Notas analíticas sobre os conceitos dissuasão e corrida armamentista aplicados ao fenômeno da cibersegurança.

Cauê Rodrigues Pimentel

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 dois temas clássicos dos Estudos de Segurança Internacional (ESI) e aplicá-los sobre o problema da cibersegurança: *dissuasão* e *dinâmica armamentista*. O primeiro elemento, 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 segundo conceito pilar, a *dinâmica armamentista*, 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. Através da delimitação conceitual destes dois elementos, pretende-se situar com melhor adequação o debate da cibersegurança dentro do pensamento dos ESI.

Introdução

> *Por que os recursos técnicos não seriam usados a serviço da tirania e da guerra? Ou – mais abstratamente ainda – a racionalização [...] não implca em que o poder venha a ser usado corretamente, e menos ainda para fins humanitários.*
>
> *Raymond Aron, A Era da Tecnologia, 1965, p. 73*

A cibersegurança é um tema recente no campo dos Estudos sobre Segurança Internacional (ESI) que despertou signficativo debate acerca das possibilidades, perigos e ameaças que conflagra. O conceito de cibersegurança emerge no final dos anos 1980 atrelado à noção de "ciberguerra" e mediado por retórica pautada pela emergência de ameaças advindas da era da informação (HANSEN; NISSEMBAUM, 2009; ARQUILLA, RONDFELD, 1989). Mais do que pura discussão acadêmica ou 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 militares devotadas a cibersegurança em 2009[1] (UNIDIR, 2009).

Sob que ótica devemos mirar o complexo fenômeno das novas tecnologias? A cibersegurança têm atraído grande atenção da academia sob diversas abordagens, o que resulta em uma bibliografia heterogênea. 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 sob a ótica do poder e do conflito, abordando o problema pela lógica da ciberguerra ou ciberpoder, leituras predominantes no mundo anglo-saxão, principalmente nos EUA, onde a ideia das novas tecnologias está diretamente associada à ideia de hegemonia e segurança nacional norte-americana. Do outro lado das abordagens, tradições diversas do pensamento europeu e sulista se debruçam sobre o tema a partir de uma aproximação crítica preocupada com os efeitos da cibersegurança sobre os conceitos de guerra, conflito, segurança, privacidade, democracia e soberania, este último um tema particularmente caro às leituras feitas ao sul e na América Latina.

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 e os desafios estratégicos engendrados pela tecnologia) (DUNN, 2007). A cibersegurança se torna um objeto especial de estudo por suas características inovadoras que distinguem o ciberespaço dos dominíos tradicionais do penamento estratégico[2], especialmente devido sua virtualidade transfronteiriça (GRAY, 2013). A sua associação ao campo da segurança internacional, resultado da crescente importancia destas tecnologias e por uma leitura deste ambiente pela ótica militar, leva a uma problematização do ciberespaço para os assuntos tradicionais dos ESI.

---

[1] 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.

[2] Complementa Cepik (2001, p.255) , sobre *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".

O objetivo deste pequeno *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 primeira aproximação ao fenômeno a partir do arcabouço intelectual da segurança internacional forjado durante o século XX. Podemos falar de dissuassão no campo cibernético? Como a cibersegurança incrementa ou prejudica os instrumentos dissuasórios já existentes? Há uma corrida armamentista por "cibercapacidades"? Por se tratar de um texto introdutório, lidaremos majoritariamente com perguntas mais do que com respostas.

Dissuasão, dinâmica armamentista e cibersegurança

A abordagem do tema da cibersegurança coloca a informação como uma importante fonte de poder na contemporaneidade, um elemento decisivo no campo de batalha e, portanto, fundamental para a sobrevivência do Estado. Ela está centrada em pensar sobre uma estratégia que garanta a segurança nacional através das novas tecnologias e que vê estes recursos como importantes armas para conseguir o máximo de eficiência com o mínimo (se possível o nível zero) de perdas humanas[3].

Para podermos pensar em segurança internacional, ao menos sobre seu panorama clássico ainda vigente em grande medida, o conceito de dissuasão é o eixo central para o debate. Não podemos negar, nem mesmo diante das RAMs ou de uma nova geração da guerra (LIND et al, 1989) que a dissuasão é o termo mais consistente na bibliografia dos ESI e que embasa o pensamento predominante de praticamente todo século XX. Não possuímos espaço para discutir amplamente os debates sobre o conceito de dissuasão que geraram uma profícua agenda de pesquisa. Por ora, ficaremos com a definição clássica de Aron (2002 p.509): dissuasão é um mecanismo social que pode ser reduzido conceitualmente ao "temor das

[3] Esta perspectiva contrasta diretamente com a teoria da paz democrática e a ideia de que democracias não entram em guerras devido aos freios que as baixas humanas impõem aos políticos dentro de democracias competitivas. Segundo Buzan e Hansen (2012, p.405-406) este é um dos problemas centrais na difusão das novas tecnologias aplicadas ao campo da segurança internacional: "é provável que essa difusão [...] crie questões sobre a democracia e a governança que mudarão o terreno no qual os ESI repousam. A maneira de lidar política e socialmente com um mundo no qual muitos indivíduos e pequenos grupos podem comandar grandes forças de destruição traz questões que vão muito além da competência de segurança dos ESI e apresenta outras amedrontadoras e desafiantes para qualquer tipo de sociedade liberal [...]De modo menos convencional, pode-se especular sobre o impacto de soldados e pilotos-robô cada vez mais sofisticados – já em utilização limitada – e suas implicações para o pensamento ético e etratégico em relação a quem utiliza a força, como e quando ela é utilizada. A tendência das sociedades capitalistas de substituir o trabalho pelo capital leva a essa direção, com propósitos de destruição e produção, conforme a relutância de sociedades ricas e com pequena taxa de natalidade em sofrer baixas. Se os 'mortos' da guerra forem máquinas, então a relação da sociedade com a guerra e os combatentes se transforma fundamentalmente. Outro cenário tecnológicamente conduzido envolve ameaças à cibersegurança, na qual terroristas ou outros atores malignos atacam estruturas físicas e digitais, derrubando , portanto, infraestrutuas críticas e redes de comunicação globais".

conseqüências possíveis, das *punições* previstas ou da execução de uma *ameaça".* No terreno da política internacional, a dissuasão funcionaria entre duas unidades soberanas e com recursos militares, cujo equilíbrio de poder resultaria na paz armada.

Fala-se muito em cibersegurança, mas o objeto parece estar descolado ou afastado dos elementos tradicionais que formam as vigas que sustentam a segurança internacional, o que prejudica o entendimento do fenômeno dentro de um contexto estratégico mais amplo. Há algumas tentativas de relacionar os dois temas, o clássico e o novo, que podem ser encontradas em uma bibliografia ainda restrita (KAMINSKI, 2010; NAGORSKI, 2010; LIBICKI, 2009, GOODMAN, 2009).

Dois elementos básicos fundam 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 (BUZAN, HERRING, 1998, p.158).

Este arcabouço clássico funciona quando se pode detectar facilmente de onde e de que inimigo parte determinado ataque/ameaça. No campo da cibersegurança, identificar a fonte dos ataques virtuais 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* (DUNN, 2007). Ainda que não seja impossível identificar a origem de um ataque (como no caso dos ataques à Estônia), 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 em função da anonimidade das redes, seu alcance global e difuso, além de sua penetração em diversas áreas de uso civil (NAGORSKI, 2010, p.1).

O problema da dissuasão na Era da Informação sofre mutações importantes impulsionadas pela tecnologia que aceleram, agudizam ou modificam características dominantes da Era Industrial, resultando em modificações táticas, estratégicas, organizacionais e perceptivas sobre segurança e guerra. O quadro abaixo ilustra algumas

destas mudanças significativas que alteram o entendimento sobre segurança internacional contemporânea:

Características da Era Industrial	Características da Era da Informação
Organização social	
Produção em massa, conscrição, 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*
Petroleo, 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[4]	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
Máximo de letalidade, grande número de baixas	Letalidade miníma/não-letal, redução (aversão) ao número de baixas.
Guerra total	Guerra especializada e limitada
Guerra mecânica	Guerra Digital
Força física	Conhecimento
Atrito, desgaste, ocupação	Precisão
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).

[4] 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.

Uma contradição fundamental que torna complexo o entendimento das novas tecnologias é a redução no número de baixas, com a perspectiva de perdas zero no caso da cibersegurança. Dissuasão sem perdas humanas se tornaria ineficaz, prejudicando a racionalidade do conceito. 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 mantéria uma paz armada.

Para que as ameaças recíprocas funcionem, é preciso que haja a imposição de custos ao adversário em para que este abdique de agir. Em suma, a dissuasão funciona por um sistema mútuo de ameaças que impõem custos suficentes a outrem. Elencamos a seguir, oito eixos que serveriam para mensurar o dos custos de ação, ajustados a partir do modelo oferecido por Buzan e 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 collateral)
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 de Buzan e Herring se centra no uso tradicional da força militar, pensado principalmente a partir do equilíbrio nuclear. Transpor este modelo para o caso cibernético implica em correções e imperfeições, mas ainda assim, lança importantes considerações sobre o problema. O que parece evidente, nesta primeira aproximação do tema, é que elementos da cibersegurança buscam reduzir significativamente os custos de ação. Os critérios 1, 2, 3, 5 e 8 são drasticamente menores do que em um cenário de conflito tradicional, nuclear ou não[5], enquanto os critérios 4, 5 e 7 são de difícil apreciação devido à novidade e complexidade do tema, mas certamente são importantes tópicos de pesquisa e discussão. 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

[5] O quesito número 1 é particularmente interessante pois retoma um problema clássico do *catchup* tecnológico na fronteira da defesa e segurança. Países periféricos possuem dificuldades adicionais para competir com a tecnologia militar produzida nos países centrais, levando a uma situação de atraso e dependência que poderia ser solucionada, *grosso modo*, através da transferência de tecnologia via importação ou da criação de capacidades próprias. Pensar este problema em relação à cibersegurança é algo importante devido ao atraso da Era da Informação na periferia.

sobre a Georgia em 2008[6]) ou de funcionarem como operações preemptivas (como no caso *Stuxnet*[7]).

Uma questão fundamental é definir até que ponto operações no campo cibernético configuram, *de facto*, uso da força (que implicitamente denota uso da força física). Esta questão coloca um desafio normativo importante e complexo para o qual não possuímos tempo para discutir, nem dados conclusivos: como podemos nos sentir ameaçados por aquilo que é virtual e que não ameaça nossa sobrevivência diretamente? Um segundo problema complementa a questão. O entendimento das ameaças advindas do ciberespaço requer um conhecimento técnico sobre essas tecnologias, diferentemente de outras épocas, onde as ameaças vindas 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, mas não é factível entender as ameaças advindas do ciberespaço sem compreender os meandros da tecnologia da informação[8].

Podemos formular este problema através de uma pergunta teoricamente diferente. Posto nos termos da Escola de Copenhague e da Teoria da Securituzação, como se criou um objeto referente no ciberespaço ou como os agentes identificaram o ciberespaço como uma ameaça à sua sobrevivência? Em seus primórdios, não havia a caracterização de perigo de

---

[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, 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 (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*, 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)

[8] O que Hansen e Nissembaum (2009) classificam como securitização por *tecnificação*. Quando técnicos e se apropriam sobre os discursos de segurança e são empoderados para dizer o que é e o que não é uma ameaça, monopolizam o debate sobre o tema se apoiando em critérios supostamente neutros e que seriam legítimos pois estariam embebidos por conhecimento científico. Para as autoras, 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. Por se tratar de um ramo cientificamente complexo e cuja operacionalizam requere determinados conhecimentos prévios, os técnicos assumiriam uma função semelhante àquela dos militares em questões táticas sobrea guerra. Eles são elevados à categoria de profissionais especializados, detentores de autoridade sobre o campo da cibersegurança, o qual não poderia ser deixado a "amadores" sob a pena da aniquilação po imprudência.

uma ameaça existencial no ciberespaço[9]. 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 marginal para 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* para a segurança nacional. Assim, o problema da segurança virtual passa de uma preocupação puramente individual em relação a dados pessoais e elementos corriqueiros de baixíssimo impacto para uma preocupação sobre soberania nacional e poder.

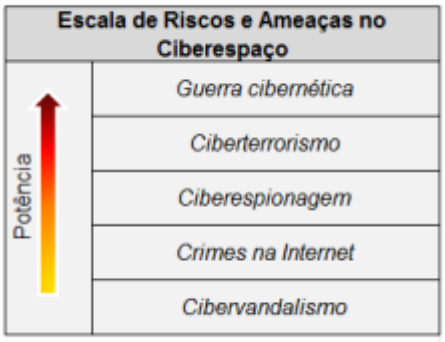
Por questões esquemáticas e de estrutura desta pequena abordagem, mantivemos a discussão sobre dissuasão no nível interestatal, ou seja, na perspectiva de forças organizadas e dirigidas politcamente por objetivos de um determinado Estado. Assim podemos pensar de que maneira poder-se-ria estruturar o problema da ciberdissuasão para o sistema internacional. Um fato crucial das novas tecnologias porém é a multipliação de agentes com capacidades no campo da cibersegurança. Diferentemente de armamentos militares tradicionais que estão restritos às Forças Armadas, há uma proliferação de capacidades entre agentes individuais. A maior expressão desta faceta é o grande número de *hackers* e *crackers* em atividade no ambiente cibernético. Este é um prolongamento de um problema da segurança internacional do final do século XX aplicado ao ciberespaço: a multiplicação de agentes capazes do uso da força e a perda do monopólio estatal sobre a mesma. Este tema é florescente na bibliografia, principalmente frente a casos de ativismo nas redes, retaliações a empresas motivadas por fatos políticos, e ações criminosas de diversos tipos no mundo digital. Em um grau mais exacerbado, há um temor sobre o ciberterrorismo que poderia minar infra-estruturas críticas, causando considerável dano político e econômico. Esta é uma característica presente, por exemplo, na estratégia estadunidense de segurança[10]. Pensar o problema da ciberdissuasão não somente frente a atores estatais torna a matéria

[9] 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.

[10] "*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"* Disponível em: <http://goo.gl/yUN2M0>. Acesso 24 Mar. 2014. Vale observar que das últimas três estratégias nacionais de segurança dos EUA - 2002, 2006 e 2010 – a palavra *cyber* foi utilizada nenhuma vez em 2002, apenas uma vez em 2006 e 24 vezes em 2010.

significativamente mais complexa, mas extrapola os limites da análise inicial aqui apresentada.

Vale indicar a miríade de ameaças no ciberespaço que devem ser classificadas de acordo com seu grau de alcance e impacto. Dunn (2010) constrói uma escala sobre diferentes graus de ameaça no ciberespaço a partir de seus potenciais danos:



FONTE: DUNN, 2010. Elaboração Própria.

Os dois níveis inferiores desta escala se resumem a problemas com pouco ou nenhum impacto sobre as relações políticas internacionais[11]. Já os três níveis superiores são aqueles que estão ligados a concepções tradicionais sobre segurança e poder e que portanto são objeto de interesse para os ESI. Ciberterrorismo e Ciberguerra são ainda eventos sem registro empírco, existindo apenas como possibilidades remotas. 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.

Apesar da ausência de conflito - ou evento que possa assim ser classificado – a cibersegurança se desenvolve em duas frentes: uma preocupada com *capacidades defensivas* e outra focada em *capacidades ofensivas*. O núcleo do problema está nas capacidades ofensivas. Quando não há imposição de custos à quem ataca - efeito derivado do problema da *atribuição* -, há incentivos para sempre atacar primeiro. Por esta razão se explica, por exemplo, a grande quantidade diária de tentativas de ataques cibernéticos no mundo todo (ainda que a maioria deles esbarrem em sistemas de proteção simples ou não causem dano significativo). No entanto, há uma considerável propensão de que Estados invistam mais em capacidades ofensivas do que defensivas, como no caso dos EUA onde o investimento se

[11] 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 (DUNN, 2010)

concentra no primeiro setor[12] (MILITARY BALANCE, 2014). 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") o qual apostava que uma superioridade ofensiva respaldada por melhoras tecnológicas que garantissem mobilidade - trens, telégrafos, logística, etc. - e maior poder de fogo - canhões com maior rapidez de tiro, metralhadoras, rifles de repetição, etc. - 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 com a cibersegurança, criando um culto à superiodade de ataques cibernéticos preemptivos efeito que se agrava pelos baixos custos para a ação cibernética[13] (SINGER; FRIEDMAN, 2014).

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 ilustram a 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[14]. 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

[12] 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).

[13] 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."*

[14] O grande problema ainda é precisar qual é o orçamento de cada país nesta área. A falta de transparência contribui para um ambiente de competição e desconfiança.

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

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	Maturidade da Era da Informação; Universidades com produção técnica; Número de

Sociais	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 de cada país, estes indicadores se tornam pouco inteligíveis em razão dos critérios difusos e ambíguos que utiliza, 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 rerforça 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 estratégico e normativo..

Notas finais e questionamentos

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 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. Possibilidades também se apresentam, sobretudo sob a forma de de questões investigativas sobre o problema: as características assimétricas da cibersegurança beneficiam mais aos pequenos ou às grandes potências? Como o advento da Era da Informação aumenta a a interdepêndencia 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

[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."*

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 cibersegurança pode 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)

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, com suas contradições, tensões e possibilidades.

Bibliografia.

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

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

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

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

DUNN, 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. Disponivel em: <http://goo.gl/jlq5U0>. Acesso: 17 Set. 2013.

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

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

HOLLIS, D. Cyberwar Case Study: Georgia 2008. *Small Wars Journal*, 6 Jan. 2011. Disponível em: <http://goo.gl/0azhhd>. Acesso: 23 Mar. 2014.

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

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

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*, Capítulo I, p.1-22, 2014.

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

SINGER, P; FRIEDMAN, A. The Cult of the Cyberoffensive: Why belief in first-strike advantage is misguided as it was in 1914. *Foreign Policy*, 15 Jan. 2014. Disponível em: <http://goo.gl/txv608>. Acesso: 21 Mar. 2014.