UNIVERSIDADE DE SÃO PAULO
FACULDADE DE FILOSOFIA, LETRAS E CIÊNCIAS HUMANAS

Trabalho de graduação individual em geografia

A Ciberguerra:
Uma nova forma de confronto entre os Estados

Orientador: Prof. Dr. Andre Roberto Martin
Jhonny Bezerra Torres

São Paulo
2015

Cyberwar:
A new form of confrontation between states

Orientador: Prof. Dr. Andre Roberto Martin

Jhonny Bezerra Torres

São Paulo

2015

"A invenção do naufrágio é a criação do navio ou a invenção do acidente ferroviário é o surgimento do trem; é imperativo que questionemos a face oculta das novas tecnologias antes que ela se imponha, contra nossa vontade, à evidência"

Paul Virilio

Agradecimentos

Considero-me um homem de sorte, como tal, tenho uma lista imensa de pessoas importantes para agradecer por fazerem parte da minha vida e me proporcionarem a leveza fundamental em minha jornada; sem estas pessoas não chegaria à conclusão de que sou um homem de sorte.

Agradeço ao meu pai (Paulo) pela confiaça e fé incontestável em mim, obrigado por me ensinar que a força e sabedoria podem habitar em um único homem. Obrigado pela humanidade que brota em suas veias pulsar pelo meu corpo. A minha mãe (Paula), além de mãe, amiga e confidente; sua alegria e simplicidade me impedem de habitar um corpo vazio e cinzento. A minha irmã (Priscila) pelo cuidado e influência de irmão mais velho em meus caminhos (agradeço também pelas horas de formatação do presente trabalho hehehe).

Agradeço a minha grande companheira Isabela por sempre voar ao meu lado, pelo seu carinho e atenção diária, por ser o meu ninho e as minhas asas; obrigado por tornar minha vida mais bela. Agradeço também pelas horas de correção desse trabalho, sei que foi difícil (som característico para esse momento que só você sabe qual). A minha pequena Kakao, um dos motivos pelo qual ficar sentado horas lendo e escrevendo foi menos sofrido.

Á meus grandes amigos de bairro (Vila Progesso- Itaquera), ensino médio e bandas (The Dung´s, No Silence e Baratas HC), principalmente: Mabelo, Neguinho, Zé, John, Guilherme, Danilo e Leo (Negão); todos os demais que carrego no peito. Não há uma só vez que me recordo a tal época sem um sorriso no rosto.

Meus hermanos de faculdade e capadoçagem: Dudu, Mestre Lana, Niloboy, Felipe Ratus Passos, Alanzito, Daniboy, Mabelão e a todos aqueles que abraçei, cantei, beijei, dancei e brindei sob sol, lua ou chuva; vocês são a geografia que vim procurar na tão sonhada FFLCH. Ás flores da primavera.

A todos meus alunos que tive a sorte de conhecer e corregar algo de vocês junto a mim. Aos meus professores e orientador (Andre Martin) que atenciosamente compartilharam um pouco de seus conhecimentos e atenção nesses anos de faculdade. A todos aqueles que estão entrando em minha vida e hoje posso chamá-los de amigos.

Dedico esse trabalho ao meu grande tio Pedro, este que foi figura importantíssima em minha história e que hoje infelizmente não pode compartilhar comigo momento tão impar. Carrego a certeza de que está imensamente feliz pelas minhas conquistas onde quer que esteja.

Resumo

O domínio de novas técnicas e ferramentas de trabalho marca a história da humanidade; junto a isso, os grandes conflitos entre grupos escrevem suas linhas em algumas das páginas do livro da história humana. Ao que parece, as guerras vêm se modificando com a evolução dos domínios das técnicas; as revoluções industriais possibilitaram novas armas e, concomitantemente, mudanças na forma de se guerrear e nas relações entre os Estados. É nessa perspectiva que o presente trabalho busca estudar um novo tipo de choque entre os Estados; nascida com as atuais revoluções técnico científicas informacionais, estudaremos a gênese, possibilidades e relevância, para a atual geopolítica, da Ciberguerra.

Palavras-chave: Novos conflitos; conflitos virtuais; ciberarmas; Ciberguerra.

ABSTRACT

The domination of new techniques and work tools mark the history of mankind. Additionally, the major conflicts between groups write their lines in some of the pages of the human history book. Apparently, wars have been changing with the evolution of techniques domination; industrial revolutions enabled the appearance of new weapons and, concomitantly, changes in the way how wars are conducted and in the relationships between states. In this perspective, this paper seeks to study a new type of shock among states; originated with current scientific informational technical revolutions, we study the origin, scope and relevance to the current geopolitics of Cyber War.

Keywords: New conflicts; virtual conflicts; cyber weapons; cyberwar

Índice

Introdução

A evolução das técnicas é uma das responsáveis pela caracterização dos diferentes períodos da história, pois quando o homem adquire a capacidade de produzir novas ferramentas, inauguram-se novos períodos, novos tempos. Com o domínio do ferro, criou-se uma nova era, do mesmo modo que, com o motor hidráulico, motor a explosão, indústria química, energia elétrica e redes de informação, novos tempos chegaram. Junto com as técnicas, as guerras também inauguraram novos tempos; ascensão e queda de impérios e povos implicaram fases distintas na história humana.

Muitas vezes, o domínio das técnicas implicou a produção de novas armas, e, consequentemente, de novas estratégias e mudanças substanciais nos conflitos. Com as revoluções industriais, muitas guerras aconteceram a fim de se conquistar mercados para a produção em massa das indústrias, e com as tecnologias inauguradas pelas revoluções industriais, novas armas e, consequentemente, táticas e estratégias de guerras foram empregadas nas batalhas.

A partir da década de setenta, a terceira revolução industrial apontou para uma nova fase da história. A robótica, mecatrônica, computação e redes de informação começam a despontar e tomar seu lugar como caracterização do mundo contemporâneo. As novas tecnologias desta etapa da revolução industrial tornam-se cada vez mais importantes para os Estados e sociedade das últimas décadas do século XX e início do século XXI.

Sendo assim, não é de se estranhar que as últimas guerras do século XX (sobretudo a primeira Guerra do Golfo) já apresentassem características da terceira revolução industrial. A computação possibilitou o uso de GPS, aviões inteligentes e artilharia avançada em um conflito. A precisão da artilharia avançou a tal grau que fez com que nascesse o termo "guerra cirúrgica", ou seja, aquela que se estabelece com uma maior precisão dos armamentos desenvolvidos a partir de então. Porém, as tecnologias oriundas da revolução informacional foram utilizadas na última década do século XX somente como suporte para melhorar armas e, concomitante, estratégias militares já existentes.

É no século XXI, com a latente importância das redes de informáticas e computadores e da dependência dos Estados e sociedade sobre estas que nasce uma nova forma de guerra, a Ciberguerra. A Ciberguerra seria uma das novas formas de choque entre os Estados, o choque pelo meio cibernético, pelas redes cibernéticas.

Objetivo

O objetivo do presente trabalho é estudar como se desenvolveu a Ciberguerra, bem como suas possibilidades e relevância na contemporaneidade.

Pretendo analisar a hipótese de a Ciberguerrapoder ser considerada uma das novas estratégias de confrontos atuais, ou ao menos se essa indica uma das possibilidades de confrontos que podem ocorrer. É um objetivo, também, evidenciar a maior importância que os países, obviamente inclua-se o Brasil, devem dar a proteção do seu espaço cibernético mostrando como perigosa pode ser a Ciberguerra.

Justificativa

Parte-se do pressuposto de que as revoluções de domínios de novas técnicas, de uma maneira ou de outra, ditam novos períodos, assim como novas formas de se guerrear. Sendo assim, estudar o desdobramento da revolução técnico-científica sobre as atuais sociedades e a possibilidade de um novo tipo de conforto entre os Estados no ciberespaço, resuldado da revolução técnico-cientifica, é peça importante para analisar a relevância que se deve dar à maior proteção do espaço virtual.

Se o espaço virtual, as redes de informação e a computação tornaram-se no século XXI condição s*inequa non* para o funcionamento das sociedades atuais, visto que praticamente todo sistema bancário, econômico, infraestrutura interna e a própria defesa de uma país são, no mínimo, amparados pelas redes de informação, estudar conflitos ou mesmo possibilidades de conflitos no ciberespaço é vital para os atuais Estados.

Material e procedimento

Para elaborar o presente trabalho, encontro com dificuldade a pouca bibliografia a respeito do assunto, Ciberguerra, uma vez que este é ainda um tema muito novo e, consequentemente, ainda pouco estudado. Devido essa problemática, estruturei o trabalho em três diferentes períodos para que melhor entendêssemos a Ciberguerra.

Em uma primeira parte, estudaremos como as diversas revoluções no domínio de novas técnicas estão relacionadas com mudanças da sociedade como um todo e sobretudo novos tipos de conflitos; importância da internet para a contemporaneidade, gênese e vulnerabilidade das redes. Para tanto, utilizarei alguns autores que debruçaram seus estudos sobre o ciberespaço; o filósofo Paul Virilio, com sua obra "O Espaço Crítico", o sociólogo Manuel Castells, em "A Sociedade em Redes", e geógrafo Milton Santos, em "Por uma Geografia das Redes".

Posteriormente, em uma segunda parte, irei analisar, para evidenciar a importância da Ciberguerra, como novas táticas, armas e estratégias de guerra foram importantes no resultado de alguns dos mais emblemáticos conflitos da história. Para tanto, iremos inquirir parte dos estudos sobre a Guerra do Peloponeso, As conquistas Mongóis, Guerra de Secessão Norte Americana e as Guerras do Golfo.

Por fim, na terceira parte, Evidências da Ciberguerra, estudaremos os possivéis primeiros exemplo da Ciberguerra; a utilização dos vírus Stuxnet, Duqu, Gauss e Flamer contra Irã, Sudão e Síria, sendo o Stuxnet responsável pela danificação de parte do programa nuclear Iraniano.

Tendo trabalhado todas as partes, espero concluir evidenciando a maior importância que deve ser dada ao espaço cibernético e, concomitantemente, a possíveis confrontos neste âmbito.

O impacto das eras industriais sobre a "Nova Guerra", Guerra instantânea

1.1 Novas tecnologias e novas formas de guerra

A história da humanidade pode ser escrita por momentos de superação do meio e dominação de novas técnicas. Quando o homem dominou o fogo, houve a possibilidade de habitar lugares antes impensáveis; com o domínio dos metais, novos objetos foram construídos, e, paralelamente, novas formas de defesa; com a escrita, o registro histórico de um povo e seu legado puderam ser passados adiante; com a revolução industrial, a produção em massa foi alcançada. Tais eventos deixaram marcas na sociedade que os presenciou e, consequentemente, nas sociedades posteriores; hábitos, valores e ritmo de vida do homem anterior e posterior à Revolução Industrial são outros.

Não à toa, após a primeira Revolução Industrial, não só a produção passa ser acelerada, mas o tempo do indivíduo também (possivelmente nosso tempo biológico, mais lento, se distancie do tempo das máquinas, mais rápido). O tempo das cidades, pós revolução industrial, parece sempre ser mais rápido que o tempo do campo, por exemplo. A forma como uma determinada sociedade em uma dada época se reproduz no espaço deixa marcas nos indivíduos.

A própria maneira de se guerrear muda-se com a chamada "Era Industrial". Por exemplo, a guerra de secessão americana (primeira grande guerra pós revolução industrial): assim como as grandes indústrias que produziam produtos em massa, a guerra entre o norte e sul dos EUA também produziu a morte em massa.

> "Mas se essas inovações tecnológicas, por um lado, trouxeram inegavelmente tantos benefícios, não se pode deixar de refletir sobre o fato de que, a partir da Guerra de Secessão, também a morte passou a ser produzida em escala industrial." (MARTIN, 2006, p.249).

A Guerra de Secessão foi marcada pela primeira etapa da revolução industrial, ou seja, produção em massa e máquina à vapor; de maneira geral, todo o século VXIII foi definido pela primeira fase da Revolução Industrial. Com a Segunda Revolução Industrial, no século XIX, a produção continua em massa, porém acrescentou-se o motor à explosão. A Terceira Revolução Industrial começa no final da Segunda Guerra Mundial (1939-1945), porém tem sua pungência a partir décadas de 1970, trazendo consigo invenções no setor da robótica e, subsequentemente, na informática.

Se a Primeira e a Segunda Revolução Industriais foram decisivas para a formulação de uma nova sociedade, não diferente das demais, a Terceira Revolução também corroborou com mudanças no comportamento dos indivíduos e, concomitantemente, no da sociedade. As relações entre os Estados também foram modificadas no decorrer das revoluções, afinal, o Neocolonialismo Europeu sobre os continentes africano e asiático foi impulsionado pela busca de novos mercados para os produtos das indústrias inglesas no século XIX. Não poderíamos falar hoje em globalização, ou ao menos globalização financeira, sem que houvesse existido a revolução informacional, ou seja, a Terceira Revolução.

Tais mudanças tanto exigiram novas políticas dos Estados como, decorrentes das novas eras industriais, proporcionaram mudanças significativas nas relações entre os Estados; assim como, da mesma forma que o surgimento das indústrias pode ter mudado a forma e estratégia das relações entre os Estados, o aparecimento do computador e da informática pode ter feito o mesmo nas formas de conflitos entre estes atores.

O filosofo Paul Virilio, em seu livro "O Espaço crítico e as perspectivas do tempo real", analisa o impacto das novas tecnologias no espaço e concomitantemente na sociedade. No decorrer de sua obra, Virilio atenta para que no atual período histórico, torna-se cada vez mais difícil estudar a sociedade e o espaço, desconsiderando os avanços tecnológicos contemporâneos. (VIRILIO, 1993).

Evidenciando a transformação que as novas tecnologias geram em nossas vidas, Paul Virilio usa como exemplo um simples ritual de entrada em uma cidade, ou seja, a passagem de acesso as cidades em tempos diferentes. No passado, anterior à era dos computadores, a via de acesso à cidade era feita por uma porta ou um arco do triunfo, para se transformar em um sistema de audiência eletrônica. "A representação da cidade contemporânea, portanto, não é mais determinada pelo cerimonial da abertura das portas, o ritual das procissões dos desfiles, a sucessão de ruas e das avenidas; a arquitetura urbana deve, a partir de agora, relacionar-se com a abertura de um "espaço-tempo tecnológico" (VIRILIO, 1993, p. 10)

Para demonstrar a enorme importância das novas tecnologias e, principalmente, da rede de troca e armazenamento de informações (internet) para a humanidade, Paul Virilio classifica a informática e suas redes como um novo tipo de energia. Assim como o carvão, petróleo, gás natural e eletricidade tiveram enorme importância ao decorrer da história humana, a informática e suas redes são imensuravelmente importantes para o homem contemporâneo.

Carvão, petróleo, gás natural e eletricidade são, sem sombra de dúvida, cruciais para as sociedades contemporâneas, afinal, não se produz um computador sem o plástico vindo do petróleo, não se acessa a internet sem a eletricidade para ligar os computadores, e, sobretudo, não se transforma minerais em componentes eletrônicos sem que se aqueçam as caldeiras das siderúrgicas, geralmente com carvão, petróleo, gás natural ou eletricidade. Questionar a importância destas fontes energéticas para o modo de vida das diversas sociedades atuais é praticamente impossível. Porém, os fluxos de informações talvez sejam hoje a nova energia e elemento melhor definidor do começo dos anos 70 do século XX e primeiras décadas do século XIX. Ainda na década de noventa do século XX, Virilio escrevia: "Se a informática, suas redes, bancos de dados e terminais é, portanto uma energética, a informação transmitida é por sua vez um modo de formação que afetará amanhã os diferentes meios da organização em questão" (VIRILIO, 1993, p. 75).

Junto com Paul Virilio, Manuel Castell é outro autor que estuda o impacto da informática e suas redes nas sociedades atuais; sobre o tema, Castell destaca:

> "No fim do segundo milênio da Era Cristã, vários acontecimentos de importância histórica têm transformado o cenário social da vida humana. Uma revolução tecnológica concentrada nas tecnologias da informação está remodelando a base material da sociedade em ritmo acelerado. Economias por todo o mundo passaram a manter interdependência global, apresentando uma nova forma de relação entre economia, o Estado e a sociedade em um sistema geométrico variável (...). O próprio capitalismo passa por um processo de profunda restruturação caracterizado por maior flexibilidade de gerenciamento; descentralização das empresas e sua organização em redes ..." (CASTELL, 2000, p. 39).

Partindo do princípio que as Revoluções Industriais deixaram marcas nas sociedades, espaço e relações entre Estados, elas também podem ter produzido um novo tipo de confronto entre países, uma nova forma de guerra.

Em "A Sociedade Em Rede", Volume I, Manuel Castells dedica um capítulo para tratar da nova forma de guerra, a "Guerra instantânea", surgida após Segunda Guerra Mundial e característica da atual sociedade informatizada e tecnológica. Segundo Castell, "A morte, a guerra e o tempo são sócios seculares, e uma das características mais surpreendentes do paradigma tecnológico emergente é que essa associação seja fundamentalmente alterada ..." (CASTELLS, 2000, p. 547). Sendo assim, o tempo de duração

de uma guerra e a própria forma de fazer uma guerra foram alterados, as grandes carnificinas da primeira e segunda guerras mundiais e conflitos antecessores, juntamente com batalhas de longa duração de meses e anos, foram substituídos pela "Guerra instantânea".

No pós-Segunda Guerra Mundial e pungência da Guerra Fria, uma nova fase da história da humanidade e consequentemente das guerras foi escrita, as grandes potências adquiriram tamanha capacidade militar, ou capacidade tecnológica nuclear, que o choque entre os "Estados Potência" poderia representar a autodestruição mútua, junto à enorme quantidade e capacidade de destruição dos seus arsenais, um grande conflito entre as potência que colocaria em perigo todo o planeta. Com isso, o advento da tecnologia nuclear impossibilitou grandes conflitos entre as potências, sendo assim, enormes perdas humanas, como verificado em períodos antecessores à segunda guerra mundial, tornaram-se cada vez mais difíceis de acontecer.

É importante salientar que, no final da Segunda Grande Guerra, não só a tecnologia nuclear foi desenvolvida, mas também, de forma geral, a guerra propiciou um grande avanço tecnológico militar e civil. Os meios de comunicação se desenvolveram com o fim da guerra; a televisão, por exemplo, se popularizou na década de 50. Com desenvolvimento dos meios de comunicação, qualquer guerra poderia ficar mais próxima da opinião pública, de modo que imagens e acontecimentos de um conflito poderiam ser melhor transmitidos, visualizados e chegariam mais rápido à população. Junto ao desenvolvimento dos meios de comunicação, e a conseqüente veiculação das milhares de mortes de pais, maridos, filhos e irmãos em guerra fez com que a opinião pública passasse a ser um obstáculo cada vez maior para um conflito nos moldes da Primeira/Segunda Guerra e antecessoras. A Guerra do Vietnã e o movimento hippies são exemplo de como a opinião pública pode interferir em um combate.

A possibilidade de "holocausto planetário" por meio de armas nucleares, junto com a força da opinião pública, podem ter sido fatores deteminantes para evitar grandes conflitos armados entre as potências na segunda metade do século XX. "Contudo, interesses geopolíticos e confrontações sociais continuam a fortalecer a hostilidade internacional, interétnica e ideológica ao limite de objetivar-se a destruição física (...) desde o fim da guerra do Vietnã os estrategistas têm se esforçado para encontrar meios de ainda fazer a guerra." (CASTELLS, 2000, p. 547) Logo, para tornar a guerra possível e aceitável de acontecer perante a sociedade, os estados democráticos tomaram três medidas práticas, segundo Castells:

- Não deve envolver cidadãos comuns, portanto deve haver um exército profissional;
- Deve ser curta, até mesmo instantânea;
- Deve ser limpa, cirúrgica, dentro de limites razoáveis e escondida o máximo possível da visão pública.

Estaríamos, então, em uma nova fase dos conflitos militares, a fase das guerras instantâneas. Uma nova fase, gerada por avanços tecnológicos, sobretudo na esfera da tecnologia nuclear, só pôde ser concretizada por avanços em tecnologia de ponta e novas estratégias militares. Porém, acredito que avanços na tecnologia militar podem ser vistos no mínimo de duas maneiras:

- Os avanços podem ser destinados à obtenção de armas mais desenvolvidas tecnologicamente, como um tanque mais eficiente, um rifle mais preciso, monitoramento por radares mais modernos, etc.
- Talvez obedecendo aos princípios da "Guerra instantânea", ou seja, que haja um exército profissional, que seja limpa, cirúrgica e escondida ao máximo da visão pública; a Ciberguerra. Ou seja, a utilização da internet não apenas como uma ferramenta de comunicação e logística, mas sim como uma arma de espionagem e ataque contra outros Estados.

1.2 Importância da internet para os países contemporâneos

Vale ressaltar que, conforme VIRILIO (1993), as redes de informação são um tipo de energia junto a outras como o gás, carvão, petróleo e eletricidade; tais energias teriam grande importância no decorrer da história da humanidade e várias batalhas ocorreram pela disputa do controle dessas. Sendo os fluxos de informação, hoje, tão importantes para a contemporaneidade (como tais energias), logo os fluxos de informação (tecnologia de informação) são alvo dos Estados.

Considerando que o atual sistema capitalista passa por uma reformulação promovida pela revolução informacional, ou terceira revolução industrial, hoje seguramente não se

poderia imaginar a economia capitalista sem a existência da internet. No presente, vivemos sobre a lógica da economia capitalista globalizada, mercados financeiros, bolsas de valores, imensa quantidade de fortunas inexistentes senão em telas de computadores são o reflexo do momento vivido.

> "Este novo mundo em que passamos a viver na Era Digital vem permitindo às grandes potências mundiais a organização de uma nova ordem mundial, representada pela padronização e aglutinação de tudo aquilo que marca a vida da sociedade global: moeda, usos e costumes, hábitos alimentares e até a própria maneira de pensar" (LUCCI, 2011, p. 13).

Recentemente, uma pesquisa realizada por uma empresa de consultoria americana, Boston Consulting Group (BCG), divulgou dados impressionantes sobre a internet; dados que demonstram um pouco da grande importância da rede. Segundo Boston Consulting Group, até 2016 haverá 3 bilhões de usuários de Internet no mundo, atingindo quase metade da população mundial da atualidade. Somente nos países participantes do G-20 (19 economias mais desenvolvidas do mundo e a União Europeia) a economia da Internet até 2016 irá atingir 4,2 trilhões de dólares; com essa cifra, a economia da internet nos próximos anos estaria entre as cinco maiores, perdendo apenas para EUA, China, Japão e Índia, segundo a pesquisa.

Ainda se considerarmos os 4,2 trilhões de dólares promovidos pela internet até 2016, essa cifra seria maior que o PIB da Alemanha de hoje, 3,875 trilhões (FMI). Ainda segundo a pesquisa do Boston Consulting Group (BCG), a Internet chega a contribuir com 8% do PIB em algumas economias dos países do G20; a pesquisa também atenta para a importância da internet na geração de empregos nas 20 maiores economias mundiais (DEAN et. al., 2012).

Para se ter ideia da potência e importância da internet para o mundo contemporâneo, basta que analisemos o desempenho das maiores corporações globais atuais. Segundo o ranking Brandz 2014[1], entre as cinco marcas mais valiosas do mundo, quatro são da área tecnológica; a marca Google é a mais valiosa, valendo US$ 158,8 bilhões, seguida pela Apple para US$ 147,8 bilhões, IBM US$ 107 bilhões, Microsoft US$ 90,1 bilhões e

[1]BrandZ é um banco de dados que detém dados de mais de 650 mil consumidores e profissionais de 31 países, comparando mais de 23.000 marcas. O banco de dados é usado para estimar as avaliações da marca para gerar uma lista das 100 maiores marcas globais.

McDonald's, US$ 85,7 bi. A supervalorização dessas empresas demonstra, de certa forma, a grande potencialidade econômica que a internet é atualmente:

BRANDZ™

	MARCA	CATEGORIA	VALOR $M
1	Google	TECNOLOGIA	158,843
2		TECNOLOGIA	147,880
3	IBM	TECNOLOGIA	107,541
4	Microsoft	TECNOLOGIA	90,185
5		FAST FOOD	85,706
6	Coca-Cola	REFRIGERANTE	80,683
7	VISA	CARTÃO DE CRÉDITO	79,197
8	at&t	TELECOMUNICAÇÕES	77,883
9	Marlboro	TABACO	67,341
10	amazon.com	COMÉRCIO ELETRÔNICO	64,255

Figura 1: As 10 maiores Marcas globais de 2014. Fonte modificada: MILLWARD BROWN (2014)

Para se explicar a tamanha importância atual das empresas de tecnologia, é necessário que entendamos um pouco melhor a expansão e popularização da internet.

A expansão da internet acontece de maneira rápida e começa, sobretudo, na década de noventa; o crescimento da rede mundial de computadores trouxe consigo uma nova fase na história da humanidade, como podemos observar na figura anterior: das dez maiores companhias do mundo, sete trabalham diretamente com tecnologia da informação, sendo dependentes da rede de computadores. As duas figuras a seguir nos ajudam a visualizar melhor a rápida expansão da internet em apenas dez anos entre 1998 (Fig. 2) a 2008 (Fig. 3):

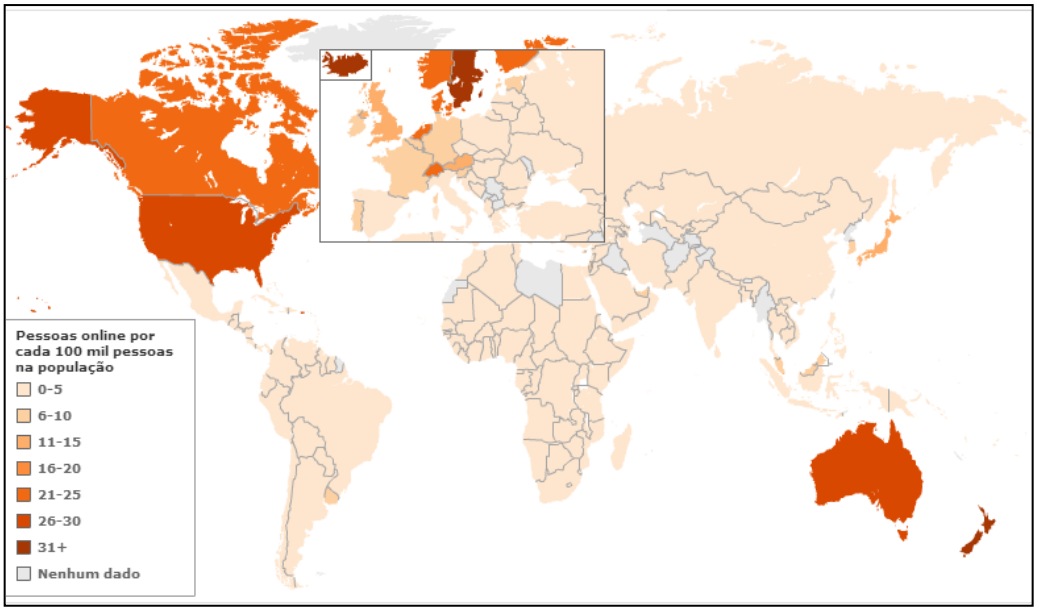

Figura 2: Uso da internet no mundo em 1998. Fonte: BBC (2010)

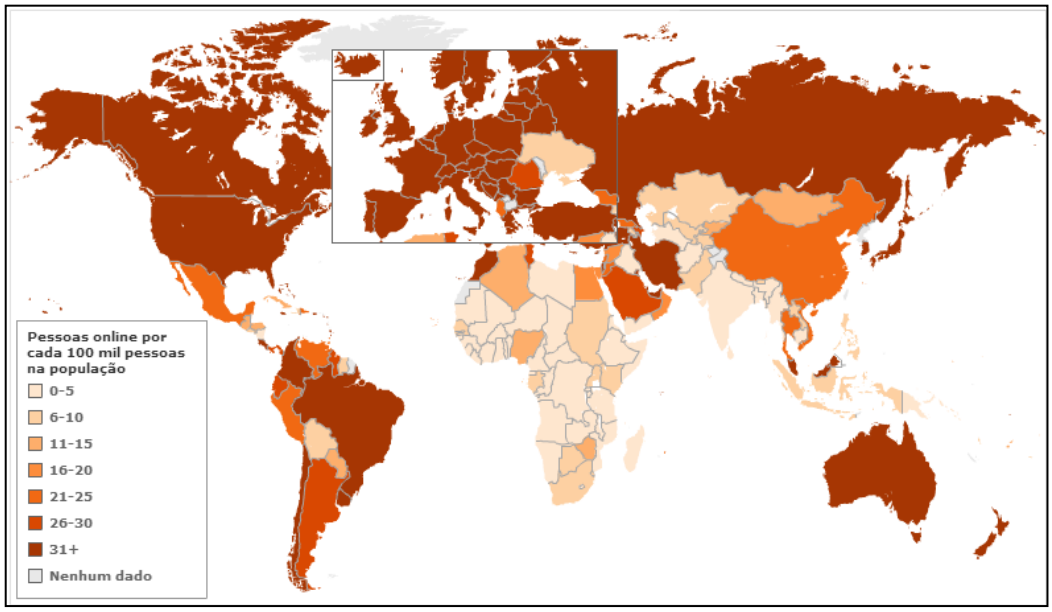

Figura 3: Uso da internet no mundo em 2008. Fonte: BBC (2010).

Só no Brasil, em 2013, o número de pessoas com acesso à internet chegou a 105,1 milhões (Dados do IBOPE em 2013), com população estimada para o mesmo período em 201.032.714 habitantes, segundo dados do IBGE (Instituto Brasileiro de Geografia e Estatística). No mesmo ano, "O número de aparelhos celulares ativos no Brasil, chegou a 267 milhões", segundo dados da ANATEL (Agência Nacional de Telecomunicações).

Ainda em um estudo realizado pela ComScore[2], em 2012, encomendado pela IAB Brasil (InteractiveAdvertising Bureau Brasil), apresenta dados que mostram a preferência dos o brasileiro, que tem acesso a internet e outras mídias pela primeira. O estudo revela também que 42% dos brasileiros passam pelo menos duas horas por dia conectados à internet. Comparado com a televisão, somente 25% dos brasileiros, com acesso à internet e televisão, passam 2 horas ou mais em frente à TV; já se pode afirmar que entre os brasileiros com acesso a mídias como televisão, rádio e internet, a internet é a favorita.

O Brasil também ganha destaque no número de smartphones[3] com as vendas deste tipo de aparelho aumentando todo ano (Fig. 4). O país já é o quarto do mundo com 70 milhões de aparelhos, segundo dados da consultoria Morgan Stanley[4]. Ainda segundo esta consultoria, um usuário de smartphone o consulta, em média, 150 vezes por dia. Em reportagem do portal G1, já se destacava em 2012 que o número de smartphones no mundo iria triplicar até 2018 conforme prevê a fabricante de equipamentos de telecomunicações Ericsson, sendo que o número de smartphones no mundo já somava 1,1 bilhão naquele ano (PORTAL G1, 2012).

Figura 4: Venda de *smartphones* no brasil entre 2010 – 2014 segundo *International Data Corporation* (IDC). Fonte: CARRENHO (2014).

[2]ComScore é uma empresa dos EUA, líder de tecnologia de internet que fornece Análises sobre o Mundo Digital.

[3]Telefone celular com sistema operacional capaz de estabelecer conexão com sites da internet.

[4]Morgan Stanley é uma empresa global de serviços financeiros sediada em Nova York. O Morgan Stanley opera em 42 países e possui mais de 1300 escritórios e 65.000 funcionários. O Morgan Stanley também é o maior banco de investimentos do mundo com 18.000 corretores de valores e ativos superiores a 1.7 trilhões de dólares.

Outro estudo divulgado pela revista EXAME, com base no mesmo relatório da fabricante de equipamentos de telecomunicações Ericsson, diz que metade da população mundial estará utilizando internet 3G até 2017: "Cerca de 85% da população mundial contará com cobertura de Internet móvel de terceira geração (3G) até 2017, enquanto 50% desse contingente estará coberto pela quarta geração da telefonia móvel (4G) dentro do mesmo período"(EXAME, 2012).

Sendo assim, podemos perceber que a internet tornou-se fundamental para a economia mundial e, sobretudo, para os países mais desenvolvidos do sistema capitalista. Até o momento, analisamos principalmente a importância da internet na economia, embora saibamos que rede mundial de computadores já tenha se tornado fundamental para troca e armazenamento de informações de todos os tipos, uma vez que a importância econômica da rede pode representar melhor seu papel fundamental na atual fase do capitalismo financeiro.

Por conseguinte, não poderia deixar de destacar a internet com veículo importante também para a organização interna dos Estados atuais. O sistema financeiro, por exemplo, é imperioso para o funcionamento destes, a mesma rede de computadores que torna possível o atual funcionamento da economia, ou seja, a internet, também é fundamental hoje para manutenção da infraestrutura que da suporte aos Estados Nacionais. Embaixadas, ministérios, congresso, senado, sistema de energia, água, manutenção de trânsito, controle de entrada e saída de um país, hoje são amparados pela internet.

Ainda em 1993, o filósofo Paul Virilio destacava em o "Espaço Crítico" que "A invenção do naufrágio é a criação do navio ou a invenção do acidente ferroviário é o surgimento do trem" (VIRILIO, 1993, pagina 65); da mesma forma, o surgimento e dependência dos países com relação à rede mundial de computadores (internet) também criou uma nova fragilidade para os Estados e, consequentemente, a possibilidade de novos tipos de ataques e guerras entre os países, a própria ciberguerra.

A Internet

2.1 Internet

> "A Internet é o tecido de nossas vidas. Se a tecnologia da informação é hoje o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quanto motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana" (CASTELLS, 2003, p. 7).

O processo de criação da internet nos ajuda a entender no que ela consiste, por tal motivo iremos a seguir analisar a formação e estruturação da internet; porém, de uma maneira geral, a internet é uma rede de fios, cabos e sinais de satélite, infraestrutura, que permite comunicação e relações entre seus usuários (SANTOS, 1996). Embora seja uma rede de infraestrutura que possibilita a interligação das antípodas, a internet não se resume somente a isso; a internet não é simplesmente uma tecnologia; é o meio de comunicação que constitui a forma organizativa de nossas sociedades (CASTELLS, 2003). Ela está completamente incrustada na sociedade:

> "Internet é sociedade, expressa os processo sociais (...) ela constitui a base material e tecnológica da sociedade em rede. (...) Esta é a sociedade (...) cuja estrutura social foi construída em torno de redes de informação a partir de tecnologia de informação microeletrônica estruturada na internet. Nesse sentido, a internet não é simplesmente uma tecnologia; é o meio de comunicação que constitui a forma organizativa de nossas sociedades; é o equivalente ao que foi a fábrica ou a grande corporação na era industrial."(CASTELLS, 2003, p. 286-287).

2.2 Origem Militar da Internet

A internet tem sua origem nas forças armadas americanas; como tal, foi projetada para dar subsídios à proteção dos interesses americanos. Porém, a internet como a conhecemos hoje sofreu diversas transformações que não foram propriamente realizadas pelos meios militares; a internet transformou-se a rede de informações que temos hoje graças aos meios científicos e, posteriormente, aos seus primeiros usuários que a moldaram.

A internet nasce entre as décadas de cinquenta e sessenta do século XX. Surge no período de guerra fria, em meio à bipolaridade mundial, em um mundo no qual duas forças hegemônicas, Estados Unidos e URSS (União das Repúblicas Socialistas Soviéticas), disputavam palmo a palmo, quaisquer que fossem os campos de batalha. Em tal perspectiva, o mundo vivia um período de extrema tensão militar, e é nesse panorama que a Internet surgiu; primeiramente como instrumento de defesa para posteriormente ser difundida e popularizada no âmbito civil (MIRANDA,2007).

Na década de 50, nos Estados Unidos, já havia uma espécie de "sistema de redes" que interligava as bases militares do país, ou seja, uma "espécie de internet", porém esse sistema baseava-se unicamente na interligação entre as bases americanas para facilitar o contato rápido e exclusivo entre elas, embora não se tratasse de uma rede propriamente (CASTELLS, 2003). A grande diferença entre a internet em rede e o antigo sistema militar que interligava as bases militares Norte Americanas reside no fato de que as informações que esse antigo sistema continha encontravam-se concentradas unicamente no Pentágono, ou seja, o Pentágono utilizava seu sistema de interligação com as bases militares pura e unicamente para transmitir ordens (CASTELLS, 2003).

Diferente da internet, em que as informações contidas na rede não se concentram em um único ponto, a antiga rede de fios e cabos (semelhantes a ela) que interligava as bases militares americanas possuía um único ponto concentrador de dados. Um ataque direto ao Pentágono poderia destruir ou trazer a público informações sigilosas dos EUA; a convergência de informações no Pentágono também tornava os Estados Unidos um pais mais vulnerável a ataques inimigos. (CASTELLS, 2003).

No final da década de cinqüenta, o governo norte americano deu o primeiro passo decisivo para a criação da internet, criou-se a ARPA (*AdvancedResearchProjectsAgency)*. Motivado pelo lançamento do satélite soviético Sputnik em 1957, os EUA lançam um plano de investimentos massivo em tecnologia integrando pesquisadores científi-

ficos e meios militares com objetivo de obter superioridade tecnológica, ou competir com os avanços soviéticos. Temendo um ataque às suas bases militares e de pesquisas, a Agência de Pesquisas Avançadas (ARPA) procurou um bom meio de compartilhar suas principais informações, descentralizando-as. Ou seja, era preciso criar uma rede que possibilitasse a comunicação entre as bases militares de modo que, em caso de ataques ao Pentágono, por exemplo, as informações estratégicas militares não estivessem centralizadas em um único lugar, consequentemente, não sendo perdidas. Assim sendo, em 1967 foi criada a ARPAnet (CASTELLS, 2003),a rede de computadores capaz de fazer com que as informações permanecem circulando em uma rede, evitando a centralização de dados.

Totalmente financiada pelo governo norte americano e claramente com fins de defesa militar, a ARPANET ficou conhecida como a "Mãe da Internet". É inegável que a ARPANET foi à precurssora da Internet com a conhecemos hoje, porém o percurso de transformação, e ou evolução, da ARPANET até a internet fugiu ao domínio militar. Cientistas não ligados aos meios militares e usuários da rede de computadores foram os responsáveis pela renovação e remodelação da rede com o passar do tempo até chegar ao que a constitui nos dias atuais.

Nos anos 1970, algumas universidades e outras instituições que faziam trabalhos relativos à defesa militar, tiveram permissão para se conectar à ARPANET. Porém, é somente na década de oitenta, com o enfraquecimento da Guerra Fria, que a ARPAnet foi difundida para a grande maioria das universidades americanas. Para se ter uma ideia da grande difusão da ARPANET na década de oitenta, comparemos as duas figuras a seguir, a primeira de setembro de 1971 e a segunda após a liberação para quaisquer meios de pesquisas interessados em usar a ARPANET, de outubro de 1980 (MIRANDA,2007).

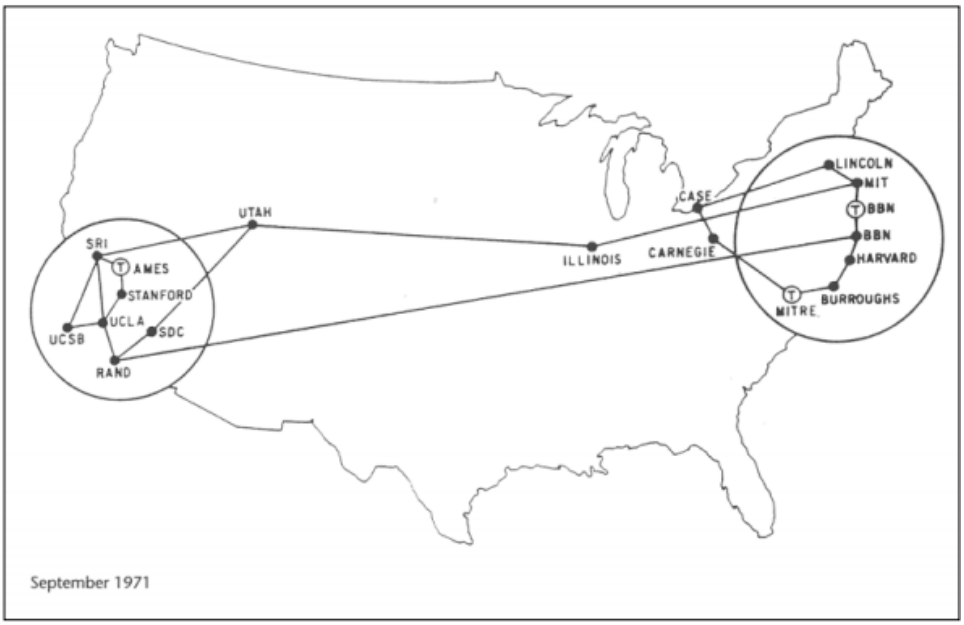

Figura 5: Distribuição da rede da ARPANET nos EUA em setembro de 1971. Fonte: HUMBOLDT (2007).

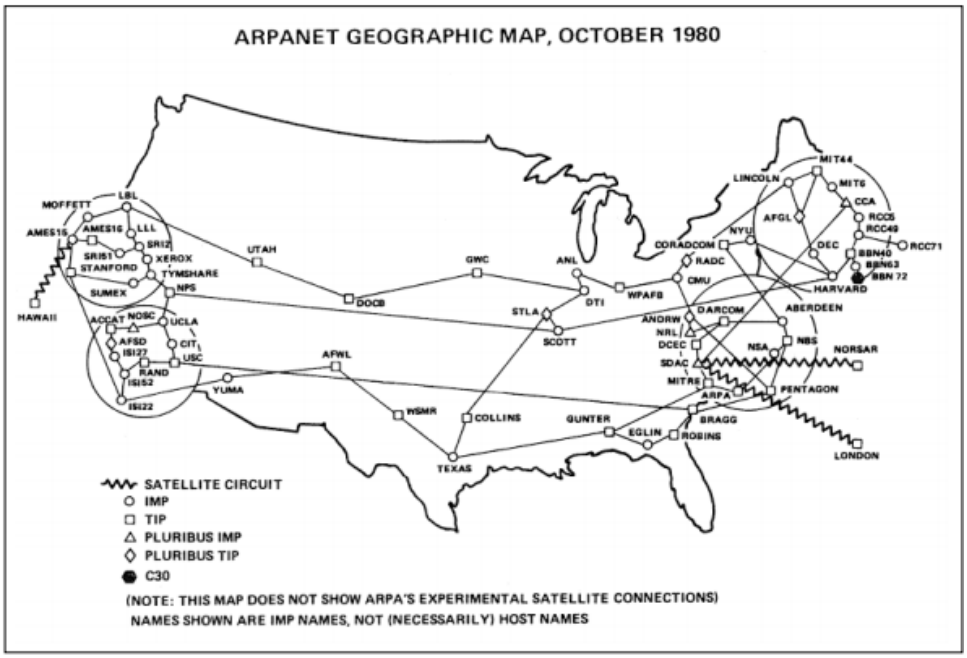

Figura 6: Distribuição da rede da ARPANET nos EUA em outubro de 1980. Fonte: HUMBOLDT (2007).

Com a grande expansão da ARPANET na década de oitenta, os militares americanos criam uma nova rede de uso exclusivo militar: A MILNET (Military Network) de 1983; mais tarde ela passa a se chamar INPRNET. A ARPANET na década de 1990 foi modificada e passou agora a ser controlada pela pelos civis, na década 1990, finalmente o nome ARPANET foi substituído por INTERNET.

2.3 Estrutura da Internet

A internet, em visão simplificada, é uma rede de computadores interligada. Portanto, para melhor entender a estrutura da internet seria necessário debruçar sobre a conceptualização do que seria uma rede. Como o objetivo do presente trabalho não é se ater às concepções e infraestrutura da internet em si, ou sequer trabalhar com as redes do ciberespaço, não irei me dedicar a estudar as redes da internet por si só. Porém, para evitar o que Milton Santos alerta, "a polissemia do vocábulo tudo invade, afrouxa seu sentido e pode, por isso, prestar-se à imprecisão e ambiguidade" (SANTOS, 1996, pagina 261), faço menção à definição de rede do geógrafo Amadeu Cardoso Junior:

> "Defini a rede como toda infra estrutura que permite o transporte da matéria, de energia ou de informação, e que se inscreve sobre um território, caracterizando-se pela topologia de seus pontos de acesso ou pontos terminais, seus arcos de transmissão, seus nós de bifurcação ou de comunicação. Mas a rede é também social e política, pelas pessoas pelas mensagens, valores que a frequentam, a rede na verdade é uma mera abstração" (JUNIOR, 2008, p. 5).

A rede de computadores Internet representa muito mais do que a simples interligação entre dois ou mais computadores, porém esta também o é. Sendo assim, para que a internet exista, é necessário termos mais de dois computadores que possam se interconectar e trocar informação em uma rede cabos, fios e sinais de satélite. Também podemos dividir os meios de comunicação em dois: comunicação orientada (fios de cobre, fibra ótica e rede elétrica) e meio de comunicação não orientado (ondas de rádio, micro-ondas, satélites). O acesso à internet pela rede elétrica representa uma opção vantajosa, visto que não dependeria da construção de uma nova infraestrutura (MIRANDA,2007).

É possível acessar a Internet utilizando qualquer desses meios, desde que se utilize os protocolos adequados. Atualmente, a estrutura física da Internet compreende cabos de fibra-ótica intercontinentais, rede telefonia pública e comunicação sem fio. Assim, para se conectar a Internet, basta ter acesso a rede telefônica, cabos ou comunicação sem fio interligados a uma Espinha Dorsal (estrutura principal da rede) da Rede Mundial de computadores (MIRANDA, 2007).

Os Backbones são a "espinha dorsal" da rede (Fig. 7). Backbones são computadores super desenvolvidos capazes de interligar uma região a outra, ou seja, eles são os pontos de intersecção da rede; os Backbones são o ponto central na Internet em rede. Para que um usuário acesse a internet ele precisa ter um computador ligado a uma rede; a rede nada mais é que o meio de conexão de seu computador em uma trama de fios de cobre, fibra ótica e rede elétrica (comunicação orientada) ou por ondas de rádio, micro-ondas, lazer e satélites (meio de comunicação não orientado) interligando seu computador a um Blackbone. A internet seria então formada por uma rede Blackbones interligada e hierarquizada; os Blackbones são hierarquizados, pois são divididos em regionais, estaduais e nacionais.

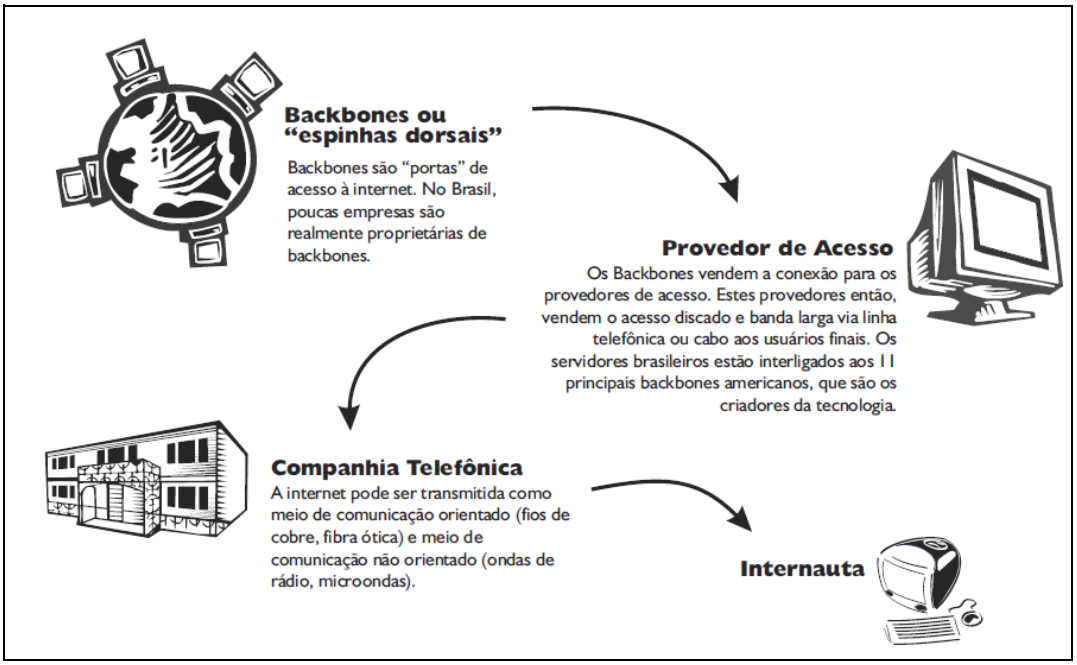

Figura 7: Ilustração da infraestrutura da Internet evidenciando a importância dos Backbones.Fonte: ONDA (2004).

Outro equipamento fundamental para o funcionamento da internet é o roteador. O roteador é responsável por direcionar o tráfego de dados em uma rede; direcionar os dados por pontos na rede, ou seja, ele decide qual é o melhor caminho a ser percorrido pelo fluxo de dados até seu destino. Sem os roteadores, a internet ficaria "congestionada"; a principal função dos roteadores é decidir qual o melhor caminho na rede que determinados fluxos de dados devem seguir sem que a rede fique "congestionada". Sempre que enviamos uma mensagem para outro computador, o roteador procura na rede caminhos que possibilitem a maior velocidade desta ao

destinatário.

Na figura a seguir é mostrada a localização dos Backbones da Rede Nacional de Ensino e Pesquisa (RNP)[5], denominado rede ipê (Fig. 8). Esta rede foi projetada para atender a certos requisitos técnicos, garantindo a largura de banda necessária ao tráfego Internet de produção (navegação Web, correio eletrônico, transferência de arquivos); ao uso de serviços e aplicações avançadas; e à experimentação. Há 27 pontos de presença (PoPs)[6]instalados em todas as capitais do país, interligando cerca de 600 unidades de instituições de ensino e pesquisa e algumas iniciativas de redes regionais, principalmente redes estaduais e redes metropolitanas de ensino e pesquisa(RPN, 2014).

[5]A RNP (Rede Nacional de Ensino e Pesquisa) é uma Organização Social (OS) vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e mantida por esse em conjunto com os ministérios da Educação (MEC), Cultura (MinC) e Saúde (MS).A RNP nasceu em 1989, e é conhecida por ter aberta o primeiro backbone para a chegada da Internet no Brasil, em 1991

[6]Os Pontos de Presença, na sigla em inglês POP (Point OfPresence), são pontos de acesso a espinha dorsal (backbone) da Internet. Os provedores de acesso a rede possuem um ou mais pontos de presença que lhe garante acesso a rede de computadores, ou seja, um usuário quando quer acessar a internet primeiro precisa contratar um provedor que possui um POP; o POP ou ponto de acesso, acessa a rede de backnones. (Fonte: http://tecnologia.uol.com.br/dicionarios/dicionario-p.jhtm acesso 20/11/2009)

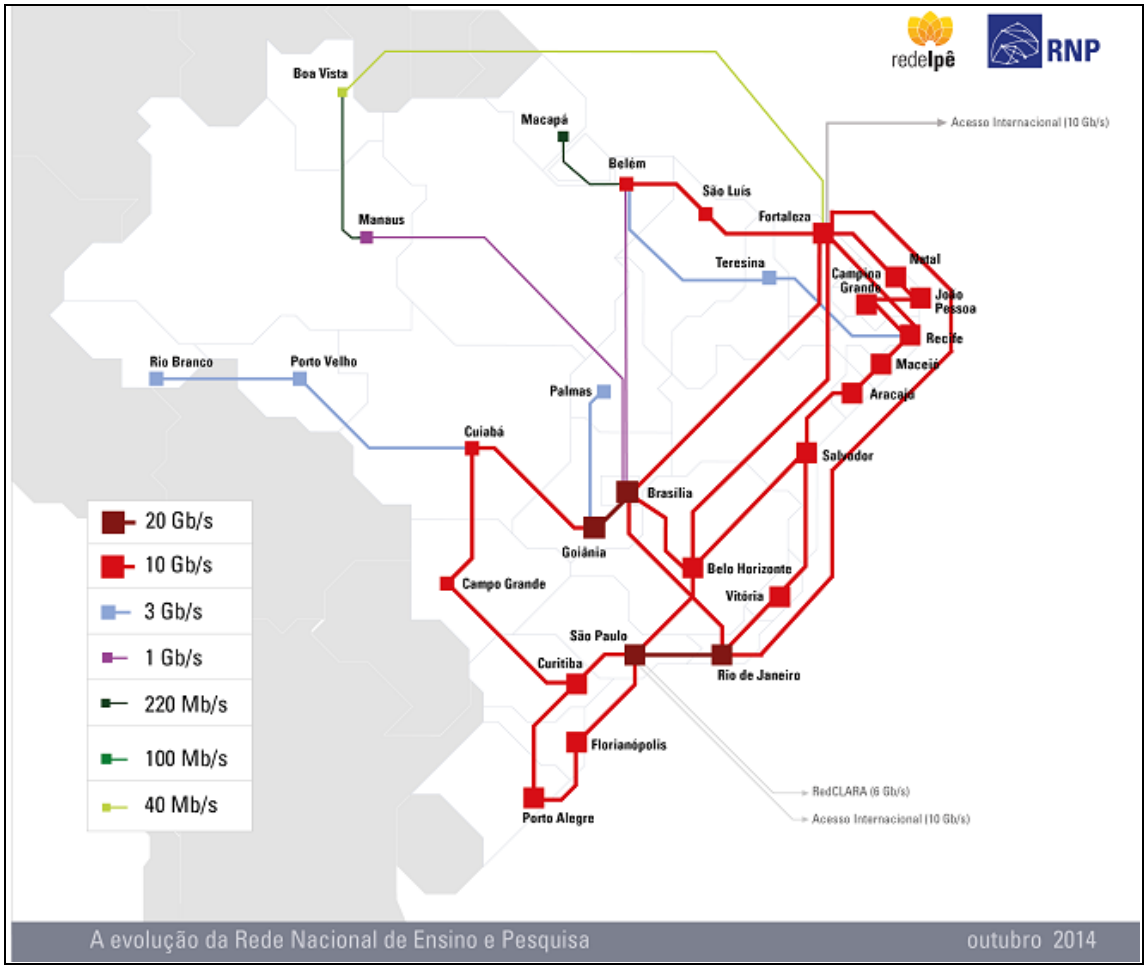

Figura 8: Topologia da rede Ipê.Fonte: RNP (2014).

Outro exemplo, porém, de backbones intercontinentais, é a conexão entre Brasil, Estados Unidos e Europa (Fig. 9). Na figura a seguir, o Backbone de São Paulo está interligado ao Backbone de Atlanta e Tampa Bay, ambos nos Estados Unidos (ressalto que a figura é apenas uma simplificação e que também há a interligação do Brasil aos Estados Unidos por meio de outros Backbones). Desse modo, os Estados Unidos se comunicam com a Europa por meio do Backbone de New York, que se comunica com os Backbones de London, Frankfurt e Paris.

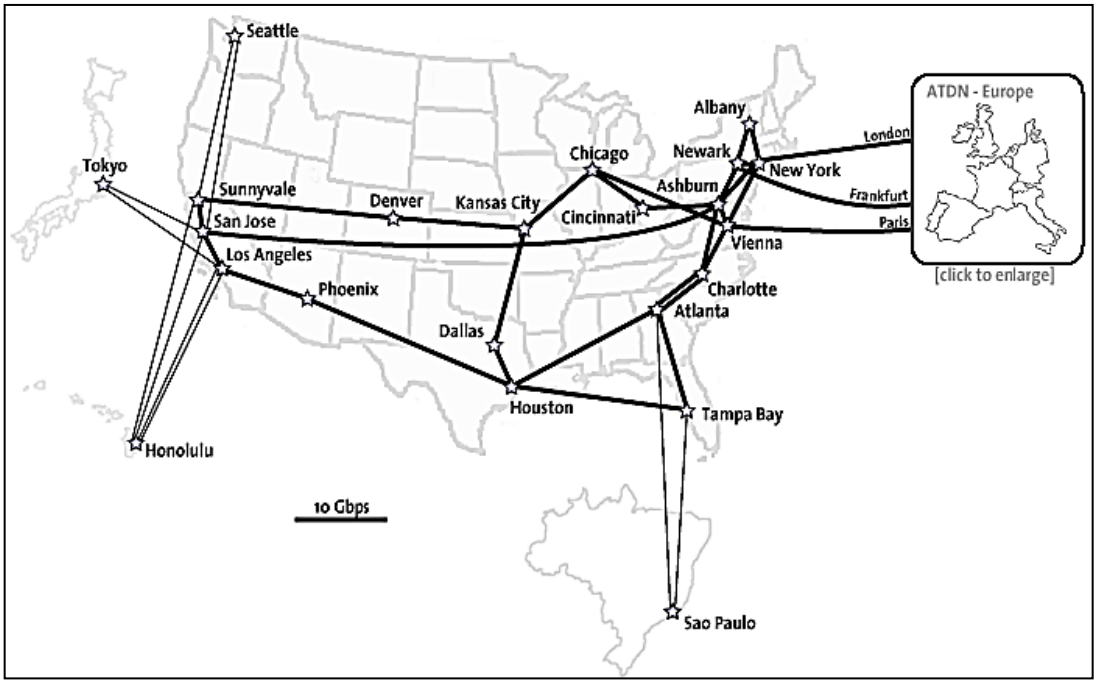

Figura 9: Backbone intercontinentais.Fonte: ATDN (2003).

2.4 Vulnerabilidades da Internet

Como já dito anteriormente, a internet se originou da necessidade dos militares norte-americanos de descentralizar informações estratégicas militares de um único ponto de concentração, o Pentágono. Sendo assim, a internet foi estruturada de modo que o fluxo de informações seja contínuo entre as instituições participantes, não acumulativo em um único lugar, e em ocorrência de um ataque, a uma base militar, ou qualquer outra instituição, a conexão não seja interrompida.

A próxima figura apresenta de forma esquemática como a internet consegue proteger informações importantes e dificultar que haja interrupção de comunicação entre pontos, ou computadores, de uma rede; nela represento sete pontos distintos interligados na mesma rede (Fig. 10).

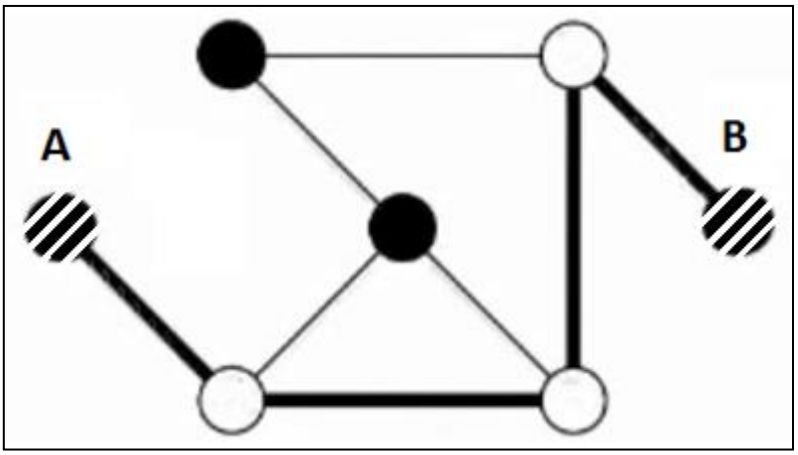

Figura 10: Informações enviadas de um computador A para o computador B. O fluxo de informação transmitido está representado pela linha grossa e os pontos por onde este passa pelas bolinhas brancas ou vazias. Fonte: Figura modificada pelo autor com base no documentário "History of the Internet" de BILGIL(2009).

É importante notar que a informação enviada pelo ponto ou computador A (também podemos representar cada um desses pontos na figura como sendo bases militares, ressaltando a origem militar da internet) para o ponto B tem mais de uma possibilidade de chegar até seu destino. Cada um desses pontos consegue armazenar informações importantes e ao mesmo tempo trocá-las de forma rápida entre todos da rede. Em caso de um ataque inimigo a um ponto desta rede, dados, segredos, estratégias, documentos importantes não seriam perdidos, ou dificilmente perdidos, visto que existe uma rede de trocas célere e constante de dados entre os computadores da rede. Na figura a seguir é retratado um ataque a um dos pontos de ligação da rede; tal ataque poderia impedir a troca de dados entre os pontos A e B (Fig. 11).

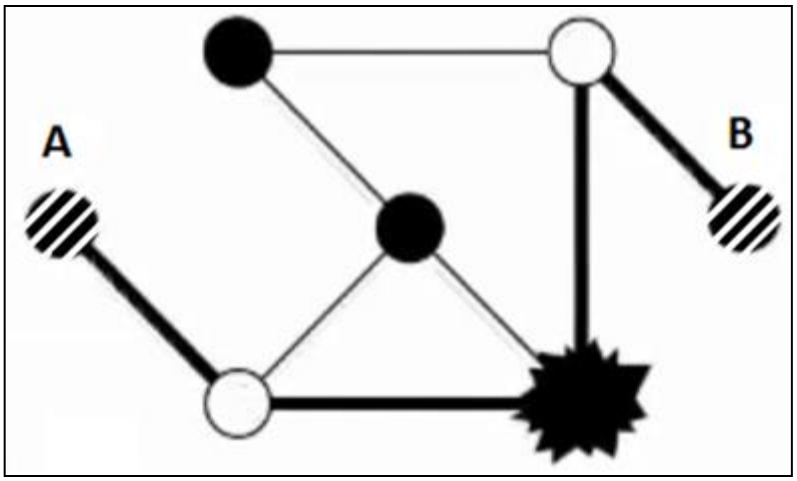

Figura 11: Informações enviadas de um computador A para o computador B sofrem um bloqueio em seu percurso por um ataque em um ponto na rede. O fluxo de informação transmitido está representado pela linha grossa e os pontos por onde este passa pelas

bolinhas brancas, ou vazias. Fonte: Figura modificada pelo autor com base no documentário "Historyofthe Internet" de BILGIL (2009).

Circunstancialmente em um ataque inimigo à rede, a comunicação entre os dois pontos ou bases A e B não será perdida. Como a rede possui vários pontos de conexão a informação é desviada para um outro caminho que conecte o ponto A ao B, possibilitando que a informação siga para seu destinatário (Fig. 12).

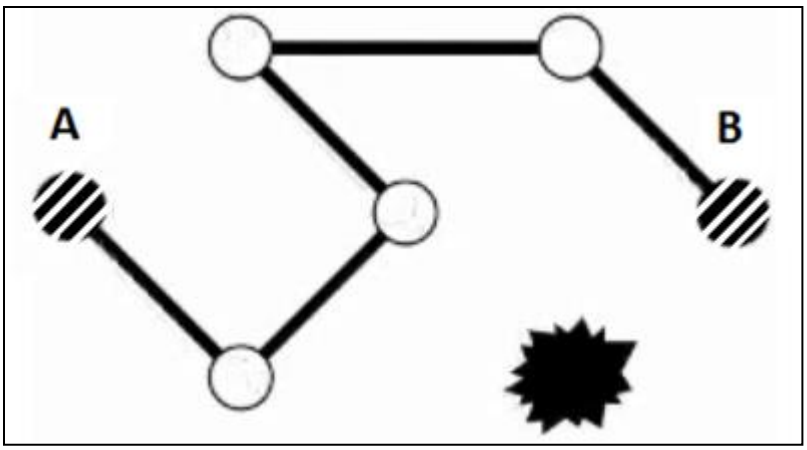

Figura 12: Informação enviada do ponto A para o ponto B consegue chegar até seu destino mesmo com um ponto na rede destruído ou danificado. O fluxo de informação transmitido está representado pela linha grossa e os pontos por onde este passa pelas bolinhas brancas, ou vazias. Fonte: Figura modificada pelo autor com base no documentário "Historyofthe Internet" de BILGIL (2009).

Como demonstrado, a internet é um meio muito eficaz de comunicação que quase impossibilita que a informação seja cortada entra dois pontos, ou mesmo que a rede e, concomitante, a comunicação entre bases distribuídas geograficamente seja cortada. Embora as figuras analisadas anteriormente demonstrem como é feita a conexão entre dois computadores ligados a uma rede de computadores de apenas sete pontos de conexão, ela é uma boa simplificação didática para demonstrar a capacidade da rede em encontrar caminhos para o fluxo de dados; como podemos conferir na figura a seguir, a internet tem muito mais que apenas sete "nós", concomitantemente muito mais possibilidades de caminhos para o fluxo de dados do que demonstrado nas simplificações anteriores.

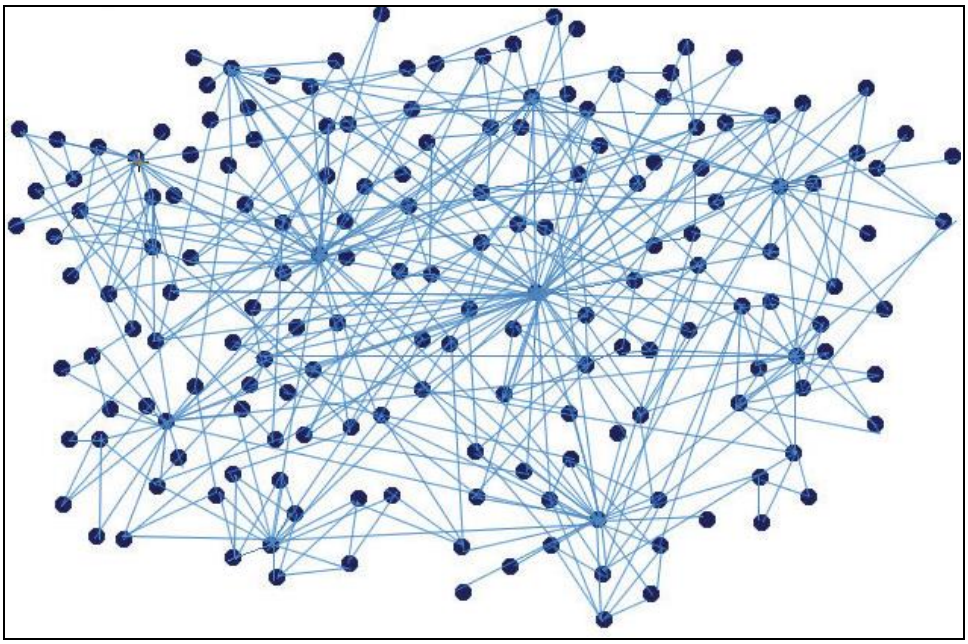

Figura 13: Rede de interligação dos sites. Fonte: modificada de BURTON (2005)

A eficiência da Internet em assegurar a comunicação entre bases e possibilitar que informações estratégicas não necessitem ser concentradas em um único lugar é o destaque da rede. A interrupção da internet não é tarefa das mais fáceis, uma vez que os pontos de interconexão são múltiplos, levando-se em consideração também que as formas de se conectar a internet são múltiplas.

Embora a internet fora criada para proteger determinadas informações, ela também possibilita que um indivíduo consiga acessar informações valiosas em um ponto qualquer da rede sem que haja a necessidade de penetra em uma fortaleza amplamente vigiada (tendo em vista que nem todas informações valiosas para um órgão irão se encontradas na internet; órgãos e governos criam suas próprias redes privadas, porém se um espião entra dentro dessas redes privadas, ele consegue acessar dados destas). Ou seja, informações do Pentágono, por exemplo, podem ser roubadas sem que um agente espião entre no Pentágono ou vá até os EUA propriamente.

É evidente que muitas empresas possuem seus próprios Backbones e se comunicam sem que seja necessário estarem conectados na internet; através de uma conexão privada como mencionado anteriormente. Esse tipo de comunicação privada leva o nome de Intranet, assim sendo, os computadores de uma empresa ou qualquer organismo que tenha a Intranet, estão todos conectados com acesso restrito a quem tem um computador ligado nessa rede. Usinas nucleares, órgãos governamentais, bancos e bases mili-

tares, setores de importância estratégica para a política e economia de um país, geralmente possuem sua própria Intranet para diminuir a probabilidades de invasões.

Embora haja essa rede interna com o intuito de resguardar as informações confidenciais, parece que a engenhosidade da proteção caminha junto com a obstinação da invasão. O próprio Pentágono, provavelmente uma das redes mais seguras do mundo, já foi alvo de diversas invasões ao seu sistema de computadores; uma das mais notáveis foi o roubo de informações do programa de modernização das aeronaves norte americanas que custou 300 bilhões de dólares, F-35 Lightning II.[7]

Mesmo existindo um avançado sistema de segurança informacional protegendo empresas e indústrias, os relatos de invasões de redes parecem que não cessam. Constantemente nascem novas formas de invadir computadores e redes; novos vírus mais potentes fazem parte do cotidiano da internet. Assim como a própria internet foi sendo moldada por seus usuários, novas formas de invasão de redes e vírus de computador geralmente são criações dos internautas. Porém, não é qualquer usuário de computadores que consegue criar um vírus ou muito menos invadir um computador; invasões e criação de vírus de computador exigem conhecimento avançado de informática e redes de computadores; o usuário da internet com essas características é, sumariamente, chamado de Hacker.

Em uma definição bem genérica e "vulgar" do termo, os hackers são usuários avançados de computador que possuem amplo conhecimento do funcionamento de programação e formatação de computadores e redes. A definição exata do termo Hacker é amplamente discutida, pois existe grande heterogeneidade entre esses usuários avançados de computador. Há quem os classifique como hackers, crackers, defacers, cyberpunks, coders, dentre outros. Embora existam diversas classificações e critérios para o enquadramento de um hacker, é unânime o grande conhecimento sistemas e redes e computadores (FILHO, 2010).

Os hackers em geral são especialistas em computação capazes de invadir os mais seguros sites e computadores; são capazes de encontrar vulnerabilidades em uma rede acessando informações valiosas. Esses usuários são quase sempre jovens, civis e independentes de qualquer órgão financiador de suas ações. Embora a internet apresente diversas barreiras de proteção a segredos valiosos, a engenhosidade dos hackers parece conseguir driblá-las.

---

[7] "Hackers invadem site do Pentágono e roubam projeto de avião de US$ 300 bi" (PORTAL G1,2009)

Se Hackers, sem investimentos, profissionalização e utilizando simples computadores pessoais conseguem invadir, controlar e roubar informações das redes mais seguras de computadores do mundo, um Estado investindo milhões em soldados e máquinas altamente sofisticadas, não seria capaz de tornar um computador um verdadeiro aparato de guerra? Não seria deveras proveitoso um Estado criar vírus e softwares capazes de espionar e danificar a rede de computadores de rivais; não seriam essas verdadeiras ciberarmas? De que forma a ciberguerra pode estar ganhando importância na geopolítica atual?

"Da espada ao mouse" (Histórias das guerras)

A importância da ciberguerra para o atual panorama geopolítico encontra-se um pouco nebulosa, visto o fato de que, embora muitos Estados tenham setores de inteligência de redes e soldados bem treinados para uma eventual guerra cibernética, nenhum admite desenvolver programas capazes de invadir e danificar computadores rivais; mesmo existindo evidencias do uso de ataques cibernéticos e mesmo confrontos cibernéticos entre Estados, nenhum governo assumiu a autoria dos ataques. Com tais dificuldades que permeiam o estudo da ciberguerra, outra indagação torna-se importante: A simples utilização de programas de computador para invadir e danificar redes é relevante para a contemporaneidade?

Talvez o uso de vírus de computador em um conflito entre Estados contemporâneos seja tão importante e revolucionário hoje como foi a atualização da catapulta em dado momento da antiguidade. Para tentar responder essa questão e, sobretudo evidenciar a importância histórica de novas armas e estratégias na formulação de dados períodos, iremos analisar, em ordem cronológica, algumas das mais importantes guerras mundiais; como determinados inventos e estratégias (algumas utilizadas até hoje) foram fundamentais para o desdobramento dessas e, concomitantemente, para a hegemonia do lado vencedor.

3.2 Guerra do Peloponeso

Travada há mais de vinte e quatro séculos, a guerra do Peloponeso, ou seja, a conflagração entre Atenas e Esparta, destacou-se de outros grandes conflitos ocorridos até então por ser o primeiro em contexto democrático, onde os rumos da guerra foram decididos em discussões públicas. Na questão tática e nas estratégias de combate, a guerra do Peloponeso, sobretudo na cidade de Atenas, também inovou "com a introdução ateniense da estratégia defensiva de abandono do campo, concentração da população na cidade, fortalecimento da Marinha e, condição *sine qua non*, introdução de um esquema de abastecimento fundado na obtenção de recursos dos seus aliados, com um

sistema imperial de sustentação do esforço de guerra" (FUNARI, 2013. p. 19). Embora a estratégia militar ateniense pareça sutil, ela representou uma grande revolução logística militar, servindo de exemplo posteriormente para o Império Macedônico e Romano.

Atenas também inovou com o realojamento dos habitantes do campo para a cidade, e com isso conseguiu aumentar a disposição de soldados para sua defesa. Porém, com tal medida, não seria possível, abastecer os soldados da acrópole Ateniense, visto que os camponeses foram enviados para cidade. Para supri tal obstáculo, o abastecimento dos soldados atenienses começou a ser feito por cidades aliadas, ou cidades do Império de Atenas, de modo que tal façanha tornou-se peça fundamental da estratégia ateniense. A reinvenção da estratégia militar ateniense é atribuída ao grande estadista Péricles, considerado a maior personalidade política da guerra do Peloponeso.

Péricles levou Atenas à conflagração contra Esparta, tomando como medidas necessárias para o fortalecimento ateniense o revigoramento do Império suas redes e reforço da esquadra naval. A estratégia de Péricles mostrou-se eficaz contra o exército espartano que se apoiava em sua grandiosa tropa terrestre e abastecimento das tropas quase que somente pela própria cidade de Esparta, agrícola e oligárquica.

"Tradicionalmente, o combate dava-se em campo aberto entre exércitos, e o resultado do embate era decidido pelas manobras e pela bravura dos combatentes. Os atenienses, com seu estado voltado para o mar e para as trocas comerciais, começaram a investir em estratégias defensivas, que evitassem o ataque e o combate decisivo." (FUNARI, 2013. p. 19). Sendo assim, Atenas utilizava-se do seu império e concomitante das redes de abastecimento do império como estratégia logística de fornecimento de suprimentos para suas tropas. Com tal estratégia, Atenas não precisou se preocupar com a produção interna de alimentos. O abastecimento de grãos para a cidade era oriundo da Crimeia e do Egito, além disso, também contava com a garantia dos tributos dos aliados, e com isso a acrópole não dependia de suas próprias plantações e riqueza, inviabilizando a eficácia do plano de um cerco tradicional, como pretendido pelos espartanos (FUNARI, 2013).

Atenas inovou não somente por utilizar uma ampla rede de abastecimento, que lhe garantiu segurança no campo de batalha. Atenas inovou também ao declarar embargos às cidades que não obedecessem a suas ordens; estratégia nova para então. Atenas utilizou-se de embargos contra Mégara, cidade grega vizinha, para impedi-lá de ajudar a Cidade vizinha, Corinto, rival ateniense, "com o fim de dissuadir Mégara e outras da ideia de ajudarem Corinto. Os Atenienses aprovaram um decreto que impedia os megá-

riosde usar os portos do Império Ateniense e de frequentar o mercado de Atenas (agorá)...” (FUNARI, 2013, p. 32). A sobrevivência ateniense dependeria, então, das redes de abastecimento do Império. O fornecimento de metais para a confecção de espadas e lanças assim como de alimentos para os soldados foi fundamental na estrutura do império Ateniense, principalmente durante a guerra.

Atenas manteve-se em vantagem com relação à Esparta durante os primeiros anos da guerra do Peloponeso (431 a 404 a.c). A guinada espartana veio com o bloqueio do abastecimento de grãos rumo a Atenas originários do Egito e da Sicilia; como Atenas dependia desses suprimentos, a campanha ateniense começou a desmoronar. A tática espartana para vencer a guerra foi minar as redes de abastecimento do Império ateniense.

Da mesma forma que as redes de fornecimento de suprimentos e metais eram vitais para a acrópole ateniense na guerra do Peloponeso, hoje as redes continuam importantíssimas para a vitalidade dos estados. Embora qualquer rede de fornecimento de suprimentos de alimentos sempre seja a mais importante rede para um estado, afinal não existe um país sem alimentos, hoje outras redes tornam-se vitais para os estados, como a rede de fornecimento de energia, rede de fornecimento de combustível, rede de fornecimento de munição, rede de fornecimento de informação.

Tratando-se da vitalidade dos países, as redes de informação, sistema financeiro e a própria internet tornam-se cada vez mais importantes, tão importantes quanto os grãos e o ferro vindo do Egito eram para Atenas. Não à toa, atualmente o governo sírio de Bashar Al-Assad, de maneira a persuadir rebeldes sírios, cortou o sinal de internet da região do foco rebelde. Em plena época do capitalismo financeiro, a internet configurou-se como ferramenta fundamental na organização dos Estados, importância semelhante aos metais na era mercantilista.

No entanto, devo salientar que, como tratamos anteriormente neste trabalho, a internet foi idealizada para que não houvesse perda ou corte de informações da rede. Além do mais, as atuais tecnologias quase não necessitam de fios ou grandes centros de armazenamentos para transmissão de sinais. Deste modo, bloquear a internet, peça estratégica e fundamental para a maioria dos países hoje, não é uma tarefa tão fácil, ou se quer mais concebível, quanto bloquear um porto atualmente.

Pela própria estrutura física da internet, bloqueá-la totalmente em um país tornou-se algo, possivelmente, muito mais difícil que um bloqueio marítimo ou terrestre. Já que impedir o acesso à internet a um país ou região seja algo de extrema dificuldade

hoje, outras formas de prejudicar a rede podem ser adotadas. Invasões, sabotagens, roubos de informação são meios que podem ser aplicados para prejudicar a rede. Talvez, melhor que impedir que uma informação qualquer chegue de um ponto a outro, é saber qual a informação transmitida.

A estratégia espartana para vencer a guerra contra Atenas foi bloquear suas redes de abastecimento de grãos e ferro, pois eram essas as principais forças motoras ateniense, algo relativamente novo até então, pois a maioria das guerras era vencida somente no campo de batalha. A experiência grega pode talvez nos orientar para o rumo das novas guerras e, concomitante, para as novas relações de Estados. Caso haja choque entre Estados, a internet pode tanto ser um dos primeiros alvos de ataque, senão o primeiro, como ela pode ser também um instrumento de ataque, ou seja, ataques cibernéticos, em que o objetivo dos ataques não seja acabar com a internet de um país propriamente, mas antes roubar informações preciosas ou danificar e sabotar alvos financeiros, infraestrutura e militares, vide o vírus Stuxnet utilizado contra o programa nuclear Iraniano, algo que iremos analisar posteriormente.

3.3 Gêngisklan e as conquistas mongóis

A estratégia ateniense de cortar rotas de suplementos foi fator decisivo para o desempenho dessa acrópole durante os primeiros anos da guerra do Peloponeso. Se por um lado a tática Ateniense de criar uma rede de suprimentos mostrou-se eficaz em dado momento, a utilização de embargos por parte de Esparta também foi decisiva para o encaminhamento da guerra. Evitando anacronismo, tais estratégias são relativamente simples hoje, porém mudaram a história do mundo grego.

Junto a novas estratégias, muitas das maiores invenções que temos hoje foram feitas em períodos de guerra. Como já salientado, a própria internet foi elaborada durante, e sobretudo, para ser usada na Guerra Fria. Táticas e invenções muitas vezes simples podem mudar o resultado de um conflito, ou até mesmo inaugurar ou terminar um período hegemônico de um país. Não é por menos que no final da Segunda Guerra Mundial os Estados Unidos se consolidaram no posto de potência militar mundial, depois do disparo das duas bombas a Hiroshima e Nagasaki, o domínio da tecnologia nuclear ajudou a estabelecer os Estados Unidos no centro da nova geopolítica mundial, ou seja, o domínio de uma nova tecnologia.

Destarte, peguemos como exemplo do maior império em extensão contínua que já existiu, o império mongol. A dimensões do império mongol eram gigantescas, se estendendo das planícies chinesas, passando pelo Mar Aral até o Mar cáspio; tamanha extensão por si só já demonstra a magnitude mongol. Como sua grandiosidade inquestionável, o principal questionamento sobre o império mongol é: Como um povo nômade conseguiu tal façanha diante de inúmeros povos sedentários?

Responder a essa pergunta poderia ser algo simples, pois podemos basear nossa resposta no choque cultural que os mongóis provocaram sobre os povos dominados, afinal, os mongóis eram um povo de hábitos totalmente estranhos aos povos dominados; a estranheza da cultura dos mongóis com relação aos povos dominados pode ter favorecido a dominação daqueles. A própria relação que os mongóis exerciam com a terra era diferente da maioria dos demais povos asiáticos e europeus da época; os mongóis eram um povo nômade, enquanto a maioria dos asiáticos e europeus dominados por este império eram sedentários.

Simples também seria atribuir todo mérito das conquistas mongóis à fragilidade que a Europa vivia no momento devido à desestabilização provocada pelo feudalismo. Embora a fragilidade europeia seja um fator relevante para entender a expansão mongol, somente isto não explica a pujança do Império; novas estratégias e armas utilizadas e adaptas pelos mongóis foram fundamentais para o sucesso imperial.

O Império Mongol pode ser representado na figura do lendário GêngisKlan. GêngisKlan ajudou a desenvolver e adaptar técnicas importantíssimas para as conquistas imperiais; dentre algumas dessas armas, o estrito e o arco e flecha mongol ganham destaque. Embora o estribo não seja uma invenção dos mongóis, sua adaptação e utilização desempenharam papel de destaque no exército de Klan. Como afirma a professora Elaine Senise Barbosa, "é com o surgimento do estribo que se desenvolve a arte da guerra, ao assegurar firmeza ao cavaleiro em movimento enquanto libera suas mãos para o combate e o manejo" (BARBOSA, 2013, p. 134).

Junto com o estribo, o cavalo mongol se destaca como uma das armas do império. Diferente do cavalo europeu, de tamanho e proporções maiores, o cavalo mongol, embora menor, era extremamente resistente e podia percorrer longas distâncias. Ainda que venha parecer irrelevante o tipo de montaria dos guerreiros mongóis para entender o êxito destes, o cavalo mongol possibilitou grande agilidade e aumentou a área possível percorrida pelos cavaleiros de Klan; sem seu cavalo, o Império mongol talvez não tivesse chegado a tamanhas proporções.

> "O cavalo mongol, que ocupa papel de destaque nas conquistas territoriais, é na verdade um "pônei duplo" medindo cerca de 1,30 m no garrote e pesando em torno de 350 kg. Eram destinados à montaria os capões, desde os 3 anos. Extremamente fortes, podiam cobrir cerca de 45 km por dia se bem descansados; por isso os mongóis costumavam usá-los um dia para três de descanso, levando consigo nas campanhas várias montarias de substituição" (BARBOSA, 2013, p. 134).

Junto ao arco e flecha e a montaria, os Mongóis foram inovadores na utilização de sistemas de espionagem. A professora Elaine Senise Barbosa também atribui a eficiência do império mongol a um competente sistema de espionagem:

> "Durante esses anos ele organiza um eficiente serviço de espiões e batedores infiltrados nas tribos rivais, explorando sempre as dissensões internas entre os inimigos e procurando as melhores condições físicas para atacar (áreas de vertentes onde assumisse posição vantajosa; gargantas entre montanhas; oferta de pasto para os animais)" (BARBOSA, 2013, p. 134).

Como descrito pela professora Elaine Barbosa, espionar o inimigo para obter informações privilegiadas não é algo novo, porém essa tática ainda é muito utilizada. Em 2013, o ex-militar e técnico de informações do exército dos Estados Unidos, Edward Joseph Snowden, divulgou ao mundo como seu país vinha espionando países inimigos e até mesmo aliados em busca de informações estratégicas. Com o advento da informática e da internet, hoje a espionagem atinge outro patamar e diferencia-se do tipo de espionagem praticada pelo império de GêngisKlan; a diferença reside na possibilidade atual de se espionar, roubar informações estratégicas, sem a necessidade de infiltrações físicas no território espionado.

Com a internet, outra mudança na espionagem entre Estados foi o próprio espião. O espião empregado no exército mongol, nos Estados Unidos e na União Soviética no auge da Guerra Fria era antes de tudo um soldado treinado para conseguir informações importantes; talvez um hábil soldado mongol e um hábil soldado soviético ou americano não se distingam para além da diferença temporal. Esses tipos de espiões podem ser caracterizados pelo famoso espião inglês, personagem hollywoodiano, James Bond.

As características que compõem esse personagem do cinema, e inúmero outros espiões retratados por hollywood, são próprias de bons soldados. James Bond e suas cópias são sempre agentes disfarçados de um órgão das forças especiais, exímios atira-

dos, ótimos lutadores, nadadores, corredores, enfim, têm qualidades que se espera do melhor dos soldados. Hoje, porém, essas qualidades parecem não serem encontradas nos espiões modernos, o espião/soldado tão retratado por hollywood perde espaço para o jovem especialista em computação. Os próprios Edward Snowden e Bradley Manning, talvez os espiões mais famosos da atualidade, não se enquadram nas características do espião/soldado hollywoodiano.

Junto com a espionagem, a organização tática e logística do exército foram fundamentais na eficiência mongol. As tropas de Gêngisklan conseguiram atingir no século XII e XIII o que os exércitos atuais chamam de C3- comando, controle e comunicação.

> "Gêngis Khan organizou seu exército da seguinte forma: à frente de dez cavaleiros colocou um decano; dez decúrias são comandadas por um centurião; dez centúrias obedecem a um milenário; dez mil homens, reunidos sob a autoridade de um capitão, formam um corpo designado tuman. Enfim, no comando do conjunto das tropas estão dois ou três generais, um dos quais tem a precedência. Se durante um combate um, dois, três ou mais homens de uma decúria fogem, todo o grupo é executado; se todos os dez deserdam a centúria à qual pertencem é executada, a menos que todos desertem ao mesmo tempo" (HÒANG, 2002, p. 174)

Como pudemos ver, estribo, arco, flecha, cavalo mongol e uso de espionagem foram imprescindíveis para expansão e êxito do Império Mongol contra os povos dominados. Estratégias e inovações tecnológicas pequenas puderam contribuir com o desempenho e reinado de Gêngis Khan.

3.4 Guerra de Secessão

Daremos agora um salto do império de Klan até o século XVIII, precisamente a guerra de secessão americana. Analisar a Guerra de Secessão (1861-1865) é importante para o presente trabalho, pois esta mudou o panorama da geopolítica; seja pela ascensão dos Estados Unidos ao cenário geopolítico global, seja pela mudança na maneira de como as guerras eram travadas; com a guerra de secessão a guerra tornou-se muito mais

uma questão de estratégia do que tática[8]. A logística de abastecimento das tropas nunca teve tamanha importância.

A Guerra de Secessão ou Guerra Civil Norte Americana (1862-1865) foi o conflito envolvendo a parte norte dos Estados Unidos, colônias do norte, contra a parte sul, colônias do sul. O motivo aparente do conflito foi divergências envolvendo o fim da escravidão, porém a contenta se destacou para, além disso, pela disputa entre dois modos de vida distintos.

Vale citar que o século XVIII e, concomitante, a Guerra de Secessão, são marcados pela transição de um "mundo lento", onde o ritmo cotidiano ainda era ditado pela pouca velocidade das carroças, barco a vela e força da água, para um novo mundo; mundo das industrial, da invenção do telégrafo, modernização dos meios de comunicação, "mundo da velocidade":

> "Até 1850, vivia-se num ritmo muito mais lento do que o atual, como as viagens terrestres sendo feitas à base da tração animal, e os barcos sendo movidos pela força dos ventos. Tambores, tochas e sinais de fumaça eram os únicos meios de conseguir-se uma comunicação rápida a distância, limitando geograficamente seu alcance à capacidade da visão humana. A s pessoas de modo geral eram muito religiosas, "tementes a Deus", e entre as classes populares ainda vida o estatuto da servidão, e a maioria das pessoas, mesmo na Europa Ocidental mais urbanizadas, obtinham seu sustento no trabalho direto com a terra. Em suma, é possível assegurar, com alguma dose de cautela, que a paisagem feudal ainda não fora apagada inteiramente em quase nenhum canto da superfície terrestre." (MARTIN, 2013, p. 221).

A Guerra de Secessão é um marco na história das grandes guerras, pois se por um lado os EUA surgem com uma grande nação, por outro, inegavelmente, foi um marco na luta por igualdades raciais e coroou o triunfo da sociedade capitalista industrial, representada pelas colônias do norte, sobre a sociedade agrária e conservadora das colônias do sul, por outro, a Guerra de Secessão foi a primeira grande guerra a ser marcada pelos avanços da Segunda Revolução Industrial. Melhorias na produção do aço, surgi-

---

[8]Para diferenciar estratégia de tática faço referência ao grande jogador de xadrez o russo SavviellyTartakower: "Tática é saber o que fazer quando há o que fazer; estratégia é saber o que fazer quando não há nada a fazer"

mento do dínamo, expansão da rede de transporte e telegramas foram peças chaves no desdobramento do conflito.

No desenrolar da guerra, a vantagem das colônias do norte, mais numerosas e industrializadas, obrigou as colônias sulistas tomarem medidas criativas e buscar desenvolver-se tecnologicamente. Exemplo disso foi a adoção, pelos sulistas, de pequenos, porém rápidos barcos para fugir do bloqueio naval imposto pelos aliados do norte em determinado momento da guerra. Outro exemplo da inovação militar sulista foi a blindagem de navios para fugir do bloqueio imposto pelo norte, medida que revolucionou não somente a guerra de secessão como as demais guerras que se sucederam.

Embora as colônias do sul tenham se desenvolvido militarmente criando novas armas, algo que poderia trazer grande vantagem sobre as colônias do norte, tal conjectura não aconteceu. Como o professor André Martim ressalta, "é preciso não superestimar a extensão e a importância que a utilização de novos armamentos teve ao longo da contenda, e sobretudo para o seu resultado final. As inovações mais revolucionarias foram experimentadas pelo lado perdedor..." (MARTIN, 2013, p. 245).

Para além dos navios blindados, outras armas foram inventadas ou apropriadas com o conflito. Os rifles, por exemplo, ganharam maior precisão por conta da adoção da "alma raiada", pequenas ranhuras dentro do cano da arma para fazer o projetil girar, e manter sua estabilidade durante o deslocamento, substituindo os rifles de cano liso. A evolução de rifles de três tiros por minuto para 25 disparos por minuto, o famoso rifle Henry (mais tarde usado como inspiração para os também históricos rifles Winchester), revolucionou a história das batalhas e da própria guerra de secessão. As colônias do sul revolucionaram também ao inventar as minas aquáticas e torpedeiros. Acredito ser difícil imaginar as batalhas no pacifico durante a Segunda Guerra Mundial (1939-1945) e a consequente vantagem que essas armas deram aos norte-americanos (MARTIN, 2013)

Talvez a necessidade, aliada à engenhosidade, ajude a superar os obstáculos impostos, tal como faziam as colônias sulistas perante o bloqueio naval imposto pela união do norte. Porventura, a necessidade também pode fazer com que se olhe com mais atenção e criatividade para o que já se tem, adaptando o conhecido para transpor os problemas. A utilização do submarino em batalha é um grande exemplo de como o que já se encontra disponível pode ser adaptado e utilizado com outra função. Sem a existência de submarinos e uso militar destes, possivelmente as disputas geopolíticas durante o período de Guerra Fria (1945-1991) teriam tomado outros rumos.

Embora o submarino já existisse, seu uso como arma de guerra modificou não só a Guerra de Secessão e guerras posteriores, como as relações entre os Estados. Durante a corrida armamentista, Estados Unidos e União Soviética disputavam a ocupação do polo ártico; vale lembra que perante um eminente conflito nuclear vivido no momento, EUA e URSS provavelmente se bombardeariam pelo ártico (voo mais curto em os dois países) ao contrário do que geralmente se imagina, onde estes lançariam bombas cruzando Europa Ocidental e oceano Atlântico norte. Devido à configuração geográfica do Ártico, poucas terras emersas e grande porção oceânica (o pólo norte consiste basicamente em uma camada de gelo sobre um grande oceano), os submarinos seriam estratégicos por facilitarem a ocupação ártica, pois eram os mais eficientes meios de penetrar no oceano gelado; submarinos nucleares também garantindo grande vantagem de permanência nesse ambiente extremamente hostil.

"A fotografia, o telégrafo, os foguetes de sinalização, os balões de observação e os trens também tiveram importância estratégica como artefatos de uso militar na Guerra de Secessão, muito embora nenhum desses inventos possa aqui ser classificado como arma, pois foram empregados antes como meios de inteligência ou logística" (MARTIN, 2013, p. 246). Embora tais inventos não tenham sido usados como armas de guerra, foram antes amparo à inteligência e logística, é inegável sua importância para a guerra de secessão e conflitos posteriores.

A logística superior das colônias do norte foi certamente um elemento que garantiu enorme vantagem para a União do norte durante a contenda. Os Casacos Azuis, como ficaram conhecidos os soldados nortistas, não sofreram com falta de suprimentos e munições; diferentemente dos Casacos Cinzentos, designação dos soldados do sul, que tiveram que combater ante a falta de comida e munições. Além do atraso dos comboios, as tropas podiam deparar-se com a inadaptação entre armas e munições; calibres diferentes foram produzidos no decorrer da guerra e era comum enviarem para uma tropa balas de um determinado calibre não compatível com as armas dos soldados.

Em função do grande avanço logístico e cabal desempenho na Guerra de Secessão "(...) os Estados Unidos aparelharam-se com uma vasta rede de 34 mil quilômetros de telégrafos, com o departamento de guerra instalando, pela primeira vez, um escritório telegráfico na casa branca de onde Lincoln recebia notícias e enviava decisões. Tratou-se sem dúvidas de um percursor da rede de internet" (MARTIN, 2013, p. 249).

Como destacado, a logística e adaptações de objetos e armas já existente como o rifle, submarino e telégrafo deu certa vantagem para as colônias do norte alcançarem a

vitória. Para além, a guerra de secessão norte americana como primeira a ser realizada sobre a influência da segunda Revolução Industrial foi amplamente marcada por esta; o uso do aço, a metalurgia, a eletricidade, a eletromecânica, o petróleo, o motor a explosão e a petroquímica ficou evidente no conflito, a indústria entrou para a guerra e a guerra começou a ser produzida em escala industrial (por isso a grande quantidade de mortos no conflito).

Da mesma forma que grandes guerras foram marcadas pelos avanços presentes em sua época, e a própria guerra de secessão americana foi tão marcada pela segunda revolução industrial; a terceira revolução industrial marcada pela informática, robótica, microeletrônica e internet não poderiam influência grandes conflitos contemporâneos; influenciar de tal maneira que um sistema de informação como a internet seria muito mais que uma ferramenta de apoio a logística e sim uma própria arma de guerra, evidenciando uma possível ciberguerra?

3.5 Guerras do Golfo

As duas Guerras do Golfo (1991 e 2003) são extremamente importantes para que, primeiro, possamos entender a presença militar americana no Oriente Médio; talvez, na virada do século, a região tenha abrigado a maior parte dos conflitos militares atuais tirando centenas de vidas todos os anos até então. E representa, também, a ascensão de um novo tipo de guerra influenciada pela revolução tecnológica, visto que já evidenciamos a influência da segunda revolução industrial sobre uma grande guerra, a Guerra de Secessão Norte Americana.

A primeira Guerra do Golfo (1991) tem seu início após a invasão do Iraque de Saddam Hussein sobre o Kuait. Porém para entender os motivos que levaram as tropas de Hussein invadir o Kuait, é necessária uma breve menção a guerra Irã e Iraque.

De 1980 a 1988 o Iraque mergulhou em uma guerra avassaladora contra o fronteiríssimo Irã; o motivo aparente para a guerra seria a renegociação de acordos que asseguravam o domínio do Irã sobre uma área importante, o canal ChateAlárabe, que divide os países e de extrema relevância para importação e exportação (principalmente do petróleo) de ambos Estados por dar acesso ao Golfo Pérsico.

Talvez o maior motivo para a guerra tenha sido a Revolução Iraniana de 1979; encabeçada pelo líder espiritual Xiita e político Ruhollah Musavi Khomeini em substituição ao governo de Mohammad Reza Pahlavi, que detinha simpatia dos países ociden-

tais. No mesmo ano de 1979, Sadam Hussein, de origem sunita, assumiu o poder no Iraque. Deve-se considerar também que a ascensão de Khomeini significava perigo às relações dos países ocidentais com o Irã e ao mesmo tempo também poderia ameaçar o governo fronteiríssimo sunita e de Saddam Hussein. Logo, com apoio ocidental na tentativa de frear a revolução islâmica iraniana, o Iraque ataca o Irã sobre o pressuposto da reivindicação do canal de ChateAlárabe. Sendo assim, o canal pode ser visto apenas como o estopim ou "start" para o conflito.

De 1980 a 1988, Irã e Iraque deflagram intensos conflitos com inúmeras reviravoltas e sem um grande vencedor ao final da guerra; fato é que ambos os países praticamente se destruíram em oito anos de contenda. Para se reconstruir no pós guerra, ambos Estados recorreram à exportação do valioso petróleo de seus sobsolos. A reconstrução destes seria freada, no entanto, por dificuldades da venda do óleo no mercado internacional.

O grande problema encontrado por Irã e Iraque para a venda de seus valiosos barris de petróleo residia no fato de o petróleo não estar tão valioso no mercado internacional com o Kuait vendendo o barril deste produto por quase metade do preço estimado para a época. Juntam-se a isso as vultosas quantias de dinheiro que o Iraque havia pegado emprestado do Kuait; Saddam Hussein vê na invasão do Kuait a solução para os seus problemas; a contragosto do ocidente, tropas iraquianas invadem o Kuait e dão início à primeira Guerra do Golfo.

> "A invasão do Kuwait parecia, do ponto de vista de Saddam, uma operação lógica. Quando acabou o desastre iraniano, o Iraque precisava desesperadamente vender petróleo a preços altos, mas o barril, que custava US$ 21,00 em janeiro de 1990, estava sendo vendido a US$11,00 na metade daquele ano. Os sheiks do Kuwait eram um dos principais responsáveis por ultrapassar a cota de cada membro da Opep naquele período. Além disso, passaram a cobrar os volumosos empréstimos feitos a Saddam durante o sangrento conflito com o Irã" (WAACK, 2013, p. 457).

Diferente dos conflitos analisados até agora, a Guerra do Golfo é a primeira grande guerra a acontecer amplamente influenciada pela revolução informacional e tecnológica. Como já salientado por Manuel Castells, a tendência das guerras ocorridas após a segunda Guerra Mundial, durante e depois da Guerra Fria, é a "Guerra instantânea". Ou seja, a guerra deve ser curta (até mesmo instantânea), haver um exército pro-

fissional, ser limpa, cirúrgica e dentro de limites razoáveis, escondida o máximo possível da visão pública (CASTELLS, 2000)

As duas Guerras do Golfo talvez sejam as primeiras, ou as que melhores sintetizam a chamada "Guerra Instantânea" descrita por Castells. Antes do começo da primeira Guerra do Golfo, acreditava-se que os EUA, principal adversário do Iraque nas Guerras do Golfo, teria bastante dificuldade de combater as tropas de Saddam Hussein, sobretudo pela experiência dos combatentes iraquianos em guerras anteriores e dificuldade de se batalhar no terreno desértico do Iraque. Ao contrário do que se esperava a ampla tecnologia dos EUA e aliados contra as tropas iraquianas foi descomunal, não dando a menor chance para o exército de Saddan.

> "Às 100 horas de lutas mostrariam de que maneira a capacidade do Exército iraquiano havia sido grosseiramente superestimada, sobretudo pela imprensa ocidental" (WAACK, 2013, p. 457).

As guerras no Iraque em 1991 e 2003 evidenciaram a grande capacidade das novas tecnologias quando empregadas em combate. A utilização de armas mais sofisticadas ajudou a garantir a vantagem americana; utilização de GPS, rifles mais precisos, aviões, helicópteros e bombas teleguiadas demonstraram o grande aparato tecnológico americano.

A primeira Guerra do Golfo (1991) demonstra o formato da "Guerra Instantânea" proposta por Manuel Castell (CASTELL, XXX). Pelo alto grau de tecnologia empregado nesta, ela foi cirúrgica (bombas teleguiadas aumentaram a precisarão de ataques dos exércitos inúmeras vezes se comparamos com a Segunda Guerra Mundial, por exemplo), foi rápida (na história das guerras tivemos exemplos de guerras enormemente longas, como a Guerra dos 100 anos; já a primeira Guerra do Golfo durou apenas 100 horas) e utilizou exército extremamente treinado, ou seja, profissional.

> "A Primeira Guerra do Golfo, como ficou conhecida a conflagração militar de janeiro a março de 1991, foi uma lição de que, em guerras convencionais modernas, o peso da tecnologia favorece de forma decisiva os exércitos "ocidentais". (...) mas o emprego dos principais elementos da revolução da informação para a conduta das operações no campo de batalha excedeu tudo o que se conhecia até então." (WAACK, 2013, p. 457).

A figura a seguir, elaborada em 2003, começo da segunda Guerra do Golfo, já atentava para a modificação dos conflitos a partir da Segunda Guerra Mundial (Fig. 14).

Após 1945, as guerras tenderam à profissionalização dos soldados com alcance e cobertura da mídia cada vez maiores.O número de baixas nos conflitos diretos tende a ser menor, embora os números de civis mortos, feridos e refugiados por conta das guerras ainda sejam altos.

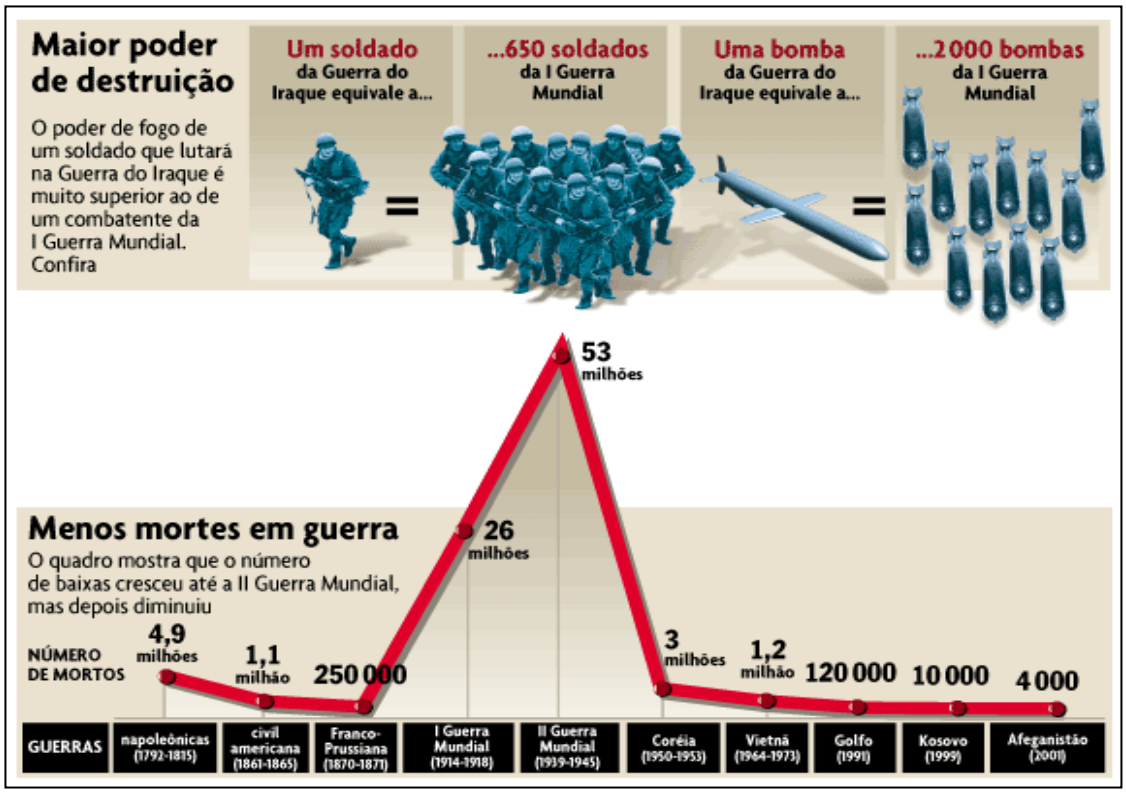

Figura 14: Redução no númerode mortes de soldados nas últimas guerras do século XX, devido a maior profissionalização e melhor eficiência nos armamentos. Fonte: Editora Abril (2003).

A mudança no tipo de guerra depois da Segunda Guerra Mundial pode ser um reflexo da influência da revolução tecnológica e informacional. Nas duas Guerras do Golfo podemos notar evidências da "Guerra Instantânea", porém devemos considerar que o Iraque não era um grande adversário para os EUA, sendo ambas as Guerras do Golfo somente uma grande demonstração da superioridade militar tecnológica americana. Ambas as guerras envolveram um país extremamente industrializado e já totalmente inserido na revolução informacional e capitalismo financeiro, EUA, contra outro recém-saído de uma guerra de oito anos que o levou às ruínas e pouco desenvolvido tecnologicamente, que mal possuía indústrias, Iraque.

> "O avanço nas tecnologias de informação permitiu que os americanos testassem não em exercícios, mas no campo de batalha, pela primeira vez, as doutrinas militares de informação em tempo real (...) o emprego dessa tecnologia permitiria que até mesmo carros de combate isolados pudessem acompanhar eventos distantes, ampliando decisivamente o horizonte dos soldados e comandantes no campo que, como se sabe, costuma ser bastante estreito." (WAACK, 2013, p. 458).

Em outro cenário, diferente do das duas Guerras do Golfo, envolvendo duas nações já inseridas, mesmo que parcialmente, na atual etapa da revolução informacional e do capitalismo financeiro, à "Guerra Instantânea" de Castell poderia ser acrescentada uma nova forma de batalha e um novo campo de batalha, seria então a ciberguerra. A ciberguerra consiste na utilização da internet por Estado para atacar, roubar informações ou danificar a rede computadores vital para o funcionamento dos Estados rivais.

Eventualmente, as Guerras do Golfo representam somente o primeiro grande conflito sobre influência da revolução tecnológica da informação; profissionalização dos soldados, guerra cirúrgica e veloz, a "Guerra Instantânea" (CASTELLS, 2000). Dentre as formas que a Guerra Instantânea pode se apresentar acredito que a Ciberguerra seja uma das suas vertentes. A Ciberguerra, reflexo da revolução informacional contemporânea, alcança, talvez de maneira sem igual, os pressupostos da Guerra Instantânea; soldados extremamente qualificados, praticamente invisível dos cidadãos, limpa e instantânea.

A Ciberguerra

O desenvolvimento e dependência dos países com relação à internet e sistema financeiro, ou seja, desenvolvimento do capitalismo financeiro, aliado às exigências sociais que deram origem a "Guerra Instantânea" – aquela que não deve envolver cidadãos comuns, portanto deve ter um exército profissional, deve ser curta, até mesmo instantânea, deve ser limpa, cirúrgica, dentro de limites razoáveis e escondida o máximo possível da visão pública - pôde tornar possível a ciberguerra.

A ciberguerra só torna-se possível devido à atual dependência social e dos Estados sobre os meios eletrônicos, com o desenvolvimento do capitalismo financeiro e consequente necessidade da rede mundial de computadores. Se para o sistema capitalista tempo é sinônimo de dinheiro, a internet possibilitou a quase instantaneidade das transações financeiras. Sendo assim, a terceira revolução industrial trousse consigo um novo momento na história do capitalismo: a dependência da rede mundial de computadores.

Visto as atuais a expansões das redes de informação e o novo cenário geopolítico pós- segunda guerra, o da Guerra Instantânea, algumas evidências já apontam para a concretização da utilização de computadores, vírus e softwares de computador no conflito entre Estados; a Ciberguerra. Iremos agora analisar alguns dos casos conhecidos dessa nova prática.

3.7 Ciberarmas

Dentre os casos mais conhecidos de ciberguerra, darei destaque para o uso dos quatro vírus (Vírus Stuxnet, Flame, Duqu e Gauss). O motivo de analisar tais exemplos se dá pelo fato de esses serem os casos mais populares da utilização de ciberataques. O mais interessante de se analisar ciberataques, ou seja, a utilização de meios cibernéticos para danificar ou roubar informações de determinadas redes, é que talvez, os mais bem sucedidos ataques jamais sejam descobertos; uma vez que os ataques cibernéticos nem sempre tem como objetivo danificar totalmente a rede de computadores de um alvo. A danificação de uma determinada rede computadores nem sempre é percebia; enquanto o

escopo dos ataques é simplesmente produzir falhas ou somente espionar um alvo, faz-se necessário que a investida seja imperceptível.

Dos casos que iremos analisar, o Vírus Struxnet é certamente o que melhor evidencia a Ciberguerra; com origem atribuída aos Estados Unidos, o Vírus Struxnet ganhou reconhecimento após danificar o programa de energia nuclear do Irã. Seria então, um dos primeiros casos onde um país teria usado um vírus de computador para atacar um outro país rival. Saliento que embora o Struxnet tenha o adjetivo vírus, ele na verdade é um Worm; os vírus de computador não conseguem se reproduzir, enquanto os Worm são autorreplicantes (CGIBR, 2006).

Em meio às tensões geopolíticas que permeavam a primeira década do século XXI, a construção e obtenção de tecnologia nuclear por parte do governo Irã era uma das de maior destaque. O Irã, junto a Cuba, Sudão e Síria fazem parte da lista de países que apóiam o terrorismo, segundo o governo dos EUA (Coreia do Norte até 2008 era considerada uma apoiadora do terrorismo; devido à cooperação dos norte coreanos com a Agencia Internacional de Energia Atômica na inspeção do seu programa nuclear, o país já não é mais considerado pertencente à "lista negra" norte americana). Frear o desenvolvimento da tecnologia nuclear no Irã e possivelmente obtenção de tecnologia de destruição em massa tornou-se uma exigência geopolítica dos EUA.

Para conseguir frear ou destruir o programa de energia nuclear iraniana, os Estados Unidos poderiam "simplesmente" invadir o Irã e acabar com a obstinação do governo persa em conseguir tecnologia nuclear. Porém, como já frisado pelo presente trabalho, com base em Manuel Castells, as formas contemporâneas de guerrear seguem os princípios da "Guerra Instantânea", guerra rápida, exercito profissional e longe o máximo possível do público; a guerra não deve se tornar alarmante deve ser disfarçada. Como em 2010, auge do programa nuclear iraniano, os EUA ainda estavam envolvidos em duas operações militares no Oriente Médio, Guerra do Afeganistão (2001) e Guerra do Iraque (2003-2011), mais uma Guerra talvez não fosse tão aceitável mesmo com base no discurso antiterrorista americano; ainda mais se tratando do Irã, que certamente iria oferecer maior resistência à guerra que Iraque e Afeganistão. A solução mais engenhosa para frear o obstinado governo persa, sem causar grandes impactos no cenário internacional, ou seja, respeitando a "Guerra Instantânea" de Castells, poderia ser a Ciberguerra.

O WormStuxnet fora peça chave para sabotar o programa nuclear iraniano. O Stuxnet foi projetado explorando uma falha no sistema operacional Windows (sistema operacional mais popular no mundo). Além da maioria dos computadores domésticos, muitos computadores industriais utilizam a plataforma Windows nos seus computadores centrais, SCADA´s. A maioria das indústrias de grande porte utilizam Sistemas de Supervisão e Aquisição de Dados, SCADA (SupervisoryControl and Data Acquisition); o SCADA é basicamente um software responsável por monitorar e controlar partes ou todo o processo industrial de uma indústria, inclusive industriais nucleares.

Como trabalhado anteriormente, geralmente grandes indústrias e empresas estratégicas para os estados possuem uma rede privada de dados não conectada à internet; sabendo-se disso, o WormStuxnet encontraria dificuldades para invadir os sistema SCADA da indústria nuclear iraniana. Quem projetou o Stuxnet programou o Worm para infetar usuários comuns, que não fossem seu alvo, sem prejudicá-los, até que um usuário infectado acabasse levando o Stuxnet para alguém envolvido no programa nuclear iraniano e, consequentemente, para dentro do alvo real. Outra particularidade do Worm diz respeito ao fato de ele ter sido programado para somente ser ativado no Sistema de Supervisão e Aquisição de Dados (SCADA) da Siemens, o mesmo utilizado pelo Irã, e mesmo que outra indústria utilizasse o SCADA da Siemens, o Worm só seria ativado se a rede tivesse um modelo de configuração especifico, ou seja o WormStuxnet foi projetado para atacar um alvo predeterminado (ALBANESIUS; SELTZER, 2010)

A eficácia do Worm foi comprovada pela destruição de parte das centrífugas iranianas em 2010. O Stuxnet conseguiu fazer com o sistema de resfriamento da usina nuclear iraniana não funcionasse corretamente, e consequentemente houve superaquecimento e explosão e avaria de parte do planta nuclear iraniana. Na época dos acontecimentos, uma matéria de revista frisava “Vírus entra em programa nuclear e salva o mundo” (SANTOS; VERSIGNASSI, 2011).

Em reportagem ao jornal Folha de São Paulo no dia 02/09/2014, um dos técnicos responsáveis pela atribuição do WormStuxnet ao governo dos Estados Unidos, Mikko Hyppönen, finlandês, direto da empresa de segurança de redes F-secure, declarou que devido à complexidade do Stuxnet, certamente foi necessária uma grande quantidade de dinheiro para elaborá-lo, restando como possível criador algum governo. Nas investigações promovidas por Hyppönen e um grupo de especialistas em 2012, eles teriam descoberto uma lista de e-mails ligadas ao Stuxnet que indica o envolvimento dos EUA, ou país aliado, com o Worm.

> "Foi em 2010, quando tivemos acesso ao Stuxnet original. Ele foi encontrado por uma pequena empresa de antivírus da Bielorrússia. As companhias do leste europeu prestam serviços de segurança para o Irã porque não têm restrições em fazer negócios com aquele país, ao contrário do resto da Europa. Começamos a prestar mais atenção porque o vírus explorava uma falha de dia zero –vulnerabilidade de um sistema, como o Windows, que não haviam sido notadas antes. Falhas de dia zero são raras, valiosas e interessantes.
> Só então encontramos outras falhas dia zero sendo exploradas. Não havíamos nunca, jamais, visto malware que explorava mais de uma falha dia zero. O Stuxnet explorava três. O que é completamente único. E isso imediatamente diz que não é normal.
> Então começamos a nos dar conta de que o que tínhamos na mão era tão grande e complicado, e provavelmente foi tão caro para ser desenvolvido, que a fonte era um governo. Também encontramos dicas de que o vírus fora encontrado no Irã e tinha a ver com o programa nuclear.
> Um amigo meu da empresa Computer Associates, da Austrália, foi o primeiro a declarar em uma lista de e-mails que, com base no que havia sido descoberto até então, era seguro dizer que tratava-se de uma operação do governo dos Estados Unidos contra o programa nuclear iraniano.
> Ele enviou esse e-mail e, dois minutos depois, enviou outro dizendo que gostaria que todos soubessem que ele nunca teve tendências suicidas –só para o caso de ser encontrado morto. Isso é o quão paranoicos estávamos" (ARAGÃO, 2014)

Outra evidência do envolvimento de um governo na criação do Stuxnet é o interesse geopolítico que recaía sobre o programa nuclear iraniano até então; não há, ou houve, indícios ou motivos que apontem para alguma entidade privada em dispensar tamanha quantidade de recursos para atacar o projeto persa. O gráfico (Fig. 15) e mapa (Fig. 16) a seguir foram elaborado pela Symantec[9], no qual se observa a maior presença do Stuxnet no Irã.

[9]Empresa americana especializada em antivírus.

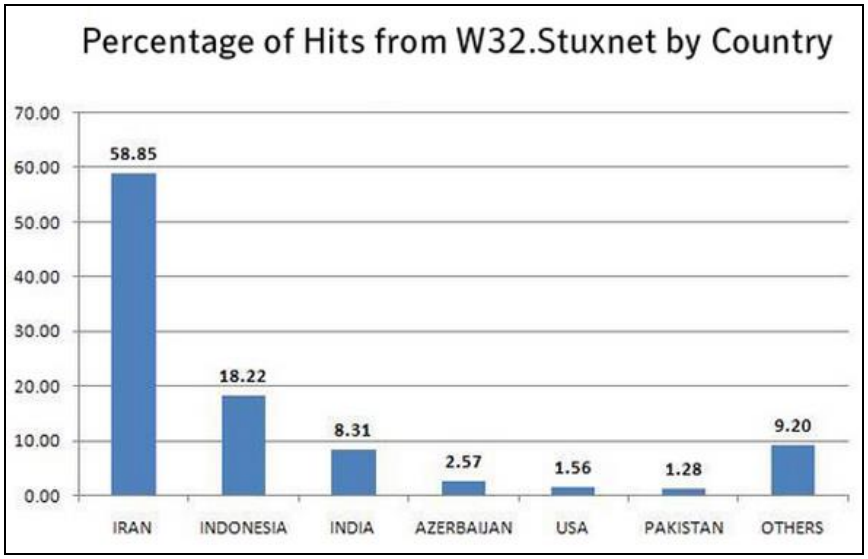

Figura 15: Porcentagens de países atingidos pelo Stuxnet. Fonte: SYMANTEC(2013).

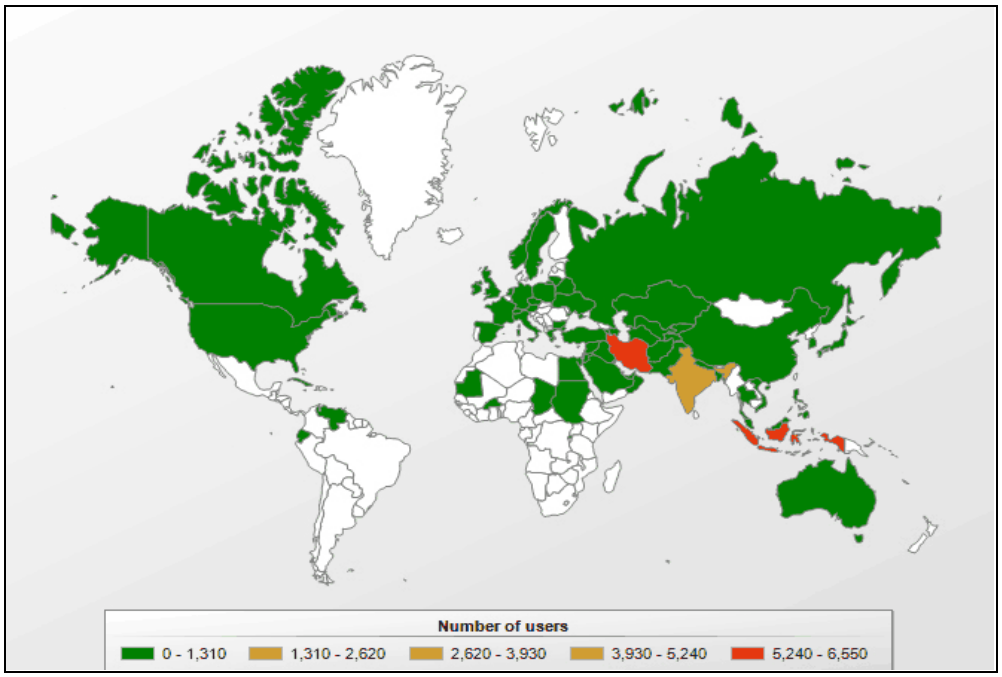

Figura 16: Abrangência do Stuxnet em setembro de 2010. Fonte: LES MOUTONS ENRAGES (2010)

O Stuxnet teve grande poder de contágio, porém seu foco principal foi sem sombra de dúvidas o Irã; dada a grande presença no país persa e as especificações do WormStuxnet, restam poucas dúvidas a respeito de qual era seu alvo.

O Stuxnet de fato conseguiu frear o programa nuclear iraniano. Junto a ele, mais três outros vírus (Duqu, Flame e Gauss) foram usados contra o Irã e demais países da "Lista Negra Norte Americana". Diferentes do Stuxnet, os três vírus, Duqu, Flame e Gauss, não tinham como objetivo destruir algum setor vital para a economia dos seus

alvos, estes eram antes vírus espiões. A espionagem também é parte importante na Ciberguerra, e esse conjunto de vírus não fugiu da mesma sofisticação, complexidade de elaboração e surgiram quase que na mesma época que o Stuxnet (2010). Analisemos separadamente cada um.

Segundo analistas da KasperskyLab[10], o Duqu tem a mesma sofisticação do Stuxnet, porém com o objetivo de ser um vírus espião (o Stuxnet foi formatado para destruir parte do sistema nuclear iraniano). O Duqu foi detectado pela primeira vez em setembro de 2011 por um usuário membro da Universidade de Tecnologia e Economia de Budapeste (não se sabe exatamente quando o vírus foi criado). O que se sabe até o momento é o Duqu é muito parecido com o Stuxnet, porém foi criado para ser um vírus do tipo Backdoor[11].

Outro potente vírus que se junta ao Stuxnet e ao Duqu é o Flame. A descoberta do Flame foi divulgada em maio de 2010 pelas fabricantes de antivírus KasperskyLab, McAfee e pelo Centro de Respostas a Incidentes de Segurança Nacional do Irã (Maher); para cada um desses órgãos o vírus recebeu um nome diferente. Para a KasperskyLab, o vírus foi batizado de "Flame", para a McAfee, "Skywiper" e para o Centro de Respostas a Incidentes de segurança Nacional do Irã, recebeu o nome de "Flamer".

O Flame foi projetado para ser um vírus espião, com capacidade de tornar o computador infectado uma janela aberta para quem comanda o Malware. Muito mais sofisticado que um Spyware[12][3], o Flame não tem como objetivo o simples roubo de senhas e contas aleatórias enviando-as um já determinado endereço, embora também possa fazê-lo. Este foi programado para permitir o livre acesso a todas as informações acessadas por um usuário de um computador invadido. Sendo assim, quem comanda o Flame pode ver todo conteúdo visto em um computador contaminado, copiar mensagens de e-mail, conversas instantâneas e vídeos, como também ter acesso a microfones e câmera disponíveis no computador, podendo gravar sons e imagens. O Flame é tão sofisticado que ele pode utilizar a conexão bluetooth (conexão sem fio entre computadores) para se espalhar de um computador para outro (GOSTEV, 2010).

[10]KasperskyLab é quarta maior companhia de antivírus do mundo proporcionando uma das protecções mais rápidas neste setor.

[11]Backdoors são vírus que permitem quem os controla acessar um computador invadido e ter acesso ao conteúdo da vítima (CGIBR, 2006).

[12]Spyware são malwares capazes de roubas informações de senha e contas dos usuários infectados (CGIBR, 2006).

Segundo pesquisadores da KasperskyLab, a complexidade do Flame é superior ao Stuxnet; a análise completa do Flame pode demorar algo em torno de 10 anos, enquanto o Stuxnet foi totalmente analisado e decifrado em cerca de um ano. A tamanha complexidade do Flame, tal como o Stuxnet, evidencia grande necessidade de recursos para sua elaboração. A ausência de interesses comerciais aparentes e grandiosa elaboração do Malware, faz com que a KasperskyLab atribua o vírus a algum Estado.

A ligação entre o Stuxnet e o Flame não é algo fácil de ser comprovada. Fato é que mal sabemos os reais criadores desses potentes vírus. Algo que atenta para o elo desses Malwares são traços semelhantes encontrados por pesquisadores da área nos seus códigos fonte. Outro possível elo entre esses, talvez resida no fato da localização geográfica de onde foram encontrados; ambos os vírus foram amplamente encontrados no Irã, principalmente, e demais países do Oriente Médio. Ou seja, quem quer tenha criado esse trio de vírus (Stuxnet, Duqu e Flame) teve como objetivo específico espalhá-los pelo Irã para atacar o país persa. Dada tamanha complexidade dos Malwares e, concomitantemente o mesmo foco, ou mesmo país inimigo, algo sugere que o criador, ou criadores, do Stuxnet, Duqu e Flame tenha muito em comum.

A respeito da ligação entre Flame e Stuxnet, os principais periódicos dos EUA, New York Times e Washington Post afirmam que seu governo em conjunto com Israel, tenha planejado atacar o programa nuclear iraniano por meio de uma grande operação batizada de "Jogos Olímpicos" (NAKASHIMA; MILLER; TATE, 2012). Outro dado interessante e que aponta contar o governo norte americano e aliados é o fato do Flame ser mais encontrado em países considerados rivais americanos, ou seja, países "aliados ao terrorismo", como podemos observar na figura a seguir, elaborada pela maior empresa de segurança de redes russa e europeia, KasperskyLab (Fig. 17):

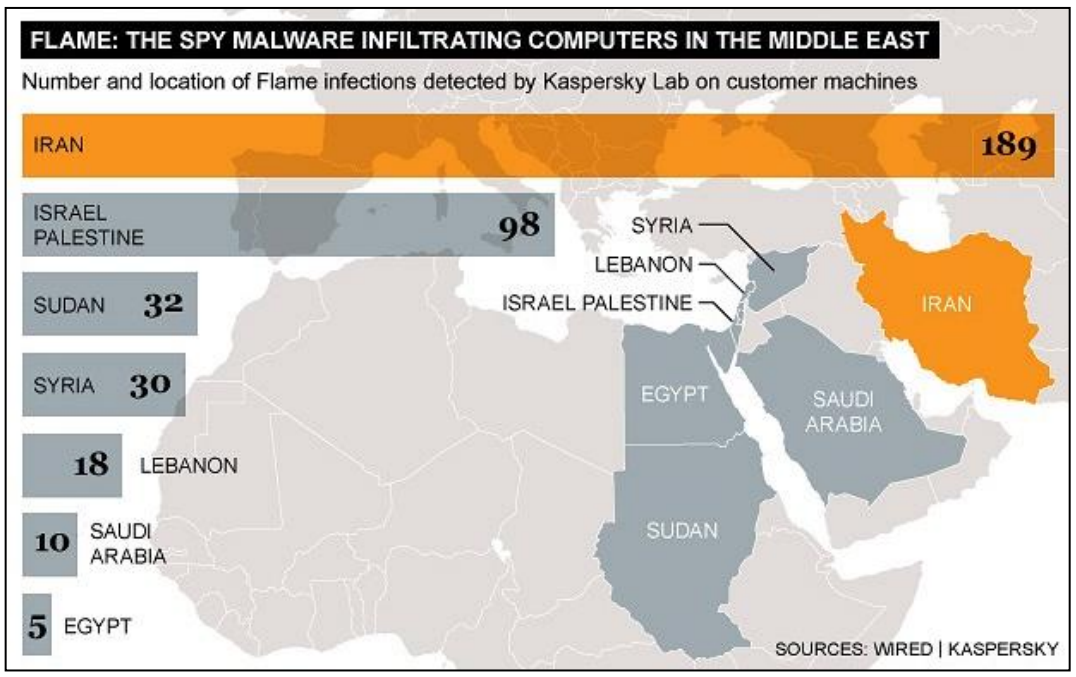

Figura 17: Abrangência do Flame em 2012. Fonte: ABOVE (2012)

Como podemos observar, os principais alvos do Flame são, concidentemente ou não, alguns países aliados dos Estados Unidos (Arabia Saudita e Israel) e, principalmente, países que compõem a "Lista Negra Norte Americana" de países que colaboram com o terrorismo. Na figura anterior, entre os quatro países onde o Flame foi mais encontrado, temos respectivamente, Irã, Israel/ Palestina, Sudão e Síria; com exceção Israel, Irã, Sudão e Síria pertencem à lista de países colaboradores ao terrorismo proposta pelos EUA. Vale salientar que a grande presença do vírus em Israel não demonstra que o país seja necessariamente um alvo do Stuxnet; pelo que tudo indica, o vírus teve um alvo certo, o Irã, e pode ter sido apenas Israel foi à porta de entrada do vírus. Reportagens dos dois principais periódicos dos Estados Unidos, New York Times (SANGER, 2012) e Washington Post (NAKASHIMA; MILLER; TATE, 2012), apontam para a cooperação dos EUA/Israel.

Completando o quadro desses supervírus atribuídos a estados, temos o Gauss. Descoberto depois do Duqu e Flame, o Gauss seria o último supervírus a compor o assim chamado pelo New York Times de "Olympic Games", atribuído aos EUA e Israel. O Gauss foi descoberto por uma investigação da Agência das Nações Unidas para a Informação e Comunicação Tecnológica (United NationsSpecializarAgency for Infotmation and Communication Technologies). A agência vinculada à ONU realizou uma serie de varreduras a procura de novos vírus que poderiam, de alguma forma, colocar em risco a segurança das telecomunições globais. Os trabalhos da organização começa-

ram de fato logo após a descoberta do Flame, em um primeiro momento buscavam encontrar novos focos do Vírus; com as buscas, foi detectado um novo vírus com estrutura tão semelhante ao Flame que acabou sendo confundido com o próprio vírus.

> "O Gauss contém semelhanças surpreendentes com o Flame, como o seu desenho e a base do código, o que nos permitiu descobrir o programa malicioso. Tal como o Flame e o Duqu, Gauss é um complexo conjunto de ferramentas de ciberespionagem, que opera com sigilo e em segredo. No entanto, o seu propósito é diferente, já que o Gauss dirige-se a múltiplos utilizadores em países selecionados, com a finalidade de roubar grandes quantidades de dados, com um enfoque específico em informação bancária e financeira" (KASPERSKY, 2012).

Embora muito parecido com o Flame, o Gauss se diferencia pela função e distribuição geográfica. Criado para roubar histórico de sites visitados, configuração do computador e principalmente senhas e credenciais bancárias, ele se diferencia do Flame uma vez que foi programado para uma função específica, roubar e gravar senhas bancárias. O Foco de localização do novo vírus também chamou atenção dos especialistas da Agência das Nações Unidas para a informação e Comunicação Tecnológica e da Kaspersky; enquanto Stuxnet, Duqu e Flame foram mais encontrados no Irã, o Gauss foi mais detectado no Líbano. Segundo as primeiras análises feitas pela KasperskyLab, o Malware foi criado pra roubar dados especificamente de bancos libaneses, seus alvos seriam os principais bancos do Líbano: Banco de Beirut, o EBLF, BlomBank, Byblos-Bank, FransaBank e CreditLibanais.

Sabendo-se do interesse dos criadores do Gauss em contas bancárias em bancos libaneses, resta a pergunta de o porquê desse interesse. Mesmo evitando fazer especulações, não poderíamos desconsiderar o fato de que os bancos Libaneses são uma das supostas entradas de dinheiro para o financiamento do Hezbollah, um dos principais grupos identificado como terrorista pelo Estado de Israel.

Ainda em julho de 2008, antes da descoberta do Gauss ou mesmo da sua criação (A KasperskyLab acredita que o Malware tenha sido criado em 2011), advogados de sessenta israelenses lesados pelo Hezbollah entraram na justiça dos Estados Unidos contra bancos libaneses pelo suposto apoio dos bancos ao grupo “terrorista”; o Título da reportagem era “Israelenses exigem indenização de bancos libaneses por apoio ao Hezbollah” (PORTAL G1, 2008)

Como podemos observar no mapa a seguir, das dezenas de vezes que o Gauss foi detectado, a enorme maioria foi no Líbano; seguido por Israel, Palestina e por seguinte Irã (Fig. 18). Se esses supervírus, ou armas cibernéticas, só poderiam ter sido criados por um Estado, com afirmam diversos relatórios e pesquisadores estudiosos dos Malwares analisados até aqui, os motivos para a utilização destes por parte dos Estados Unidos e Israel, como afirma o New York Times e Washington Post, em países como Irã e Líbano existe ou existiu.

O conjunto de supervírus Duqu, Flame e Gauss foram mais encontrado consecutivamente em Israel/Palestina, Líbano, Irã, Sudão e Síria. Entre as cinco localidades de maior ocorrência dos vírus, quatro são consideradas rivais ou de interesses dos EUA e Israel; Irã, Sudão e Síria compõem a lista de países apoiadores do terrorismo elaborada pelo governo norte americano e o Líbano é reduto do grupo "terrorista" Hezbollah, um dos principais rivais israelenses na região.

Muito embora ainda não tenha havido pronunciamento oficial por parte de nenhum governo reivindicando a autoria dos ataques, a possibilidade que esses supervírus sejam as primeiras "Ciberarmas" utilizadas no conforto entre Estados é enorme. Novas armas como os supervírus analisados até agora são tanto consequência do desenvolvimento do capitalismo financeiro informacional, como da mudança nos novos tipos de guerra, ou seja, a composição da "Guerra Instantânea" proposta por Manuel Castells. Visto isso, não é de se admirar o aumento da importância dada aos setores informacionais pelos países no século XXI; da mesma forma cresce, também, a atenção a uma nova forma de Guerra, a Ciberguerra.

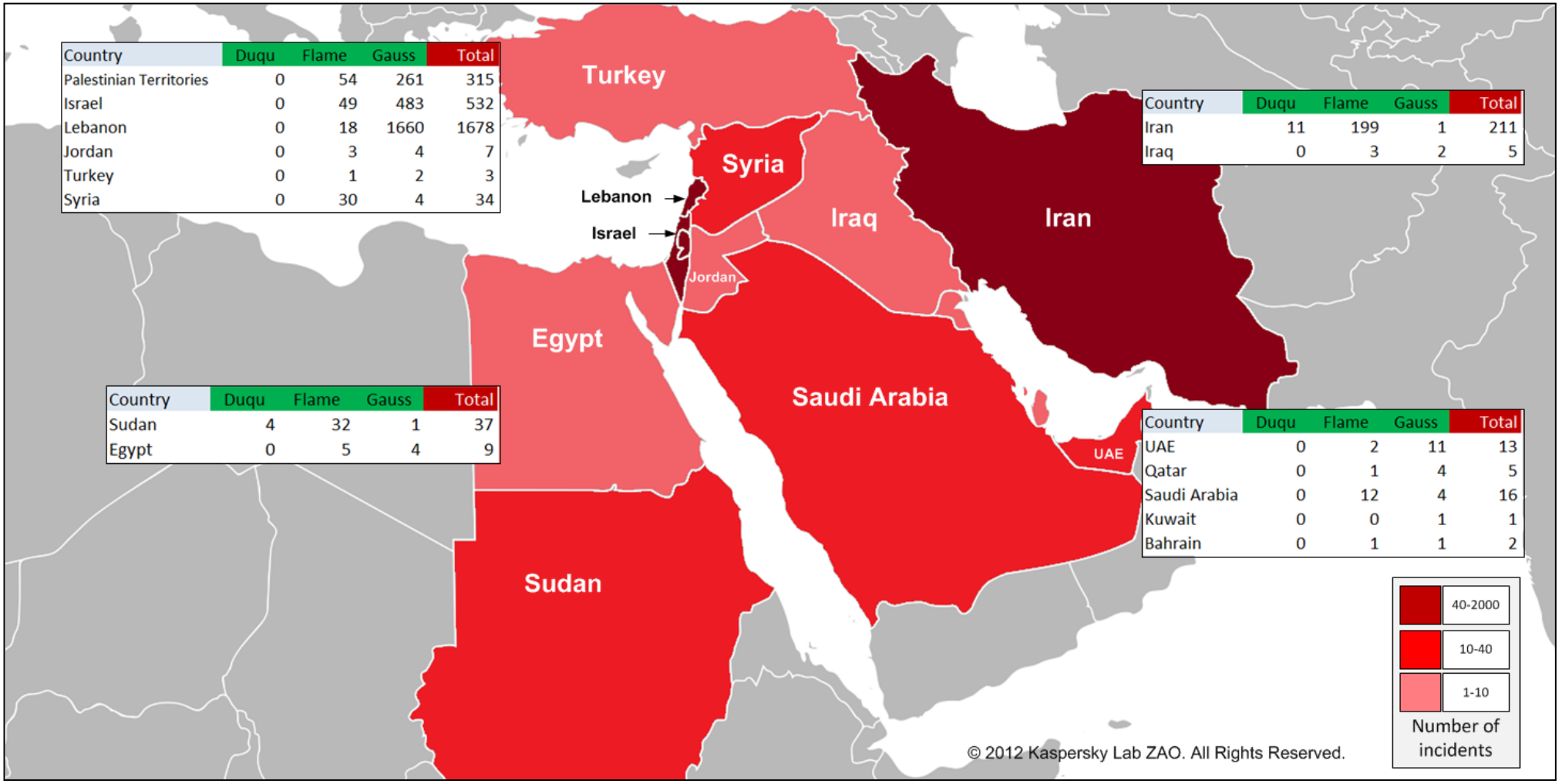

Figura 18: Comparação entre países cujos computadores foram infectados por Duqu, Flame e Gauss. Fonte: GREAT (2012)

Conclusão

Como podemos perceber, o espaço virtual tornou-se condição s*inequa non* para o funcionamento das sociedades atuais na era do capitalismo financeiro. Desse modo, a dependencia gerada pela revolução informacional sobre as redes nunca havia atingido tamanha imensidão como podemos constatar hoje, tendência essa que não para de aumentar. Os limites territoriais, os bens naturais e mesmo o espaço geográfico sem dúvida algumas são peças fundamentais para a geopolítica, porém pode estar "entrando em cena" uma nova questão a ser considerada, o ciberespaço e, sobretudo, os conflitos ocorridos dentro deste.

Uma vez que as diversas revoluções industriais e o domínio de novas técnicas marcaram novos períodos, as próprias guerras apresentam traços dessas mudanças; até mesmo o advento da tecnologia nuclear e desenvolvimentos de meios de comunicação podem ter feito com que houvesse mudanças substancias nas guerras tradicionais, dando lugar à "Guerra Instantânea" proposta por Castells; a Ciberguerra vem como fruto desse novo período e vê que neglicenciar as batalhas no ciberespaço pode ser um tanto quando perigoso para a maioria dos paises da contemporaneidadae.

Como retratado, a internet surgiu nos meios militares com o principal objetivo de defesa e, posteriormente, nas décadas de 80 e 90, com os desdobramentos da revolução informacional, ela foi aprimorada e ampliada pelos poucos civis usuários da rede. Não demorou muito para que essas novas tecnologias, oriundas dos meios acadêmicos e militares, fossem empregadas em guerras ou ao menos incorporadas a arsenais militares de diversas potências mundiais.

Se esse grande desenvolvimento tecnológico vivido por parte das potências mundiais, sobretudo ocidentais, permitiu armas mais avançadas e eficientes na contenta entre Estados, ele também tornou a guerra muito mais próxima do cidadão comum; a transmisão de uma guerra pela televisão, internet ou mesmo por rádio fez com que os horrores de uma guerra pudessem ser vistos quase que de perto pela opinião pública. Isso vem, segundo Castells, colocando limites aos Estados e seus governantes, e tornando o ato de declaração de guerra, ou mesmo o próprio modo de se guerrear, mais distantes das tomadas de decisões dos países em relação a antes do desenvolvimento das tecnologias de informação.

Partindo-se do pressuposto de que ainda existem e provavelmente haverá novos conflitos, os Estados possivelmente teriam que adaptar ou encontrar novas formas de se fazer a guerra. Soma-se a essa necessidade o pungente crescimento e dependências dos países sobre as novas tecnologias e a rede mundial de computadores, a internet, de modo que teremos, possivelmente, um novo espaço vital para se fazer a guerra. Embora seja quase que utópico imaginar que os países deixarão de se enfrentar em suas fronteiras para guerrear somente pelas redes de computadores, as redes (graças a sua imensa importância) vêm se tornando um novo palco de conflitos e a Ciberguerra pode ser vista como uma etapa, e ou, nova forma de batalha dentro das "Guerras Instantâneas".

Embora nenhum Estado tenha assumido algum ciberataque, as evidências e os fatos tornam-se imperiosos para apontar o envolvimento de setores governamentais na criação de vírus como o Stuxnet, Frame, Glauss e Duqu; soma-se a isso os maiore investimentos estatais em proteção das redes e criação de setores militares responsáveis por estas.

Nenhum país assumir a criação de super vírus com fins militares é condizente com o objetivo da Ciberguerra, levando-se em conta que uma vez plenamente assumida, a guerra virtual pode se tornar menos letal, visto que os sistemas de segurança de rede obrigatóriamente teriam que ser mais cuidadosos e dispor mais investimentos em proteção; junto a isso a Ciberguerra perderia seu caráter oculto.

Com a revolução tecno-cientifica-informacional, o ciberespaço tornou-se peça importante para o funcionamento dos atuais Estados, do sistema financeiro ou mesmo da ampla gama de novas tecnologias desenvolvidas e aprimoradas todos os dias. Talvez agora seja tempo de olharmos para o ciberespaço de outra forma, sobretudo na geopolítica devemos considerar não só a influência do ciberespaço nas novas tecnologias e na forma dos conflitos, como também a própria guerra dentro desse universo, a ciberguerra.

Referências bibliográficas

ABOVEtop secret. Flame Virus Update: UK Servers UsedtoControlMalware. 2012. Disponível em: <http://www.abovetopsecret.com/forum/thread848503/pg1>. Acesso em: 10 ago. 2014.

ALBANESIUS, A.; SELTZER, L. Report: StuxnetWormAttacks Iran, Who isBehind It? PCMAG. 2010. Disponível em: <www.pcmag.com/article2/0,2817,2369745,00.asp>. Acesso em: 12 set. 2014.

ARAGÃO, A. Analista revelou vírus de computador instalado pelos EUA no Irã. Folha de São Paulo. 2014. Disponível em: http://www1.folha.uol.com.br/tec/2014/09/1509250-analista-revelou-virus-de-computador-instalado-pelos-eua-no-ira.shtml. Acesso em: 10 set. 2014.

ATSN. AOL Transit Data Network (ATDN). Disponível Em: <http://www.atdn.net/images/usa.gif>.Acesso em: 20 nov. 2009.

BARBOSA, E.S. Gêngis Khan e as conquistas mongóis. História das Guerras: Editora Contexto, 2013.

BBC. SuperPower: Visualisingthe internet. 2010. Disponível em: <http://news.bbc.co.uk/2/hi/technology/8552410.stm>. Acessoem: 10 ago. 2014.

BILGIL, M.Historyofthe Internet.PICOL icons.2009. Disponível em: http://vimeo.com/2696386. Acesso em: 17 out. 2014.

BURTON, M. S. Connectingthe Virtual Dots: Howthe Web CanRelieveOurInformationGlut and GetUsTalkingtoEachOther. **Studies in intelligence**, v. 49, n. 3, 2005.

CASTELLS, M. A sociedade em rede. Volume I. São Paulo: Paz e terra, 2000.

CASTELLS, M. A galáxia da Internet: reflexões sobre a Internet, negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CARRENHO, C. O Brasil não é o país do e-reader. Tiposdigitais. 2014. Disponível em: <http://www.tiposdigitais.com/2014/04/brasil-n%C3%A3o-%C3%A9-pa%C3%ADs-do-ereader.html>. Acesso em: 25 set. 2014.

CGIBR. Cartilha de Segurança da Internet. Parte VIII: Códigos Maliciosos (Malware). CGIBR-Comitê Gestor da internet no Brasil, Versão 3.1. 2006. Disponível em: <http://www.ertech.com.br/artigos/docs/cartilha-08-malware.pdf>. Acesso em: 14 out. 2014.

DEAN, D. et al. The internet economy in the G-20. The Boston consultinggroup. 2012. Disponível em: <https://www.bcg.com/documents/file100409.pdf>. Acesso em: 07 mai. 2013.

EXAME. Metade da população mundial deverá ter 4G até 2017. 2012.Disponível em: <http://exame.abril.com.br/tecnologia/noticias/metade-da-populacao-mundial-devera-ter-4g-ate-2017>.Acesso em: 23 jul. 2014.

FILHO, G.L.M. Hackers e Crackers na internet: as duas faces da moeda. Revista Eletrônica Temática, Ano VI, n. 01, jan. 2010.

FUNARI, P. P.Guerra do Peloponeso. In: Demétrio, M. História das guerras. São Paulo: Editora contexto, 2013. p. 19-46.

HOÁNG, Michel. Gengis Khan. São Paulo: Globo, 2002.

HUMBOLDT-Universitätzu Berlin. Geschichtedes Internets. 2007. Disponível em: <http://medienwissenschaft.uni-bayreuth.de/dimensionen/unterrichtsentwuerfe/Unterrichtsentwurf_Geschichte_des_Internets.pdf>. Acesso em: 30 set. 2014.

JUNIOR, A. C. A dimensão geográfica da internet no Brasil e no mundo. 2008. 246 f. Dissertação (Mestrado em geografia humana) - Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de SãoPaulo, São Paulo, 2008.

KASPERSKY. KasperskyLab descobre 'Gauss' - uma nova ciber-ameaça que monitoriza contas bancárias online. 2012. Disponível em: <http://www.kaspersky.com/pt/about/news/virus/2012/kaspersky_lab_descobre_gauss_uma_nova_ciber-ameaca_que_monitoriza_contas_bancarias_online>. Acesso em: 24 set. 2014.

KASPERSKY. Whatis Flame? Disponível em: http://www.kaspersky.com/flame>. Acesso em: 10 mar. 2014.

LES MOUTONS ENRAGES. Lessurprises que nousréserve2011…..Ben voilàquoi, enfin…vous m'avezcompris… 2010. Disponível Em: http://lesmoutonsenrages.fr/2010/12/. Acesso em:16 set. 2013.

LUCCI, E. A. A nova ordem mundial e a geografia do poder. Ciências geográfica, v. XV, n. 1, p.13-17, 2011.

MARTIN, A. Guerra de secessão. In: Demétrio, M. História das guerras. São Paulo: Editora contexto, 2013. p. 219-252.

MILLWARD BROWN. BrandZ™ Top 100 MostValuable Global Brands 2014. 2014. Disponível em: http://www.millwardbrown.com/docs/default-source/global-brandz-downloads/global/2014_BrandZ_Top100_Report.pdf. Acesso em: 20 out. 2014.

MIRANDA, A. D. A. Introdução ás redes de computadores. ESAB – ESCOLA SUPERIOR ABERTA DO BRA-SIL LTDA, 2007.

NAKASHIMA E.; MILLER, G.; TATE, J. U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. 2012. Disponível em: <http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html>. Acesso em: 29 set. 2014.

ONDA. Como funciona a internet. 2004. Disponível em: <curso-yai.googlepages.com/internet.pdf>. Acesso em: 16 nov. 2009.

PORTAL G1. Israelenses exigem indenização de bancos libaneses por apoio ao Hezbollah. 2008. Disponível em: <http://g1.globo.com/Noticias/Mundo/0,,MUL640201-5602,00-ISRAELENSES+EXIGEM+INDENIZACAO+DE+BANCOS+LIBANESES+POR+APOIO+AO+HEZBOLLAH.html>.Acesso em: 24 set. 2014.

PORTAL G1. Hackers invadem site do Pentágono e roubam projeto de avião de US$ 300 bi. 2009. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1092884-6174,00-HACKERS+INVADEM+SITE+DO+PENTAGONO+E+ROUBAM+PROJETO+DE+AVIAO+DE+US+BI.html>. Acesso em: 28 jan. 2014.

PORTAL G1. Número de smartphones no mundo vai triplicar até 2018, aponta estudo. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/11/numero-

de-smartphones-no-mundo-vai-triplicar-ate-2018-aponta-estudo.html>. Acesso em: 23 Jul. 2014.

RNP. Rede Ipê. Rede nacional de ensino e pesquisa (RNP). 2014. Disponíve-lem<http://www.rnp.br/servicos/conectividade/rede-ipe>. Acesso em: 28 out. 2014.

SANGER, D. E. Obama Order Sped Up Wave of CyberattacksAgainst Iran. Ney Yok Times. 2012. Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=2&>. Acesso em: 29 set. 2014.

SANTOS , Milton. Por uma geografia das Redes. In: A Natureza do Espaço. Técnica e Tempo. Razão e Emoção. São Paulo. HUCITEC, 1996.

SANTOS M. R.; VERSIGNASSI, A. Vírus entra em programa nuclear e salva o mundo. Super Interessante. 2011. Disponível em: <http://super.abril.com.br/tecnologia/virus-programa-nuclear-salva-mundo-619652.shtml>. Acesso em: 28 jan. 2014.

SYMANTEC. W32.Stuxnet. 2013. Disponível em: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>. Acesso em: 24 set. 2014.

VEJA. As armas dos EUA para fritar Saddam. 2003. Disponível em: <http://veja.abril.com.br/190303/p_052.html>. Acesso em 24 jul. 2014.

VIRILIO, P. O espaço crítico e as perspectivas do tempo real. São Paulo: editora 34, 1993.

WAACK, W. Guerras do Golfo. In: Demétrio, M. História das guerras. São Paulo: Editora contexto, 2013. p. 453-477.

Anexos

Exército do Reino Unido cria força especial de soldados do Facebook para guerras cibernéticas

fevereiro 1, 2015 10:03

Veja também

Soldados britânicos com habilidades em jornalismo e familiaridade com mídias sociais estão entre os mais procurados para compor 77ª Brigada

Por Opera Mundi

O Exército britânico está criando uma força especial de guerreiros do Facebook, especializados em operações psicológicas e no uso das mídias sociais para se envolver em guerras cibernéticas, reportou o *Guardian* neste sábado (31/01).

A 77ª Brigada será sediada em Hermitage, a cerca de 100 quilômetros de Londres, e será formada por cerca de 1.500 pessoas. Para o recrutamento, a instituição vai incluir regulares e reservistas. Soldados com habilidades em jornalismo e familiaridade com as mídias sociais estão entre os mais procurados.

A criação da entidade será formalmente anunciada apenas em abril, antecipou o veículo inglês. Ela será responsável por aquilo que é descrito como uma guerra não letal. Exércitos de Israel e dos Estados Unidos, por exemplo, já têm experiência e envolvimento em operações do gênero.

"A 77ª Brigada está sendo criada para enfrentar os desafios da guerra moderna. Trata-se de reconhecer que as ofensivas em um campo de batalha moderno podem ser afetadas de maneiras que não são necessariamente violentas", explica um porta-voz do Exército do Reino Unido.

A decisão de elaborar a brigada é, em parte, resultado de experiência em operações de contra-insurgência no Afeganistão. A criação da entidade também é vista como uma resposta aos acontecimentos de 2014, que incluem a anexação da península ucraniana da Crimeia pelos russos e a tomada de terras do Estado Islâmico em áreas na Síria e no Iraque. O grupo extremista sunita, em particular, revelou forte habilidade na exploração das mídias sociais para atrair milicianos ao redor do mundo.

Foto: Flickr/ U.S Army

Comentários

Fonte: http://www.revistaforum.com.br/blog/2015/02/exercito-reino-unido-cria-forca-especial-de-soldados-facebook-para-guerras-cibernetica s/

Ciberataques

"A China tem um exército de hackers", diz professora do MIT

Nazli Choucri fala sobre as dezenas de ataques de hackers que empresas americanas e órgãos do governo sofreram a partir de computadores localizados na China

por Vivian Eichler 07/06/2013 | 05h03

Autora do livro **Cyber Politics in International Relations**, Nazli Choucri fala sobre as dezenas de ataques de hackers que empresas americanas e órgãos do governo sofreram a partir de computadores localizados na China. O tema deve ser um dos mais polêmicos no encontro entre o presidente americano, Barack Obama, e o novo presidente chinês, Xi Jinping, hoje e amanhã, na Califórnia. Para Nazli, os Estados Unidos estão chocados diante da capacidade chinesa, mas não conseguem organizar um front para se defender das ameaças.

Fonte: http://zh.clicrbs.com.br/rs/noticias/noticia/2013/06/a-china-tem-um-exercito-de-hackers-diz-professora-do-mit-4162359.html

15/03/2013 - 09h16

Coreia do Norte acusa EUA e sul-coreanos de ataques cibernéticos

DA REUTERS, EM SEUL

A Coreia do Norte acusou nesta sexta-feira os Estados Unidos e a Coreia do Sul de realizar ataques digitais aos servidores de internet do país. A reclamação foi feita após vários meios da mídia oficial na rede saírem do ar.

A acusação ocorre num momento de crescente tensão entre a reclusa Coreia do Norte e a Coreia do Sul, junto com os EUA, país aliado dos sul-coreanos, causada pelo aumento das sanções da ONU (Organização das Nações Unidas) ao país devido a um teste nuclear realizado em fevereiro.

O regime comunista chama as sanções de uma declaração de guerra e também se queixou dos exercícios militares conjuntos que são realizados pelos EUA e a Coreia do Sul. Devido à ação militar, o ditador Kim Jong-un rompeu unilateralmente o armistício vigente desde a Guerra da Coreia (1950-1953).

Segundo a agência de notícias russa Itar-Tass, "um poderoso ataque cibernético do exterior" derrubou todos os servidores norte-coreanos, o que impediu o acesso a alguns sites. O canal de TV sul-coreano MBC disse que os serviços noticiosos do Norte estão entre os afetados pelo ataque cibernético.

Dentre eles, estão a agência de notícias KCNA e o jornal oficial "Rodong Sinmun", que estariam supostamente com instabilidades -- embora fossem acessados normalmente na quinta (14) e sexta-feira. Os dois são os principais meios de comunicação para o país.

Fonte: http://www1.folha.uol.com.br/mundo/1246704-coreia-do-norte-acusa-eua-e-sul-coreanos-de-ataques-ciberneticos.shtml

Coréia do Norte cria exército de hackers para atacar defesa inimiga

0

POR VIA COMERCIAL EM 6 DE JULHO DE 2014 — POLÍTICA

A Coreia do Norte duplicou o número de pessoas envolvidas em ciberataques durante os últimos dois anos e estabeleceu bases no estrangeiro, informou neste domingo a agência de imprensa sul-coreana. O objetivo é fragilizar os sistemas de defesa dos inimigos.

A unidade de "pirataria informática" da Coreia do Norte conta agora com 5.900 pessoas, contra cerca de 3.000 há dois anos, garante a agência Yonhap.

Os hackers norte-coreanos também estão atuando a partir de bases no estrangeiro, especialmente no Japão, Estados Unidos e países europeus.

Nos últimos anos, os hackers norte-coreanos atacaram vários objetivos na Coreia do Sul, como agências militares, bancos, órgãos do governo, redes de televisão e sites de comunicação.(Notibras)

Fonte: http://www.viacomercial.com.br/2014/07/coreia-do-norte-cria-exercito-de-hackers-para-atacar-defesa-inimiga/

OLHAR DIGITAL Notícias ▾ Vídeos ▾ Olhar Digital PRO Fórum Downloads

Home » Últimas notícias » Hackers do Estado Islâmico atacam contas do Exército dos EUA

Hackers do Estado Islâmico atacam contas do Exército dos EUA

Por Redação Olhar Digital - em 12/01/2015 às 19h02

Avaliação: ★★★★ Avaliar: ☆☆☆☆☆

Hackers

(Foto: Reprodução)

Curtir 41 Share 9 Tweetar 82 +1 +8

Fonte: http://olhardigital.uol.com.br/noticia/hackers-do-estado-islamico-atacam-contas-do-exercito-dos-eua/46183

mundo

China contrata hackers desde 2002; veja mais revelações do WikiLeaks

DE SÃO PAULO

29/11/2010 ⊙ 12h40

Compartilhar 243 Tweetar 80 0 OUVIR O TEXTO + Mais opções

WIKI LEAKS especial

Cerca de 250 mil documentos diplomáticos confidenciais do Departamento de Estado dos EUA vieram à tona neste domingo, divulgados pelo site WikiLeaks. Os chamados "cables" revelam detalhes secretos -- alguns bastante curiosos-- da política externa americana entre dezembro de 1966 e fevereiro deste ano, em um caso que começa a ficar conhecido como "Cablegate".

Fonte: http://www1.folha.uol.com.br/mundo/2010/11/837822-china-contrata-hackers-desde-2002-veja-mais-revelacoes-do-wikileaks.shtml

Bolsa de valores NASDAQ foi hackeada por malware possivelmente russo

7.386 Visualizações | Por Leonardo Müller 18 jul 2014 - 12h 39

A bolsa de valores especializada em ações de empresas de tecnologia, a NASDAQ, sofreu um ataque hacker em 2010, mas só agora o acontecido se tornou de conhecimento público, quando a Bloomberg Businessweek publicou uma reportagem que relatava os passos das investigações feitas pelo FBI, CIA e NSA sobre o assunto.

Apesar de tanto esforço do governo norte-americano para encontrar a origem do malware que atacou os servidores da bolsa de valores, foi considerado praticamente impossível rastrear os hackers responsáveis, dada a bagunça generalizada que eram os registros da NASDAQ na época. As agências de segurança que realizaram investigações separadamente encontraram rastros de diversos ataques de anos anteriores que se acumulavam sem a bolsa de valores ter feito praticamente nada.

Esse descaso com a segurança na NASDAQ seria o principal problema para o rastreamento dos culpados pelo ataque. Originalmente, a Businessweek publicou que a compra e venda de ações na bolsa poderia ter sido comprometida pelo ataque em 2010, mas ontem mesmo o antigo chefe da NASDAQ afirmou que este não era o caso, já que o ataque não conseguiu atingir os sistemas de compra e venda de ações naquela oportunidade.

Fonte: http://www.tecmundo.com.br/ataque-hacker/59276-bolsa-valores-nasdaq-hackeada-malware-russo.htm

Guerra de hackers: Anonymous provoca Exército Eletrônico da Síria

2

Por Redação em | 05.09.2013 às 18h30

Os Estados Unidos e outras potências mundiais continuam debatendo uma possível intervenção militar na Síria, mas enquanto eles não chegam a um veredito, o grupo Anonymous já se manifestou e começou sua própria intervenção, enfrentando o temido Exército Eletrônico Sírio (EES). É uma batalha de hackers, e o Anonymous deu o primeiro golpe.

Fonte: http://canaltech.com.br/noticia/hacker/Guerra-de-hackers-Anonymous-provoca-Exercito-Eletronico-da-Siria/

Jornalista ligado a Snowden diz que EUA não espionam só alvos terroristas

Bernardo Caram - O Estado de S. Paulo
06 Agosto 2013 | 23h 26

Glenn Greenwald acusa Washington de usar sistema de vigilância global para beneficiar empresas americanas

BRASÍLIA - Glenn Greenwald, o jornalista do The Guardian responsável pela publicação das informações sobre o sistema de espionagem eletrônica dos EUA, disse neta terça-feira, 6, no Senado brasileiro, ter provas de que os americanos usam a rede para obter vantagens comerciais e tecnológicas. A afirmação derruba o argumento do governo de Barack Obama de que a Agência de Segurança

Fonte: http://internacional.estadao.com.br/noticias/geral,jornalista-ligado-a-snowden-diz-que-eua-nao-espionam-so-alvos-terroristas,1061270

Próximo Milênio: Richard Clarke e a guerra cibernética

sex, 25/02/11 por Equipe Milênio | categoria Notas, Programas, Vídeos | tags 11 de setembro, Al-Qaeda, CIA, contraterrorismo, cyber guerra, cyber war, EUA, FBI, guerra cibernética, hacker, inteligência, invasão, Iraque, Richard Clarke, segurança, terrorismo, vírus, worm

A **guerra cibernética** já começou. Quem faz o alerta é **Richard Clarke**, o homem que foi o chefe da segurança antiterrorista de quatro presidentes dos EUA (**Reagan**, **Bush pai**, **Clinton** e **Bush filho**) e o autor do livro "**Cyber War: The Next Threat to National Security and What to Do About It**" (em tradução livre: "Guerra Cibernética: a próxima ameaça à segurança nacional e o que fazer a respeito disso").

Fonte: http://g1.globo.com/globo-news/milenio/platb/2011/02/25/proximo-milenio-richard-clarke-e-a-guerra-cibernetica/

Sites do governo russo foram atacados por hackers; na foto, o presidente Vladimir Putin (foto: EPA)

14 MARÇO, 12:48 • MOSCOU • ZBF

(ANSA) - O governo russo confirmou nesta sexta-feira (14) que o site do Kremlin sofreu um forte ataque de hackers nesta manhã.
De acordo com o porta-voz do presidente Vladimir Putin, Dmitri Peskov, o portal www.kremlin.ru "sofreu um ataque massivo, iniciado durante a manhã, e que em parte prossegue até o momento". "No entanto, foram tomadas todas as medidas necessárias para proteger os dados informáticos do presidente", disse Peskov.
Em comunicado, o Banco Central da Rússia também confirmou que está com problemas em seu sistema devido a um ataque de hackers.
Já na Ucrânia, outros ataques atingiram hoje os sites do governo da Crimeia, região cujo Parlamento declarou independência e que domingo realizará um referendo para decidir sobre sua anexação à Rússia. Os ataques atingiram sites como o da Alta Corte de Simferopol e do Comitê Eleitoral que organiza o referendo.

Fonte: http://ansabrasil.com.br/brasil/noticias/mundo/noticias/2014/03/14/Sites-Russia-Crimeia-sofrem-ataques-hackers_7647955.html

/ tecnologia / espionagem

08/04/09 - 13h08 - Atualizado em 08/04/09 - 13h08

Rede elétrica dos EUA sofreu ataque espião, diz jornal

'WSJ' diz que softwares deixados na rede poderiam prejudicá-la. Objetivo seria investigar sistema elétrico e seus controles.

Da Reuters

editorias

Primeira Página
Blogs e Colunas
Brasil
Carros
Ciência e Saúde
Cinema
Concursos e Emprego
Economia e Negócios
Esporte
Mundo
Música
Política

saiba mais

Justiça dos EUA condena 'espiões do Vale do Silício' à prisão

Acusado de assassinato em Londres pode ser candidato a prefeito na Rússia

Comissão Europeia alerta para espiã 'loira e de pernas longas'

Ex-agente diz que EUA espionaram Tony Blair

Espiões entraram na rede elétrica dos Estados Unidos e deixaram nela alguns softwares que poderiam ser usados para prejudicar o sistema, informou o "Wall Street Journal" nesta quarta-feira (8).

Os espiões vieram da China, Rússia e outros países, segundo a reportagem. Acredita-se que sua missão fosse investigar o sistema elétrico dos EUA e seus controles, informou o jornal, citando antigos e atuais dirigentes dos serviços de segurança norte-americanos.

Fonte: http://g1.globo.com/Noticias/Tecnologia/0,,MUL1078121-6174,00-REDE+ELETRICA+DOS+EUA+SOFREU+ATAQUE+ESPIAO+DIZ+JORNAL.html

01/06/2012 - 14:55 COMPARTILHAR IMPRIMIR

Recomendar 67 +1 11 Tweet 71 Share Pin it

Ciberataque

Governo americano criou o vírus Stuxnet para atacar o Irã

Segundo o jornal The New York Times, o malware foi criado pelo Pentágono para retardar o programa nuclear iraniano

Tela de computador com vírus (Vladimir Mucibabic/iStockphoto/Getty Images)

O jornal americano *The New York Times* revelou hoje novos detalhes daquele que parece ter sido o primeiro grande ataque militar cibernético da história. Entre 2010 e 2011, um vírus

Fonte: http://veja.abril.com.br/noticia/vida-digital/governo-americano-e-responsavel-pelo-malware-stuxnet

EUA sabotaram programa nuclear do Irã

Em parceria com Israel, norte-americanos desenvolveram vírus complexo capaz de danificar centrífugas iranianas
Processo incluiu a construção de réplica de equipamentos iranianos; vírus saiu do controle em 2010

DAVID E. SANGER
DO "NEW YORK TIMES", EM WASHINGTON

Desde o começo de seu mandato, o presidente norte-americano, Barack Obama, vem ordenando ataques sigilosos e cada vez mais sofisticados contra os sistemas de computação usados para controlar as instalações de enriquecimento nuclear do Irã.

Assim, expandiu de maneira significativa o primeiro uso continuado de armas cibernéticas pelos EUA, afirmam participantes do programa.

Obama decidiu acelerar os ataques, iniciados no governo de George W. Bush sob o codinome "Olympic Games" ("Jogos Olímpicos"), mesmo depois que um dos elementos do programa chegou acidentalmente ao conhecimento do público em 2010.

Fonte: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all