UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE FILOSOFIA E CIÊNCIAS HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA

Marcelo Mesquita Leal

GUERRA E CIBERESPAÇO:
UMA ANÁLISE A PARTIR DO MEIO FÍSICO

Porto Alegre
2015

Marcelo Mesquita Leal

GUERRA E CIBERESPAÇO:
UMA ANÁLISE A PARTIR DO MEIO FÍSICO

Dissertação de Mestrado apresentada à Universidade Federal do Rio Grande do Sul como requisito parcial à obtenção do título de Mestre em Ciência Política.

Orientador: Dr. Marco Aurélio Chaves Cepik

Porto Alegre
2015

CIP - Catalogação na Publicação

Leal, Marcelo Mesquita
Guerra e Ciberespaço: uma análise a partir do meio físico / Marcelo Mesquita Leal. -- 2015.
58 f.

Orientador: Marco Aurélio Chaves Cepik.

Dissertação (Mestrado) -- Universidade Federal do Rio Grande do Sul, Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Ciência Política, Porto Alegre, BR-RS, 2015.

1. Ciberguerra. 2. Ciberoperações. 3. Guerra cibernética. I. Cepik, Marco Aurélio Chaves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Marcelo Mesquita Leal

GUERRA E CIBERESPAÇO:
UMA ANÁLISE A PARTIR DO MEIO FÍSICO

Dissertação de Mestrado apresentada à Universidade Federal do Rio Grande do Sul como requisito parcial à obtenção do título de Mestre em Ciência Política.

Dr. Marco Aurélio Chaves Cepik (Orientador) – UFRGS

Dr. Carlos Schmidt Arturi - UFRGS

Dr. Fabiano Pellin Mielniczuk - Audiplo

Dr. Reginaldo Mattar Nasser – PUC SP

Porto Alegre
2015

AGRADECIMENTOS

À Universidade Federal do Rio Grande do Sul e seu corpo docente, pela educação de qualidade e gratuita. Em especial, ao Prof. Paulo Visentini, pela orientação inicial e pela inspiração enquanto pesquisador. Ao meu orientador, Prof. Marco Cepik, pelo incentivo e pelas oportunidades de crescimento pessoal e profissional que ele me proporcionou.

Aos meus colegas do Centro de Estudos Internacionais sobre Governo, pelo ambiente de trabalho incrível, pelo conhecimento compartilhado e pelas ótimas risadas. Em especial, aos amigos que o trabalho me trouxe: à Bruna, à Joana e ao Gustavo, por serem as melhores companhias que uma pessoa pode ter.

Aos meus amigos, que, cada um a sua maneira, enchem meus dias de felicidades. Em especial às Camilas, eternas companheiras, pelas conversas e pelos afagos. Também ao Paulo, pelo carinho fraterno, ainda que distante.

Aos meus pais, Renato e Dirce, por sempre acreditarem no meu sucesso e me incentivarem a ir mais longe do que eu podia imaginar. À minha irmã, Renata, que se tornou a principal inspiração da minha vida. Ao meu sobrinho ou sobrinha, que já me traz tantas alegrias. Ao Diego, por fazer dessa jornada a mais agradável o possível.

RESUMO

O presente artigo tem por objetivo demonstrar a importância do meio físico como variável explicativa fundamental para o estudo da ciberguerra. O argumento central desenvolvido afirma que o transporte efetivo de informações no ciberespaço durante a guerra depende da posse de ativos estratégicos que garantam a interconexão entre dispositivos eletrônicos por meio de redes resilientes e seguras, e que a posse, a localização e o controle desses ativos é condição prévia e necessária para a consecução de uma estratégia de defesa cibernética. A partir de um arcabouço teórico clausewitziano e de uma análise de redes em camadas, esse artigo conclui que tanto no plano estratégico (ativos nacionais) quanto no plano operacional e tático (redes militares críticas) o acesso e a livre movimentação no ciberespaço é fortemente dependente do meio físico.

Palavras-chave: Ciberguerra – Ciberoperações – Meio físico.

ABSTRACT

This paper aims to demonstrate the importance of the physical medium as a key explanatory variable for the study of cyberwar. The central argument defends that the effective transport of information in cyberspace during war depends on the possession of strategic assets to ensure the connection between electronic devices via resilient and secure networks, and that the ownership, location and control of these assets is a prior and necessary condition to the achievement of a cyber defense strategy. From a Clausewitzian theoretical framework, and through an analysis of layered network architecture, this paper concludes that in both strategic (domestic assets) and operational and tactical (critical military networks) levels the access and unrestricted movement in cyberspace depends greatly on the physical medium.

Keywords: Cyber warfare – Cyber operations – Physical medium.

LISTA DE SIGLAS

BFT	Blue Force Tracker
C4ISR	Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento.
Darpa	Defense Advanced Research Projects Agency
DDoS	Ataque de Negação de Serviço Distribuído
DoD	Departamento de Defesa dos EUA
FBCB2	Force XXI Battle Command Brigade and Below
FTP	Protocolo de Transferência de Arquivos
GCHQ	Government Communications Headquarters
HTTP	Protocolo de Transferência de Hipertexto
IP	Protocolo de Internet
IRIS	Integrity and Reliability of Integrated Circuits
JBC-P	Joint Battle Command–Platform
MANET	Rede Ad Hoc Móvel
NSA	National Security Agency
PEO-C3T	Program Executive Office: Command, Control and Communications-Tactical
PTT	Ponto de Troca de Tráfego
SMTP	Protocolo de Transferência de Correio Simples
TCP	Protocolo de Controle de Transmissão
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TRUST	Trusted Integrated Circuits

SUMÁRIO[1]

[1] Conforme art. 30 do Regimento Interno do Programa de Pós-Graduação em Ciência Política, a dissertação de mestrado em Ciência Política se dará sob a forma de artigo científico. Conforme o parágrafo único do art. 3 da Resolução nº 93/2007 da Câmara de Pós-Graduação da UFRGS, dissertações que contenham artigos prontos para submissão a publicação devem conter, além do artigo, seções de Introdução, Considerações Finais e Referência Bibliográficas, além dos Anexos, quando for o caso.

Parte I

Introdução

O emprego extensivo de tecnologias da informação e comunicação (TIC) para a criação, armazenamento, modificação, troca e exploração de informações fomentou, nas últimas décadas, o debate acerca do uso dessas ferramentas na paz e na guerra. Alegações de que qualquer pessoa com algum conhecimento técnico seria capaz de realizar um ataque contra a infraestrutura crítica de um país a partir de qualquer lugar do mundo tornaram-se recorrentes[2]. Na política, a ideia de que uma ciberguerra era eminente fez com que diversos governos criassem comandos específicos para lutar nesse novo domínio. A percepção de ameaça aumentou a ponto de, em 2012, durante um discurso proferido para empresários do ramo de segurança, o então Secretário de Defesa dos Estados Unidos, Leon Panneta, reiterar uma ideia já recorrente e alertar os presentes sobre a possibilidade de um "*cyber Pearl Harbor*".

A comunidade científica não se furtou ao debate. Nas Ciências Humanas, em especial na Ciência Política, nas Relações Internacionais e nos Estudos Estratégicos, a expansão da produção intelectual interessada no fenômeno da ciberguerra resultou em um campo de pesquisa próprio. Não obstante, tanto no meio político quanto no meio acadêmico, analistas superestimaram as causas e os efeitos de um ataque cibernético, levando-os a projetarem cenários alarmistas para a conjuntura atual (ERIKSSON; GIACOMELLO, 2007, p. 8-9; BETZ; STEVENS, 2013, p. 148). Seus argumentos, de modo geral, baseiam-se na dependência do homem moderno em sistemas de TI, na crescente interdependência e interconexão desses sistemas por meio de redes computacionais, e nas vulnerabilidades inerentes a essas tecnologias. Mais especificamente, suas apreensões tendem a ser baseadas na suposta facilidade com que sistemas de controle e de automação de infraestruturas críticas nacionais podem ser corrompidos.[3]

Em razão da inexistência de maiores incidentes gerados até o momento, essas análises fundamentaram sua argumentação, muitas vezes, em hipóteses e narrativas idiossincráticas de cenários alusivos aos possíveis efeitos de uma ciberguerra (LAWSON, 2011, p. 4; MAHNKEN, 2011, p. 58). Entre os cenários mais recorrentes estão os blecautes causados por

[2] Ver, por exemplo, http://www.bbc.co.uk/news/technology-22524274. Acesso em: 13 fev. 2014.
[3] Ver, por exemplo McGRAW, 2011; WAXMAN, 2011.

meio da invasão a sistemas de controle da rede elétrica, a crise econômica gerada pela exclusão de dados do sistema financeiro, e a paralisia governamental provocada pelo colapso dos sistemas de comunicação.

Um dos exemplo mais extremados desse tipo de argumentação é a afirmação de Clarke e Knake (2010), a respeito de um eventual ataque coordenado contra a infraestrutura crítica dos EUA, o qual, reivindicam os autores, conseguiria levar o país ao caos em apenas 15 minutos sem que os atacantes sequer necessitassem pôr os pés em território estadunidense. Conforme eles:

> "Dentro de um quarto de hora, 157 das maiores áreas metropolitanas se viram em apuros sendo lançadas em um apagão de energia em todo o país durante a hora do *rush*. Nuvens de gás venenoso estão flutuando em direção a Wilmington e Houston. Refinarias estão queimando o fornecimento de petróleo em diversas cidades. Metrôs colidiram em Nova Iorque, Oakland, Washington e Los Angeles. Trens de carga descarrilharam fora dos principais cruzamentos e pátios ferroviários em quatro grandes ferrovias. Aeronaves estão literalmente caindo do céu como resultado de colisões em pleno ar através do país. Gasodutos carregando gás natural para o Nordeste explodiram, deixando milhões no frio. O sistema financeiro também congelou por causa de *terabytes* de informação de centros de dados dizimados. Satélites meteorológicos, de navegação e de comunicação estão girando fora de suas órbitas no espaço. E as Forças Armadas estadunidenses são uma série de unidades isoladas, lutando para se comunicar umas com as outras." (CLARKE; KNAKE, 2010, p. 119-120, tradução nossa).

Entretanto, os ataques cibernéticos referenciados pela literatura especializada não se assemelham à descrição acima. Na prática, as evidências utilizadas pelos ciberpessimistas de que a guerra cibernética está vindo usualmente restringem-se a ataques de negação de serviço distribuídos[4], à tomada momentânea de sítios governamentais ou à espionagem militar. Além disso, estudos desenvolvidos em outras áreas de pesquisa têm apresentado dados que se contrapõem aos prognósticos defendidos pelos ciberpessimistas. Na Sociologia, pesquisas com foco no estudo de desastres tem demonstrado que as sociedades tendem a ser mais resistentes e a ter um poder de recuperação maior do que o usualmente pressuposto.[5] E na

[4] Os ataques de negação de serviço distribuídos, também conhecidos como ataques DDoS (do inglês, *distributed denial of service*) são ataques onde um computador mestre coordena milhares de máquinas contra um servidor ao enviar um grande volume de tráfego ao sistema da vítima. Eles utilizam uma das três técnicas para derrubar um sistema: (1) envio de inúmeros pacotes para o alvo, de tal modo que o servidor pare de aceitar novos pacotes; (2) estabelecimento de inúmeras conexões TCP, congestionando a conexão; ou (3) uso de vulnerabilidade para envio de código malicioso com o intuito de derrubar o servidor alvo. (KUROSE; ROSS, 2013, p. 57).

[5] Análises relacionadas a essa campo de estudos tem relatado, por exemplo, que um dia após à queda da bomba atômica em Hiroshima, os habitantes que não foram resgatados e retirados da cidade já haviam religado a energia elétrica em algumas áreas e restaurado parcialmente as linhas de bonde da cidade, enquanto os bancos locais se reuniram para procederem ao pagamento dos cidadãos (LAWSON, 2011, p. 13).

História Militar e nos Estudos Estratégicos, especialistas têm constatado que a percepção de ameaça referente ao uso ofensivo de novas tecnologias está, usualmente, equivocada.[6]

A incorporação do poder aéreo à guerra na primeira metade do século XX, por exemplo, gerou temor parecido com a apreensão em torno da ciberguerra na atualidade. Em 1923, o coronel J.F.C. Fuller, também por meio de um cenário, previu o caos que uma grande operação aérea contra Londres produziria após trinta minutos do ataque:

> "Imagine, se você puder, qual será o resultado: Londres será por diversos dias um vasto delírio de Bedlam [hospital psiquiátrico londrino], os hospitais serão invadidos, o tráfego irá cessar, os sem tetos irão gritar por ajuda, a cidade estará em pandemônio. O que será do governo em Westminster? Ele será varrido pela avalanche de terror. Então o inimigo irá ditar seus termos, os quais serão aproveitados como uma palha é por um homem que se afoga. Assim uma guerra pode ser lutada em quarenta e oito horas e as perdas do lado vencedor podem ser verdadeiramente nulas!" (FULLER, 1923, p. 150, tradução nossa).

No entanto, apesar do cenário vislumbrado por Fuller, a sociedade e os sistemas que a compõem se mostraram mais resilientes do que o previsto pelos analistas.[7] Conforme Betz e Stevens (2011, p. 84, tradução nossa), "as similaridades entre os antigos teóricos do poder aéreo e os atuais teóricos do poder cibernético são mais do que semânticas. Ambos, na raiz, estão preocupados em restaurar o caráter decisivo à guerra e veem na nova tecnologia o meio potencial para fazer isso."

Entretanto, não há evidência na história da ciberguerra que nos permitam comprovar os cenários apocalípticos[8] vislumbrados por esses autores (HEALEY, 2012, p. 16). Um dos principais problemas dessas análises é justamente a falta de evidências para comprovar seus argumentos (LAWSON, 2011, p. 14; LINDSAY, 2013a, p. 368; LOCATELLI, 2013, p. 3). Não obstante, o medo do desconhecido e de novas tecnologias, aliado atualmente ao medo do terrorismo têm produzido essas análises discrepantes com as evidências da história do ciberespaço. Na verdade, a implementação de redes telefônicas, telegráficas e radiofônicas tem causado alarmismos parecidos desde o início do século XX, com medo de que o uso

[6] Cf. BETZ, 2012; BETZ, STEVENS, 2011; BIDDLE, 2004; GRAY, 2013; LINDSAY, 2013b. Para um contraponto a este argumento, ver KELLO, 2013, p. 39.
[7] Cf. PAPE, 1996; LINDSAY, 2013b, p. 19.
[8] Healey (2012, p. 15) argumenta que se não foi possível atingir efeitos estratégicos nos bombardeamentos aéreos, não deve se esperar que seja possível atingir efeitos estratégicos tão grandiosos a partir do ciberespaço, tendo em vista os limites técnicos e políticos desse ambiente.

deturpado das novas tecnologias pudesse levar ao colapso americano (LAWSON, 2011, p. 8-11).

Ainda assim, mesmo no caso bem mais recente do Stuxnet, é possível qualificar melhor esse tipo de percepção. Apesar de terem sido identificadas três variantes do vírus, cada uma com uma grande onda de infecção, a variante responsável pelo ataque a Natanz foi a primeira, visto que os principais danos à infraestrutura local ocorreram antes de março de 2010, quando a segunda variante foi compilada (LINDSAY, 2013a, p. 381). Conforme o levantamento feito pela Symantec[9], o principal método de propagação do vírus foi por meio de dispositivos removíveis, utilizando arquivos autorun.inf. Isso, nos leva a deduzir que, apesar de alguns analistas proporem que é possível lançar um ataque imediato contra a infraestrutura crítica de um país com um simples aperto de botão, existe, por trás destes ataques, uma complexidade técnico-social que não pode ser desconsiderada.

De fato, o Stuxnet demonstra como a relação entre potencialidades técnicas e efeitos estratégicos não é tão direta quanto se afirma. Neste caso, Linday (2013a, p. 391, tradução nossa) é categórico ao afirmar que "em resumo, o Stuxnet errou os alvos mais valiosos em Natanz, o enriquecimento continuou ou melhorou ao longo do ataque, e os iranianos repararam o dano". Além disso, há de se levar em conta o tempo de desenvolvimento e maturação de um vírus como esse. Estima-se que o desenvolvimento dele remonte a 2006, ano de início da Operação Jogos Olímpicos, mas os efeitos pretendidos só ocorreram a partir de 2010. Ou seja, a alardeada imediaticidade dos ciberataques, temida pelos ciberpessimistas, precisa ser avaliada com mais cuidado.

Outro problema recorrente nas análises desenvolvidas pelos ciberpessimistas é o uso de inferências falsas em seus argumentos. O uso dessa falácia permite que esses analistas recorrentemente argumentem, por exemplo, que os dados das inúmeras tentativas de ataque a redes específicas são prova da fragilidade dos sistemas de TI. Entretanto, essa assertiva não permite inferir que parte significativa dessas tentativas acarretem em intrusões bem sucedidas. E, caso essas intrusões aconteçam, isto tampouco permite inferir que a ruptura na rede atinja regiões importantes e sensíveis do sistema, as quais, por segurança, não deveriam estar conectadas à rede externa. Além disso, a invasão de uma rede não implica em total liberdade de ação dentro dela, sendo necessário a obtenção de permissões de acesso específicas para a execução de determinados comandos. A intrusão também não garante que o atacante será

[9] Cf. FALLIERE; MURCHU; CHIEN, 2011.

capaz de infligir danos à rede. E, infligindo, que será capaz de torná-los persistentes (LIBICKI, 2009, p. III; LIBICKI, 2013).

De fato, existe uma grande diferença entre desabilitar momentaneamente um sistema alvo e torná-lo permanentemente desabilitado (HEALEY, 2012, p. 15). Por conta disso, o sucesso de uma operação lógica no ciberespaço depende da coleta de informações do sistema alvo e de seus usuários (LINDSAY, 2013b, p. 14). A partir dessas informações o atacante tem como mirar nos dados a serem atacados (nem toda informação tem o mesmo valor) e projetar como manter o ataque no tempo. Neste sentido, o conhecimento técnico sobre o sistema específico e sobre o seu uso operacional é importante (LIBICKI, 2009, p. XX). No caso Stuxnet, a inteligência e os testes prévios[10] à infecção do vírus permitiram seu sucesso posterior.

Obviamente, o uso ofensivo do ciberespaço para fins políticos é real e potencialmente grave, envolvendo ameaças concretas para o sistema internacional e seus membros. Mas há, de fato, uma superestimação quanto aos possíveis usos e desusos do ciberespaço na guerra, advinda principalmente da imprecisão conceitual em torno do fenômeno e da falta de rigor analítico em torno de suas implicações (ERIKSSON; GIACOMELLO, 2007, p. 9; MCGRAW; FICK, 2011, p. 41-54). É contra essa superestimação e imprecisão que temos argumentado em diferentes trabalhos do CEGOV a respeito do tema.[11] Uma maior precisão conceitual e uma avaliação menos impressionista das evidências disponíveis podem ajudar, mais do que os exageros retóricos, a esclarecer o público sobre o uso do ciberespaço, bem como sobre as consequências sociais e políticas para os cidadãos, os governos, as empresas e para a segurança internacional como um todo (BETZ, 2012, p. 706-707). Assim, se algumas das projeções feitas pelos ciberpessimistas se tornarem realidade no futuro estaremos todos melhor preparados a entender o problema e a atuar sobre ele.

A interconexão entre diferentes dispositivos e redes, aliado à crescente dependência das sociedades modernas nesses sistemas, pode, em tese, fazer com que um ataque gere efeitos cascata e se propague pela rede, causando destruição por onde passa. Contudo, devido

[10] No caso Stuxnet, é sabido que os EUA haviam comprado uma centrífuga igual a iraniana em 2003 e que uma atividade conjunta entre o Laboratório Nacional de Idaho e a Siemens, com o objetivo de detectar vulnerabilidades nos seus sistemas de controle industriais (utilizado na instalação iraniana), ocorreu em 2008 (LINDSAY, 2013a, p. 387).

[11] Estão envolvidos com esse programa de pesquisa o grupo de trabalho Governança Digital e o GT Políticas de Segurança, Inteligência e Segurança do Centro de Estudos Internacionais sobre Governo (CEGOV), da Universidade Federal do Rio Grande do Sul (UFRGS). Entre as produções dos pesquisadores do CEGOV sobre o tema, destacamos CANABARRO; BORNE; 2013; CANABARRO, 2014; CEPIK; CANABARRO; BORNE, 2014; PIMENTA; CANABARRO, 2014; CEPIK; CANABARRO, BORNE, 2015.

aos atuais requisitos técnicos e à estrutura do ciberespaço, assim como aos limites físicos, políticos e financeiros da atualidade, pode ser descrito como tendo baixa probabilidade e alta consequência, o que em si mesmo já é motivo suficiente para investirmos energia, tempo e recursos em pesquisas nessa área (MANHKEN, 2011; MCGRAW; FICK, 2011). Por isso, estudos baseados em evidências, ao invés de anedotas, tal como o elaborado aqui, são fundamentais para o avanço deste campo de pesquisa (ERIKSSON; GIACOMELLO, 2007, p. 182; LAWSON, 2011, p. 2).

Parte II

Artigo

GUERRA E CIBERESPAÇO:
Uma análise a partir do meio físico

O presente artigo tem por objetivo demonstrar a importância do meio físico como variável explicativa fundamental para o estudo da ciberguerra. O argumento central desenvolvido afirma que o transporte efetivo de informações no ciberespaço durante a guerra depende da posse de ativos estratégicos que garantam a interconexão entre dispositivos eletrônicos por meio de redes resilientes e seguras, e que a posse, a localização e o controle desses ativos é condição prévia e necessária para a consecução de uma estratégia de defesa cibernética. A partir de um arcabouço teórico clausewitziano e de uma análise de redes em camadas, esse artigo conclui que tanto no plano estratégico (ativos nacionais) quanto no plano operacional e tático (redes militares críticas) o acesso e a livre movimentação no ciberespaço é fortemente dependente do meio físico.

1. INTRODUÇÃO

Na última década, o aumento de ataques cibernéticos fomentou o desenvolvimento de pesquisas sobre o uso do ciberespaço para os fins da guerra. A produção acadêmica sobre o fenômeno concentrou-se no debate acerca da existência da guerra cibernética, do ataque a infraestruturas críticas nacionais e do uso da Internet em conflitos. A partir da análise de eventos cibernéticos, passando pela explosão do gasoduto soviético em 1982[12], pelas chamadas *webwars* da Estônia e da Geórgia em 2007 e 2008, respectivamente, e pelo ataque contra a usina nuclear iraniana em 2010, essas pesquisas tentaram compreender como é possível atingir fins políticos, em um contexto de guerra, por meio do uso de código malicioso no ciberespaço.

Não obstante, o desenvolvimento desta área de pesquisa nas Ciências Sociais foi limitado pela tecnicidade do tema e pelo dinamismo das mudanças tecnológicas da era digital. As poucas produções significativas do assunto focaram suas pesquisas nas questões lógicas da ciberguerra, o que tem se refletido em abordagens rudimentares sobre os aspectos estratégicos do fenômeno. (GRAY, 2013, p. 7). Em áreas de pesquisa como a Ciência Política e as Relações Internacionais, pouca atenção foi dada aos vetores que possibilitam a existência do

[12] Diversos autores tem se referido ao incidente do gasoduto soviético, ocorrido em 1982, na região da Sibéria, como o primeiro ataque cibernético que se tem conhecimento. Segundo relatos, o gasoduto *Urengoy-Surgut-Chelyabinsk* requeria um sistema de controle e automação que não estava ao alcance da União Soviética, sendo necessário a sua compra. Durante o processo de fabricação do software, a Central de Inteligência Americana (CIA) teria incluído um *malware* no código fonte, o qual faria o sistema sobrecarregar o gasoduto, provocando por fim uma grande explosão. No entanto, não há evidências que comprovem o envolvimento dos EUA na sabotagem (BETZ; STEVENS, 2011, p. 20-21). Ademais, uma fonte da inteligência estadunidense afirma que a explosão ocorreu devido a um vazamento de gás que incendiou quando da passagem de um trem na região (CARR, 2013, p. 34).

ciberespaço e a propagação de dados através dele, principalmente no que se refere às questões geopolíticas, estratégicas, operacionais e táticas advindas do seu uso.

Ainda que o ciberespaço possa ser visto como uma realidade virtual, ele é composto de dispositivos físicos reais. Neste sentido, este artigo visa demonstrar qual a importância do meio físico para o ciberespaço, assim como o meio físico pode ser usado para afetar eventos e operações militares nesse ambiente. Argumenta-se que: (1) o transporte efetivo de informações no ciberespaço durante a guerra depende da posse de ativos estratégicos que garantam a interconexão entre dispositivos eletrônicos por meio de redes resilientes e seguras. Argumenta-se também que (2) a posse, a localização e o controle desses ativos é condição prévia e necessária para a consecução de uma estratégia de defesa cibernética.

O argumento é elaborado em três seções. Na primeira seção, o artigo debate os principais problemas políticos advindos de uma má conceituação da ciberguerra e apresenta o arcabouço conceitual utilizado, visto que o debate sobre a natureza desses conceitos não está pacificado na literatura especializada. Na segunda seção, o artigo introduz algumas das configurações básicas de uma rede cibernética para, a seguir, discutir como tais requisitos se desdobram no plano estratégico, por meio do exame de ativos estratégicos nacionais, e no plano operacional e tático, por meio do exame das chamadas redes militares críticas. Na última seção, apresenta-se o desdobramento do argumento no plano geopolítico. Conclui-se o artigo enquadrando a análise em camadas do ciberespaço no arcabouço teórico clausewitziano, ou seja, integrando a novidade heurística representada pelo ciberespaço e pela ciberguerra a um programa de pesquisa científico capaz de explicá-los mais adequadamente do que a retórica alarmista tem sido capaz de fazer até aqui, de modo a compreender como é possível produzir impactos estratégicos na guerra através do uso instrumental do ciberespaço.

2. DELIMITANDO CONCEITOS: CIBERESPAÇO, GUERRA E CIBERGUERRA

No meio acadêmico, a imprecisão conceitual (CAVELTY, 2008, p. 4; BETZ; STEVENS, 2013, p. 148; GRAY, 2013, p. 65; KELLO, 2013, p. 7; NYE, 2013, p. 9) em torno da ciberguerra, a existência de poucos ataques de grande intensidade ligados ao fenômeno (DENNING, 2007, p. 87; LINDSAY, 2013a, p. 374) e o sigilo em que o assunto é envolto têm suscitado explicações de cunho indutivista, por meio de analogias, e dedutivistas, a partir das características técnicas do ciberespaço e dos dispositivos que o constituem. Ambas abordagens, entretanto, apresentam problemas substantivos. As análises por analogia

tendem a ignorar os requisitos técnicos e a arquitetura do ciberespaço (WINNER, 1996), assim como a complexidade do tema (ERIKSSON; GIACOMELLO, 2007, p. 180-181), ao passo que o segundo tipo de abordagem tende a ignorar os constrangimentos políticos e sociais a que as tecnologias estão submetidas (FOUNTAIN, 2011), assim como as "fundações políticas e sociais do conflito" (LINDSAY, 2013b, p. 4, tradução nossa). Imbuída de um determinismo tecnológico, essa última abordagem tem como pressuposto a concepção de que as questões estratégicas e táticas relacionadas à ciberguerra são inerentes ao ciberespaço.

No entanto, esse problema afeta o processo político e transcende o interesse puramente intelectual (BETZ; STEVENS, 2013, p. 81; CANABARRO, 2014, p. 285; CAVELTY, 2008, p. 14; MAHNKEN, 2007, p. 63; STRACHAN, 2007, p. 231). No âmbito doméstico, a percepção de que eventos cibernéticos são uma ameaça emergente contra os interesses e a segurança nacional influencia a definição da agenda, a formulação e a implementação de políticas públicas na área de defesa. Mais especificamente, a securitização[13] do tema afeta a alocação de recursos orçamentários para programas de defesa cibernética, servindo a ameaça, independentemente de sua materialidade, como justificativa para a autonomização e/ou fortalecimento dos órgãos burocráticos responsáveis por esses programas[14] (BRITO; WATKINS, 2011; GARTZKE; LINDSAY, 2014, p. 37). No plano econômico, isso tende a se refletir em despesas supérfluas com eventos de baixa probabilidade, ainda que de alto impacto (SILVA, 2011, p. 129). Nas Forças Armadas, essas distorções nas políticas de gastos e investimentos são responsáveis por *trade-offs* entre políticas de modernização tecnológica e políticas de expansão de efetivo, as quais não podem ser implementadas em conjunto, *ceteris paribus*.[15]

[13] Hansen e Nissebaum (2009), a partir de uma análise baseada na Escola de Copenhague, argumentam que a cibersegurança tem passado por um duplo processo que tem despolitizado o fenômeno: de um lado, há um processo de securitização; de outro, um processo de tecnificação. Este último, é resultado de um empoderamento excessivo dos técnicos da área, e é marcado pela ideia que as tecnologias modernas são motivadas por uma agenda politicamente neutra.

[14] Um exemplo recente disto foi a aprovação na França da nova Lei de Informação, aprovada logo após o ataque terrorista ao jornal Charlie Hebdo. A nova lei foi fortemente atacado por grupos de defesa de liberdades civis ao permitir o acesso a dados digitais de indivíduos sem ordem judicial. A partir de sua implementação será possível grampear toda a comunicação digital de indivíduos supostamente vinculadas a grupos terroristas, assim como inserir dispositivos que gravem toda e qualquer tecla digitada nos computadores de pessoas-alvo. Além disso, o governo irá manter consigo, por cinco anos, todos os metadados de computadores alvos e os provedores de Internet serão obrigados a instalar algoritmos complexos que detectam padrões de comportamento suspeitos na web, como palavras chave e sites visitados.

[15] Biddle (2004, p. 19, tradução nossa) argumenta que o *trade-off* existente entre a implementação de cada política representa um dilema de difícil solução para os tomadores de decisão, visto que "sugerir que ambas importam é de pouca ajuda para os formuladores de políticas, os quais precisam saber *quanto* e *de que maneira* cada uma delas importa a fim de tomar decisões sólidas". Para o autor, o sucesso último será advindo mais de

Além disso, o processo de securitização do fenômeno também tem como consequência a militarização de eventos que, de outra forma, seriam tratados como concernentes à esfera da segurança pública, no âmbito doméstico, ou como conflitos de menor monta, no âmbito internacional. A ausência de um instrumental analítico que permita identificar e comparar eventos em que haja o uso do ciberespaço para os fins políticos e objetivos estratégicos da guerra não tem permitido a distinção entre esse e outros tipos de conflitos gerados através do ciberespaço.

Neste caso, corre-se o risco de tratar-se, tanto analiticamente quanto politicamente, cibercrime, ciberativismo e ciberguerra como problemas da mesma natureza e necessitando da mesma resposta (BETZ; STEVENS, 2011, p. 81; GRAY, 2013, p. 10). No plano nacional, a atuação de órgãos militares em eventos cibernéticos, em especial os relacionados a atividades de ciberativismo, tem levantado questões quanto aos impactos dessa atuação em regimes democráticos. No Brasil, por exemplo, o monitoramento *online* de ativistas que participaram das manifestações populares ocorridas em junho de 2013, feito pelo Centro de Defesa Cibernética do Exército (CDCiber), suscita questões quanto à legalidade e moralidade destas ações.[16] Atividades de monitoramento em massa, sobretudo pelos Estados Unidos, também têm fomentado a discussão em torno do direito à privacidade, com críticas ao que se considera uma prevalência da defesa do Estado em contraposição à defesa do cidadão.

No plano internacional, a categorização de um evento cibernético como um ato de guerra possui consequências para as relações internacionais, visto que a resposta pode ser desproporcional ao evento em si, podendo levar a uma escalada do conflito para uma guerra convencional. Ademais, a distinção deste fenômeno de outros tipos de conflitos impacta a construção da doutrina militar, a composição das forças combatentes, a condução da guerra, e, inclusive, a decisão de entrar ou não nela (ECHEVARRIA II, 2007, p. 58; LONDSDALE, 2007, p. 231). Nos EUA, após a Segunda Guerra Mundial, a crença da Força Aérea Americana de que a bomba atômica iria acabar com ataques continentais promoveu, por exemplo, uma grande reorganização com o intuito de preparar este ramo das Forças Armadas para a nova era atômica. Isto resultou, segundo Biddle (2004, p. 198-199) em erros e riscos estratégicos nas Guerras da Coréia e do Vietnã.

---

mudanças organizacionais e doutrinárias para incorporar as potencialidades advindas dessas tecnologias do que do simples uso das tecnologias em si.

[16] As informações sobre o monitoramento de ativistas foram repassadas pelo então chefe do Centro de Defesa Cibernética, general José Carlos dos Santos. Cf. SASSINE, 2013.

Por conta disso, se por uma lado é importante que intelectuais e políticos compreendam a complexidade técnica por trás do ciberespaço, por outro lado é primordial que os técnicos entendam a complexidade social e política do contexto no qual surge e se desenvolve esse ambiente (ERIKSSON; GIACOMELLO, 2007, p. 180-181). Para tanto, ainda que uma abordagem estritamente conceitual da ciberguerra seja insuficiente[17], o processo de delimitação conceitual desse novo fenômeno é necessário (LAWSON, 2011, p. 25-26). Para isso, há de se considerar os problemas semânticos derivados do termo ciberguerra, o qual deriva da junção de dois conceitos polissêmicos[18], a saber, guerra e ciberespaço. É a partir da construção desses conceitos e das relações formuladas entre eles que conseguimos identificar, descrever e explicar esta nova dinâmica da política internacional.[19] Do mesmo modo, esse processo permite que comparações sejam realizadas entre diferentes casos relacionados ao fenômeno.

Ciberespaço

Dentre as diferentes conceituações do ciberespaço apresentadas pela literatura, a desenvolvida por Kuehl (2009, p. 24-42), e adotada neste artigo, possui o benefício de não restringir o ciberespaço à questão da digitalização ou ao caráter virtual deste meio. Ou seja, apesar de categorizar o ciberespaço como um ambiente virtualizado, Kuehl dá destaque às condições materiais necessárias para a existência do próprio ciberespaço, as quais são usualmente negligenciadas pela literatura não técnica sobre o assunto. Para o autor, o ciberespaço é:

---

[17] Pesquisas que fazem uso de uma abordagem estritamente conceitual da ciberguerra são usualmente criticadas por não serem capazes de dimensionar esse novo fenômeno e as implicações advindas dele para a segurança internacional. Este tipo de crítica tem como pressuposto a noção de que a política internacional não é dicotomicamente representada pela paz e pela guerra, e conclui que este novo fenômeno pode, mesmo não sendo conceitualmente definido como guerra, tornar-se uma das principais dinâmicas das relações sócio-políticas da contemporaneidade. Para esses críticos, este tipo de apego conceitual tende a restringir a análise do fenômeno ao mundo acadêmico. Cf. GARTZKE, 2013, p. 49; KELLO, 2013, p. 22.

[18] Betz (2012, p. 692, tradução nossa) fala em dois "sistemas complexos não-lineares", os quais não têm uma definição precisa na literatura de estudos estratégicos. Como resultado, surgem ameaças vagas e intangíveis, além de um discurso que vê a cada novo ciclo tecnológico uma mudança substancial na natureza da guerra.

[19] JACCARD e JACOBY, 2009, p. 11-16. Apesar de alguns autores terem se debruçado na análise crítica desse conceito, boa parte da produção científica sobre o tema tem ou ignorado o problema (fazendo uso do senso comum no que se refere ao termo ciberguerra), ou tem promovido um alargamento conceitual do fenômeno. Qualquer uma dessas posições tem, por sua vez, promovido um debate repleto de indefinições e imprecisões analíticas (CAVELTY, 2008, p. 4; NYE, 2013, p. 9; HAYDEN, 2011). Entretanto, apesar de destacar a importância da construção de um arcabouço teórico, com o intuito de compreender as ameaças e consequências da ciberguerra, Kello (2013, p. 9) argumenta que os analistas que não concordam com as atuais visões políticas em torno do fenômeno deveriam apontar os desafios teóricos e empíricos que ele traz.

> um domínio global dentro do ambiente informacional cuja característica distintiva e única é moldada pelo uso de eletrônicos e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informação via redes interdependentes e interconectadas usando tecnologias da informação e comunicação (KUEHL, 2009, p. 28, tradução nossa).[20]

Essa delimitação conceitual possibilita, por um lado, que o ciberespaço seja caracterizado como um ambiente virtual construído pela humanidade, um artefato distinto dos demais meios físicos naturais (terra, ar, mar e espaço sideral). Por outro lado, seu caráter derivado da ação humana, artificial nesse sentido, não o livra da geografia e de outros constrangimentos físicos (GRAY, 2013, p. 17). Deste ponto de vista, o ciberespaço é compreendido como um ambiente que, apesar de ser criado pelo homem, está além do seu domínio. Ou seja, é importante recusar a visão de que o ciberespaço seria uma grande caixa-preta, onde o fluxo informacional se dá de forma livre e caótica, assim como a visão que crê que o fluxo se dá de maneira extremamente controlada e sobredeterminada.

Na verdade a existência deste ambiente virtualizado necessita que pelo menos dois dispositivos com circuitos elétricos ou eletrônicos estejam conectados e dependam um do outro para a manipulação de dados. Admite-se que todo e qualquer equipamento que possua um circuito elétrico pode, a princípio, fazer uso do eletromagnetismo para trocar informações com equipamento semelhante, por meio de redes interdependentes. Desse modo, a interconexão entre rádios, telefones, computadores e quaisquer outros dispositivos que usem a eletricidade e o eletromagnetismo para troca de dados geram ciberespaços entre si.[21] E neste sentido, o ciberespaço pode ser compreendido como o conjunto de todas as redes que apresentem as pré-condições acima.[22]

---

[20] Existe um grande debate na literatura especializada sobre a concepção de que o ciberespaço representa um domínio militar no sentido estrito da palavra. Para saber mais sobre esse debate, ver CEPIK; CANABARRO, BORNE, 2015.

[21] A troca de informação entre dois computadores conectados via um cabo de rede, por exemplo, criaria um ciberespaço específico no local. Um questionamento subsequente pode ser se a troca de dados entre computadores por meio de um USB, por exemplo, também cria um ciberespaço entre si. Uma análise mais detalhada demonstra que a comunicação entre esses dispositivos também se dá no ciberespaço, apesar de sua existência não ser contínua nesse caso. Isto se deve pois ao ligar um dispositivo USB a cada um dos computadores, uma interconexão é criada, a qual utilizada circuitos elétricos/eletrônicos e o espectro eletromagnético para manipular dados. Desse modo, apesar da transferência de dados não criar um ciberespaço entre os dois computadores, um ciberespaço existe entre cada computador e o USB.

[22] Em redes mais complexas, a interdependência entre dispositivos conectados é mais evidente, pois para estabelecer uma comunicação ponto-a-ponto, os dispositivos na periferia do sistema dependem de inúmeros outros equipamentos posicionados no núcleo desse sistema, os quais são responsáveis por processos de

Essa abordagem produz algumas implicações lógicas. Primeiramente, ela nos permite compreender o ciberespaço como um meio físico, tal como a terra, o ar, o mar e o espaço sideral, mas distinto deles pelo uso de dispositivos dotados de circuitos elétricos que utilizam o espectro eletromagnético. Em segundo lugar, ela permite que afirmemos que nem todos os dispositivos estão conectados na mesma rede. Em terceiro lugar, dela depreende-se que o ciberespaço não é, definitivamente, o mesmo que a Internet. Se a conexão entre diferentes dispositivos eletrônicos que utilizam o espectro eletromagnético para manipular dados é a única condição necessária para a existência do ciberespaço, a Internet deixa de ser igual a este ambiente e passa a estar contida nele.

Na verdade, a Internet é uma rede caracterizada pelo uso do pacote de protocolos TCP-IP (*Trasmission Control Protocol – Internet Protocol*) que são responsáveis pela transmissão de dados e interconexão entre os diferentes dispositivos da rede, os quais são endereçados por meio de um endereço IP. Já a *web*, que muitas vezes é usada com o mesmo sentido da Internet, é apenas uma aplicação da última. Ela roda na camada de aplicação por meio do protocolo HTTP (*Hypertext Tranfer Protocol*) para a transmissão de hipermídia[23]. Outras aplicações da Internet são, por exemplo, o e-mail (SMTP – *Simple Mail Transfer Protocol*) e a transferência de arquivos via FTP (*File Transfer Protocol*).

Mas se assim é, porque mesmo autores que fazem a diferenciação entre esses dois ambientes tendem a desenvolver uma análise mais baseada na Internet do que no ciberespaço? Parte da explicação está na atual convergência em torno do padrão IP[24] e na necessidade de interligar redes autônomas/internas com a Internet com o intuito de maximizar o fluxo informacional[25]. Isto, somado ao número de dispositivos interligados, à infraestrutura física de suporte e à abrangência territorial da Internet, aumenta a importância dessa última como a principal rede do ciberespaço e justifica as preocupações existentes com ela (CAVELTY, 2008, p. 67). Não obstante, a definição de Kuehl permite desenvolver uma análise do

---

comutação, roteamento, entre outros. Do mesmo modo, o núcleo de uma rede depende de sua periferia, visto que sem ela não existiria, em teoria, dados para serem trafegados.

[23] Definidas pela RFC 1945 e RFC 2616. Disponíveis em: <http://tools.ietf.org/html/rfc1945> e <http://tools.ietf.org/html/rfc2616>. Acesso em: 01 dez. 2014.

[24] Essa convergência é resultado, em parte, da separação lógica entre as diferentes camadas que compõem a rede mundial de computadores, facilitando a criação de aplicações com base no IP. Porém, isto não quer dizer que esses sistemas que utilizam o IP fazem parte automaticamente da Internet, mas que potencialmente podem entrar na rede, visto que usam o protocolo padrão de comunicação necessário para trafegar dados nela. Para estar na rede, é preciso que o número IP esteja em tabelas de roteamento dos servidores que fazem parte da Internet. Cf. KURBALIJA; GELBSTEIN, 2005, p. 42-45.

[25] Há incentivos para a conexão de redes isoladas à Internet, visto que o valor de uma rede estaria no número de conexões que os nodos dela possuem. Logo, quanto maior a rede, maior seu valor. Cf. TANEMBAUM; WETHERALL, 2011, p. 425.

ciberespaço para além do enfoque em Internet. Isto se releva ainda mais importante no contexto de estudos de ciberguerra, em que, por questões de segurança e defesa, parece plausível/racional que as Forças Armadas utilizem redes autônomas protegidas ao invés da Internet, uma rede aberta e de fácil interceptação.[26] Nesse sentido, é premente uma análise mais abrangente do ciberespaço que considere todos os sistemas autônomos que não estão interligados na Internet.

Guerra

Este artigo adota uma abordagem clausewitziana[27] sobre a guerra. Clausewitz (2007, p. 13) a definiu como um "ato de força para compelir nosso inimigo a fazer nossa vontade". A guerra, deste modo, surge do antagonismo entre vontades distintas e tem no uso da força, ou na ameaça do uso da força, a solução para o conflito. Sua essência está no combate, na interação, na reciprocidade entre as partes. Por isso, ela não é um ato unilateral de força, sendo antes fruto da resistência do que da indiferença das partes envolvidas. Ela também não é um fim em si mesma, nem a vitória militar o seu objetivo final. A guerra é instrumental: seu emprego é um meio que as partes envolvidas podem optar para garantir que suas vontades serão respeitadas. Ela é um meio para alcançar um propósito político.

Vista de uma perspectiva puramente lógica, essa definição permite que a guerra escale constantemente, pois cada lado do conflito possui incentivos para incrementar sua força *ad infinitum* como modo de garantir o êxito de suas vontades. Em um cenário sem constrangimentos, a escalada levaria a uma guerra absoluta: um ato isolado e instantâneo com o máximo dispêndio de força e de recursos, tendo como fim desarmar completamente o inimigo. No mundo real, entretanto, constrangimentos políticos e físicos impedem que a escalada infinita se concretize. Sendo a guerra um meio para atingir um objetivo político, ela deve ser delimitada por esse e outros interesses políticos que os atores envolvidos no combate venham a perseguir. De fato, os fins políticos da guerra determinam os objetivos militares e o

[26] Apesar de utilizar a mesma arquitetura que outras redes cibernéticas, argumenta-se que a Internet possui facilidade de interceptação porque sua infraestrutura física é, de certa maneira, "compartilhada".

[27] Kello (2013, p. 8) acredita que, apesar das novas tecnologias não terem modificado substancialmente a natureza da guerra, os estudos que partem da análise clausewitziana da guerra não são capazes de dimensionar ou compreender os problemas que a ciberguerra traz para a relações internacionais. Já Libicki (2009, p. 5) argumenta que pelo ciberespaço ser tão diferente dos outros meios, é possível que o conceito de guerra convencional não se aplique à ciberguerra. Apesar disso, argumenta-se aqui que a teoria clausewitziana da guerra é capaz de explicar a novidade heurística representada pelo uso do ciberespaço para a obtenção de fins políticos em contextos de conflito.

nível de força e esforço dispendido nela. E como os recursos disponíveis para emprego no combate são finitos, os limites da guerra também são delimitados pelo fator físico.

Outros fatores que também restringem as implicações lógicas do conceito são a neblina e a fricção da guerra (*fog and friction*), no sentido clausewitziano em que tais termos são empregados para descrever incerteza e desgaste. A primeira, ligada à natureza imperfeita da informação; a segunda, ligada ao acaso, inerente à vida, e ao esforço físico e perigo, inerentes à guerra. De fato, a inevitabilidade da realidade física é um dos principais diferenciais da análise clausewitziana em comparação com as abordagens elaboradas por outros teóricos da guerra, que acreditavam ser possível superá-la através de técnicas específicas. Echevarria II (2007, p. 107, tradução nossa) aponta, neste sentido, que "a identificação e análise da fricção geral é de fato normal: é uma condição reconhecida e aceita da realidade física".

Todos esses elementos demonstram as dificuldades de lançar e sustentar um ataque em uma guerra. Por isso Clausewitz argumenta que o lado mais forte da guerra é a defesa, ainda que ela assuma uma posição negativa na guerra. Além disso, a única forma de afetar a natureza da guerra seria através de vitória assegurada no nível estratégico, visto que o sucesso tático não é suficiente. Por isso, em uma guerra, de modo a compelir um adversário a manter ou alterar seu *status quo*, usualmente faz se necessário a presença de tropas terrestres em campo, para garantir a vantagem estratégica sobre o inimigo (LONDSDALE, 2007, p. 239-240).

Ciberguerra

A partir das definições de ciberespaço e guerra apresentadas acima, a ciberguerra pode ser entendida como um ato de força, gerado a partir de dispositivos eletrônicos interconectados, para compelir nosso inimigo a fazer nossa vontade. Entretanto, não é pacífico entre os analistas que tipo de força[28] é possível aplicar pelo/no ciberespaço.

[28] A distinção entre força e violência, e sua relação com a Teoria da Guerra de Clausewitz, é um debate em aberto na área. De um lado, há o argumento de que a concepção de força clausewitziana está intimamente ligada ao conceito de violência, e que a violência só existe se há letalidade no conflito (RID, 2013a; RID, 2013b, RID 2013c;). De outro, existe o argumento que o uso da força não depende de violência, e que a violência, por sua vez, não tem como consequência a letalidade, visto que a violência causa dano, em pessoas ou coisas, só sendo letal para o primeiro grupo (JUNIO, 2013, p. 126; STONE, 2013).

De maneira geral, a força é utilizada na guerra para, por um lado, punir ou compelir um adversário, ou, por outro, conquistar (GARTZKE, 2013, p. 54). Entretanto, devido às questões técnicas do ciberespaço, não é possível dominar o espaço cibernético completamente. É somente possível monitorar, patrulhar, exercer influência e deter agressão sobre sistemas específicos (MCGRAW; FICK, 2011, p. 46; MCGRAW, 2013, p. 114). Neste sentido, o conceito adotado neste artigo defende que a ciberguerra[29] é caracterizada pelo uso da força para modificar, degradar ou destruir os dados transmitidos pelo ciberespaço, de modo a infligir danos no poder de fogo do inimigo. Ou seja, uma força combatente deve depreciar a disponibilidade, integridade e confidencialidade dos dados do inimigo enquanto tenta proteger seus próprios dados.

Contudo, tal como nos outros meios físicos (terra, ar, mar e espaço sideral), não é possível proteger todo e qualquer dado transportado pelo ciberespaço, sendo necessário selecionar e priorizar os alvos chaves conforme questões operacionais (EUA, 2013, p. II-9). Uma das principais questões que se impõem nessa avaliação é o *trade-off* existente entre o número de alvos atingidos e a intensidade do ataque. Operações destinadas a atingir um número elevado de alvos não produzem grandes danos no poder de fogo do inimigo, visto que para abarcar um número grande de dispositivos faz-se necessário diminuir a especificação das funcionalidades a serem modificadas, degradadas ou destruídas. Assim, quanto maior a quantidade de dispositivos ou redes atacadas, mais genérico será o código malicioso e menos destrutivo será seu poder.

De modo semelhante, quanto menor o número de alvos, mais customizável será o código, e maior poder destrutivo ele terá, visto que ele conseguirá atingir partes mais específicas de uma rede e/ou sistema. Entretanto, ataques de alta intensidade requerem uma boa inteligência sobre o alvo a ser atacado, assim como profissionais da área com treinamento e suporte organizacional amplos, tendo um alto custo de desenvolvimento (CRUZ JR., 2013, p. 11). Surpresas inesperadas em tempo de execução, devido a evoluções nas práticas dos usuários ou nos sistemas atacados, podem comprometer a operação, causar danos colaterais ou mesmo identificar o atacante.

De fato, ciberoperações envolvem alvos difíceis de compreender e acidentes difíceis de prever. A complexidade técnico-social afeta tanto atacantes quanto atacados. No plano

[29] Na literatura de língua inglesa, é comum diferenciar *cyberwar* de *cyberwarfare*. O primeiro caso é utilizado para se referir ao uso independente do ciberespaço na guerra, ou seja, a uma guerra travada somente no ciberespaço. Já o segundo, se refere ao uso instrumental do ciberespaço na guerra (MAHNKEN, 2011, p. 58). Este artigo assume a segunda posição.

cinético, os dispositivos ainda sofrem danos com poeira, areia e clima, ao passo que os operadores desses dispositivos continuam sofrendo com estresse, desgaste e medo. Por isso, essas operações, tais como quaisquer outras operações de guerra, estão envoltas em neblina e fricção (BETZ, 2006, p. 515; GRAY, 2013, p. 47; LINDSAY, 2013a, p. 393; LONDSDALE, 2007, p. 233-234), ainda que alguns analistas apressem-se, a cada nova tecnologia, em alardear o fim da incerteza e do desgaste na guerra. Constrangimento físicos, financeiros e políticos continuam a agir sobre a guerra no ciberespaço, limitando a possibilidade de ação nesse ambiente (ECHEVARRIA II, 2007, p. 75; GARTZKE, 2013, p. 44).

Além disso, a credibilidade de um ataque, real ou potencial, é contrastante com o sigilo que essas operações precisam para ocorrerem. O anonimato característico de ciberoperações dificulta a sinalização do atacante quanto às suas vontades: um inimigo atacado através do ciberespaço precisa compreender que não satisfazer as vontades implícitas resultaria em ataques danosos a si. O problema é que para que o atacado possa consentir com o atacante, é necessário que ele possa atribuir o ataque a alguém, só assim a força coercitiva da guerra pode funcionar (GARTZKE, 2013, p. 42-43; GARTZKE; LINDSAY, 2014, p. 40; LIBICKI, 2009, p. XVIII).

Independentemente do quão incômodo um ataque cibernético possa vir a ser, sua relevância estratégica para a guerra contemporânea encontra-se na sua capacidade de infligir danos reais e persistentes no poder de fogo do inimigo (GARTZKE, 2013, p. 43; GRAY, 2013, p. 49). Para atingir esse objetivo, alguns pré-requisitos são necessários, ainda que não suficientes. Primeiramente, os distúrbios causados por operações militares precisam ultrapassar os problemas cotidianos originados pela complexidade técnico-social do ciberespaço (LINDSAY, 2013a, p. 402). Falhas, defeitos e panes, causados por usuários, dispositivos ou aplicações, são rotineiras no ciberespaço, de tal modo que o usuário comum dificilmente consegue diferenciar se a interrupção de um canal de comunicação foi resultado de um ataque de negação de serviço, de uma manutenção do canal, ou simplesmente de um golpe de pá contra uma fibra ótica.[30] Em campo de batalha, onde o acesso ao ciberespaço tende a ser mais escasso e intermitente, a mesma proposição se aplica: um militar não especializado dificilmente saberia dizer se a interrupção na transferência de dados ocorreu

[30] Em 2011, a Armênia e parte da Geórgia ficaram sem acesso à Internet por um "ataque" de menor monta se comparado à ofensiva russa do ano anterior. Desta vez, uma senhora de 75 anos foi a responsável por negar acesso à parte importante do ciberespaço dos dois países ao cortar um cabo com uma pá quando estava à procura de ferro. Cf.: SHACHTMAN; SINGER, 2011; DEIBERT, 2013, p. 29-30.

devido à queda de conexões com satélites, a problemas de configuração da rede ou à interferência na radiodifusão provocada pelo inimigo.

Além de causarem distúrbios maiores que os do dia-a-dia, operações militares no ciberespaço também precisam ser persistentes, resistindo a soluções alternativas de rápido emprego, como reconfigurações de rede e reinicializações de servidores. Para isso, faz-se necessário que os ciberataques superem a resiliência e a redundância de redes críticas, de modo a negar o uso efetivo do ciberespaço pelo adversário ou infligir dano constante a seus sistemas. Em redes não críticas, a possibilidade do operador da rede simplesmente desconectar seu sistema autônomo de outras redes ou aprimorar mecanismos de bloqueio de acesso ao seu sistema é outro obstáculo a ser superado (PETERSON, 2013, p. 122-124). Ainda que neste caso isso gere constrangimentos ao uso do ciberespaço, redes que não sejam tão dependentes de canais externos podem ser desconectadas sem maiores custos, principalmente para a população (LIBICKI, 2009, p. 124). Além disso, em ambos os casos, ainda é necessário superar o fator social, visto que as sociedades sabem conviver com restrições a um serviço, podendo, inclusive, substituir seus sistemas e redes por soluções análogas (LINDSAY, 2013b, p.19). Por conta disso, ataques aos meios físicos podem ser a melhor solução para prolongar o efeito de operações militares no ciberespaço, principalmente contra adversários que não possuam rotas alternativas para o tráfego de dados.

Não obstante, também torna-se necessário que ataques cibernéticos tenham como alvo principal dispositivos e/ou aplicações utilizadas em atividades de C4ISR. Essas atividades, quando executadas por meio do ciberespaço, elevam os eletrônicos e o espectro eletromagnético constituintes desse meio à categoria de ativos estratégicos. Além disso, se o centro de gravidade de uma guerra for compreendido em termos clausewitzianos, ou seja, como um ponto de balanço e de unidade entre as forças combatentes[31], forças armadas

[31] ECHEVARRIA II, 2003, p. 108 – 123. O centro de gravidade de uma guerra encontra-se, conforme explica Echevarria II, onde a unidade e interdependência das forças combatentes existem de tal modo que faz com que elas se concentrem. Assim, o centro de gravidade de um inimigo não está em sua força ou capacidade, nem sua fraqueza reside aqui. Em outras palavras, o conceito de centro de gravidade, na concepção clausewitiziana, parte de uma abordagem baseada em efeitos e não em capacidades. Como exemplo, Echevarria II cita a derrota de Napoleão na campanha de 1814, descrita por Clausewitz no livro V do Da Guerra. Para o militar, a derrota teria sido evitada se Napoleão tivesse reconhecido que o comandante das tropas prussianas, Blücher, era o centro de gravidade da guerra, devido ao seu espírito empreendedor, e com sua derrota as tropas austríacas também se retirariam do campo de batalha. Entretanto, Napoleão preferiu ter duas vitórias rápidas sobre cada tropa, que rapidamente se reestabeleceram e o venceram na batalha seguinte. Na doutrina militar estadunidense, concepções de operações baseadas em efeitos defendem que ataques em alvos de segunda-ordem podem causar efeitos em alvos de primeira-ordem, como parece ser o caso em operações militares no ciberespaço. Cf. GREATHOUSE, 2014, p. 30.

altamente dependentes do ciberespaço para fins de comando e controle tem nesse ambiente seu centro de gravidade.[32]

Apesar dos pontos levantados aqui, algumas análises acreditam que a guerra combatida somente no ciberespaço será o principal tipo de conflito do futuro. Usualmente, essas abordagens tratam o futuro da guerra como absoluta: instantânea, com o uso do máximo de força e de todos os recursos disponíveis. No entanto, ela vai de encontro às configurações do ciberespaço. Ainda que a transferência de dados dentro de uma rede ocorra em milissegundos, as diferenças temporais entre as fases de infecção e de *payload* tiram a instantaneidade de operações cibernéticas. Outro fator que deve ser considerado são as diferenças temporais entre a concepção, o desenvolvimento, a infecção e a ativação de códigos maliciosos (HEALEY, 2012, p. 14-15).[33] Durante esse período, as mudanças nas práticas cotidianas dos usuários e/ou nas configurações do sistema, assim como interações não previstas com o sistema podem reduzir a potência do código, impedindo o uso da máxima força possível (LIBICKI, 2013, p. XI). De fato, o "terreno" mapeado pode ter mudado tanto após um ataque a ponto de ser impossível lançar um segundo assalto (LIBICKI, 2009, p. 126). E como ataques cibernéticos fazem uso de vulnerabilidades de dia zero[34], as quais quando expostas podem ser corrigidas, utilizar todos os recursos disponíveis torna-se inviável/improdutivo. Ademais, sendo a guerra um ato político, o lançamento de operações que reúnam as características de uma guerra absoluta sofrem constrangimentos políticos, além de terem de se adaptar aos recursos finitos disponíveis (GARTZKE, 2013, p. 51).

Outras análises argumentam que os efeitos limitados de ataques cibernéticos restringem o poder de coação deste meio, sendo improvável uma guerra travada puramente no

[32] Isto, contudo, não significa, tal como apoiadores da RMA argumentam, que ataques via ciberespaço garantam a supremacia informacional e, logo, a vitória na guerra. Na verdade, como salienta Londsdale (2007, p. 255), a vitória na guerra depende mais do sucesso estratégico do que de sucessos táticos. Assim, mesmo que o ciberespaço seja considerado o centro de gravidade em uma guerra, o ataque à ele não se traduz, necessariamente, em um sucesso estratégico. Em outras palavras, a informação não é necessariamente o elemento decisivo, principalmente levando-se em conta os problemas de coleta, processamento e disseminação de informação relevante (BETZ, 2006, p. 515). Além disso, a conquista de uma suposta supremacia informacional pode causar efeito contrário e tornar as forças combatentes menos produtivas.

[33] Ainda que a transferência de dados no ciberespaço possa ocorrer em milissegundos, isso não implica que a execução de um comando seja instantâneo. No caso Stuxnet, por exemplo, Lindsay (2013a, p. 378) afirma que a diferença temporal mínima entre a compilação do código malicioso e a infecção de Natanz foi de doze horas, e a maior foi de vinte e oito dias. Contudo, o enfoque dado à suposta rapidez com que os ciberataques acontecem pode ter reflexos na práticas cotidianas de operações militares. Geers (2011, p. 20) é um dos pesquisadores que apoia a simplicação do ciclo de decisão em ciberoperações, de modo a dar maior poder de decisão ao operador militar para ele tomar as atitudes necessárias para conter e/ou retaliar um ataque. Ainda que seja improvável que os tomadores de decisão apoiem esta ideia, devido à possibilidade de propagação e de danos colaterais (PAUL, 2008, p. 96), sua aplicação futura traz consequências para a escalada dos conflitos.

[34] Vulnerabilidades de dia zero são vulnerabilidades de *softwares* desconhecidas pelos seus fabricantes.

ciberespaço. Contudo, se por um lado a ciberguerra total não é possível, devido às limitações para conquista, por outro, o ciberespaço, tal como outros meios, pode ser utilizado tática e estrategicamente para os fins da guerra. De fato, os efeitos do ciberespaço sobre a guerra são multiplicadores (*force multiplier*)[35], ainda que não seja possível dominar o ciberespaço, nem desarmar completamente um inimigo ou destruí-lo apenas utilizando ataques cibernéticos (LIBICKI, 2009, p. 119). Por isso, ainda que potências militares sejam alvos de ciberataques, os atores com maiores capacidades militares convencionais tendem a reforçar seu poder por dois motivos: por um lado, como os ataques cibernéticos são usualmente temporários, as forças combatentes que possuam mais meios de tirar proveito do ataque a redes se beneficiam mais do que forças que não possuem os ativos necessários para explorar esse ataque (BETZ, 2012, p. 695; GARTZKE, 2013, p. 57-65; LINDSAY, 2013a, p. 399); por outro lado, forças convencionais tem maiores chances de punir um oponente que as tenham atacado, criando uma barreira para atores fracos, os quais, devido à complexidade de ataques de alta intensidade, possuem maior dificuldade para transformar um código em uma arma.

3. DEFESA NACIONAL, REDES MILITARES CRÍTICAS E CIBERGUERRA

Qualquer rede que faça parte do ciberespaço possui pelo menos um dispositivo transmissor e um dispositivo receptor responsáveis por manipular os dados analógicos ou digitais enviados por seus usuários. Para que a transferência ocorra, ambos equipamentos transformam a informação recebida em ondas eletromagnéticas, as quais são transportadas através um canal de comunicação (HYAKIN; MOHER, 2008, p. 23). Entretanto, a heterogeneidade de dispositivos eletrônicos, de protocolos de comunicação[36] e de topologias de redes existentes gera problemas analíticos na análise do ciberespaço. Implementados segundo configurações técnicas próprias, as diferentes redes que compõem esse meio formam um sistema complexo de difícil apreensão. Com o intuito de simplificar essa complexidade, diversos pesquisadores, principalmente na área da Tecnologia da Informação, adotaram uma análise de redes em camadas.[37] Essa abordagem divide cada rede em um número específico de

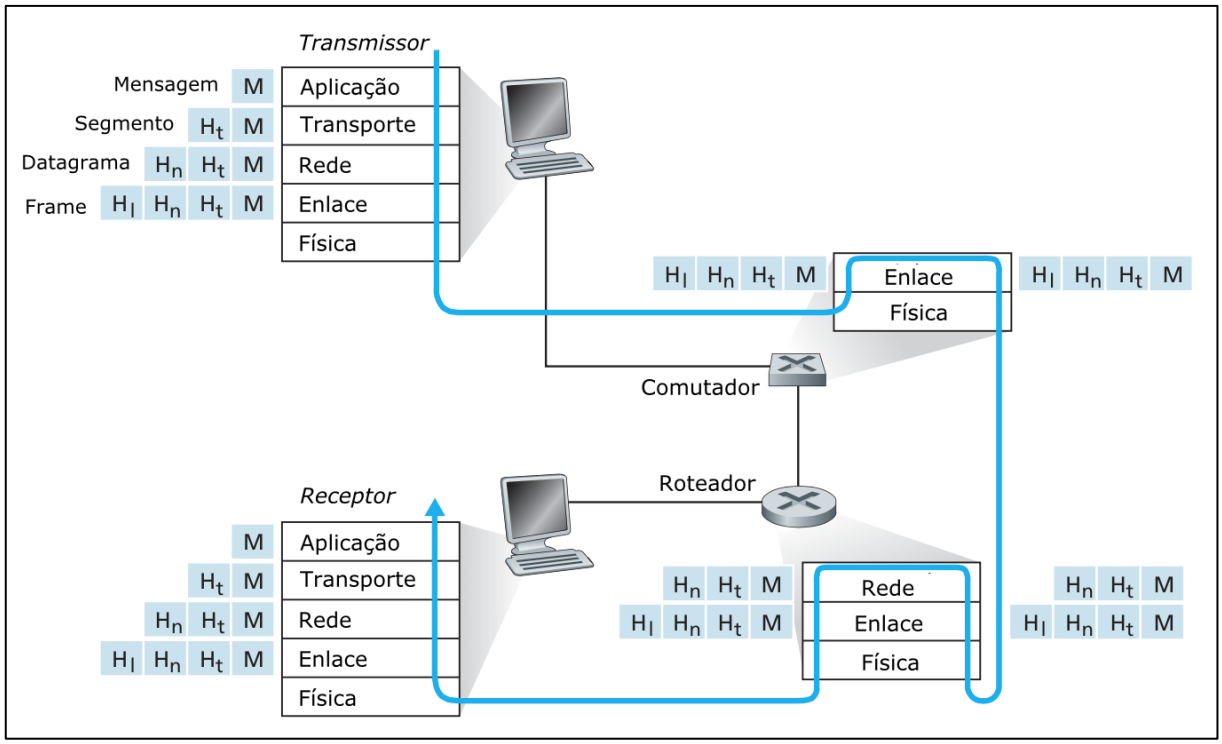
[35] Libicki (2009, p. XV) argumenta que a ciberguerra tem função de suporte (*support function*) no desarmamento de inimigos. Cf. também GRAY, 2013, p. 57-58.

[36] Conforme Kurose e Ross (2013, p. 9, tradução nossa), "um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades de comunicação, assim como as ações tomadas na transmissão e/ou recebimento de uma mensagem ou evento".

[37] Um dos principais modelos de análise em camadas foi produzido em 1994 pela *International Organization for Standardization* (ISO) e pela *International Electrotechnical Commision* (IEC) com o intuito de padronizar a comunicação entre diferentes sistemas computacionais. Cf. ISO/IEC, 1994. Boa parte da comunidade científica ou faz uso de um modelo adaptado da ISO (KUROSE; ROSS, 2013; TANENBAUM; WETHERALL, 2011), ou

camadas, onde cada uma implementa protocolos específicos e realiza tarefas independentemente das outras. Não obstante, cada camada depende de serviços oferecidos pelas camadas inferiores para transferir dados.

Figura 1 – Modelo de Rede com Cinco Camadas



Adaptado de: KUROSE; ROSS, 2013, p. 54.

O modelo adotado aqui prevê uma divisão da rede em cinco camadas, conforme demonstrado na Figura 1. Segundo esse modelo, a transferência de dados entre dispositivos tem início na camada de aplicação, a qual fornece serviços às aplicações disponíveis na rede e empacota os dados a serem transferidos em mensagens. As mensagens são repassadas para a camada de transporte, a qual é responsável por iniciar e finalizar as conexões entre as aplicações envolvidas, além de transportar os dados seguindo padrões de eficiência, confiabilidade e custo-benefício. Entre suas principais funções estão o endereçamento e o controle de fluxo dos pacotes de dados, os quais são empacotados em segmentos. Na camada de rede, a próxima do modelo, os segmentos são entregues para o *host* de destino, sendo essa

usa um modelo que separa a rede em uma camada física, uma camada lógica e uma camada semântica (KELLO, 2013, p. 18; LIBICKI, 2009, p. 12).

camada a responsável pela interconexão entre diferentes redes. A principal função desempenhada por ela é a de roteamento, descobrindo e calculando a melhor rota para a entrega dos pacotes de dados. Nessa camada, os segmentos são empacotados em datagramas, os quais são repassados para a camada de enlace de dados, responsável pelo transporte dos dados entre máquinas adjacentes de forma eficiente e confiável. Ela desempenha tarefas de detecção e correção de erros dentro da rede, assim como regulamenta o fluxo de dados, empacotando os datagramas em *frames*. Por fim, a camada física, transporta *bits* individuais através das conexões entre os nodos da rede, sendo responsável pelas atividades de modulação e transmissão.

Entretanto, como mostra a Figura 1, os dispositivos de uma rede não precisam implementar todas as camadas do modelo, ainda que seja mandatório o uso das camadas de rede, de enlace de dados e física para a conexão entre os dispositivos. Além disso, abaixo de todas as camadas do modelo, encontra-se o meio físico, através do qual os dados da rede trafegam como sinais eletromagnéticos. Ele é a única conexão física entre os dispositivos de uma rede, sendo todos os outros *links*, entre as camadas de diferentes dispositivos, virtuais (YOO, 2013, p. 1723). Por conta disso, independentemente das configurações que uma rede possa ter, ela é dependente de *hardware* para processar e transmitir dados, sendo o meio físico[38] uma das principais variáveis na explicação da condução de operações militares no ciberespaço e na sua integração com outras facetas do fenômeno. A seguir, o argumento pode ser melhor evidenciado a partir da análise da infraestrutura crítica nacional de acesso ao ciberespaço e das chamadas redes militares críticas, fundamentais no plano estratégico, operacional e tático da guerra.

Ativos estratégicos nacionais e ciberguerra

Sendo as redes dependentes de elementos físicos para sua existência, a posse, a localização e o controle de componentes que permitam o processamento e trânsito de dados é condição primordial para o acesso e uso efetivo do ciberespaço na guerra. Ou seja, os nodos (dispositivos eletrônicos) e as conexões (canais de comunicação) de redes sensíveis são ativos estratégicos no âmbito da defesa nacional do ciberespaço. A livre movimentação e manobra

[38] A escolha de um meio físico para o transporte de dados depende dos custos relativos e dos benefícios medidos em termos da redução de ruído (perda informacional) durante a transmissão pelo canal. De maneira geral, este meio pode ser guiado, como no caso da fibra ótica, ou não guiado, como no caso da radiofrequência.

no espaço cibernético depende, neste sentido, da implementação, manutenção e proteção desses ativos.

No quesito posse, ainda que o acréscimo de nodos e conexões de uma rede distribuída aumente os pontos de entrada de *malwares*, o crescimento da rede tende a criar maior redundância e, logo, resiliência no caso de mal funcionamento de uma parte dos componentes. Por isso, a posse de uma rede grande e complexa é entendida como sendo melhor que a posse de uma rede pequena e simples, a nível doméstico. O transporte de dados sigilosos por redes próprias, compostas de artefatos diversos como cabos, satélites, roteadores e comutadores, é, assim, um dos fatores primordiais de uma estratégia de defesa nacional.

Somada à posse, a localização desses ativos é outra variável a ser considerada no cálculo estratégico para o acesso e uso do ciberespaço. Tal como a utilização de componentes que sejam de posse alheia suscita problemas de acesso e uso indevido de dados sensíveis, a localização de ativos estratégicos nacionais em territórios que estejam sob a soberania de outro Estado faz com que os dados trafegados corram maior risco de serem interceptados. Além disso, a concentração de componentes em uma pequena área facilita o ataque a eles, sendo preferível que eles estejam distribuídos por diversas localidades, aumentando a segurança da rede.

Por fim, o controle de ativos estratégicos é fundamental para que a rede possa ser confiável e gerenciável. O uso da Internet como principal rede para a transferência de dados sensíveis, deste modo, suscita problemas pois seu controle, localização e posse são compartilhados (ainda que de maneira não equitativa) com outros países do mundo. Ainda que não seja possível proteger todos os cabos, roteadores e comutadores de uma nação para garantir o pleno uso do ciberespaço, é possível priorizar certos componentes, elevá-los a categoria de ativos estratégicos, e protegê-los dos riscos de interferência ou queda.

Entretanto, ainda que a posse, a localização e o controle de nodos e conexões seja uma condição necessária para uma estratégia de defesa cibernética, ela suscita problemas de ordem financeira e temporal. De um lado, esses equipamentos precisam ser implementados, o que acarreta custos financeiros e temporais consideráveis; de outro, eles precisam ter manutenção, o que nem sempre é fácil devido a questões de adaptação, a herança de sistemas legados ou ao local em que eles estão instalados[39]. Apenas no caso estadunidense, estima-se que somente o

[39] O cabo transártico, que deve ligar diretamente Londres a Tóquio, é um bom exemplo dos custos de implementar e manter esses ativos. Para que o cabo seja instalado, é necessário mapear cada metro do percurso

Departamento de Defesa do país precisava manter, em 2010, mais de 15 mil redes e sete milhões de computadores, os quais estavam espalhados por quatro mil instalações em 88 países (LYNN III, 2010).

Além disso, devido a cadeia de produção global de peças computacionais, o controle desses componentes nem sempre pode ser 100% garantido. A procedência das peças de alguns ativos estratégicos tem aumentado a sensação de ameaça dos Estados (KELLO, 2013, p. 29), os quais buscam formas de minimizar esse problema por meio de programas de qualidade ou pelo fomento da produção nacional de peças. Nos EUA, a redução acentuada da produção local de *hardware* elevou a apreensão governamental quanto à existência de *backdoors* e *kill switches*[40] em instalações e equipamentos estratégicos na área de segurança e defesa nacional.

A transferência da manufatura de microeletrônicos para países com mão de obra barata e especializada começou na década de 1960, mas os efeitos desse processo sobre o setor militar não foram imediatos para os EUA, visto que o país manteve certa influência sobre a produção devido à significativa participação de seu setor de defesa na compra de circuitos integrados (ADEE, 2008). Entretanto, os próximos anos viram o aumento da dependência tecnológica do setor e a sua queda de participação na aquisição destes dispositivos (estima-se que o setor de defesa dos EUA corresponda a apenas 1% das vendas mundiais atualmente)[41].

A preocupação com os circuitos integrados utilizados fez, em 2003, o então vice-secretário de Defesa dos EUA redigir um memorando estabelecendo uma estratégia para fomentar a indústria nacional de *chips* e a certificação de produtores, o qual foi seguido em 2005 por um relatório do Conselho Consultivo de Ciência do DoD sobre a confidencialidade, integridade e disponibilidade de microeletrônicos utilizados em aplicações militares. Nesse mesmo esforço, em 2007 a *Defense Advanced Research Projects Agency* (Darpa), órgão de pesquisa e desenvolvimento ligado ao Ministério da Defesa dos EUA, lançou um programa de certificação de circuitos integrados, o *Trust Integrated Circuit (*TRUST*)*, o qual foi substituído pelo *Integrity and Reliability in Integrated Circutis* (IRIS).[42] Apesar desses

---

proposto com sonares e detectores de metais, o qual, após validado, é percorrido por navios a uma velocidade de aproximadamente 2 km/h. E tudo isto precisa ser feito durante o curto verão ártico, que vai de agosto a outubro, período em que o gelo derrete e é possível passar pela região. A manutenção do cabo, após instalado, deve sofrer os efeitos do tempo frio, somente sendo possível consertá-lo, em caso de rompimento, durante esta janela de tempo.

[40] *Backdoors* são programas que permitem o acesso remoto de um dispositivo. *Kill switch* são programas que destroem o sistema ou dispositivo.

[41] EUA, 2005, p. 17.

[42] Cf. http://www.darpa.mil/ e MARKOFF, 2009.

esforços, conforme Markoff (2009), os EUA fabricam atualmente, em instalações seguras, somente 2% de todos os circuitos integrados utilizados em equipamentos militares. Além disso, o fato da principal produção ser localizada no leste asiático tem suscitado polêmica nos EUA. Ainda que não seja possível fabricar todos os chips de todos os equipamentos em um único país (ADEE, 2008), trata-se sim de uma vulnerabilidade potencial ainda não devidamente analisada.

Entre os componentes que devem ser elevados a ativos estratégicos, estão os cabos coaxiais, de par trançado e de fibra ótica de redes sensíveis, instalados em territórios soberanos ou em águas internacionais desde meados do século XIX. Incorporados pelo setor militar na condução da guerra antes da I Guerra Mundial, esse componente foi rapidamente utilizado pelas principais potências mundiais para alcançar objetivos estratégicos em conflitos militares. O Reino Unido, principal produtor, financiador e mantenedor de cabos submarinos do mundo até meados do século XX, fez uso desse ativo para os fins políticos de suas guerras nas suas colônias. E sendo seus os principais cabos instalados no mundo, isso lhe permitiu negar acesso de inimigos a importantes redes, assim como demandar a entrega dos livros de código secreto dos Estados amigos, caso estes quisessem utilizá-las (HEADRICK; GRISET, 2011, p. 563).

De fato, o uso de cabos para a transmissão de mensagens amigas ou para a interceptação e corrupção de mensagens inimigas, por meio da inserção de informações falsas em cabos, assim como o rompimento intencional dessas conexões, tornaram-se práticas recorrentes na história militar. Já na década de 1860, a nascente rede telegráfica estadunidense foi extensivamente utilizada pela União e pelos Confederados, durante a Guerra Civil Americana, tanto para a transmissão quanto para a interceptação de mensagens (BROWNE; THURBON, 1998, p. 3). E na I Guerra Mundial, menos de 24 horas após ter declarado guerra à Alemanha, uma frota britânica foi enviada para cortar os cinco cabos submarinos alemães que ligavam o país à Europa Ocidental e aos EUA, limitando a conexão alemã com o resto do mundo. (WINKLER, 2008, p. 5-7).

Ciente da possibilidade de interceptação de mensagens transferidas por esse meio, o Reino Unido, no início do século XX, criou uma rede telegráfica mundial, a qual cruzava o globo, mas passando somente por terras sob o domínio da coroa britânica, conhecida como *All Red Line*. E pelos mesmos motivos o país incentivou o uso de seu território como *hub* das linhas de comunicações internacionais (HEADRICK; GRISET, 2011), gerando um controle e

redundância que mostram-se estratégicos para os interesses ingleses ainda hoje, como demonstrado recentemente pela revelações de Edward Snowden e do programa *Tempora*.[43]

Entretanto, em determinados países, devido a limitações geográficas ou econômicas, a chegada e a saída dos cabos submarinos está concentrada em pequenas áreas, gerando pontos de estrangulamento dos cabos. Estes gargalos são um problema, ainda mais se tem-se em conta que boa parte dos dados transcontinentais passam por cabos submarino. Estima-se, por exemplo, que 90% do fluxo da Internet, uma das principais redes do ciberespaço, passe por eles (ZUCCARO, 2011, p. 58). No Mediterrâneo, importante rota de conexão da Europa com o Oriente, dois cabos submarinos quebrados em 2008 derrubaram 70% e 60% do fluxo de dados do Egito e da Índia, respectivamente, com os impactos desse rompimento se estendendo pelas redes do Afeganistão, Arábia Saudita, Bahrein, Emirados Árabes Unidos, Kuwait, Maldivas, Paquistão e Qatar.[44]

O processo de digitalização do final do século XX também elevou os satélites a ativos estratégicos. Com o espaço sideral sendo utilizado como força multiplicadora da defesa nacional e com o satélite tornando-se uma das principais ferramentas para atividades de suporte militar, ele tornou-se indispensável para a condução da guerra. Em especial, o satélite tornou-se um componente necessário para a manipulação de dados, principalmente em lugares remotos e/ou com pouco acesso a redes. Na Guerra do Iraque (2003-2011), por exemplo, estima-se que atividades de comunicação, vigilância e reconhecimento, assim como os sistemas de navegação estadunidenses, tenham sido quase que 100% abastecidos com informações provenientes de satélites (MACHADO, 2014, p. 40).

Outros dois componentes que ganharam destaque com a interconexão de dispositivos foram os roteadores e os comutadores. Entre eles, os responsáveis por serem pontos de troca de tráfego (PTTs) tornaram-se ativos estratégicos, pois permitem que um Estado corte a conexão internacional sem a necessidade de derrubar sua rede nacional – apenas limitando-a. Os PTTs são *hubs* que permitem que provedores locais realizem troca de dados sem a necessidade de utilizar redes de terceiros. De fato, a inexistência de PTTs em países de

[43] Snowden revelou que o serviço de inteligência inglês grampeou diversos cabos submarinos que desembarcam na ilha, dentro do programa *Tempora*. Através de acordos com as empresas donas desses cabos ou donas das estações de desembarque desses cabos, o GCHQ (*Government Communications Headquarters*) teve acesso a boa parte da comunicação mundial, visto que o Reino Unido é um dos principais hubs do *backbone* da Internet hoje em dia. Segundo informações do órgão britânico, esses dados passavam direto para um filtro, que descartava tráfego intenso e de pouco valor de dados, e selecionava dados conforme uma lista de seletores elaborada pelo GCHQ e pela NSA (*National Secutity Agency*). Cf. MACASKILL et al, 2013.

[44] BORLAND, 2008.

pequeno porte os deixa vulneráveis a operações cibernéticas, visto que a rede doméstica torna-se extremamente dependente de conexões internacionais.

Ainda que de forma indireta, a posse de alguns desses componentes auxiliou a coalização liderada pelos EUA na Guerra do Golfo (1990-1991). Isto deveu-se a cooperação de empresas de comunicação ocidentais, que haviam construído parte da rede militar iraquiana e forneceram as informações sobre a localização dos principais nodos e conexões dela (BROWNE; THURBON, 1998, p. 38-39). Na Guerra do Kosovo (1999), especula-se que ataques contra os sistemas da OTAN não tenham ocorrido (ou sido bem sucedidos) pois a organização utilizada sistemas operacionais e *softwares* próprios, não disponíveis no mercado, e, logo, com menos chance de terem suas vulnerabilidades descobertas (CAVELTY, 2008, p. 78). Na Guerra do Iraque e do Afeganistão, especula-se que os EUA tenham utilizado armas cibernéticas para o auxílio de operações militares cinéticas, como o uso de *jammers* para interceptar radares (CARR, 2013, p. 35).

Entretanto, dois eventos recentes, catalogados como ciberguerras, chamaram a atenção dos analistas. De um lado estão os ciberataques à Estônia em 2007. De outro a Guerra na Ossétia do Sul entre Rússia e Geórgia, em 2008. No primeiro caso, conforme Kello (2013, p. 24, tradução nossa), o ataque DDoS na Estônia "congelou as atividades governamentais e financeiras do país por aproximadamente três semanas". Entretanto, isto precisa ser contextualizado. O ataque realmente derrubou sítios governamentais e, conforme relatos, deixou vários caixas eletrônicos fora do ar. No entanto, a interrupção desses serviços não durou, como o texto dá a entender, três semanas ininterruptas. A queda dos sítios e dos ATMs durou poucas horas e só ocorreu em dois/três dias.

Além disso, duas questões importantes, ainda não esclarecidas, precisam ser pontuadas: (1) a princípio, a queda dos sítios governamentais não causaria o bloqueio a nenhum serviço fundamental para o governo ou a população, por mais incômodo que o ataque possa ser (SHACHTMAN; SINGER, 2011); e (2) é incerto que o serviço de ATMs tenha sido prejudicado diretamente pelo ataque DDoS, visto que tais equipamentos não estão, usualmente, conectados à Internet, sendo necessário o acesso físico ao caixa eletrônico.[45] Inclusive, um dos cientistas que acompanhou a instalação do Centro de Defesa Cibernética da OTAN na Estônia, afirmou que os danos foram mínimos e que nenhum serviço essencial foi prejudicado com os ataques cibernéticos de 2007 (LAWSON, 2011, p. 6). Portanto, no caso

[45] CHOO, 2011, p. 722. Hansen e Nissembaum (2009) falam apenas em queda de serviços online.

da Estônia, ainda que particularmente agudo, é controverso (e equivocado segundo o que se sabe efetivamente) caracterizar o ataque cibernético como um ataque a infraestruturas nacionais críticas, os quais seriam, caso comprovados, atos de guerra (HANSEN; NISSEMBAUM, 2009, p. 1170).

A minimização deste evento cibernético se deve porque, de modo geral, ataques DDoS, apesar de irritantes, usualmente não possuem impacto estratégico ou tático relevantes para a condução da guerra, visto que eles normalmente não têm como alvos IPs sensíveis para o comando e controle durante a guerra. Isto não significa, contudo, que eles nunca possam ter valor estratégico. Um exemplo claro disso é a Guerra da Ossétia do Sul, travada entre o governo da Geórgia e forças separatistas (estas últimas com apoio russo). O fato de não existir um Ponto de Troca de Tráfego na Geórgia, aliado ao fato de a Internet ter apenas uma entrada/saída no país, tornou-o extremamente vulnerável ao limite de banda e tráfego desta conexão. Assim, o ataque DDoS contra o país congestionou as linhas de comunicação da rede e forçou o governo georgiano a fechar a conexão do país com o resto do mundo, produzindo um impacto estratégico grande nas comunicações dependentes da Internet no país. A Estônia conseguiu driblar o ataque DDoS contra sua rede graças a um par de PTTs na sua capital, Tallinn. Desse modo, não seria incorreto afirmar que a interligação de provedores domésticos por meio de PTTs é parte fundamental de uma boa defesa cibernética.[46]

E ainda que o conflito entre russos e georgianos tenha sido amplamente utilizado como exemplo de guerra no ciberespaço devido aos ataques DDoS que derrubaram sítios governamentais e de políticos na Internet, o principal problema cibernético para a Geórgia decorreu da destruição física de parte da infraestrutura de acesso ao ciberespaço do país, operada por meio da aplicação de ataques cinéticos. O rompimento da principal linha de fibra ótica georgiana e o bombardeamento de transmissores de radiodifusão restringiram as comunicações estratégicas do país.[47] Além disso, é sabido que o curto alcance dos satélites russos limitou a movimentação e manobra russa no ambiente cibernético (DEILBERT; ROHOZINSKI; CRETE-NISHIHATA, 2012, p. 9-10).[48]

[46] STAPLETON-GRAY; WOODCOCK, 2011; HEALEY, 2013, p. 72.
[47] Cf. DEILBERT; ROHOZINSKI; CRETE-NISHIHATA, 2012. Conforme os autores, um noticiário georgiano afirmou que um grupo criminoso cibernético havia tomado controle de roteadores na fronteira da Geórgia, redirecionado as telecomunicações da Geórgia para a rede russa. No entanto, os pesquisadores não conseguiram verificar a veracidade esses rumores.
[48] Deilbert, Rohozinski e Crete-Nishihata (2012, p. 9) destacam que as falhas do satélite russo chegaram ao ponto de um comandante russo ter pego emprestado um telefone de um jornalista para se comunicar com suas tropas.

Portanto, ainda que Arquilla (2011, p. 63) argumente que um ataque contra a infraestrutura do ciberespaço nos Estados Unidos da América possa ser devastador para aquele país, é importante ter em mente que tal ataque envolveria necessariamente a combinação de operações de guerra convencionais e cibernéticas, sendo que apenas dois países no mundo teriam condições (mas não a intenção) de tentar algo assim. Além disso, os próprios ataques cibernéticos esbarrariam na resiliência e redundância da rede cabeada estadunidense. De fato, os eventos na Geórgia[49] demonstraram que "o controle da infraestrutura física do ciberespaço é crítico tanto estrategicamente quanto taticamente" e que "cientistas sociais precisam prestar muito mais atenção na infraestrutura física do ciberespaço" (DEILBERT; ROHOZINSKI; CRETE-NISHIHATA, 2012, p. 17, tradução nossa).

Redes militares críticas

Ainda que a infraestrutura de redes nacionais dependa de cabos para a transmissão de dados, forças combatentes, sejam elas expedicionárias ou mesmo de defesa do território nacional, não podem depender apenas dessa estrutura fixa para a condução de operações militares. Nesses casos, devido a questões geográficas, econômicas e de mobilidade, a interconexão entre dispositivos eletrônicos depende mais de conexões sem fio do que de conexões cabeadas (POISEL, 2008, p. 249).

Entretanto, em virtude das características dos *links* sem fio, seu uso gera constrangimentos para a condução da guerra. O uso deste tipo de conexão aumenta a probabilidade de perda de dados, visto que *links* sem fio possuem taxas de erro consideráveis[50] devido ao formato como a informação é repassada: por meio de radiodifusão. Além disso, as conexões sem fio apresentam maiores taxas de erro conforme a distância entre o emitente e o receptor aumenta, prejudicando a dispersão de tropas.[51] Em redes militares, em especial as que são implementadas em campo de batalha, a perda de dados, a pequena largura de banda e os atrasos precisam ser superados por meio da implementação de protocolos

[49] Hollis (2008) argumenta que a Rússia deliberadamente só atacou sítios web que não fossem provocar caos, evitando sítios ligados a redes elétricas e de petróleo. Entretanto, ele não explica como a queda desses sítios provocaria algum efeito na distribuição de energia e ou o oleoduto, além de carecer de comprovação empírica.
[50] Tecnologias cabeadas também podem apresentar taxas de erro consideráveis. Entretanto a comparação feita aqui se refere à fibra ótica, largamente utilizada e que apresenta uma das menores taxas de erro entre os meios de transmissão da atualidade.
[51] E conforme Tanenbaum e Wetherall (2011, p. 202, tradução nossa), esses erros "não podem ser evitados a um custo ou despesas razoáveis em termos de performance".

específicos e por uma infraestrutura física robusta. A Internet, por exemplo, não consegue providenciar quaisquer garantias de tempo e taxa de transferência atualmente (KUROSE; ROSS, 2013, p. 95).

Por conta dessas características, em ambientes adversos, como o campo de batalha, redes móveis *ad hoc*, conhecidas como MANETs (do inglês, *mobile ad hoc networks*), tendem a ser implementadas. Essas redes são compostas de dispositivos móveis que podem configurar a si mesmos conforme a movimentação das tropas, facilmente alterando a topologia da rede e, logo, o fluxo de informações dentro dela. Sem a necessidade de uma central de controle, o funcionamento da rede depende dos dispositivos que a compõem para o gerenciamento dos recursos disponíveis e de canais de radiodifusão para a distribuição do conteúdo.

Entretanto, as MANETs apresentam, em período de execução, grandes variações em suas topologias e nas capacidades de seus canais de transporte, prejudicando a distribuição de conteúdo entre os nodos. O afastamento de um nodo do perímetro de sinal da rede pode ser o suficiente para degradar a rede como um todo, sendo necessário ou uma menor dispersão das tropas ou uma movimentação mais conjunta das unidades.

Outro problema ligado às redes móveis está no fato de seus dispositivos serem os responsáveis por administrar as políticas de roteamento da rede. Por causa disso, um nodo comprometido na rede pode, ao comunicar ao nodo remetente de uma mensagem que ele possui a rota mais curta até o nodo destinatário, forjar uma conexão que pode ser utilizada tanto para a destruição quanto para a interceptação e/ou alteração dos dados. Neste último caso, como o nodo comprometido faz parte da rede e é considerado válido, não há como, para o nodo destinatário, distinguir que a mensagem foi alterada. Em um sistema que desempenhe a função de mapear forças inimigas, uma informação inválida sobre a localização de uma unidade inimiga não é facilmente distinguível.

Além disso, os dispositivos móveis destas redes, como o nome sugere, precisam de baterias para funcionarem, o que pode ocasionar problemas de suprimento de energia. Um nodo egoísta deve reduzir suas atividades na rede para poupar energia, afetando a topologia dela. Por isso, um ataque que faça diversas solicitações a um nodo específico pode descarregar sua bateria rapidamente, alterando o trânsito de informações em campo de batalha. Ademais, essas redes não são facilmente escaláveis, ou seja, o aumento do número de dispositivos acessando a rede aumenta o tráfego de dados e diminui a banda destinada a cada

nodo, *ceteris paribus*, causando *delays* ou até a queda de *links*.[52] Isto é preocupante principalmente considerando-se problemas de *big data*, visto que cada vez mais informações são trafegadas no campo de batalha e que esse tráfego deve ficar mais intenso devido ao tamanho dos aplicativos e documentos transmitidos. Em resumo, o crescimento da dependência da força combatente em relação a informações compartilhadas e o aumento do fluxo dessas informações são primariamente problemas de processamento e comunicação.

Se o processamento e a comunicação de informações realmente são o fator chave na guerra contemporânea, é esperado que as forças inimigas façam o possível para romper o fluxo de dados, de tal modo que o funcionamento eficaz de redes militares torna-se fundamental para a condução da guerra no século XXI.[53] Entretanto, o uso do ciberespaço em campo de batalha parece estar longe de ser eficaz, como demonstrou Dan Hugues, responsável pelo programa executivo de comando, controle e comunicação tático do Exército estadunidense, conhecido pela sigla PEO-C3T, em apresentação organizada pelo sítio *C4ISR & Networks* em 2014.[54] Segundo ele, o planejamento e a implementação de redes militares nesses cenários pode durar semanas. E quando em funcionamento, essas redes tendem a possuir procedimentos onerosos no que se refere à mobilidade e velocidade das unidades militares. Conforme Hugues, um militar em solo que queira interconectar duas redes por meio de uma conexão de satélite precisa posicionar e ativar quatorze comutadores em uma ordem específica, padronizar os parâmetros dos dispositivos a serem conectados e esperar pelo menos doze minutos para o sistema funcionar. Outro problema são os centros de operações táticas, que são muito dependentes de cabos e tornaram-se um problema logístico em campo de batalha.

Sistemas de georreferenciamento militarizados, como o *Blue Force Tracker* (BFT), o *Force XXI Battle Command Brigade and Below* (FBCB2) e o *Joint Battle Command-Platform* (JBC-P) também têm demonstrado algumas das dificuldades de utilizar, de maneira eficaz, o ciberespaço em ambiente hostil como o campo de batalha. Ainda que o BFT estivesse em uso na Guerra do Iraque, as unidades militares em campo tiveram que depender da aproximação visual para localizar tropas amigas e hostis e de rádios FM para comunicações de curta distância. Apesar do sistema ter como propósito o rastreamento e comunicação entre essas

[52] *Ceteris paribus*, a taxa de transferência em uma rede será a taxa mínima que existe entre a origem e o destino dos dados. Usualmente, esse constrangimento nas taxas encontram-se nos pontos de acesso. Mas como o tráfego na rede também influencia essa taxa de transferência (quanto mais pacotes bits, mais congestionada fica uma rede), o gargalo da rede pode estar no seu miolo.
[53] PERERA, 2006; POISEL, 2008, p. 1.
[54] Cf. http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1454. Acesso em: 15 set. 2014.

unidades, a restrição de equipamentos disponíveis para as companhias e as falhas de conexão desses dispositivos com os satélites, responsáveis por disseminar os dados pelo sistema, dificultaram o uso do ciberespaço nas operações militares.[55] Isto não quer dizer, no entanto, que esses sistemas não tenham auxiliado e aprimorado a conduta da guerra no Iraque. Ao contrário: o uso do BFT e a comunicação via satélite são apontados como fundamentais para o rápido avanço durante a invasão do país e na descentralização das atividades de comando e controle, que puderam ser realizadas a partir de Washington.

Por causa dos problemas relatados acima, a Darpa vem desenvolvendo uma série de programas com foco na melhoria das redes militares. Uma das iniciativas busca superar a facilidade com que sistemas de navegação usados por militares sofrem *jamming* e a inconstância na disponibilidade do sinal desses sistemas em ambientes fechados ou densos através de melhorias na arquitetura dessas redes. Outra, procura melhorar o uso do espectro eletromagnético através do mapeamento das frequências utilizadas em ambientes complexos, de modo a evitar frequências congestionadas e dar insumos ao administrador da rede para melhor utilizar os meios disponíveis. O comum entre essas e outras iniciativa está na preocupação com as redes móveis *ad-hoc*, visto que elas são necessárias para que as informações desçam ao nível das companhias. No entanto, o campo de batalha exige algumas características dessas redes: eficiência, velocidade, escabilidade, confiabilidade, segurança, redundância, distribuição transparente e flexibilidade. [56]

A importância da camada física, nesse contexto, é que os problemas e características que ela envolve permitem uma abordagem mais realista, materialista e consequente do fenômeno da ciberguerra. É o meio físico, em última instância, que determina as condições de movimentação e manobra no ciberespaço. Neste sentido, os dispositivos e os canais de comunicação empregados precisam estar preparados para receber o fluxo de dados que for necessário para a condução da guerra. E por isso o gerenciamento do espectro eletromagnético é um dos fatores fundamentais para a livre movimentação dentro de uma rede (EUA, 2014, p. II-11). Outro questão importante é a necessidade de, em operações conjuntas, haver uma harmonia entre as partes responsáveis por ataques cinéticos e cibernéticos. Se um canal de comunicação é utilizado, no plano operacional e tático, para conseguir informações do adversário, ou inserir informações falsas em sua rede, por meio de um ataque cibernético,

[55] BOOT, 2005. SHACHTMAN; AXE, 2006.
[56] Para uma visão geral dos programas atualmente em desenvolvimento na Darpa, acesse http://www.darpa.mil/Our_Work/STO/Programs/.

não faz sentido que um ataque cinético derrube esta conexão, inviabilizando o seu uso (PAUL, 2008, p. 37).

4. CONCLUSÃO

Um dos efeitos da ubiquidade e da descentralização do ciberespaço é promover, no plano teórico, um empoderamento de atores não-estatais e de Estados que não se encaixam na categoria de grande potência,. Em um sistema internacional estruturalmente anárquico e no qual poucos atores possuem capacidades para a projeção de poder em longas distâncias (BUZAN; WAEVER, 2003), o uso desse domínio promove um processo de desterritorialização do poder no sistema internacional devido aos ganhos assimétricos advindos dele. Não obstante, tanto a definição de ciberespaço quanto as configurações das redes autônomas que o constituem nos permitem afirmar que, ainda que este meio seja menos dependente da geografia (ARQUILLA; RONFELDT, 1997, p. 44), o "mundo virtual" possui características físicas bem reais. E essa infraestrutura está localizada em espaços bem definidos e, muitas vezes, soberanos (BETZ; STEVENS, 2013, p. 150).

Como demonstrado, o meio físico que permite a existência do próprio ciberespaço é possuído e controlado, e está localizado, em Estados soberanos. Os cabos submarinos, apesar de estarem majoritariamente em águas internacionais (sem jurisdição de nenhum Estado), partem e chegam de Estados soberanos e são propriedades de empresas privadas com sede em Estados soberanos. Lógica igual vale para os satélites, roteadores e comutadores. Extrapolando, podemos afirmar que mesmo o espectro eletromagnético está localizado em determinado Estado, apesar de não ser delimitado por ele. O *backbone* da Internet, uma das principais redes do ciberespaço, também segue o mesmo princípio: ele comporta, conforme levantamento realizado, um total de 13 servidores raiz, sendo dez deles nos EUA, um na Holanda, um na Suécia e um no Japão.

Essa territorialidade do ciberespaço permite, inclusive, que governos promovam outras formas de delimitações legais e de padronização (DEIBERT, 2013, 14). O uso do espectro magnético, por exemplo, é delimitado por convenções internacionais e legislações locais, com bandas de frequências sendo alocadas para fins específicos conforme os interesses de cada país. Estão sujeitas a legislações nacionais também as empresas donas ou responsáveis pelos nodos e conexões por onde os dados transitam. Isto tem permitido que Estados restrinjam o acesso a conteúdos sensíveis, como ocorre regularmente em países como a China e a Rússia,

ou bloqueiem o acesso a serviços digitais, como os EUA promovem através de sanções contra países como Cuba, Sudão, Síria, Irã e Coréia do Norte.[57]

De fato, nenhuma das tecnologias desenvolvidas até o momento foi capaz de tornar o terreno irrelevante, não podendo a importância da geografia ser reduzida drasticamente (BETZ, 2006, p. 522; BETZ; STEVENS, 2013, p. 152; LONDSDALE, 2007, p. 243-244). Além disso, ainda que a geografia do ciberespaço seja bastante mutável, variáveis técnicas e físicas não permitem que essas tecnologias ultrapassem todo e qualquer terreno e/ou objeto. Neste sentido, o ciberespaço não surge como um ambiente capaz de modificar os outros meios físicos existentes, mas apenas de reforça-los.

Para isso, entretanto, um ciberataque precisa infligir dano substancial e duradouro ao oponente, o que usualmente envolve a destruição da infraestrutura de acesso ao ciberespaço e/ou a interferência constante de comunicações militares, principalmente no campo de batalha. Por isso, e tendo em vista que todas as operações cibernéticas são dependentes do domínio físico, os nodos e as conexões de redes sensíveis para a manipulação de dados tornam-se os principais ativos estratégicos de uma guerra cibernética, a nível nacional. Assim, se há um terreno chave no ciberespaço a ser conquistado, esse terreno é o que contém os componentes de acesso e uso do ciberespaço de forças amigas e inimigas.

A partir dessa constatação, podemos avaliar de forma mais realista as potencialidades e vulnerabilidades que os Estados possuem em relação às suas redes nacionais. Analisemos, por exemplo, o caso brasileiro. A existência de diversos cabos submarinos atracando no país e de vários pontos de troca de tráfego espalhados pelo território nacional torna improvável uma negação de acesso total ao ciberespaço nacional por meio desses ativos. Entretanto, o fato do país ser um *hub* de vários cabos submarinos foi um dos motivos que levou o governo americano a focar sua espionagem no Brasil, conforme revelou Snowden. Além disso, a

[57] Cf. CANABARRO, 2014, p. 197-198. Essas sanções restringem a oferta de *hardware* e *software* de empresas com sede nos EUA, impedindo o acesso dos residentes desses países a essas ferramentas. Ironicamente, apesar da crítica estadunidense às restrições que esses países fazem ao livre fluxo de informação e conhecimento, o governo dos EUA acaba por auxiliar esses governos no bloqueio a *softwares* de comunicação, como argumenta a *Eletronic Frontier Foundation* (organização não-governamental em prol dos direitos digitais). Cf. https://www.eff.org/deeplinks/2014/06/sudan-tech-sanctions-harm-innovation-development-us-government-and-corporations-must-act. No início de 2014, as sanções afetaram a atuação de cursos on-line gratuitos e massivos (MOOCs, na sigla em inglês), com um dos principais portais do ramo, o Coursera, tendo que restringir o acesso aos residentes de Cuba, Sudão e Irã ao serviço (para cumprir a legislação vigente, o site bloqueou os IPs dos usuários desses países que tentavam acessar suas contas). Cf. http://blog.coursera.org/post/74891215298/update-on-course-accessibility-for-students-in-cuba. Acesso em: 01 ago. 2014. A lista de todos os países que sofrem sanções dos EUA, assim como a descrição das sanções impostas, podem ser conferidas no site do *Office of Foreign Assets Control*, disponível em: http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx (Acesso em: 01 ago. 2014).

ênfase dada pela Estratégia de Defesa Nacional (BRASIL, 2008) à proteção da região da Amazônia e do Atlântico Sul levanta questões quanto ao uso do ciberespaço em operações militares em áreas remotas dependentes de redes não cabeadas para a transferência de dados. Em áreas tão amplas como essas, a impossibilidade de colocar unidades militares em distâncias razoáveis para manter a comunicação por meio de *wi-fi* faz com que o uso do satélite seja fundamental. E nesse caso, o Brasil não possui nenhum satélite 100% controlado por instituições nacionais, tendo de confiar informações sensíveis a instituições estrangeiras, prejudicando a defesa dessas regiões em situações de guerra.

Por conta disso, é importante que os Estados construam redes resilientes ao invés de se resignarem com a suposta inevitabilidade da ciberguerra (CHOO, 2011, p. 720). Isto perpassa pela construção de softwares mais seguros, mas como tem se observado pelos conflitos dos últimos anos, também perpassa pelo investimento em redes, visto que não é possível atingir camadas mais abstratas de uma rede se o canal de transporte de dados estiver indisponível (PAUL, 2008, p. 36). Ou seja, a garantia da resiliência, segurança e confiabilidade de redes sensíveis é fundamental para a consecução de uma estratégia de defesa cibernética. Entretanto, como nem sempre é possível garantir esses requisitos na implementação de redes, as forças combatentes devem ser preparadas para situações em que a rede esteja degradada. Para isso, a preparação para a condução da guerra deve prever o uso de meios de comunicação substitutos aos usuais, assim como prever mecanismos de recuperação rápida (EUA, 2014, p. I1-I2), principalmente em guerras centradas em rede, as quais demandam informações em maior quantidade e de forma mais precisa (PAUL, 2008, p. 03).

Parte III

AGENDA DE PESQUISA

Apesar dos grandes avanços que o programa de pesquisa em ciberguerra apresentou nos últimos anos, é premente a sua evolução para uma abordagem mais pragmática. Um caminho possível é o desenvolvimento de análises que atrelem teoria e prática com metodologias diversas, de modo a dar conta da complexidade técnico-social do tema. Essa abordagem deve auxiliar na elaboração de generalizações condicionais/contingentes sobre o fenômeno, mesmo com o ritmo acelerado de mudança tecnológica das últimas décadas. (ERIKSSON; GIACOMELLO, 2007, p. 22-23).

Desse modo, a agenda de pesquisa a ser percorrida nos próximos anos deve avançar na análise de quatro grande perguntas relacionadas à ciberguerra: (1) qual o impacto do ciberespaço nas causas da guerra; (2) como o ciberespaço foi utilizado em conflitos militares contemporâneos; e (3) quais as capacidades cibernéticas instaladas nas principais potências mundiais; (4) como a apreensão em torno da ciberguerra afeta as políticas públicas para os setores de segurança e defesa nacionais. Abaixo, segue uma breve reflexão sobre cada ponto levantado.

Causas da guerra

Talvez uma das questões mais importantes que o ciberespaço traga, quanto à questão geográfica, esteja ligado à projeção de poder. Se após o fim da Guerra Fria há um processo de regionalização das relações internacionais, tanto pelo menor interesse da grande potência vencedora quanto pelas limitadas capacidades de projeção de poder da grande maioria dos países, a era digital altera, de certo modo, esse prognóstico. Além disso, pesquisas que argumentam que a proximidade territorial é uma das principais causas da guerra (Gartzke, 2011) levantam a questão de se a era digital aumenta a probabilidade de guerra interestatal entre países distantes geograficamente.[58] Espera-se que, caso a contiguidade territorial represente maior facilidade de projeção de poder ou maior interação social (e, logo, tensão), a era digital afete as causas da guerra, ainda que de modo mais ou menos intenso em cada uma

[58] Além da contiguidade territorial, Gartzke (2011) argumenta que capacidades e interesses tem influência sobre a guerra. Enquanto a primeira afeta onde o conflito acontece, a segunda afeta a probabilidade dele ocorrer.

delas. Apesar disso, ainda não é possível inferir que o ciberespaço tenha diminuído a contiguidade territorial como uma das principais causas dos conflitos contemporâneos.

Conduta da guerra

Uma das principais carências desse programa de pesquisa são as escassas análises históricas sobre o uso estratégico, operacional e tático do ciberespaço na guerra. Ainda que existam pesquisas relevantes sobre o assunto, poucas produções científicas tem realizado análises sistemáticas sobre como esse ambiente foi utilizado nas guerras contemporâneas. Um dos poucos trabalhos que supre essa deficiência é o desenvolvido por Deibert, Rohozinski e Crete-Nishihata (2012), o qual versa sobre a Guerra Russo-Georgina (2008). De modo geral, entretanto, o uso do ciberespaço em guerras convencionais ocorridas no pós-Guerra Fria pouco foram explorados pela literatura. O que se encontram são vários relatos esparsos do fenômeno sobre modificações, degradações e destruições de dados em guerras como a do Golfo, do Kosovo, do Iraque e do Afeganistão, para citar alguns.

Estudos de caso sobre essas guerras devem permitir uma melhor compreensão sobre como se dá a movimentação e manobra no ciberespaço dentro do campo de batalha. Do mesmo modo, esse tipo de abordagem deve auxiliar na obtenção de boas práticas para a proteção e manutenção de ativos estratégicos, gerando maior resiliência e segurança para redes militares críticas. Aliados à metodologia de *process tracing*, os estudos de caso também permitem desenvolver análises de trajetórias de mudança e causalidade em eventos cibernéticos, o que deve auxiliar no entendimento do impacto desse ambiente na condução e escalada de guerras na atualidade.

Capacidades cibernéticas

Outra carência da área são as precárias análises de conjuntura sobre os Estados e seu grau de preparação para ataques cibernéticos. Apesar do alarde feito em torno dos supostos arsenais cibernéticos possuídos por países como Rússia e China, poucas pesquisas se debruçaram sobre as configurações das redes domésticas desses países, assim como de seus ativos estratégicos nacionais. Com a identificação de como o ciberespaço pode ou não ser utilizado na guerra, os Estados podem se preparar para cenários mais realistas do que os apresentados por boa parte da literatura sobre o fenômeno, desenvolvendo politicas públicas

de defesa mais condizentes com seu entorno estratégico (ERIKSSON; GIACOMELLO, 2007, p. 181-182; MAHNKEN, 2011, p. 65?).

Políticas públicas para segurança e defesa

Nas últimas décadas, o debate acerca do uso do ciberespaço em situações de paz e guerra tem se refletido em um aumento da percepção de ameaça dos Estados quanto a esse meio. No entanto, se, por um lado, o processo de politização de eventos cibernéticos é bem vindo, dada a relevância deste ambiente para o fluxo de informações na era digital, por outro, o processo de securitização do fenômeno levanta problemas no âmbito doméstico e externo dos Estados (RUDZIT; NOGAMI, 2010). De fato, o processo de securitização do ciberespaço e, mais especificamente, da Internet, tem afetado as políticas públicas de segurança e defesa no Brasil. No caso brasileiro, os conceitos e práticas adotados pelo Estado nos últimos anos, tem como consequência a militarização de eventos que, de outra forma, seriam tratados como concernentes à esfera da segurança pública, gerando uma incompatibilidade entre as principais ameaças cibernéticas no Brasil e a políticas pública do Estado para o setor, visto que apesar do país ter como principais ameaças o cibercrime e o ciberativismo, os principais investimentos tem sido em soluções militares.

REFERÊNCIAS BIBLIOGRÁFICAS

ADEE, Sally. **The Hunt for the Kill Switch**. IEEE Spectrum, 1 maio 2008. Disponível em: <http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>. Acesso em: 14 mar. 2014.

ARQUILLA, John. From Blitzkrieg to Bitskrieg: the military encounter with computers. **Communications of the ACM**, v. 54, n. 10, p. 58-65, 2011.

ARQUILLA, John; RONFELDT, David. Cyberwar is Coming!. In: _____ (orgs.). **In Athena's Camp**: preparing for conflict in the information age. Santa Monica: RAND, 1997.

BARROS, Otávio; GOMES, Ulisses; FREITAS, Whitney (orgs.). **Desafios Estratégicos para Segurança e Defesa Cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

BETZ, David. The More You Know, The Less You Understand: the problem with information warfare. **Strategic Studies**, v. 29, n. 3, p. 505-533, 2006.

_____. Cyberpower in Strategic Affairs: neither unthinkable nor blessed. **Journal of Strategic Studies**, v. 35, n. 5, p. 689-711, 2012.

BETZ, David; STEVENS, Tim. **Cyberspace and the State**: towards a strategy for cyber-power. Nova Iorque: Routledge, 2011.

_____. Analogical Reasoning and Cyber Security. **Security Dialogue**, v. 44, n. 2, p. 147-164, 2013.

BIDDLE, Stephen. **Military Power**: Explaining Victory and Defeat in Modern Battle. Princeton: Princeton University Press, 2004.

BOOT, Max. The Struggle to Transform the Military. **Foreign Affairs**, v. 84, n. 2, 2005. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2005-03-01/struggle-transform-military>. Acesso em: 07 mar. 2014.

BORLAND, John. **Analysing the Internet Collapse**. 2008. Disponível em:<http://www.technologyreview.com/news/409491/analyzing-the-internet-collapse/>. Acesso em: 20 out. 2014.

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

BRITO, Jerry; WATKINS, Tale. Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. **Harvard National Security Journal**, v. 3, n. 1, p. 40-41, 2011.

BROWNE, J. P. R., THURBON, M. T.. **Eletronic Warfare**. Londres: Brassey's, 1998.

BYRES, Eric; LOWE, Justin. **The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems**. 2004. Disponível em: < http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf>. Acesso em: 17 mar. 2014.

BUZAN, Barry; WAEVER, Ole. **Regions and Powers**. Cambridge: Cambridge University Press, 2003.

CANABARRO, Diego; BORNE, Thiago. **The Fog of (Cyber)War**. 2013. Disponível em: < http://files.isanet.org/ConferenceArchive/55fca0e0b6494d23955495403fc75ed6.pdf>. Acesso em: 01 fev. 2014.

CANABARRO, Diego. **Governança Global da Internet**: tecnologia, poder e desenvolvimento. 2014. Tese (Doutorado em Ciência Política) – Instituto de Filosofia e Ciências Humanas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CARR, Jeffrey. The Misunderstood Acronym: why cyber weapons aren't WMD. **Bulletin of the Atomic Scientists**, v. 69, n. 5, p. 32-37, 2013.

CAVELTY, Myriam. Is Anything Ever New? – Exploring the Specificities of Security and Governance in the Information Age. In: CAVELTY, Myriam; MAUER, Victor; KRISHNA-HENSEL, Sai. **Power and Security in the Information Age**: investigating the role of the State in cyberspace. Hampshire: Ashgate Publishing, 2007, p. 19-44.

CEPIK, Marco ; CANABARRO, Diego ; BORNE, Thiago . Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica. In: SOUZA, André; NASSER, Reginaldo; MORAES, Rodrigo (Orgs.). **Do 11 de setembro de 2001 à guerra ao terror**: reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014, v. 1, p. 162-186.

_____. Cyberwar: Clausewitzian encounters. **Space & Defense**, v. 8, n. 1, p. 19-33, 2015.

CLARKE, Richard; KNAKE, Robert. **Cyber War**: the next threat to national security and what to do about it. Nova Iorque: HarperCollins Publishers, 2010.

CLAUSEWITZ, Carl von. **On war**. Nova York: Oxford University Press, 2007.

CHOO, Kim-Kwang. The Cyber Threat Landscape: challenges and future research directions. **Computers & Security**, v. 30, n. 8, p. 719-731, 2011.

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

DEIBERT, Ronald. **Black Code**: surveillance, privacy and the dark side of the Internet. Toronto: Signal, 2013.

DEIBERT, Ronald; ROHOZINSKI, Rafal; CRETE-NISHIHATA, Masashi. Cyclones in Cyberspace: information shaping and denial in the 2008 Russia-Georgia War. **Security Dialogue**, v. 43, n. 1, p. 3-24, 2012.

DENNING, Dorothy. Assessing the Computer Network Operations Threat of Foreign Countries. In: ARQUILLA, John; BORER, Douglas. **Information Strategy and Warfare**: a guide to theory and practice. New York: Routledge, 2007, p. 187-210.

ECHEVARRIA II, Antulio J. Clausewitz's Center of Gravity. **Naval War College Review**, v. 56, n. 1, 2003, p. 108 – 123.

_____. **Clausewitz and Contemporary War**. Oxford University Press, 2007.

ERIKSSON, Johan; GIACOMELLO, Giampiero (Orgs.). **International Relations and Security in the Digital Age**. Abingdon: Routledge, 2007.

ESTADOS UNIDOS DA AMÉRICA. **Joint Publication 3-12 - Cyberspace Operations**. 2013. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>. Acesso em: 01 mar. 2015.

_____. **Defense Science Board Task Force on High Performance Microchip Supply**. 2005. Disponível em: <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>. Acesso em: 15 ago. 2014.

FALLIERE, Nicolas; MURCHU, Liam; CHIEN, Eric. **W32.Stuxnet Dossier**. Cupertino, 2011. 68p.

FOUNTAIN, Jane. **Building the Virtual State**: information technology and institutional change. Washington: Brookings Institution Press, 2001.

FULLER, John. **The Reformation of War**. Londres: Hutchinson & Co., 1923. Disponível em: <https://archive.org/details/reformationofwar00fulluoft>. Acesso em: 29 mar. 2014.

GARTZKE, Erik. **Where Nations Fight**: capabilities, interests and contiguity in interstate disputes. 2011 Disponível em: < http://pages.ucsd.edu/~egartzke/papers/wherenationsfight_09232011.pdf>. Acesso em 19 set. 2014.

_____. The Myth of Cyberwar: bringing war in cyberspace back down to Earth. **International Security**, v. 38, n. 2, p. 41-73, 2013.

GARTZKE, Erik. LINDSAY, Jon. **Weaving Tangled Webs**: offense, defense, and deception in cyberspace. 2014 Disponível em: < http://www.jonrlindsay.com/research/papers/GartzkeLindsay2014_Deception.pdf>. Acesso em: 27 set. 2015.

GEERS, Kenneth. **Sun Tzu and Cyber War**. 2011. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf>. Acesso em: 23 abr. 2014.

GRAY, Colin. **Making Strategic Sense of Cyber Power**: why the sky is not falling. Carlisle: Strategic Studies Institute, 2013.

GREATHOUSE, Craig. Cyber War and Strategic Thought: do the classic theorists still matter? In: KREMER, Jan-Frederik; MÜLLER, Benedikt (orgs.) **Cyberspace and International Relations**: theory, prospects and challenges. Berlin: Springer, 2014, p. 21-40.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quartely**, v. 53, p. 1155-1175, 2009.

HAYDEN, Michael. The Future of Things Cyber. **Strategic Studies Quartely**, v. 5, n. 1, p. 3-7, 2011.

HEADRICK, Daniel; GRISET, Pascal. Submarine Telegraph Cable: Business and Politics, 1838-1939. **Business History Review**, v. 75, n. 03, p. 543-578, 2011.

HEALEY, Jason. Claiming the Lost Cyber Heritage. **Strategic Studies Quartely**, v. 6, n. 3, p. 11-19, 2012.

HYAKIN, Simon; MOHER, Michael. **Introdução aos Sistema de Comunicação**. Porto Alegre: Bookman, 2008.

HOLLIS, David. Cyberwar Case Study: Georgia 2008. **Small Wars Journal**. Disponível em: <http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>. Acesso em: 29 abr. 2014.

ISO/IEC. **Information Technology – Open Systems Interconnection – Basic Reference Model**: The basic model. Genebra: ISO/IEC, 1994.

JACCARD, James; JACOBY, Jacob. **Theory Construction and Model-Building Skills**: a practical guide for social scientists. Nova Iorque: The Guilford Press, 2009.

JULIO, Timothy. How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate. **Journal of Strategic Studies**, v. 36, n. 1, p. 125-133, 2013.

KELLO, Lucas. The Meaning of the Cyber Revolution. **International Security**, v. 38, n. 2, p. 7-40, 2013.

KUEHL, Daniel. From Cyberspace to Cyberpower: defining the problem. In: KRAMER, Franklin; STUART, Starr; WENTZ, Larry. **Cyberpower and National Security**. Duller: National Defense University Press, 2009, p. 24 – 42.

KURBALIJA, Jovan; GELBSTEIN, Eduardo. **Gobernanza de Internet**: assuntos, actores y brechas. Genebra: Diplo Foundation, 2005.

KUROSE, James; ROSS, Keith. **Computer Networking**: a top-down approach. Nova Jersey: Pearson, 2013.

LAWSON, Sean. **Beyond Cyber-Doom**: cyberattack scenarios and the evidence of history. Mercatus Center Working Paper n. 10-77. 2011. Disponível em: <http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history.pdf>. Acesso em: 01jul. 2014.

LINDSAY, Jon. Stuxnet and the Limits of Cyber Warfare. **Security Studies**, v. 22, n. 3, p. 365-404, 2013a.

_____. Proxy Wars: control problems in irregular warfare and cyber operations. Disponível em: <http://files.isanet.org/ConferenceArchive/1a381131aa014f02ab15a7b55b8509d7.pdf>. Acesso em: 14 ago. 2014.

LYNN III, William. Defending a New Domain: the Pentagon's Cyberstrategy. **Foreign Affairs**, 2010. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. Acesso em: 15 jun. 2014.

LOCATELLI, Andrea. **The Offense/Defense Balance in Cyberspace.** 2013. Disponível em: < http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_203_2013.pdf>. Acesso em 04 ago. 2014.

LONDSDALE, David. Clausewitz and Information Warfare. In: STRACHAN, Hew; HERBER-ROTHE, Andreas (orgs.). **Clausewitz in the Twenty-First Century**. Nova Iorque: Oxford University Press, 2007, p. 231-250.

MACASKILL, E. et al. **GCHQ taps fibre-optic cables for secret access to world's communications**. 2013. Disponível em: <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Acesso em: 27 jun. 2014.

MACHADO, Felipe. **Estratégia Nacional de Desenvolvimento das Atividades Espaciais do Brasil**: justificativas, requisitos e componentes. 2014. Dissertação (Mestrado em Ciência Política) – Instituto de Filosofia e Ciência Humanas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

MAHNKEN, Thomas. Cyberwar and Cyber Warfare. In: KRISTIN, Lord; SHARP, Travis (Org.). **America's Cyber Future**: security and prosperity in the information age. Washington: Center For a New American Security, 2011. Volume II, p. 55-64.

MARKOFF, John. **Old Trick Threatens the Newest Weapons**. 2009. Disponível em: <http://www.nytimes.com/2009/10/27/science/27trojan.html>. Acesso em: 24 mar. 2014.

MCGRAW, Gary. Cyber War is Inevitable (Unless we Build Security in). **Journal of Strategic Studies**, v. 36, n. 1, p. 109-119, 2013.

MCGRAW, Gary; FICK, Nathaniel. Separating Threat from the Hype. In: KRISTIN, Lord; SHARP, Travis (Org.). **America's Cyber Future**: security and prosperity in the information age. Washington: Center For a New American Security, 2011. Volume II, p. 41-53.

NYE, Joseph. From Bombs to Bytes. **Bulletin of the Atomic Scientists**, v. 69, n. 5, p. 8-14, 2013.

PAPE, Robert. **Bombing to Win**: air power and coercion in war. Ithaca: Cornell University Press, 1996.

PAUL, Christopher. **Information Operations**: Doctrine and Practice. Westport: Praeger Security International, 2008.

PERERA, David. **Netcentric in a Snap**. 2006. Disponível em: <http://www.govexec.com/magazine/features/2006/06/netcentric-in-a-snap/22006/>. Acesso em: 25 ago. 2014.

PETERSON, Dale. Offensive Cyber Weapons: construction, development, and employment. **Strategic Studies**, v. 36, n. 1, p. 120-124, 2013.

PIMENTA, Marcelo; CANABARRO, Diego (orgs.). **Governança Digital**. Porto Alegre: Editora da UFRGS, 2014.

POISEL, Richard. **Introduction to Communication Eletronic Warfare Systems**. Norwood: Artech House, 2008.

RFC #1945. Hypertext Transfer Protocol -- HTTP/1.0. 1996. Disponível em: <http://tools.ietf.org/html/rfc1945>. Acesso em: 01 dez. 2014.

RFC #2616. Hypertext Transfer Protocol -- HTTP/1.1. 1999. Disponível em: <http://tools.ietf.org/html/rfc2616>. Acesso em: 01 dez. 2014.

RID, Thomas. **Cyber War Will not Take Place**. Nova Iorque: Oxford University Press, 2013a.

_____. More Attacks, Less Violence. **Strategic Studies**, v. 36, n. 1, p. 139-142, 2013b.

_____. Cyberwar and Peace. **Foreign Affairs**, v. 92, n. 6, p. 77-87, 2013c.

RUDZIT, Gunther; NOGAMI, Otto. Segurança e Defesa Nacionais: conceitos básicos para uma análise. **Revista Brasileira de Política Internacional**, v. 53, n. 1, p. 5-24, 2010.

SASSINE, Vinicius. Exército Monitorou Líderes de Atos pelas Redes Sociais. **O Globo**, 16 jul. 2013. Disponível em: <http://oglobo.globo.com/brasil/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915>. Acesso em: 04 mar. 2014.

SHACHTMAN, Noah; AXE, David. **Winning – and Losing – the First Wired War**. 2006. Disponível em: <http://www.popsci.com/scitech/article/2006-06/winning-and-losing-first-wired-war>. Acesso em 15 abr. 2014.

SHACHTMAN, Noah; SINGER, Peter. **The Wrong War**: the insistence on applying Cold War metaphors to cybersecurity is misplaced and counterproductive. 2011. Disponível em:

<http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman>. Acesso em: 13 mar. 2014.

SILVA, Otávio da. A Segurança e as Ameaças Cibernéticas: uma Visão Holítica. In: BARROS, Otávio; GOMES, Ulisses (Org.). **Desafios Estratégicos para Segurança e Defesa Cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011, p. 129-144.

STAPLETON-GRAY, Ross; WOODCOCK, Bill. National Internet Defense – Small States on the Skirmish Line. **Communications of the ACM**, v. 54, n. 3, p. 50-55, 2011.

STONE, John. Cyber War Will Take Place!. **Journal of Strategic Studies**, v. 36, n. 1, p. 101-108, 2013.

STRACHAN, Hew. **The Changing Character of War.** Oxford: Europaeum, 2007.

STRACHAN, Hew; HERBER-ROTHE, Andreas (orgs.). **Clausewitz in the Twenty-First Century**. Nova Iorque: Oxford University Press, 2007.

TANEMBAUM, Andrew; WETHERALL, David. **Computer Networks**. Boston: Prentice Hall, 2011.

WAXMAN, Matthew. Cyber-Attacks and the Use of Force. **The Yale Journal of International Law**, v. 36, n. 421, p. 421-459, 2011.

WINNER, Langdon. **The Whale and the Reactor**: a search for limits in an age of high technology. Chicago: University of Chicago Press, 1989.

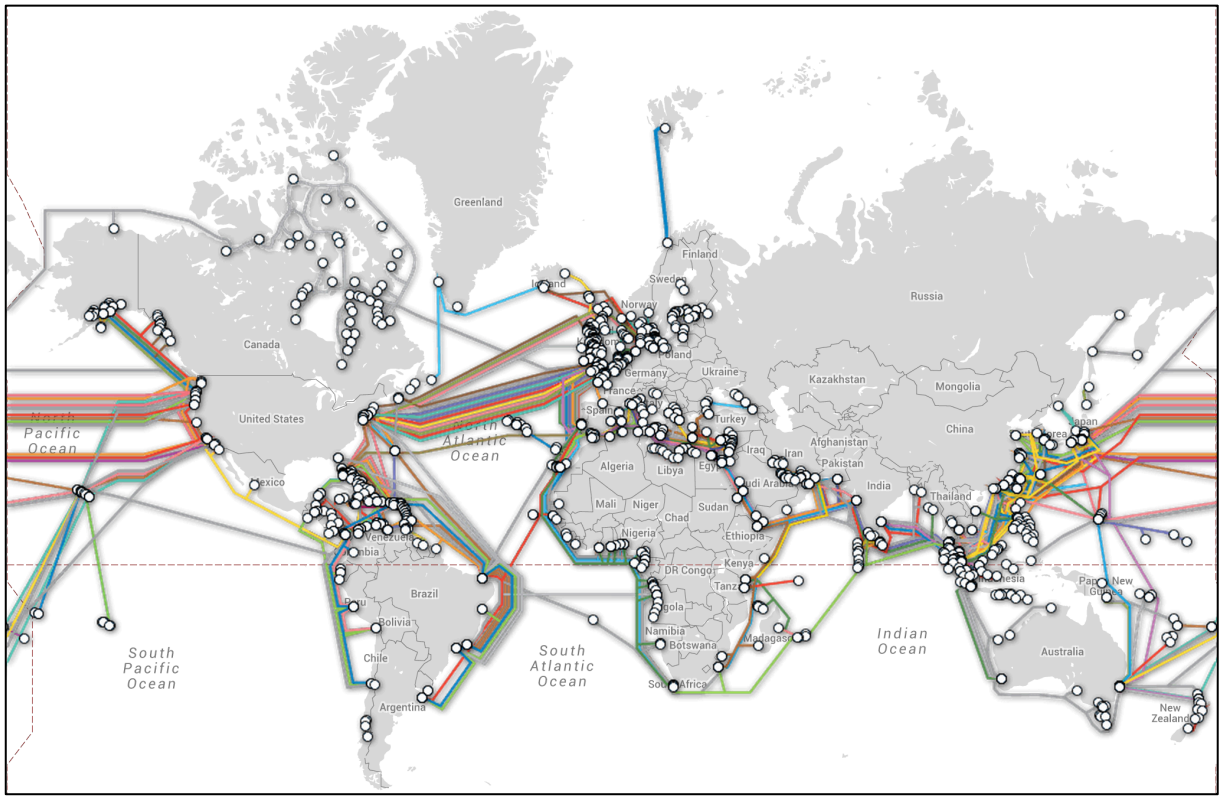
WINKLER, Jonathan. **Nexus**: Strategic Communications and American Security in World War I. Cambridge: Harvard University Press, 2008.

YOO, Christopher. **Protocol Layering and Internet Policy**. 2013. Disponível em: < http://ssrn.com/abstract=2278451>. Acesso em: 24 maio 2014.

ZUCCARO, Paulo. Tendência Global em Segurança e Defesa Cibernética. In: BARROS; GOMES; FREITAS. **Desafios Estratégicos para Segurança e Defesa Cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011, p. 49-78.

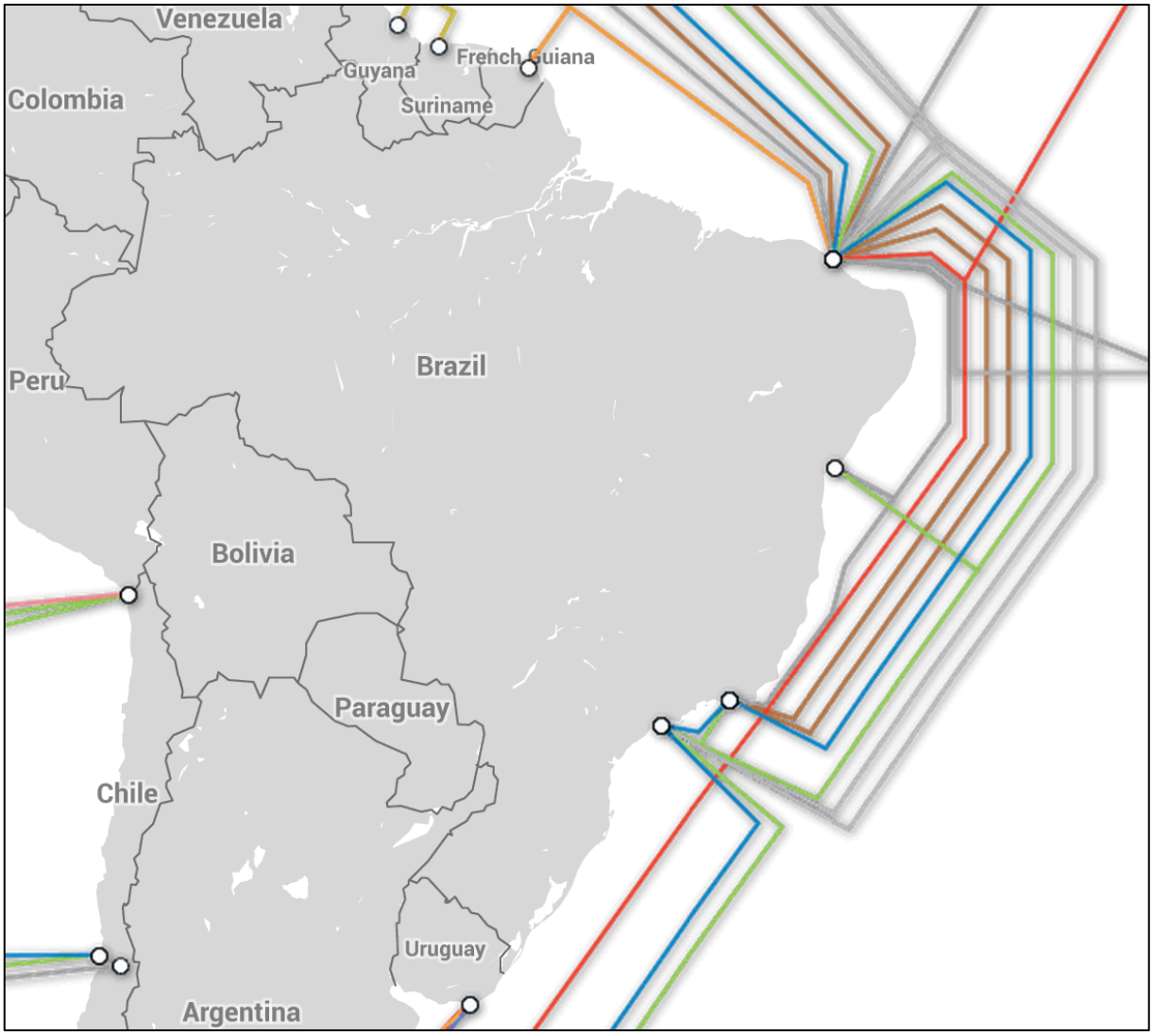
ANEXOS

Anexo 1: Mapa de cabos submarinos no mundo



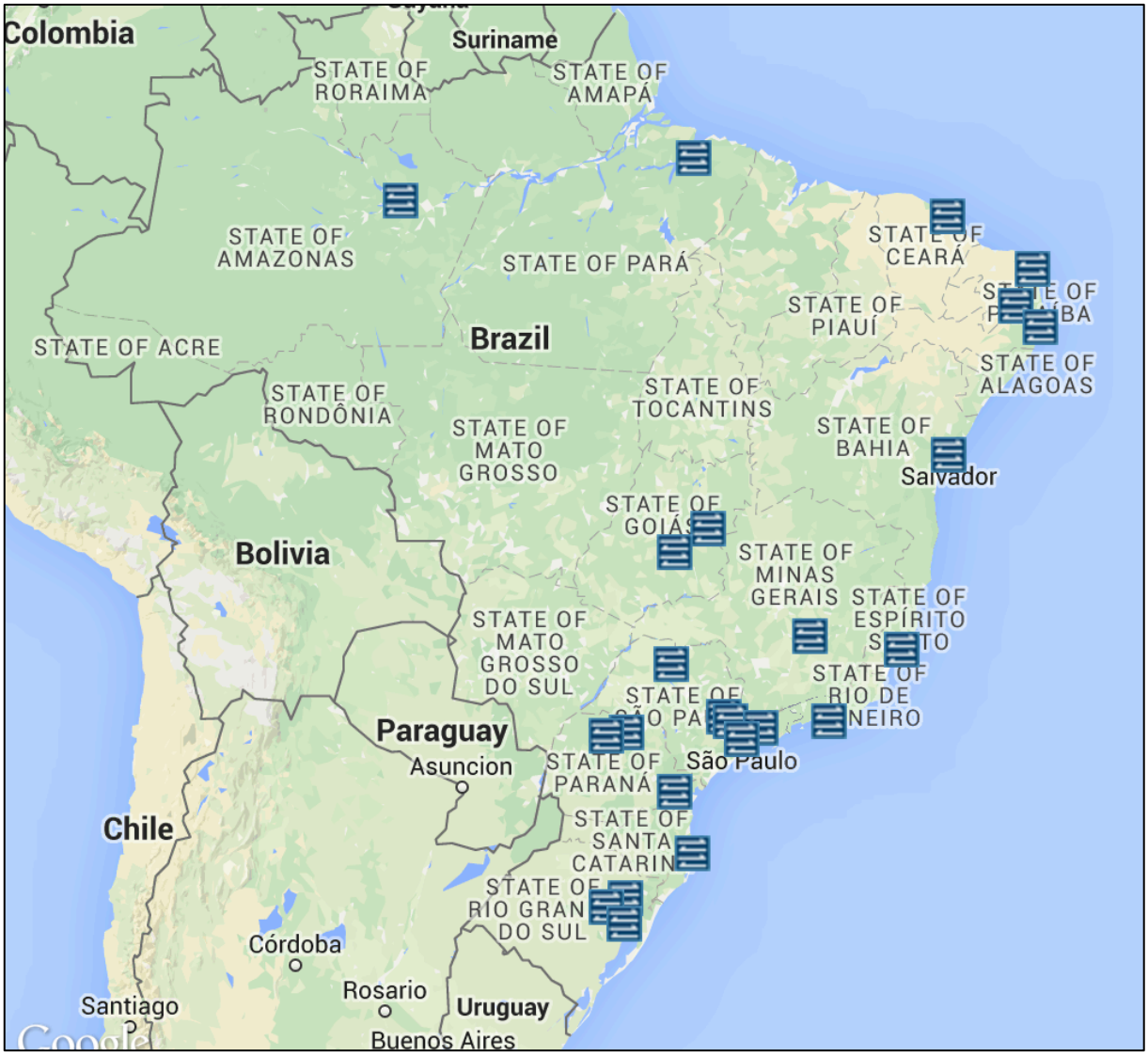
Disponível em: http://www.submarinecablemap.com/. Acesso em: 01 jun. 2015.

Anexo 2: Mapas de cabos submarinos que chegam ao Brasil



Disponível em: http://www.submarinecablemap.com/. Acesso em: 01 jun. 2015.

Anexo 3: Mapa de PTTs no Brasil



Disponível em: http://ix.br/localidades/atuais. Acesso em: 01 jun. 2015.