO AOS NOVOS CENÁRIOS E AMEAÇAS

O Brasil estabeleceu sua atual política nacional de defesa no ano de 2008 com o intuito de adequar-se às necessidades de segurança e reforçar sua principal vocação inclinada à estratégia de dissuasão. As previsões dessa política, associadas à aprovação do Livro Branco e da Estratégia Nacional de Defesa, tiveram como um de seus objetivos a reestruturação das capacidades das forças armadas, com fins de mantê-las com relativa hegemonia regional (BRASIL, 2008).

Desta forma, merece destaque a correlação das capacidades das forças de segurança brasileiras com a continua evolução dos conflitos, seja em nível internacional ou regional, como propulsora de uma constante necessidade de revisão e adequação das políticas de defesa e das capacidades militares. Destaca-se que, não necessariamente, as adequações devam ocorrer apenas por meio de aquisições de equipamentos e armamentos, mas também pelas experimentações doutrinárias, planejamentos estratégicos e cooperações internacionais de instrução.

No modelo assimétrico em curso nos diversos conflitos contemporâneos, o país não se colocou marginalizado e buscou, dentro das capacidades e pretensões brasileiras, adaptar-se. A evolução do modo como se dão os conflitos obriga uma constante revisão da política de defesa nacional para que as capacidades de defesa acompanhem, no mínimo em mesmo patamar, as aspirações políticas e econômicas do Brasil. Sendo assim, merecem destaque alguns dos atuais projetos estratégicos do Exército Brasileiro que integram um esforço de adaptabilidade às capacidades necessárias para o emprego contemporâneo da Força Terrestre no que tange a operacionalidade e a própria estratégia da dissuasão.

No que se refere ao Exército Brasileiro, a Portaria nº 134-EME, de 10 de setembro de 2012, criou o escritório de Projetos do Exército (EPEx) para atuar na

coordenação de sete projetos estratégicos, os quais têm a intenção de atuar como indutores da transformação do Exército Brasileiro, até o ano de 2022, em áreas julgadas essenciais para adequação das capacidades militares da Força, sendo eles: Defesa Cibernética, SISFRON, PROTEGER, GUARANI, RECOP, ASTROS 2020 e Defesa Antiaérea.

Figura 02 – Projetos Estratégicos do Exército

(Fonte: TEIXEIRA, 2014)

O relacionamento desses projetos com a indústria de defesa também é um viés bastante explorado conforme ressaltou Prado Filho (PRADO FILHO, 2014):

> […]. Alguns resultados da transformação do EB já são percebidos por intermédio dos Projetos Estratégicos do Exército. Eles, juntamente com o novo SCTIEx proporcionarão oportunidades para o fortalecimento da Base Industrial de Defesa, particularmente nos aspectos referentes à geração de empregos, capacitação de pessoal e absorção de tecnologias sensíveis desenvolvidas em âmbito nacional ou obtidas por processo de transferência. Ressalta-se que essas oportunidades, por fim, contribuem com o desenvolvimento do País e com o fortalecimento do Poder Nacional, o que facilita a consecução dos Objetivos Fundamentais, dentre eles, a Soberania Nacional […].

O Projeto Defesa Cibernética é gerenciado pelo Centro de Defesa Cibernética, uma Organização Militar já em atividade no Exército, e será objeto de detalhamento nos itens posteriores. Como síntese dos demais projetos estratégicos podem ser destacados os seguintes aspectos conforme descrito em Prado Filho (2014).

O SISFRON – ou Sistema de Monitoramento de Fronteiras – objetiva entregar aos escalões decisórios uma potente ferramenta que integrará diversos sistemas de sensoriamento posicionados na faixa de fronteira brasileira. O sistema propõe, além da consciência situacional permanente, uma alternativa de apoio no combate aos crimes transfronteiriços, como o tráfico de drogas e de armas, os quais são responsáveis, segundo o atual Comandante do Exército, por cerca de 80% da violência urbana no Brasil.

Já o Sistema Integrado de Proteção de Estruturas Estratégicas – ou PROTEGER – tem o objetivo de capacitar a Força para atuar preventivamente e/ou responsivamente às ameaças contra as estruturas sensíveis, seja em apoio a Defesa Civil, em operações contra ações QBRN (Química, biológica, Radiológica ou Nuclear) ou operações de Garantia da Lei e da Ordem (GLO).

O Projeto Guarani trata do processo de substituição dos blindados sobre rodas do Exército e atua como indutor da capacidade de projeção de poder da Força Terrestre. A fabricação nacional da família de blindados Guarani prevê um total de 2044 (duas mil e quarenta e quatro) viaturas, o que aquece a indústria de defesa nacional gerando grande quantidade de empregos diretos e indiretos, além da retomada do desenvolvimento e tecnologia nacional na fabricação de blindados, antes atribuída à montadora ENGESA que fabricou as Viaturas Blindadas de Transporte de Pessoal (Urutu) e Viatura Blindada de Reconhecimento (Cascavel).

Na Defesa Antiaérea, o objetivo é readequar os equipamentos para ultrapassar a obsolescência do material atual, colocando o país em situação de garantir a soberania do espaço aéreo em locais críticos. Um exemplo de produto nacional, dentro do Projeto de Defesa Antiaérea, é a atual produção do radar SABER M60, desenvolvido pelo Centro de Tecnologia do Exército (CTEx).

Em relação à artilharia do Exército, o Projeto ASTROS 2020 é um dos que se encontra em estágio mais avançado, atribuindo capacidade de dissuasão extrarregional ao Brasil. Trata-se de sistema de apoio de fogo de longo alcance que se utiliza lançadores de foguetes e diversas tecnologias necessárias ao seu funcionamento.

O RECOP – ou Projeto de Recuperação da Capacidade Operacional –diz respeito à distribuição de material condizente e atualizado para as frações do Exército espalhadas no território nacional de modo que lhes dê capacidade de manterem-se em situação ideal para seu emprego na em missões de defesa da pátria. O projeto é amplo e engloba desde a modernização e/ou substituição de equipamentos e armamentos individuais até embarcações e aeronaves para o transporte de tropa.

De modo sintético, o acima descrito sobre cada projeto tem a finalidade de entregar o que foi proposto para a transformação do Exército Brasileiro até o ano de 2022, sendo aquele ano o ponto de inflexão de mudanças fundamentais para o melhor preparo e emprego das capacidades militares, bem como para favorecer modificações doutrinárias tão necessárias para adaptação aos cenários conjunturais em constante evolução.

Antes de pormenorizar o caso da cibernética como ferramenta de poder nos conflitos, cabe ressaltar que, infelizmente, a quase totalidade desses projetos, os quais já estão em andamento há alguns anos, sofreram grandes atrasos devido ao agravamento, no ano de 2015, da crise econômico-política brasileira. Conforme entrevista concedida ao Jornal Zero Hora, em outubro de 2015, pelo atual Comandante do Exército – Gen Ex Eduardo Dias da Costa Villas Bôas – do total destinado ao SISFRON, por exemplo, apenas 7,2% foram recebidos. Esses mesmos atrasos (ou “diminuição de repasses orçamentários”) que os projetos estratégicos estão sofrendo, podem inviabilizar o processo de transformação ao passo que diversas implementações já estarão em fase de obsolescência caso o ritmo de investimento dos anos de 2015 e 2016 não seja revertido.

3. A "*CYBERWAR*" NO CONTEXTO DO CONFLITO DE QUINTA GERAÇÃO E O DESENVOLVIMENTO DE SUA DOUTRINA NO BRASIL

Acrescente-se ao descrito sobre conflitos de quarta geração e guerra assimétrica, o incremento tecnológico em corrente desenvolvimento no século XXI e ter-se-á aquilo que estudiosos dos fenômenos de guerra e paz denominam guerra de quinta geração (5GW).

Uma vez que as evoluções no modo como ocorrem os conflitos bélicos coincidiram com mudanças historicamente marcantes na organização do sistema internacional, agora aponta-se para a próxima geração de guerra atrelada as recentes evoluções tecnológicas, na qual os conflitos estendem-se também ao meio cibernético, configurando a guerra cibernética ou *cyberwar* (HAMMES, 2007).

Em consonância com as transformações político-sociais, na 5GW há uma tendência de que cada vez mais atores, configurados por grupos com interesses em comum e possuidores de capacidade e motivação para uso da força, distintos dos exércitos regulares estatais, estejam presentes nos conflitos vindouros.

Em outro alicerce da guerra de quinta geração, a evolução tecnológica deverá culminar em profundas modificações nas batalhas com o uso vertentes outras além do uso do espaço cibernético, como a biotecnologia e a nanotecnologia. O emprego de ataques cibernéticos parece bem lógico ao se indagar sobre o que causaria maior dano, o arrebatamento por um bombardeio convencional ou um ataque cibernético coordenado em infraestruturas críticas como energia e telecomunicações?

Outras questões ainda deverão ser respondidas. Um indivíduo sentado em frente ao computador de seu apartamento, invadindo o sistema de segurança de uma usina nuclear, pode ser considerado um combatente à luz do direito internacional dos conflitos armados? Um contra-ataque seria justificável? São condições que inexistiam durante as Convenções de Genebra e que devem permear os debates acerca dos conflitos de quinta geração pelos próximos anos, tanto nas academias quanto nos centros de estratégia e doutrina militares.

O próprio conceito de território cibernético, por si só, é digno de melhor explicação. Trata-se de um espaço onde não há fronteiras físicas e no qual diferentes atores "navegam" livremente, com exceção para os domínios protegidos nos quais

algum ente, seja ele público ou privado, exerça seus direitos sobre ele. Pode-se afirmar, ainda, que o espaço cibernético é composto por duas partes (PINHEIRO, 2013): uma estrutura não-física (abrangendo os dados e as informações) e uma estrutura física (equipamentos, *data center* e servidores)

Esse espaço cibernético, ou *cyberspace*, é o teatro de operações no qual a *cyberwar* pode ocorrer na medida em que a "política por outros meios"[2], evocando a célebre definição de Clausewitz, é feita por meio do ataque aos domínios protegidos do espaço cibernético citados acima, locais estes onde predomina uma certa soberania por parte de quem o detém (NYE, 2010). Se uma ação ofensiva encontra sua antítese em uma operação defensiva, pode-se dizer que o Estado que detém infraestrutura e capacidade cibernética, acima de qualquer outra coisa, é um estado capaz de monitorar e proteger seu próprio *cyberspace* contra tentativas de ataques maliciosos.

Ainda em relação aos ataques cibernéticos, sabe-se da improbabilidade da evocação de sua autoria por parte de um Estado. A responsabilização pública pelos casos conhecidos e veiculados em meios de comunicação têm sido, principalmente, por parte de grupos ativistas não-governamentais, mas cabe pontuar que isso não exclui as diversas agências estatais como fontes propagadoras de ataques.

Em Joseph Nye (2010), a cibernética é abordada como um recurso de poder que pode se "comunicar" com os demais recursos, servindo como ferramenta para consecução de objetivos em outras esferas de poder. O autor ainda aponta a cibernética como catalizador da Terceira Revolução Industrial, ou Revolução Tecno-informacional, na medida em acelera o fluxo informacional nas sociedades contemporâneas, cabendo o lembrete, neste ponto, de como coincidiram, historicamente, as mudanças no modo de conflito com as revoluções tecnológicas recapituladas no início deste trabalho.

Em relação aos atores presentes no campo da cibernética, tem-se a potencialidade técnica da ação do indivíduo, seja sozinho ou em grupos, para realizar ações no ciberespaço. Os grupos organizados de ativistas *hackers*, organizações

[2]CLAUSEWITZ, Carl Von. **Da Guerra**. Disponível em: <https://www.egn.mar.mil.br/arquivos/cepe/DAGUERRA.pdf>. Acesso em: 12 de novembro de 2015.

criminosas e agencias estatais e não-estatais contemplam boa parte dos que podem agir nesse campo específico.

3.1 O uso de ataques cibernéticos em casos recentes

Alguns casos de ações no espaço cibernético que obtiveram relativa repercussão nos meios de comunicação merecem destaque, ainda que, em diversos deles, a autoria não tenha sido assumida pelas partes apontadas como origem do ataque.

Por Ataque Cibernético tomaremos a seguinte definição contida na proposta de Política Nacional de Inteligência para o Brasil, elaborada pelo Gabinete de Segurança Institucional da Presidência da República, no ano de 2009, e até os dias de hoje não publicada pelo planalto:

> […] referem-se a ações deliberadas com o emprego de recursos da Tecnologia da Informação e Comunicações (TIC) que visem interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional. Os prejuízos das ações no espaço cibernético não advêm apenas do comprometimento de recursos de TIC. Decorrem, também, da manipulação de opiniões, mediante ações de propaganda ou de desinformação […]. (GSI/PR, 2009)

Talvez como caso de maior repercussão, ao menos no Brasil, deva-se começar pelo sistema *Echelon*. Trata-se de um sistema complexo de análise de dados obtidos por meio de dados telefônicos com o intuito de identificar possíveis ameaças aos Unidos e seus aliados. A grande repercussão teve causa no provável uso daquela ferramenta para atender interesse políticos e de grandes empresas norte-americanas. O emprego do sistema *Echelon* está associado a National Security Agency (NSA), criada pelo presidente norte-americano Harry S. Truman, sigilosamente, em 1952, com atribuição de cuidar da segurança das comunicações (WEBB, 2008). A origem da NSA, ainda na década de 50, destaca a preocupação norte-americana em possuir *know-how* na área e pode ser apontada como razão do desponte dos Estados Unidos como um dos principais países a atuar nessa área atualmente.

Agora em sequência cronológica destacando-se, como uma das primeiras ações relatadas de guerra cibernética, o ocorrido durante o conflito sérvio em 1999,

no qual *hackers* kosovares e sérvios atuavam uns contra os outros. A participação militar americana naquele conflito ocorria, principalmente, pelo bombardeio aéreo de estruturas da Sérvia, o qual acabou por atingir a embaixada chinesa levando *hackers* chineses a atacar sistemas norte-americanos em retaliação (MESSMER, 1999).

Em 2007, o sistema antiaéreo sírio foi incapaz de identificar as aeronaves israelenses que voaram sob seu território com objetivo de atacar uma instalação nuclear. Apesar da sofisticação do sistema sírio, foi relatado que uma ação cibernética israelense implantou um *bug* que fez com que suas aeronaves não fossem apontadas nos radares da Síria (NUNES, 2010).

Outros casos, como os que se seguem, foram bem ilustrados em publicação da revista *The Economist*[3], em edição especial sobre a *Cyberwar*. A publicação relata que no mesmo ano do ataque israelense à Síria, ocorreu uma ação de ataque cibernético tão característica de ataques daquela natureza que foi denominada, na época, *Web-War I*. A ação ocorreu como protesto contra uma decisão do governo da Estônia para remoção de um memorial soviético. Foi realizado um ataque do tipo *denial-of-service*, ou negação de serviço, que impediu que o governo da Estônia acessasse seus próprios servidores.

Em 2008, ocorreu caso semelhante ao da Estônia, porém a autoria por parte de um Estado, neste caso a Rússia, tornou-se mais evidente. Trata-se da ação militar russa na Geórgia, quando ocorreu um ataque de negação de serviço simultânea ao avanço das tropas russas.

No ano de 2009, foi reportada uma suposta tentativa de penetração no sistema de controle de fornecimento de energia elétrica norte-americano. Ainda no ano de 2009, foi divulgado um caso de vazamento de informações sobre o avião de combate F-35 que teria sido obtido por meio de ataques aos bancos de dados norte-americanos.

Como um dos casos mais noticiados em relação aos ataques cibernéticos, no ano de 2010, ocorreu um ataque aos sistemas de controle de infraestruturas nucleares do Irã pela infiltração de um tipo de vírus denominado *Stuxnet*. O programa tomou

[3]WAR in the fifth domain – Are the mouse and keyboard the new weapons of conflict? *The Economist*. Londres, 3 Jul. 2010: p. 25-28.

controle da operação de centrífugas nucleares iranianas e as fez funcionar em modo exaustivo até que diversas delas fossem danificadas.

No ano de 2015, o grupo de ativismo *hacker* conhecido como *Anonymous* anunciou publicamente que iniciaria uma guerra digital contra a Turquia[4] devido ao apoio dado pelo país à um grupo terrorista. Como consequência, em dezembro daquele ano, os domínios turcos ".tr" foram atacados impedindo o acesso aos sistemas de bancos, das forças armadas e governamentais.

No mais atual caso de uso da *cyberwar* em cenários de conflito assimétricos, os EUA têm realizado ataques contra a organização terrorista Estado Islâmico em território sírio. Os ataques, segundo o Secretário de Defesa norte-americano, Ash Carter, visam impedir coordenações táticas por parte das lideranças do grupo terrorista ao fazerem uso de equipamentos de tecnologia da informação. Nesse mesmo intuito, Ash Carter ainda prevê um aumento no investimento de 15,5 % [5]para a defesa e guerra cibernética nos EUA, apontando que o aumento da atividade *on*-line do grupo Estado Islâmico e as frequentes invasões e roubos de dados de cidadãos norte-americanos no ambiente virtual mostram que a guerra cibernética está em plena expansão.

3.2A defesa cibernética brasileira: infraestrutura e doutrina

É da concepção de proteção do espaço e domínios da tecnologia da informação que vem sendo implementada a defesa cibernética brasileira. O tema ganhou agenda nacional em 2008 ao ser previsto na Estratégia Nacional de Defesa (END) como um dos setores estratégicos, ao lado do aeroespacial e nuclear (BRASIL, 2008, p.6), ficando a defesa cibernética à cargo do Exército Brasileiro. Em sua redação, a END destaca que devem ser adotadas medidas para a segurança das áreas de infraestrutura críticas e ainda prevê:

> "As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os

[4] Conforme disponibilizado em http://www.defesanet.com.br/cyberwar/noticia/21710/EUA-travam-guerra-cibernetica-contra-o-Estado-Islamico/, acesso em 02 de março de 2016.

[5] Disponível em http://www.defesanet.com.br/cyberwar/noticia/21683/Pentagono-aumenta-em-15-por-cento-orcamento-para-guerra-informatica/, acesso em 27 de fevereiro de 2016.

> contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (...) O aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI-PR." (Brasil, 2008, p. 33 e p. 66).

Para a atuação em rede, a END fomenta que que as Forças Armadas tenham como objetivo a melhoria da capacidade de Comando, Controle, Comunicações, Computação e Inteligência (C4), utilizando como meio as ferramentas de Tecnologia da Informação e Comunicações (TIC).

Há uma distinção a se fazer sobre os conceitos de segurança e defesa cibernética. A Segurança Cibernética diz respeito à proteção das redes de comunicação com cooperação entre os órgãos públicos e privados para garantia do funcionamento das infraestruturas críticas civis brasileiras. Já a Defesa Cibernética tem maior relação com a defesa e pronta resposta ativa em casos de crise, funcionando também como um módulo em permanente vigília em condições de condições de neutralizar ameaças. A Segurança Cibernética foi atribuída, no Brasil, ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), enquanto a Defesa ficou atribuída às Forças Armadas.

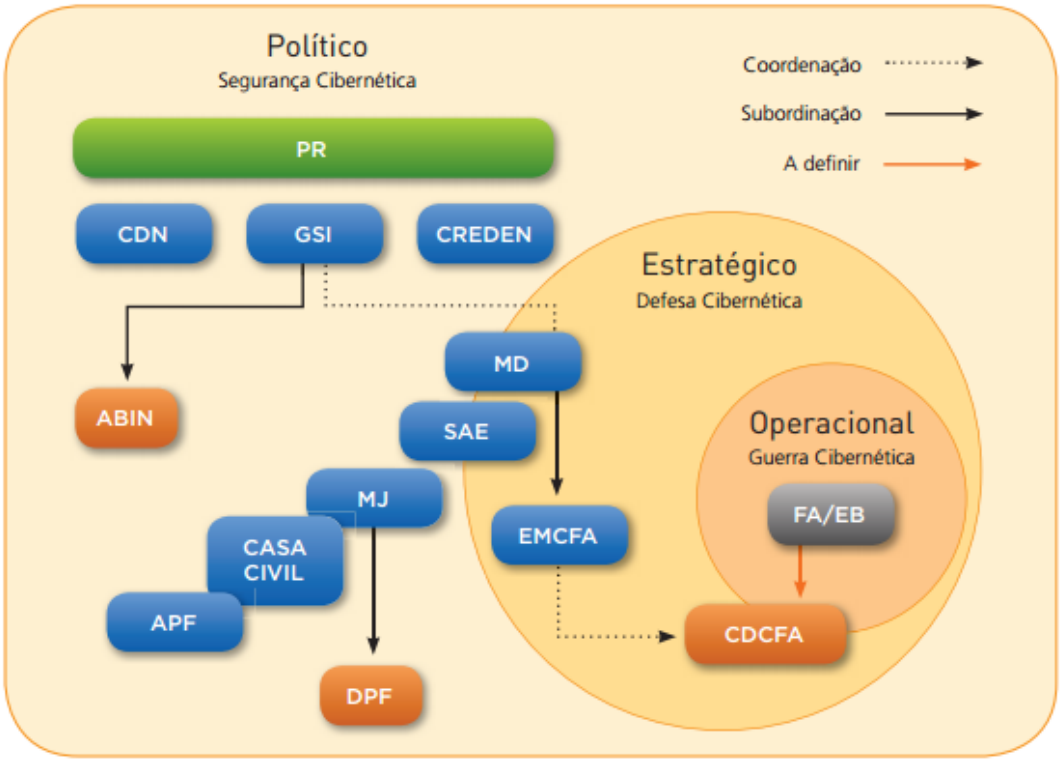

Figura 03 – Sistema de Segurança e Defesa Cibernética
(Fonte: SAE, 2011, p.26)

Atendendo esse intento, foi determinada pelo Exército Brasileiro, a criação de um Centro de Defesa Cibernética (CDCiber), o que ocorreu em 04 de agosto de 2010, objetivando a integração das forças de defesa na proteção do ambiente cibernético brasileiro no que diz respeito às infraestruturas próprias à defesa e soberania nacionais, ou seja, a Defesa Cibernética também atua no campo da Segurança Cibernética ao proteger infraestruturas críticas nacionais.

O CDCiber passou a funcionar no Quartel General do Exército, situado no Setor Militar Urbano, em Brasília-DF. O centro segue a tradição defensiva brasileira e atua como barreira de defesa contra ações de ataque cibernético, não tendo como sua atividade principal a obtenção de dados protegidos, cabendo lembrar que para saber defender-se é preciso saber como funcionam e quais são as possibilidades de ataque.

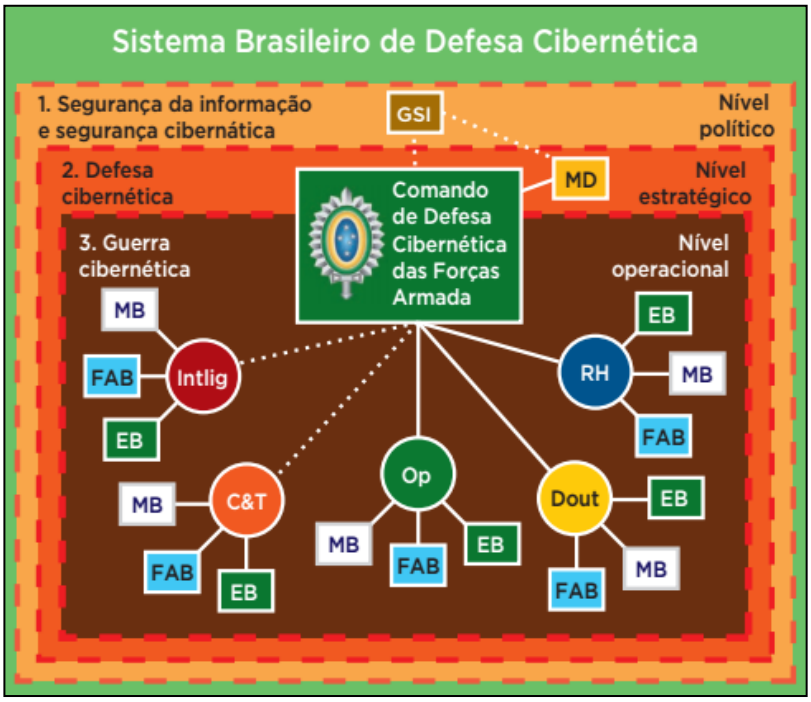

Figura 04 –Defesa Cibernética Brasileira
(Fonte: SAE, 2011, p.26)

Como exemplo do trabalho desenvolvido naquela organização militar, poucos anos sua implementação, foi divulgado o número de ataques que o Brasil sofre diariamente: 30 mil ataques diários. Para o adestramento em *cyberwar*, o CDCiber conta com equipamento simulador de conflitos digitais, como o SIMOC[6], que possibilita exercitar os procedimentos operacionais para os diversos tipos de ataques virtuais simulados possíveis.

Após o início da estruturação, ainda em curso, da defesa cibernética brasileira, o setor ganhou importância que foi refletia em recursos orçamentários e capacitação de pessoas. Entretanto, o mesmo não ocorreu com a Segurança Cibernética. Segundo a Pesquisa Global de Segurança da Informação, realizada pela empresa PWC[7], o número de ataques cibernéticos no Brasil, incluído as fraudes virtuais, subiu 274% apenas no ano de 2015, enquanto a média de crescimento global desse número foi de 38%.

[6] Simulador de Operações Cibernéticas: é o único disponível no país com a capacidade de virtualizar estruturas de redes críticas e simular diversos cenários de ataque e defesa cibernética.
[7]Disponível em: www.radios.ebc.com.br/revista-brasil/edicao/2016-02/pesquisa-revela-crescimento-de-274-em-numero-de-ataques-ciberneticos, acesso em 25 de fevereiro de 2016.

De acordo com outra empresa especializada em segurança digital, a Akamai Technologies, o Brasil é apontado como terceiro maior propagador de ataques cibernéticos do mundo, com 11% dos casos, ficando atrás apenas de EUA e Rússia. Dentre os países que mais sofreram ataques cibernéticos, o país ficou em segundo lugar, com 7% dos casos, sendo os EUA os ocupantes da primeira posição.

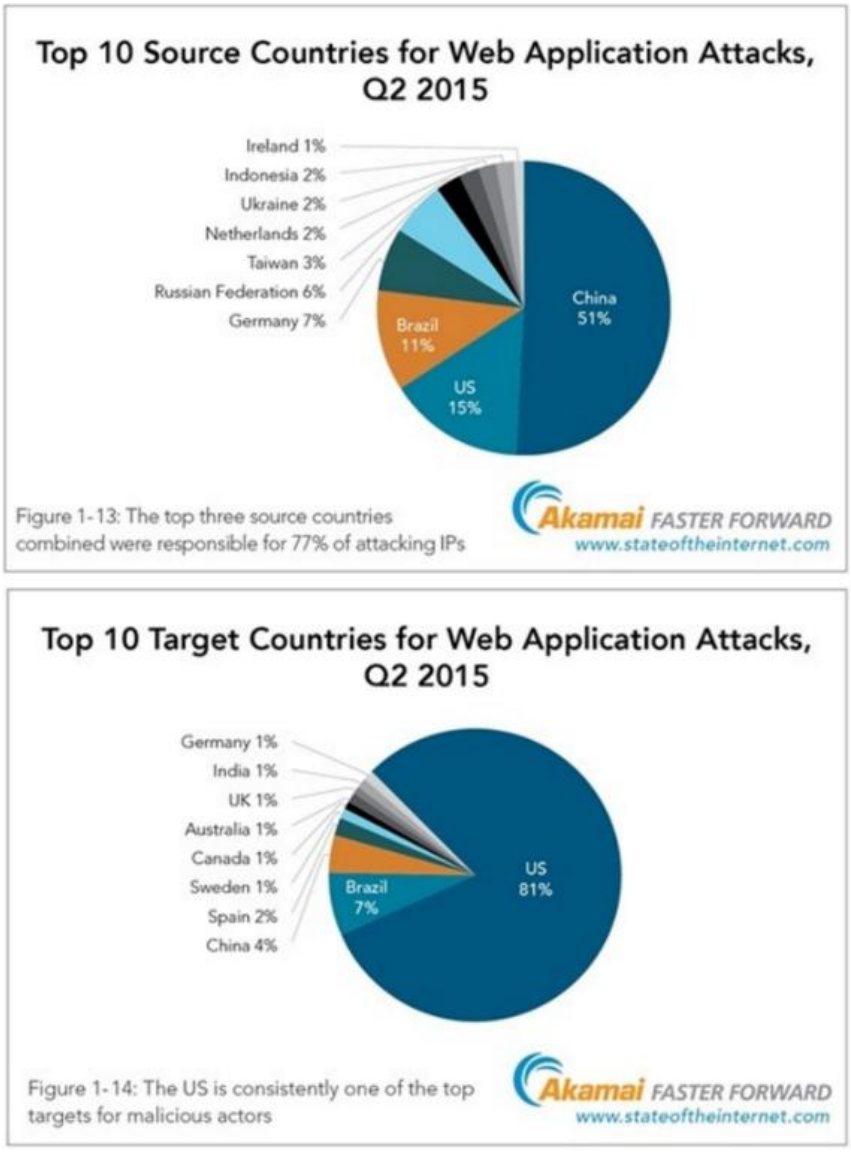

Figura 05 – Gráfico por incidência no mundo
(Fonte:http://static.psafe.net/blog/wp/blog/wpcontent/uploads/2015/08/ciberataques.jpg)

Contudo, é no trabalho divulgado pela empresa Kaspersky Lab que o impacto do problema da segurança digital no Brasil fica mais evidente. Em documento denominado *"Beaches, carnivals and cybercrime: a look inside the Brazilian*

underground"[8], a empresa classifica o país como um dos mais perigosos do mundo no quesito *cybercrime* tendo o Brasil a maioria dos casos referentes a fraude contra indivíduos e empresas. Em 2014, o Brasil já havia sido indicado como número um em ataques financeiros. Além disso, foi constatada a conexão de criminosos brasileiros com outros do Leste Europeu relacionados com a criação de ataques como SpyEye e ZeuS, ambos programados para atacar redes bancárias.

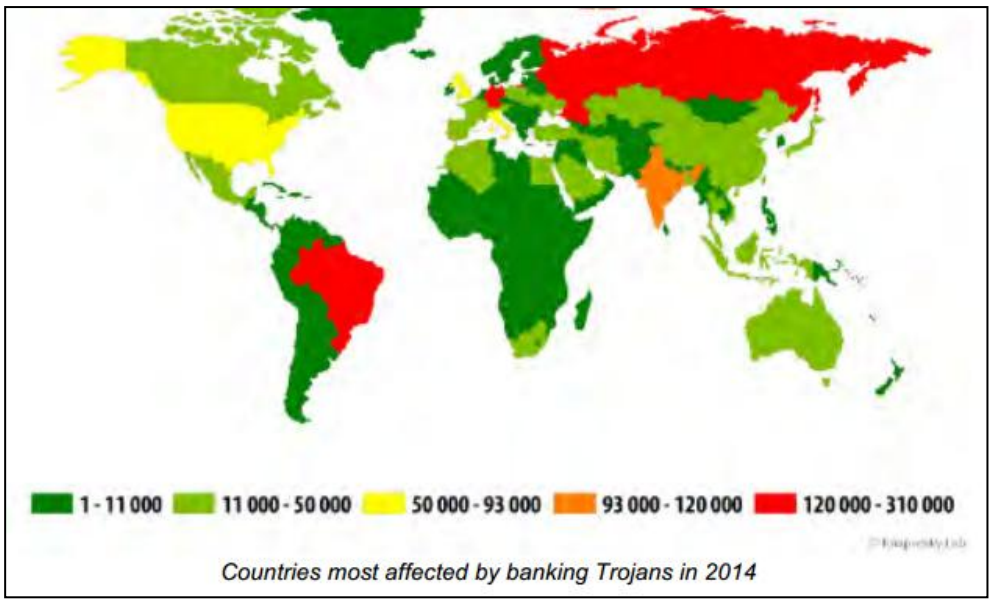

Figura 06 – Países mais atacados por vírus "*cavalo de tróia"* em 2014
(Fonte: Kaspesky Lab)

Como exemplo de ataque à órgão do governo brasileiro, uma ação contra o sistema do IBAMA resultou na emissão de licenças para 23 (vinte e três) madeireiras que estavam suspensas por crimes ambientais. O resultado foi de 11 milhões de reais em madeiras extraídas ilegalmente. O mais intrigante é que serviços desse tipo são oferecidos abertamente na própria rede, conforme exemplificado na figura abaixo.

[8]Disponível em https://securelist.com/analysis/publications/72652/beaches-carnivals-and-cybercrime-a-look-inside-the-brazilian-underground/, acesso em 12 de dezembro de 2015.

Figura 07 – "Pacotes" de ataques cibernéticos oferecidos no Brasil
(Fonte: Kaspesky Lab)

CONSIDERAÇÕES FINAIS

É improvável que ações de insurgência um dia deixarão de existir, assim como as táticas de combate de terceira geração não estão extintas dos conflitos atuais. O que se aponta é uma tendência prática devido a própria evolução da conjuntura internacional – em seus aspectos social, político, econômico e tecnológico – e a persistente incapacidade humana de encontrar formas pacíficas para resolução de controvérsias na esfera das políticas de poder.

O Brasil é ator de relevância no cenário internacional, embora viva momento de declínio de sua atuação em foros internacionais e projeção externa. Os assuntos de defesa devem ter sua importância no debate acadêmico e político assim como os demais temas estratégicos para a manutenção da soberania e interesses nacionais. O tem de segurança e defesa cibernética ainda é restrito aos órgãos da Administração Pública Federal (APF) com atribuições na área e algumas produções acadêmicas. Sobre a difusão e conscientização da importância da agenda Raphael Mandarino Jr explica:

> "O primeiro, o grande desafio, é cultural. Vamos ter que estabelecer, de alguma forma, um projeto de cultura de segurança cibernética. Estamos fazendo isso nos cursos, mas para dentro do Estado, e temos que fazer isso para fora também. Pode ser com um hotsite que ensine como fazer, e que todos os provedores

> divulguem, com seminários, ou que a gente comece a ensinar na escola. ” (MANDARINO JUNIOR, 2009)

O baixo valor atribuído à defesa no debate político atual faz com que seja necessário ainda um maior incentivo para esses estudos no meio acadêmico, com o intuito de fomentar uma mentalidade de defesa – não apenas cibernética – na própria sociedade brasileira, que ainda tem dificuldade em distinguir o tema defesa nacional do tema segurança pública.

Os cortes orçamentários dos últimos anos frearam significativamente os projetos estratégicos no âmbito da defesa, enquanto pode-se pensar que agenda de defesa mereceria melhor prioridade na destinação das verbas federais, mesmo considerando as concretas e urgentes necessidades de outros setores como educação e saúde.

Após análise do apresentado neste trabalho, aponta-se para o próximo importante passo em direção ao fortalecimento da segurança cibernética brasileira, que seria uma implementação de uma estrutura, semelhante à realizada pelo Exército Brasileiro no campo da Defesa Cibernética, para proteção dos dados e infraestruturas privadas do Brasil visando a segurança empresarial. Por enquanto, a consolidação vem ocorrendo de modo mais concreto apenas no meio militar.

A proteção do espaço virtual brasileiro, seja pela defesa dos domínios e informações governamentais e militares ou pela própria repressão à fraude virtual, só estará completa caso os diferentes setores, públicos e privados, capacitem seus recursos humanos e invistam em tecnologia de proteção de modo a aumentar o escudo do espaço cibernético brasileiro. A cooperação entre empresas e órgãos governamentais será essencial à realização da tarefa.

Finalmente, em se mantendo este debate ativo, reforça-se a tarefa de evitar o efeito de um tipo de miopia, muito comum às decisões políticas atuais no Brasil, a qual permitem que apenas as soluções de curto prazo recebam a atenção devida, fazendo com que as visões de futuro e as decisões estratégicas de longo prazo permaneçam, invariavelmente, em segundo plano.

REFERÊNCIAS

BRASIL. ***Estratégia Nacional de Defesa***. Brasília: Ministério da Defesa, 2008.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. ***Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa***. Brasília, 2010.

_____. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. ***Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008***. Brasília, 2008.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. ***Livro Verde: segurança cibernética no Brasil*.** Claudia Canongia e Raphael Mandarino Júnior (org.). Brasília: GSIPR/SE/DSCI, 2010.

_____. Presidência da República. Secretaria de Assuntos Estratégicos. ***Desafios estratégicos para segurança e defesa cibernética.*** Organizadores: Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. Brasília, 2011

BISHARA, M. ***Um Inimigo Difuso***. Le Monde Diplomatique Brasil. Disponível em:<http://www.diplomatique.org.br/acervo.php?id=358>. Acesso em: 16 de julho de 2015.

BUZAN, Barry. WEAVER, Ole. WILDE, Jaap de. ***Security: A New Framework for Analysis.*** Boulder and London: Lynne Rienner Publishers, 1998.

CRUZ JÚNIOR, Samuel César da. ***A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual***. IPEA, 2013.

HAMMES, T. X. ***A Guerra de Quarta Geração Evolui, A Quinta Emerge.*** Military Review (edição brasileira), p. 16-27, set/out. 2007.

JOHNSON, Robert A. ***Prevendo a Guerra do Futuro*.** Doutrina Militar Terrestre em Revista, p. 68-82, ed. 006, 2014.

KEOHANE, Robert O. ***After Hegemony: Cooperation and discord in the world political economy.*** Princeton: Princeton University Press, 2005.

_____.; Nye, J. S. ***Power and interdependence***. 3 ed. New York: Longman, 2001.

MANDARINO JR., Raphael. ***Segurança e Defesa do Espaço Cibernético Brasileiro.*** Brasília, 2010.

MATTOS, Carlos de Meira. ***A Geopolítica e as Projeções de Poder***. In: Geopolítica. Vol I. Rio de Janeiro: Editora FGV, 2011.

MESSARI, N.; NOGUEIRA, J. ***Teoria das Relações Internacionais: Correntes e Debates.*** Rio de Janeiro: Elsevier, 2005.

METZ, Steven. ***Strategic Asymmetry***. *Military Review*, p. 23-31, Jul./Aug. 2001.

MORGENTHAU, Hans J. ***A Política entre as Nações: A luta pelo poder e pela paz.*** Brasília: Editora Universidade de Brasília: Imprensa Oficial do Estado de São Paulo: Instituto de Pesquisa de Relações Internacionais, 2003.

NYE, Joseph S. ***Intervenção, instituições e conflitos regionais***. In: Compreender os Conflitos Interacionais: Uma Introdução a Teoria e a História. 3. ed. Lisboa: Gradiva, 2002.

_____. ***Cooperação e Conflito nas Relações Internacionais***. 7 ed. São Paulo: Gente, 2009.

_____. **Is Military Power Becoming Obsolete?** Project Syndicate, Cambridge, 2010. Disponível em: < http://www.projectsyndicate.org/commentary/nye78/English >. Acesso em: 18 de novembro de 2015.

_____. ***Cyber Power***. Cambridge: Belfer Center for Science and International Affairs at Harvard Kennedy School, 2010.

PEDROSA, Afonso H. ***A transformação do Exército Brasileiro e o Fim da História.*** Doutrina Militar Terrestre em Revista, p. 66-74, ed. 005, 2014.

PINHEIRO, Fábio Ponte. ***A Cibernética como arma de combate***. Rio de Janeiro: Escola Superior de Guerra, 2013.

PRADO FILHO, Hildo Vieira. ***A Transformação do Exército Brasileiro e o novo Sistema de Ciência, Tecnologia e Inovação do Exército: contribuições para a Soberania Nacional.*** Rio de Janeiro: Escola Superior de Guerra, 2014

SARAIVA, J. F. S. (Org.) ***História das relações internacionais contemporâneas***. 3 ed. São Paulo: Saraiva, 2008.

WALTZ, Kenneth. ***Estruturas políticas***. In: Teoria das Relações Internacionais. Lisboa: Gradiva, 2002.

WEBB, D. C. ***ECHELON and the NSA*.** In: COLARIK, A. M.; JANCZEWSKI, L. J. ***Cyber warfare and cyber terrorism***. Nova Iorque, EUA: Information Science Reference, 2008.

WESTER, Franklin. ***Preemption and Just War: Considering the case of Iraq.*** Parameters, 2005.