IX ENCONTRO DA ABCP

Área – Política Internacional

NOTAS ANALÍTICAS SOBRE O CONCEITO DE DISSUASÃO APLICADO AO FENÔMENO DA CIBERSEGURANÇA

Cauê Pimentel

DCP-USP

Brasília, DF
04 a 07 de agosto de 2014

Notas analíticas sobre os conceito dissuasão aplicado ao fenômeno da cibersegurança

Cauê Pimentel – DCP-USP

Resumo do trabalho:A cibersegurança é um tema crescente no pensamento estratégico e crítico sobre segurança internacional. A velocidade acelerada das transformações tecnológicas torna a cibersegurança um objeto de difícil apreciação teórica já que suas características peculiares desafiam definições tradicionais que compõem o campo intelectual da segurança (território, fronteira, ameaça, risco e a própria definição de guerra). Este trabalho tem como objetivo retomar o tema clássico dos Estudos de Segurança Internacional (ESI) e aplicá-lo sobre o problema da cibersegurança: *dissuasão* e *dinâmica armamentista*. A dissuasão é fundamental para todo o pensamento estratégico em torno da guerra e da paz. Cabe explorar as possibilidades de aplicação deste conceito ao contexto contemporâneo da cibersegurança, problematizando como a inclusão de elementos da era da informação podem remediar ou agravar o dilema de segurança e a eficácia da dissuasão. O problema da cibersegurança será analisado sob seu viés político, ponderando as consequências que uma corrida por capacidades tecnológicas podem ocasionar para a estrutura do ciberespaço e da configuração da política internacional na encruzilhada entre ciência, prática, segurança e espaço público.

Palavras-chave: Cibersegurança; Dissuasão; Segurança Internacional;

Introdução

> *The simple fact that technological progress is leading in so many instances straight into disaster […] has reached a stage where there's no damn thing you can do that can't turn into war*[1].

A cibersegurança, tema recente no campo dos Estudos sobre Segurança Internacional (ESI), despertou signficativo debate acerca das possibilidades e ameaças que conflagra. O conceito de cibersegurança emerge no final dos anos 1980 e junto com ele emerge uma forte retórica sobre a ideia de "ciberguerra" (HANSEN; NISSEMBAUM, 2009; ARQUILLA, RONDFELD, 1989). Para além da discussão acadêmica ou puramente conceitual, a pauta da cibersegurança está presente nas estratégias nacionais de defesa e no orçamento dos principais *players* globais: mais de 40 países possuíam doutrinas, políticas ou organizações militaresdevotadas a cibersegurança em 2009[2] (UNIDIR, 2009).

Sob que ótica devemos mirar o complexo fenômeno destas novas tecnologias da Era da Informação? A cibersegurança têm atraído grande atenção da academia sob diversas abordagens, o que resulta em uma bibliografia heterogênea e de densidade dispersa. De maneira geral, todavia, podemos estabelecer duas grandes tendências ou programas de pesquisa sobre a temática. Por um lado, análises que observam o advento das tecnologias da informação a partir da lógica do poder e do conflito iminente, abordando o problema pela lógica da ciberguerra ou ciberpoder, leituras predominantes no mundo anglo-saxão, principalmente nos EUA, onde as novas tecnologias estão diretamente associadas à ideia de hegemonia e segurança nacional norte-americana. Do outro lado, abordagens diversificadas que se debruçam sobre o tema a partir de uma aproximação crítica preocupada com os efeitos negativos da cibersegurança sobre os conceitos de guerra, conflito, segurança, privacidade, democracia e soberania.

Para a discussão que se segue, defineremos provisioramente o problema da cibersegurança como a (in)segurança produzida pelas novas tecnologias da informação, referindo-se tanto aos problemas de natureza técnica (pautados pela engenharia e pela ciência da computação) como pelos problemas de natureza política (sobretudo, as relações de poder, os desafios estratégicos e os dilemas ético-políticos engendrados pela tecnologia). A cibersegurança se torna um objeto especial de estudo por suas

---

[1] Jerome Lettvin, 1969 in: ARENDT, H. New York: Harcourt. On Violence. P.16.

[2] África do Sul, Albânia, Alemanha, Argentina, Austrália, Áustria, Bielorússia, Brasil, Canadá, Cazaquistão, China, Cingapura, Colômbia, Croácia, Cuba, Coréia do Norte, Coréia do Sul, Dinamarca, Eslováquia, Espanha, Estados Unidos, Estônia, Fiji, Finlândia, França, Georgia, Grécia, Holanda, Hungria, Índia, Indonésia, Irã, Israel, Itália, Japão, Lituânia, Malásia, Mianmar, Noruega, Polônia, Rússia, Sri Lanka, Suíça, Turquia, Ucrânia, Reino Unido e Vietnã.

características inovadoras que distinguem o ciberespaço dos dominíos tradicionais do penamento estratégico[3], especialmente devido a sua virtualidade transfronteiriça. A sua associação ao campo da segurança internacional é resultado da crescente convergência digital e ubiquidade onipresente das redes digitais (Uma leitura deste ambiente pela ótica militar leva a uma problematização do ciberespaço para os assuntos tradicionais dos ESI (CAVELTY, 2007; CEPIK; CANABARRO; BORNE, 2014; GRAY, 2013).

O objetivo deste breve *paper* é discutir de maneira introdutória dois conceitos fundamentais dos ESI frente ao fenômeno da cibersegurança: *dissuasão* e *dinâmica armamentista.* Este exercício conceitual é uma aproximação ao fenômeno a partir do arcabouço intelectual da segurança internacional forjado e consolidado durante o século XX.Visamos averiguar se e como estes conceitos basilares podem contribuir para o entendimento do fenômeno. Podemos falar de dissuassão no campo cibernético? Como a cibersegurança incrementa ou prejudica os instrumentos dissuasórios já existentes? Podemos identificar uma corrida armamentista por "cibercapacidades"? Por se tratar de um texto introdutório, lidaremos majoritariamente com perguntas mais do que com respostas.

Dissuasão, dinâmica armamentistae cibersegurança

A cibersegurança coloca a informação como uma importante fonte de poder na contemporaneidade. Parte integrante do conceito de *Guerra de 4º Geração*, o ciberespaçoganha fôlego na agenda internacional ao se transformar em um importante vetor para fins políticos e estratégicos de atores estatais e não-estatais. A partir de 2001, a cibersegurança se torna um objeto central dos debates estratégicos em consequência da "guerra global contra o terror" (GGcT) propagada por Washington e que potencializou o ciberespaço como um vetor de ameaça terrorista e de importância estratégica[4](CEPIK; CANABARRO; BORNE, 2014; BUZAN, HANSEN; 2012).

[3] Complementa Cepik (2001, p.255) , sobre a*Information Warfare* (IW): "o conceito de IW resulta da tentative de integração e expansão das operações de guerra eletrônica, guerra de comando e controle (C2 *warfare*) e disciplinas defensivas em inteligência. [...] A guerra informacional compreende o conjunto de ações ofensivas e defensivas conduzidas no ambiente informacional para controlar o ões ofensivas e defensivas conduzidas no ambiente informacional para controlar o cyberspace. Ciberespaço é aqui entendido como o 'lugar' onde interagem computadores, programas, sistemas de comunicação e equipamentos que operam via irradiação de energia no espectro eletromagnético. Porém, menos por um 'lugar' ou um conjunto classificável de ações, a guerra informacional define-se melhor por seus objetivos: obter e manter superioridade informacional na batalha ou na guerra".

[4] Buzan e Hansen (2010, p.373) ressaltam que a importância do ciberespaço como objeto estratégico antecedia a GGcT como evidencia a importância que o Governo Clinton havia dado à matéria, principalmente através do documento basilar *Critical Foundations: Protecting America's Infrastructures*. A GGcT, no entanto, elevou o tema a um nível mais abrangente e mais complexo.

A conceitualização das distintas gerações da guerra está ligada ao amplo debate das Revoluções nos Assuntos Miltares (RMA's). Neste escopo, são discutidas as transformações tecnológicas e estratégicas que moldam a condução da guerra: A 1º geração seria caracterizada pela formação das tropas em linhas e colunas no campo de batalha, somada à conscrição das massas preconizada pela Revolução Francesa, consagrando o princípio da multiplicação da massa por velocidade e durando até meados do século XIX. . A 2º geração foi resultado do desenvolvimento de armamentos leves como os rifles de repetiçãoe pelo uso ampliado da artilharia como fogo indireto, tendo as guerras de unificação alemã e a I Guerra Mundial como exemplos mais enfáticos. A 3º geração tem início na I GM – demonstrando o *overlap* entre as diferentes gerações – e é marcada pelo desenvolvimento tático da guerra de manobra e da blitzkrieg, cuja principal transformação tática-estratégica é a substituição da guerra de atrito pela guerra não-linear, predominante desde a II Guerra Mundial. A 4º geração é a transformação mais significativa desde Westphalia, pois involve a presença decisiva de atores não-estatais e pela utilização intensiva de novas tecnologias que se caracterizam pelo grande poder de fogo, pela dispersão de missões em pequenos grupos concentrados e pela utilização de tecnologias da informação e de veículos não-tripulados (LIDELL-HART, 1982; LIND et al, 1989; DUARTE, 2012).

As tecnologias da informação estão intimamente relacionadas ao pensamento sobre a G4G, principalmente devido a sua definição como o "sistema dos sistemas", integrando diversas interfaces de uso militar e civil (DUARTE, 2012, p.37).Assim, a Era da Informação impulsiona mutações importantes que aceleram, agudizam ou modifica características então dominantes na Era Industrial, resultando em alterações táticas, estratégicas, organizacionais e subjetivas sobre o entendimento da guerra e da segurança. O quadro abaixo ilustra algumas destas mudanças significativas que alteram o entendimento sobre segurança internacional contemporânea:

Figura 1 – Mutações na Guerra e Estratégia.

Era Industrial	Era da Informação
Organização social	
Produção em massa, conscrição em massa, destruição em massa.	Fragmentação da produção, altamente especializada, acesso barato a tecnologias.
Política internacional entre unidades semelhantes (Estados)	Presença marcante de atores não-estatais.
Tecnologias dominantes	
Hardware	*Software*
Petróleo, gasolina e diesel	Eletricidade
Grandes máquinas	Pequenos dispositivos
Standardização	Diversificação

Quantidade e concretude	Qualidade e abstração
Percepção de eventos e armas como "reais"	Borramento do real e ficcional (percepção subjetivada)
Modelos organizacionais	
Coleta de informação seletiva e pequenas quantidades[5]	Coleta de informação indiscriminada e em larga escala*
Adaptabilidade fácil entre funções/ tarefas civis e militares	Pessoal altamente especializado e com conhecimentos específicos
Controle humano/mecânica	Controle automâto/robótica/digital
Modelos táticos/estratégicos	
Controle do território	Velocidade de ação e reação
Máximo de letalidade, grande número de baixas	Letalidade miníma/não-letal, redução (e aversão) ao número de baixas.
Guerra total	Guerra especializada e limitada
Guerra mecânica	Guerra Digital
Força física	Conhecimento
Atrito, desgaste, ocupação	Alta Precisão e Distância
Destruição de capacidades materiais (*Hard kill)*	Incapacitação de capacidades e vontades sem necessidade de destruição física *(soft kill)*
Pólvora, explosivos, ogivas nucleares	Cibernética, robótica, alta-precisão

FONTE: BUZAN; HERRING, 1998 (p.24) (adaptado).

O entendimento deficitário sobre a aplicação estratégica e tática destas tecnologiasproblematiza o debate sobre cibersegurança dos elementos tradicionais que formam as vigas de sustentaçãoda segurança internacional. Por esta razão, este artigo busca explorar a utilidade e viabilidade de um termo clássico dos ESI, a dissuasão, aplicado ao problema da cibersegurança.Existe uma biblografia crescente sobre este eixo analítico e cujo principal esforço é relacionar o clássico e o novo em busca de definições e conceitos que possam a proximar o mundo da cibersegurança das preocupações políticas e estratégicas da segurança internacional. Parte desta bibliografia tem se focado nas possibilidades de se replicar mecanismos de segurança tradicionais como dissuasão para o controle das ameaças no ciberespaço (KAMINSKI, 2010; NAGORSKI, 2010; LIBICKI, 2009, GOODMAN, 2009; SINGER; FRIEDMAN, 2014a).

Uma definição clássica de dissuasão pode ser encontrada em Aron (2002 p.509):dissuasão é um *mecanismo social* que pode ser reduzido conceitualmente ao "temor das *conseqüências* possíveis, das *punições* previstas ou da execução de uma *ameaça".* Em outras palavras, a dissuasão funciona como um mecanismo social básico entendido como a

[5] No original apresentado por Buzan e Herring, há uma inversão destas categorias. A Era Industrial seria caracterizada por coleta de vastas quantidades de informação ("*Indiscriminate gathering of vast amounts of information*") enquanto a Era da Informação se focaria em coleta específica ("*Specialized gathering of small amounts of information"*). Propomos aqui a inversão destas características, principalmente devido á emergência de tecnologias de *big data* e *metadata* que capturam quantidades massivas e indiscriminada de informações de usuários de sistemas eletrônicos.

a habilidade de *alterar o comportamento* dos agentes ao impor-lhes um custo significativo para agir. A dissuasão é, portanto, um mecanismo material e subjetivo capaz de moldar o comportamento dos atores. Dois elementos básicos sustentam o princípio da dissuasão: *retaliação* e *negação* ("*denial*"). A *retaliação* é o elemento direto que prevê uma punição frente a uma agressão. Já a *negação* é a resistência pela força a ataques vindos de outrem. Juntas, essas duas componentes conformam a ideia básica da dissuasão cuja essência se resume ameaças militares que visam impedir um outro ator de agir pela força, ou seja, deter ações indesejadas antes de que elas ocorram.

A dissuasãofunciona de acordo com um sistema de custos para o uso da força. Podemos sistematizar, resumidamente, oito eixos que serviriam para mensurar os custos de ação para os atores(BUZAN, HERRING; 1998, p.135):

1. Custos materiais para construir e manter os instrumentos do uso da força
2. Custos de operação (logística) do uso da força.
3. Custos das perdas das forças armadas decorrente do uso da força
4. Custos da destruição de propriedade civil e não-militar decorrente do uso da força (dano colateral)
5. Custos de oportunidade para a economia nacional
6. Custos ambientais decorrentes da construção, teste e uso dos armamentos
7. Custos politicos e morais da coerção
8. Custos humanos e sociais da violência

O modelo acima foi desenhado para se pensar o uso tradicional da força militar, principalmente a partir do equilíbrio nuclear. Transpor este modelo para o caso cibernético implica na necessidade correções e na existência de imperfeições. Isto não impede que o modelo seja uma referência importante que lança considerações incisivas sobre o problema da cibersegurança, já que alguns dos elementos das novas tecnologias buscam reduzir significativamente os custos de ação. Os critérios 1, 2, 3, 5 e 8, por exemplo, são drasticamente menores em operações no espaço cibernético do que em um cenário de conflito tradicional, nuclear ou não, enquanto os critérios 4 e 7 são de difícil apreciação devido à recente e complexa evolução do tema, mas certamente são importantes tópicos de pesquisa e discussão. A possibilidade de que a cibersegurança cause interrupção ou danos à infra-estrutura física em larga escala torna difícil precisar quais seriam as potencialidades e os efeitos colaterais de um ataque deste tipo. Por outro lado, é difícil prever qual seria a reação das audiências frente a um ataque cibernético. Este segundo ponto é particularmente interessante para pensar a eficácia destas tecnologias para alcançar objetivos militares ou de política de segurança, tal como exemplifica o caso norte-americano

em que os amplos programas de coleta de dados e vigilância digital causaram um severo revés e constrangimento para a política externa de Washington. Outras perspectivas levam a diferentes reflexões, tal como a possibilidade de no futuro operações cibernéticas servirem para inutilizarem sistemas de defesa e comunicação - como no ataque da Rússia sobre a Georgia em 2008[6] - ou de funcionarem como operações preemptivas - como no caso *Stuxnet*[7] -, o que tornaria o quadro estratégico muito mais complexo.

O arcabouço clássico da dissuasão funciona quando se pode detectar facilmente de *onde* e de *quem* parte determinado ataque/ameaça. Neste ponto, identificamos o primeiro problema crucial na utilização da dissuasão aplicada ao ciberespaço. No campo da cibersegurança, identificar a fonte dos ataques é um dos problemas cruciais que prejudicam a estruturação de um pensamento consistente sobre *ciberdissuasão*. O problema da *atribuição* dos ataques dificulta a identificação da origem dos ataques e portanto invalidaria a *retaliação.*Ainda que não seja completamente impossível identificar a origem de um ataque - como no caso dos ataques partindo da Rússiaque derrubaram parte das redes de comunicação daEstônia -, a tecnologia atual não possibilita uma identificação 100% precisa e, mais crucial, com um tempo de resposta rápido. Podemos desmembrar este problema em quatro vetores: *atribuição* (quem ataca quem); *localização* (o local de onde parte o ataque), *resposta* (ou capacidades de resposta mesmo depois de ser alvo de um *first-strike*) e *transparência* (a percepção do inimigo de que seu alvo possui capacidades para revidar).Devido as características das novas tecnologias, há uma grande dificuldade de tornar estes quatro vetores realizáveis de modo a serem efetivamente incorporados no ambiente tático-estratégico em função da anonimidade das redes, seu alcance global e

---

[6] Durante o breve conflito entre os dois países, diversos *websites* do governo georgiano foram derrubados, além do registro de supostas interferências nos sistemas de comunicação das forças armadas. Os ataques foram atribuídos ao governo russo, porém sem confirmação definida. No primeiro caso, as páginas da *internet* sofreram com ataques DDOS, enquanto a interferência no sistema de comunicação provavelmente ocorreu pela exploração de uma deficiência de segurança nestes sistemas que haviam sido importados previamente da Rússia (HOLLIS, 2008; MILITARY BALANCE, 2014).

[7] *Stuxnet* é o nome de um *malware* de grande complexidade que foi utilizado para paralisar o programa nuclear iraniano, mais precisamente as instalações de enriquecimento de urânio em Natanz. Devido à complexidade do código e seu *design* específico para atacar instalações industriais – o vírus atacava especificamente um modelo de centrigugas utilizadas pelo governo iraniano -, há fortes indícios de envolvimento estatal em sua elaboração e propagação, porém não há dados definitivos capazes de confirmar esta afirmação ou de identificar sua origem com 100% de certeza (o que remonta ao problema da *atribuição*). Alguns pontos merecem destaque: primeiro, o fato de que um tipo de ataque deste tipo acaba se espalhando para além do alvo designado (60% dos computadores infectados estavam localizados no Irã, provavelmente o *primary-target* de tal ação, mas outros países foram afetados (Indonésia - 18%; Índia – 8%; outros países 14%). Uma versão mais antiga do mesmo vírus - *Stuxnet 0.5* - teria se espalhado inclusive nos EUA (21% do total de computadores infectados), supostamete o patrocinador da criação do *Stuxnet*. Segundo, é preciso relativizar a eficácia deste tipo de ataque: dados disponíveis sugerem que houve uma redução significativa no enriquecimento de urânio pelo Irã, porém não é possível atribuir esta queda ao sucesso do ataque ou a algum outro evento explicativo (Disponível em: <http://goo.gl/IL7VsB> e < http://goo.gl/ORsZbY>. Acesso 23 Mar. 2014).

difuso, além de sua penetração em diversas áreas de uso civil (CAVELTY, 2007;NAGORSKI, 2010).Mais do que a somente a localização da origem dos ataques, há uma dificuldade e pouco entendimento em como relacionar o *contexto* destes ataques a uma perspectiva ampliada da estratégia devido à posibilidade de que ataques de atores não-estatais partam de um determinado país que não seja necessariamente beligerante ou belicoso, criando, portanto, uma dificuldade adicional para a eficácia da retaliação[8]. Esta possibilidade de anonimato favorece principalmente atores não-estatais em busca de vantagens assimétricas, mas também Estados que podem manter um alto nível de hostilidade contra um adversário sem se comprometer com um confrontamento direto, como indica ser o caso Rússia, Irã e China contra os Estados Unidos e vice-versa. (CEPIK; CANABARRO; BORNE, 2014; SINGER, FRIEDMAN; 2014).Outra contradição fundamental que torna o entendimento das novas tecnologias ainda mais complexo é a ênfase na redução no número de baixas, o oitavo elemento da escala de Buzan e Herring, sendo plausível a perspectiva de perdas zero no caso da cibersegurança. Teoricamente, dissuasão sem perdas humanas seria um mecanismo desprovido de sua essência, o que prejudicaria a racionalidade e aplicabilidade do conceito, favorecendo uma inclinação ao ataque e a atitudes belicosas. A dissuasão nuclear funcionava, em linhas gerais, pois seus resultados catastróficos levavam a um imobilismo de ambas as partes. Quando se remove o elemento humano e se transporta a guerra para o espaço virtual, a dissuasão perderia força e deixaria de ser o nó górdio que impediria os atores de um movimento ofensivo.Quando não há imposição de custos a quem ataca - efeito derivado do problema da *atribuição* -, haveria incentivos suficientes para atacar primeiro e se antecipar ao inimigo. A ausência de baixas somada ao anonimato e ao baixo custo de açãoexplica a grande quantidade diária de tentativas de ataques e fraudes cibernéticas no mundo todo, aindaque a maioria deles esbarrem em sistemas de proteção simples ou não causem dano significativo. Seguindo esta mesma lógica de baixos custos, porém em um plano estratégico ampliado, há uma considerável propensão para que Estados invistam mais em capacidades ofensivas do que

[8]Ainda sobre o caso da Estônia, mesmo que haja evidências consistentes de que os ataques partiram da Rússia, não é possível determinar se os ataques foram coordenados pelo Kremlin ou se partiram de outros agentes não-estatais situados em território russo. Singer e Friedman (2014a) salientam que os EUA tem utilizado diferentes estratégias para contra-atacar ameaças cibernéticas vindas de grupos terroristas, estados-pária e grandes potências. Os autores argumentam, hipoteticamente de acordo com as diretrizes estratégicas norte-americanas, que o tratamento do incidente na Estônia seria sensivelmente diferente caso a origem dos ataques fosse retraçada para outros Estados, tais como Irã ou Coréia do Norte. Esta postura corrobora o argumento de que a cibersegurança deve estar a serviço de objetivos políticos e estratégicos muito mais amplos. Nesta linha, é de importante o destaque da postura norte-americana em relação à ciberespionagem chinesa de companhias estadunidenses para o suposto roubo de informações confidenciais. Ao invés de contra-atacar tais investidas com respostas equivalentes, os EUA decidiu indiciar formamelmente cinco militares chineses, gerando um impasse entre a chancelaria das duas potências (HARRIS, 2014).

defensivas, como no caso dos EUA onde o investimento se concentra fortemente no primeiro setor[9]. Em um plano comparativo, esta propensão ao ataque em detrimento da defesa é semelhante ao pensamento militar tático do final do século XIX e início do XX em que o paradigma da estratégia operava em torno da ideia de *attaque à outtrance* - "ataque excessivo" -que apostava em uma superioridade ofensiva respaldada por superioridades tecnológicas que garantissem mobilidade - trens, telégrafos, logística, etc. - e maior poder de fogo - canhões com maior frequência de disparos, metralhadoras, rifles de repetição, etc. –que levariam à vitória militar. Se fosse possível surpreender e arrasar o inimigo com um ataque massivo, capaz de inutilizar a maior parte das capacidades inimigas, a vitória estaria garantida. É este tipo de confiança na capacidade ofensiva que se repete, ainda que com significativas diferenças estruturais, com a cibersegurança, criando um culto à superiodade de ataques cibernéticos preemptivos efeito que se agrava pelos baixos custos para a ação[10] (SINGER; FRIEDMAN, 2014b).

Dentro do debate da cibersegurança, surgem indagações sobre até que ponto seria lícito e razoável definir operações no campo cibernético como uso da força*de facto,* já que a atividade bélica denota, implicitamente, o uso da força física. Esta questão aponta paraum desafio normativo importante sobre como podemos nos sentir ameaçados por aquilo que é virtual e que não atenta diretamente contranossa sobrevivência, além de colocar desafios éticos e táticos sobre quem utiliza a força, quando e como (BUZAN; HANSEN, 2012).

Um segundo problema complementa o raciocínio: oentendimento holístico das ameaças advindas do ciberespaço requer um conhecimento técnico avançado sobre estas tecnologias, diferentemente de outras épocas onde a ameaça dos armamentos militares eram auto-evidentes. Por exemplo, não é necessário compreender a ciência da física nuclear para perceber os efeitos destrutivos de uma ogiva nuclear;é muito mais complexo e menos factível entender as ameaças advindas do ciberespaço sem compreender os meandros da tecnologia da informação. Este efeito pode ser classficado como*securitização por tecnificação*queocorre quando técnicos e especialistas se apropriam e monopolizam os discursos sobre segurança e são empoderados à condição de determinar o que é e o que não é uma ameaça. Esta condição é agravada pelo fato de escorarem este discurso sobre os critérios supostamente neutros da ciência, mascarando e relegando para um segundo

[9] O orçamento estadunidense para operações cibernéticas cresceu de US$3,9 bilhões em 2013 para US$4,7 bilhões em 2014, um aumento de 20% em um período de retração de gastos em defesa pelo país, demonstrando a importância atribuída a este setor pelo Departamento de Defesa. A maior parte deste aumento no orçamento é destinado à pesquisa e desenvolvimento de "*computer network attacks*" (MILITARY BALANCE, 2014, p.20).

[10] Esta ideia foi plasmada na doutrina estratégica francesa que admitiria "tão somente a tática ofensiva". Um problema crucial nesta aposta pela ofensividade no ciberespaço é o fato de que é menos custoso atacar do que se defender, como cita o diretor da DARPA "*Cyber defenses have grown exponentially in effort and complexity, but they continue to be defeated by offenses that require far less investment by the attacker".*

plano as implicações políticas das escolhas técnicas. Esta gramática específica da securitização é particularmente importante para determinar o futuro do ciberespaço pois os técnicos possuiriam o poder de (de)securitizar a matéria de modo decisivo. Por se tratar de um ramo cientificamente complexo e cuja operacionalização requere determinados conhecimentos prévios, os técnicos assumiriam uma função semelhante àquela dos militares em questões táticas sobrea guerra, sobretudo no século XIX, quando um corpo profissional é elevado à categoria de autoridade sobre determinado assunto de segurança,tema que não poderia ser deixado a "amadores" sob a pena da aniquilação por imprudência (HANSEN; NISSEMBAUM, 2009).

Podemos formular este problema através de uma pergunta teoricamente diferente:posto nos termos da Escola de Copenhague e do conceito da Securituzação, como se criou um objeto referente no ciberespaço ou como os agentes identificaram o ciberespaço como uma ameaça à sua sobrevivência? Quando da criação da rede mundial de computadores, não havia nenhuma caracterização de perigo ou uma ameaça existencial no ciberespaço[11]. No começo de seu desenvolvimento e popularização, a segurança no ciberespaço era uma preocupação restrita de alguns agentes que possuíam informação sigilosa ou de alto valor, comercial ou político, circulando nas redes, ou seja, limitada a agentes com interesses essencialmente individuais. O salto de uma preocupação individualpara uma questão de segurança nacional acontece quando diversos setores da economia e do governo passam a depender de sistemas eletrônicos para seu funcionamento cotidiano, criando a ideia de que um ataque cibernético poderia colocar em xeque *infraestruturas críticas*[12] para a segurança nacional. Assim, o problema da segurança virtual passa de uma preocupação puramente individual em relação a dados pessoais e

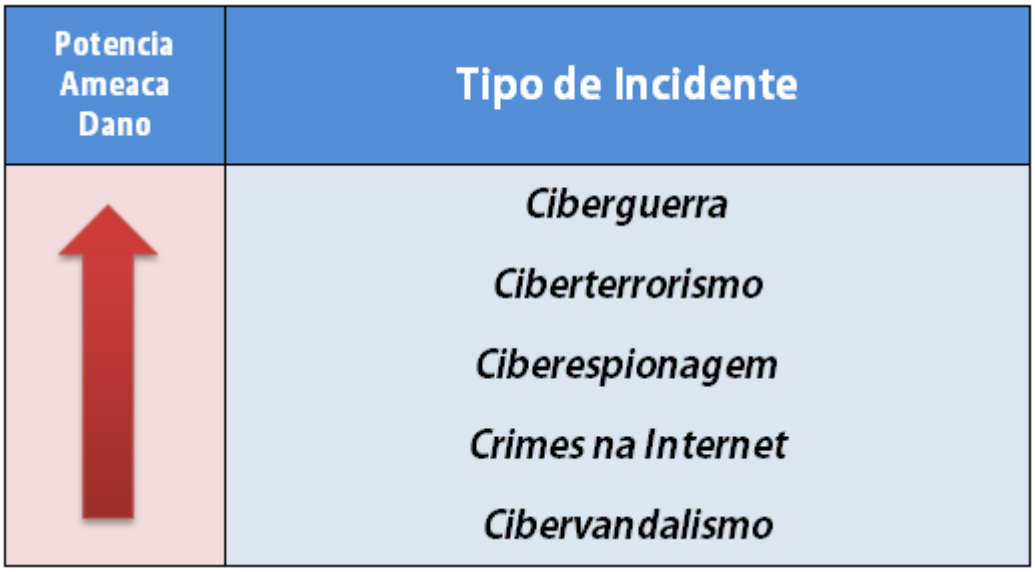
[11] A rede surgiu como uma necessidade militar de um sistema de comunicações que não fosse desruptível por um ataque nuclear. Não havia, no entanto, uma preocupação sobre a rede como uma ameaça endógena.

[12] A ideia de ameaçaàsestruturascríticasaparece de modoexplícitonapolíticaestadunidensena*Executive Order* nº13636 do Governo Obama, intitulada "*Improving Critical InfrastrutctureCybersecurity*" e ondeinfraestruturascríticassãodefinidascomo: *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"*. Ouainda: *Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. […] The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. […]Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority. We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks"*Disponívelem: <http://goo.gl/yUN2M0>. Acesso 24 Mar. 2014. Vale observar que das últimas três estratégias nacionais de segurança dos EUA o problema da cibersegurança aparece nenhuma vez em 2002, apenas uma vez em 2006 e 24 vezes em 2010.Referência semelhante se verifica no Livro Branco de Defesa nacional publicado em 2012 e que destaca que "*A ameaça cibernética tornou-se uma preoupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional".*

elementos corriqueiros de baixíssimo impacto para uma preocupação sobre soberania nacional e poder. O número crescente de ataques e a exposição midiática cada vez mais difundida destes incidentes fez com que o problema da cibersegurança deixasse de ser um tema de debate entre uma comunidade de técnicos e profissionais da informática para entrar na agenda de *policy-makers* e das estratégias nacionais de defesa, contribuindo para a formação da imagem de que o ciberespaço é cada vez mais inseguro e disputado.

Frente a enumeração de diversas ameaças no ciberespaço – fraudes, espionagem, vigilância, roubo de informações comerciais, ciberativismo, terrorismo e mesmo a possibilidade de conflito – é preciso conceituar as ameaças no ciberespaço de acordo com suas implicações para a segurança dos indivíduos e em nível nacional. A figura abaixo constrói uma escala sobre diferentes graus de ameaça no ciberespaço a partir de seus potenciais danos:

Figura 2. Escala de ameaças advindas do ciberespaço



FONTE: Cavelty, 2010; 2012.

Os dois níveis inferiores desta escala se resumem a problemas com pouco sobre as relações políticas internacionais. São diversos tipos de fraudes e ações que visam interromper o acesso a servidores e *websites,* com finalidades políticas – *Hackativismo* – ou não[13].Já os três níveis superiores são aqueles que estão ligados a concepções tradicionais sobre segurança e poder e quesão objeto de interesse para os ESI. Ciberterrorismo e Ciberguerra são ainda eventos sem registro empírco, existindo apenas como possibilidades

[13]Ainda que haja um registro médio de 82 ataques diários contra *websites* de governos ou grandes corporações (UNIDIR, 2009), estes ataques não fazem parte de objetivos militares ou de estratégias visando poder, sendo, portanto, classificados como cibercrimes ou cibervandalismo (CAVELTY, 2010).

remotas[14]. Já a ciberespionagem é um dos temas centrais envolvendo o ciberespaço. A Era da Informação afetou diretamente as atividades de inteligência e espionagem, sendo que os principais *players* neste cenários são países centrais do sistema internacional, sobretudo, os Estados Unidos e sua espionagem em massa pós-11 de setembro.

Paralelamente ao conceito de dissuasão corre o conceito de "*Corrida armamentista*", subproduto do primeiro. Este é, no entanto, um termo de difícil conceituação pela plasticidade da situação empírica que busca descrever. A atualização ou compra de arsenal militar, mesmo em quantidades significativas, pode não necessariamente representar um passo em direção a uma competição armamentista, assim como pequenas aquisições militares podem ser vistas por dois atores como sinais de uma competição à vista. Por estas razões, *corrida armamentista* é melhor definida como uma competição entre dois países concorrendo diretamente em direção a um objetivo (vitória) ou em busca de uma decisiva vantagem militar bilateral, resultando em uma competição militar intensa e anormal para os padrões de relacionamento entre as unidades do sistema (BUZAN; HERRING, 1998).

Os gastos militares no campo da cibersegurança ilustrama situação dinâmica do problema. Investimentos na área de cibersegurança se difundiram em diversos países, não havendo uma dinâmica de competição direta entre dois atores específicos. Como o conceito de corrida armamentista está centrado em uma mecânica bilateral, ele não é o mais adequado para descrever uma situação em que vários atores buscam incremento ou modernização de suas capacidades

Um conceito mais adequado para descrever está realidade é a ideia de "*dinâmica armamentista",*definida como as pressões externas e internas que impulsionam os atores (estatais) a adquirerem e modificarem a composição de suas forças armadas. O termo se aplica tanto para processos de caráter global, tal como o fenômeno da cibersegurança, como para descrever situações particulares de corte regional ou a um grupo reduzido de Estados (a dinâmica do Oriente Médio ou do Sudeste Asiático) (BUZAN; HERRING, 1998).

A dificuldade central para descrever a dinâmica armamentista da cibersegurança é a falta de instrumentos comparitivos para descrever as capacidades de cada país. Este problema é produto de três características importantes: 1) a natureza dual dos instrumentos em jogo; 2) o caráter secreto (*stealth*) das operações de ciberseguraça; 3) a falta de transparência dos Estados em relação ao problema da cibersegurança, o que contribui para o aumento da desconfiança e tensões, alimentando um novo dilema da segurança.

O uso dual de novas tecnologias é um elemento fundamental no pensamento estratégico pelo menos desde de o advento da Revolução Industrial e a crescente

[14]Cavelty (2012, p.108-109) lista pelo menos 35 incidentes importantes que contribuíram para uma securitização do ciberespaço devido à natureza e abrangência destes eventos. No entanto, o mesmo autor ressalta que a classificação destes episódios como sinais de uma guerra porvir contribuem apenas para agravar os problemas já existentes no ciberespaço.

transferência de tecnologias de uso civil para fins militares (e vice-versa). Na Era da Informação, esta dualidade se torna um elemento indissolúvel, resultado da característica totalizantes que as tecnolgias da informação produzem sobre a sociedade contemporânea, tornando-se a interface que controla todos os demais sistemas – economia, finanças, infraestruturas, serviços, comunicação, etc. (DER DERIAN, 2009). Por esta razão, é extremamente difícil mensurar capacidades militares de um determinado país no campo da cibersegurança. Diferentemente de um avião militar cuja finalidade é direcionada fins bélicos, computadores e conexões de rede não podem ser adequados à instrumentos de mensuração de cibercapacidades. A ausência de instrumentos com esta finalidade torna difiícil estabelecer um panorama mais detalhado sobre o fenômeno.

Na tentativa de criar um mecanismo inteligível para observar o fenômeno, o*Military Balance 2014*sugere que a mensuração de cibercapacidades necessita de uma avaliação das integral das capacidades estratégicas, tecnológicas e políticas de um país, além de uma análise de como este se projeta frente o problema do dominío cibernético. Seguindo esta proposição, o documento sugere os possíveis indicadores para a mensuração de cibercapacidades :

Figura 3. Possíveis indicadores de mensuração de cibercapacidades.

Indicadores Políticos	Sistema Político; Estabilidade Social; Ambições Nacionais; Posicionamento Internacional; Relações entre Hackers e Estado; Ações Regulatórias.
Indicadores Militares	Existência de Estratégia e doutrina em cibersegurança; organização estrutural; Educação e treinamento em cibersegurança; Operações em cibersegurança; Inteligência, Material, logística e infraestrutura
Indicadores Econômicos	Orçamentos de defesa; Orçamentos de programas de cibersegurança; PIB; produção nacional; restrições de importação/exportação; Aquisições e licitações; Patentes registradas; Investimento em P&D; Companhias públicas de alta tecnologia; Capacidades manufatureiras de alta-tecnologia
Indicadores Sociais	Maturidade da Era da Informação; Universidades com produção técnica; Número de graduandos e pós-graduandos em Ciências e Engenharias; Quantidade de Hackers; Concentração de pesquisa em P&D.
Tecnologias da Informação	Controle de TI; *Know-how*; Inovação; Tecnologia de ponta; Sistemas avançados (robótica, sistemas de controle remoto).
Indicadores de Infraestrutura	Redes de informação militar; Comunicações; Conexões de alta velocidade; Números de IPs; Capacidades industriais e de exploração espacial;
Outros Indicadores	Anúncios de fabricantes; compras e vendas estratégicas; atenção ao problema da segurança (na rede).

FONTE: *The Military Balance, 2014*. p.22.

Apesar de oferecer alguns elementos interessantes para investigar as cibercapacidades, estes indicadoresse tornam pouco inteligíveis em razão dos critérios difusos e ambíguos que utilizam, o que acaba resultando em uma leitura exacerbadamente belicosa do problema da cibersegurança. Alguns critérios sugeridos são especialmente problemáticos, tal como o número de graduados em ciências duras, ou ainda o critério amplo e vago sobre a maturidade da Era da Informação em um determinado país. Devido a estas dificuldades, é atualmente impossível mensurar adequadamente o problema da cibersegurança, ao mesmo tempo que esta ambiguidade contribui para uma visão generalizada de uma dinâmica armamentista acelerada.As características de anonimidade e invisibilidade no ciberespaço rerforçam a falta de transparência na divulgação das capacidades de cada país. Esse problema não é exclusivo da cibersegurança, mas um efeito comum no relacionamento entre tecnologia e estratégia. Sempre que há uma nova tecnologia com potencial vantagem estratégica sobre um adversário, esta tende a permanecer secreta, gerando desconfiança sobre o problema e resultando em uma dinâmica acelarada por mais capacidades.

Esta dinâmica acelerada não permite que haja uma estabilização estratégica das novas tecnologias, amadurecendo sua utilização técnica e tática (modelo de curva “S”). Os avanços são tão numerosas e em tão curto espaço de tempo que modificam a relação dialética entre estratégia e tecnologia: ao invés do primeiro guiar o segundo, os avanços técnicos e materiais passam a definir as prioridades e possibilidades estratégicas (BUZAN; HERRING, 1998, p.129). Este é o caso do desenvolvimento recente da cibersegurança, um campo que avança rapidamente no quesito tecnológico, mas que possui tímido desenvolvimento tático-estratégico. Estamos diante de um caso bastante comum fruto do ritmo acelerado das descobertas tecnológicas: sem evolução organizacional, doutrinária, estratégica e normativa, a tecnologia se torna um potente catalisador do dilema de segurança ao invés de ser um elemento estabilizador da segurança internacional.

Notas finais

Uma das perguntas instigantes sobre esta temática é entender o porquê da popularidade e da alta importância atribuída à cibersegurança por vários países mesmo quando não há empiria suficiente para provar a eficácia ou a vantagem tática destes instrumentos - com exceção da sua aplicação à inteligência que passou a ser dominada pelas novas tecnologias. O tradicional dilema da segurança ganha nova forma e contorno no

ciberspaço sem uma justificativa intelígevel que legitime uma dinâmica armamentista[15]. Não podemos nos esquivar então da pergunta que norteia as abordagens críticas sobre este tema: até que ponto as ameaças do ciberespaço são reais ou imaginadas? Como a construção de uma retórica de segurança sobre o ciberespaço atende a outros objetivos políticos e econômicos que extrapolam o campo da segurança e da sobrevivência?

Sobrepor conceitos clássicos dos ESI ao tema da cibersegurança oferece alguns pontos importantes de reflexão, mas obviamente possui seus problemas. Trata-se, em última instância, de aplicar tipos-ideais a uma realidade plástica e pouco clara ao observador da política internacional. Certamente a componente "virtual" da cibersegurança torna o objeto ainda mais complexo, mas como já apontara o filosófo Pierre Levy (1999)sobre a Sociedade da Informação, o mundo virtual se torna extremamente real quando se mescla e engendra relações de poder estabelecidas na ordem das coisas materiais.

Há, no entanto, uma série de dificuldades para abordar o problema a partir das Relações Internacionais: a falta de uma bibliografia consolidada, as barreiras técnicas que balizam o fenômeno, a novidade do tópico e a falta de instrumentos empíricos confiáveis e representativos para precisar a realidade que se busca descrever em direção ao seu entendimento estratégico. Possibilidades também se apresentam, sobretudo sob a forma de de questões investigativas sobre o problema: as características assimétricas da cibersegurança beneficiam mais as pequenas ou as grandes potências? Como o advento da Era da Informação aumenta a ainterdepêndencia entre os Estados, ao mesmo tempo que o seu subproduto, a cibersegurança, se torna um campo de disputa e atrito entre as nações? Quais são os argumentos que poderiam embasar um ataque cibernético (e até que ponto eles seriam plausíveis para uma audiência pública democrática)? Quais são os instrumentos que poderiam levar a uma governança global da *internet*reduzindo a exploração securitiva do ciberespaço? Há padrões de comportamento distintos em relação aos problemas da cibersegurança em regimes democráticos e não-democráticos? Qual deve ser o posicionamento dos países em desenvolvimento, sobretudo o Brasil, no âmbito diplomático e militar, frente a estes problemas?

Quando confrontamos conceitos clássicos como a dissuasão e a dinâmica armamentista, estamos na verdade lançando dúvidas sobre a possibilidade de que a

[15] A questão é: o dilema da segurança deriva de um cálculo racional sobre a realidade ou de uma percepção subjetiva e précondicionada sobre a realidade? Herz (1950, p.157) formulou o problema de forma ambígua: "*Groups or individuals living in such a constellation must be, and usually are, concerned about their security from being attacked, subjected, dominated, or annihilated by other groups and individuals. Striving to attain security from such attack, they are driven to acquire more and more power in order to escape the impact of the power of others. This, in turn, renders the others more insecure and compels them to prepare for the worst. Since none can ever feel entirely secure in such a world of competing units, power competition ensues, and the vicious circle of security and power accumulation is on."*

cibersegurança possa realmente modificar todo o quadro tradicional sobre segurança internacional. Não podemos tratar seriamente do problema da cibersegurança se não balizarmos suas inovações pelos conceitos que estruturam o paradigma de segurança, ou removermos o tema de um contexto maior do que é a guerra, o conflito e a política internacional. As dinâmicas da cibersegurança não "devem ser tomadas como configurando uma 'guerra' à parte. A guerra permamence una e indivísivel enquanto realidade" (CEPIK, 2001, p.255). É igualmente necessário ponderar os limites estratégicos da tecnologia, desmistificando suas capacidades e inserindo-a dentro de noções mais abrangentes sobre o que é e o que deve ser a arquitetura da segurança.

Para que a dissuasão no meio cibernético possa funcionar seria necessário uma arquitetura dos sistemas de informação que ainda não se apresenta eficaz e plausível. Seria necessário investir em pesquisa e desenvolvimento de sistemas voltados para a construção de mecanismos de confiança (*confidence building-measures* – CBM) e transparência,possibilitando uma governança da internet que preserve o ciberespaço como um ambiente livre e democrático. O debate da cibersegurança e seus impactos será um importante tópico multilateral para os próximos anos, mesmo diante das diversas barreiras técnicas e das indisposições e diferenças políticas.

Bibliografia

ARON, R. Paz e Guerra entre as Nações. Brasília: Universidade de Brasília, 2002.

BUZAN, B; HANSEN, L. *A Evolução dos Estudos de Segurança Internacional.* São Paulo: Unesp, 2012.

BUZAN, B; HERRING, E.*The Arms Dynamic in World Politics*.Londres: Lynne Rienne, 1998.

CAVELTY, M. Cyber-security. IN: COLLINS, A. *Contemporary Security Studies.* New York: Oxford University Press, 2012.

_____. Cyberwar: Concept, Status Quo and limitations. *CSS Analysis in Security Policy*, n.71, 2010. Disponivelem: <http://goo.gl/jlq5U0>,Acessoem: 17 Set. 2013.

_____. The Militarisation of Cyber Security as a source of Global Tension. In: MOCKLEY, D. (ORG). *Strategic Trends 2012: Key Development in Global Affairs.*Zurich: CSS. 2012. Capítulo 5, p.103-124.

CEPIK, M. *Serviços de Inteligência. Agilidade e Transparência como Dilemas de Institucionalização*. 2001. Tese (Doutorado em Ciência Política) – IUPERJ, Rio de Janeiro, 2001.

CEPIK, M; CANABARRO, D; BORNE, T. A securitização do ciberespaço e terrorismo: uma abordagem crítica. In: SOUZA, A; NASSER, R; MORAES, R. *Do 11 de Setembro de 2001 à Guerra ao Terror: Reflexões sobre o terrorismo no século XXI.* Brasília: IPEA, 2014. cap. 7, p.161-186.

DER DERIAN, J. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. New York: Routledge, 2009.

GRAY, C. *Making Sense of Cyber Power: Why the Sky is Not Falling*. Army War College Strategic Studies Institute, 2013**.**

HANSEN, L; NISSEMBAUM, H. Digital Disaster, Cyber Security, and the Copenhagen School.*International StudiesQuaterly*, v.53, p.1155-1175, 2009.

HARRIS, S. Caught Red-Handed. Washington is punishing China's cyberspies for the first time. Will Beijing come after U.S. spooks in response?*Foreign Policy*, 19 maio 2014.Disponívelem: <http://goo.gl/xDXPjF>. Acessoem: 22 Mai. 2014.

HERZ, J. Idealist Internationalism and Security Dilemma.*World Politics*, Vol. 2, No. 2,p. 157-180, 1950.

HOLLIS, D. Cyberwar Case Study: Georgia 2008. *Small Wars Journal*, 6jan. 2011. Disponívelem: <http://goo.gl/0azhhd>. Acessoem: 23 mar. 2014.

KAMINSKI, *R. Escaping the cyber state of nature: Cyber deterrence and International Institutions*. 2010. Disponível em: <http://goo.gl/al4bD3>. Acesso em: 21 mar. 2014.

LEVY, P. *Cibercultura*. São Paulo: Ed.34, 1999.

LIDDELL HART, B. *As grandes guerras da história.* São Paulo: IBRASA, 1982

LIBICKI, M. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND. 2009. Disponível em: <http://goo.gl/PHBh3Y>. Acesso: 21 mar. 2014.

MILITARY BALANCE. Conflict Analysis and Conflict Trends.*The Military Balance 2014*, cap.1, p.1-22, 2014.

NAGORSKI, A. (org.) *Global Cyber deterrence: views from China, the US, Russia, India and Norway.* New York: EastWest Institute, 2010. Disponívelem<http://goo.gl/jsmVAe>. Acessoem: 21 mar. 2014.

SINGER, P; FRIEDMAN, *A Cybersecurity and Cyberwar*. New York: Oxford University Press, 2014a.

_____. The Cult of the Cyberoffensive: Why belief in first-strike advantage is misguided as it was in 1914. *Foreign Policy*, 15 jan. 2014b. Disponívelem: <http://goo.gl/txv608>. Acessoem : 21 mar. 2014b.