

Poder Cibernético Brasileiro: uma nova expressão do poder nacional

LUIS EDUARDO POMBO CELLES CORDEIRO -MAJOR- FABRA

Introdução



O quão importante é o setor de Defesa para um país como o Brasil, com problemas crônicos em diversas outras áreas como saúde, segurança e educação? Nós costumamos ouvir esta pergunta várias vezes em debates, seja em programas, em ambos os artigos científicos ou em matérias de imprensa.

A premissa desta pergunta é normalmente baseada nos ambientes interno e externo, com base na ausência de ameaças “tradicionais” externas e internas (como consideradas nas teorias de Relações Internacionais) que possam afetar nossa integridade como uma nação. Essa lógica pode levar-nos à conclusão de que a Defesa não deve ser uma área prioritária no desenvolvimento das políticas nacionais, e deve ser olhado como uma questão de “low politics” (que não afeta diretamente nossa sobrevivência como Estado).

Para refutar esse raciocínio, optamos por utilizar a teoria da Pressão Lateral (Choucri, 2012), que explica como uma tendência natural das nações o movimento de expansão da sua influência e / ou território para atender às demandas internas de sua população. Portanto, a fim de aumentar a sua presença (física ou não) além de suas fronteiras um país vai aplicar uma “pressão late-

ral” em outro país ou países na posição desejada. Concluímos, pois, que a “pressão lateral” faz parte das relações internacionais entre os Estados.

Portanto, podemos supor que o Brasil (como qualquer outro país) irá exercer pressão lateral no cenário internacional para satisfazer suas demandas internas e sofrerão a pressão dos outros nações da mesma maneira.

A intenção deste artigo é, então, focar em um elemento particular deste jogo que atualmente afeta o núcleo funcionamento da nossa sociedade: o Poder Cibernético. Para isso, é necessário primeiro definir o que chamamos de Poder Cibernético para depois de identificar a sua área de influência em nossa sociedade e só então propor soluções sobre como desenvolver instrumentos de atuação nesse campo em nome da nossa defesa nacional.

Poder

O Poder em si normalmente é um conceito abstrato com uma certa dificuldade de definição. Galbraith escreveu um livro sobre o assunto e concluiu que: “Apesar do exercício do poder ser um fato, poucas palavras são usadas de forma tão explícita, com quase nenhuma explicação do seu significado” (Galbraith, 1986).

Max Weber, argumentou que o exercício do poder, a partir do estado, é simplesmente a dominação do homem em uma posição de autoridade que lhe permite impor sua vontade sobre os seus semelhantes. (Weber, 2001).

Já com a perspectiva da relação das pessoas em sociedade Raffestin escreveu que onde existem seres humanos em relação social haverá uma relação de poder, porque sempre haverá interesses divergentes que deverão ser resolvidos (Raffestin, 1993).

Portanto, podemos concluir que o conceito de poder aplicado entre dois indivíduos (ou grupos de indivíduos) significa impor a vontade do outro, sendo esta uma noção básica para discutir as relações de poder.

Poder Nacional

Em relação ao parâmetro de poder do Estado em Relações Internacionais optamos por usar as idéias do Manual Básico da Escola Superior de Guerra do Brasil (ESG), porque entendemos a sua visão interdisciplinar e seu foco na Defesa Nacional, tal como descrito por seu próprio manual (ESG, 2011), a visão mais adequada do assunto para este artigo.

Assim, segundo a doutrina ESG, o Estado deve tentar servir aos desejos da Nação (os chamados Objetivos Nacionais) através do uso de seus recursos disponíveis (o Poder Nacional) para alcançar os objetivos definidos através de uma Política Nacional, de modo que, ao final, a correta aplicação do Poder Nacional permitirá a Nação alcançar os Objetivos Nacionais em acordo com as metas estabelecidas pela Política Nacional.

Assim, a capacidade de garantir os objetivos declarados dependem diretamente da capacidade do Estado de trabalhar tanto com os seus aliados internacionais quanto com sua própria população em diferentes ambientes (econômico, cultural, militar, social, etc ...).

Neste cenário, a ESG estabelece dois conceitos: Segurança, que é o sentimento do indivíduo (e, portanto, alargada à sociedade como um todo) de que ele / ela é protegida contra ameaças internas e externas; e a Defesa são as ações para garantir a sensação de Segurança de um Estado. Como o manual explica: “Em conclusão Segurança é um sentimento, enquanto a Defesa é a ação” (ESG, 2011).

Para essa ação temos então cinco expressão do Poder Nacional: Político, Militar, Científico Tecnológico, Econômico e Psicossocial; sendo estes os instrumentos utilizados nas ações de Defesa, a fim de fornecer o sentimento de segurança da Nação.

O Ministério da Defesa brasileiro afirma que para fazermos o melhor uso dessas expressões é necessário saber que a relação entre eles pode variar no espaço e no tempo de acordo com os grupos e interesses envolvidos (MD51-M-04, 2007). Em particular, no uso da expressão militar, esta relação entre o espaço-tempo é um fator crítico para a liberdade de ação dos atores, e, portanto, da sua capacidade de impor sua vontade (MD30-M-01, 2011).

Dessa maneira, ao relacionarmos a Defesa como um produto da correta noção de espaço e tempo, devemos estabelecer a noção de tempo (quando) e espaço (onde) utilizada neste artigo e como Poder Cibernético está relacionado com isso.

Espaço e Tempo

Pode-se considerar o espaço de muitas maneiras, como na física clássica onde consideramos o espaço como uma relação direta do tempo que demoramos para percorrer determinada distância. Utilizando esse conceito, temos a idéia Harvey de “compressão do tempo-espaço.” Em sua linha de raciocínio, se em 1840 um carta poderia viajar a uma velocidade de 16 quilômetros por hora, em 1930 essa de velocidade teria aumentado para 100 km / hora, em 1940 para 640 km/hora e, finalmente, em 1960, para 1.100 km/hora (Harvey, 1989).

Nesta lógica, pode-se concluir que no atualmente a informação se move à velocidade da luz (limitado pelo sistema de transmissão) através da Internet, de uma rede Extranet ou uma Intranet. Com base nesse raciocínio e usando como exemplo um telegrama enviado de São Paulo para o Rio de Janeiro, veríamos que a distância entre as duas cidades não se alterou significativamente desde a sua fundação no século 16, já a velocidade que a informação viaja aumentou exponencialmente.

Então, o que estamos vivenciando hoje é a transformação do espaço em algo efêmero, onde pedir uma xícara de açúcar para o seu vizinho pode consumir mais tempo do que enviar e receber uma mensagem instantânea, uma fotografia ou um texto de um amigo em Pequim.

Assim, podemos concluir que, se a sensação de espaço é basicamente ligado ao conceito de tempo, podemos dizer com certeza que o espaço não é a mesma coisa que a distância quando estamos falando de comunicação. Porque enquanto a distância é fixa com base na medição utilizado pelo observador (metros, pés, milhas), o espaço em comunicação depende do tempo necessário para que a informação seja produzida e enviada pelo transmissor para então ser recebida e interpretada pelo receptor, independentemente da distância.

Esta comunicação rápida que vemos hoje cria a percepção de que passamos de uma sociedade rígida, onde o fluxo de comunicação é rígido, para uma sociedade onde a informação “flui” entre os indivíduos em uma atmosfera de anarquia (no sentido de liberdade ou falta de controle) não mais governada pela distância entre as partes envolvidas, mas sim pelas ferramentas que permitem este tempo real comunicação.

Este ponto de vista foi proposto por Bauman no início deste século, no que ele chama de “modernidade líquida”. Neste conceito as mudanças da sociedade “fluem” e assumem a forma do ambiente que as contenha, diferentemente das mudanças anteriores de uma sociedade “sólida” que requeriam força e pressão para ser moldadas em uma nova forma (Bauman, 2001) . Este liquidez no mundo de hoje permite mudanças de penetrar todas as camadas da vida, incluído a relação espaço-tempo citado anteriormente, permitindo a da importância da presença física pela presença virtual do usuário de tecnologia.

Assim, a pessoa não precisa de mais estar presente em um determinado lugar fisicamente, pois sua “presença” (assim como os outros que fazem parte da sua vida social, familiar ou círculo profissional) é substituída por certo tipos de software no computador que cria o indivíduo virtual. Então, uma vez que a noção de espaço-tempo se torna extremamente fugaz, não é necessário ir a algum lugar para estar “presente”, ou melhor, a interação não é mais feita no mundo real, mas no mundo virtual.

Percebemos, portanto, que a “real” necessidade de se deslocar de um lugar para outro, a fim de interagir (e, portanto, ser capaz de agir em uma relação de poder) deve ser substituído, se não completamente, pelo menos em parte, pelas relações no mundo virtual. Esta necessidade influencia diretamente a noção de passado, presente e futuro nas relações humanas ao encolher nossa noção de espaço em um mundo onde o acesso à informação e à capacidade aumenta exponencialmente de comunicação.

Isso representa uma revolução nas relações humanas na medida em que, devido a evolução da tecnologia (portátil ou não) e sua capacidade de fornecer acesso a redes de comunicação, um indivíduo pode agora representar os seus desejos, opiniões e reclamações, sem a necessidade de ser amarrado a uma representação coletiva como associações, sindicatos, partidos políticos, ONGs e entidades similares (Choucri, 2012).

E estas ferramentas de informação nós permitiram, nos anos 90, entrar no que Peter Drucker chamou a Era da Informação. Neste cenário, a riqueza será gerada pela capacidade de produção e disseminação de conhecimento (Drucker, 1999).

Então, notamos a importância desses dispositivos que nos permitem interagir desta forma moderna, e é fácil de compreender que mantê-los funcionando é importante para o sentimento de Segurança mencionado antes, não só para indivíduos, mas para as instituições do Estado brasileiro.

Portanto, torna-se necessário fornecer a capacidade de comunicar-se com segurança mas sem perder os valores consagrados no nosso contrato social: a liberdade de expressão, o direito de escolher suas preferências políticas, à propriedade de seus bens (sejam eles reais ou virtuais) e todos os outros direitos garantidos em nossa constituição. Em outras palavras, é necessário que o Estado seja capaz de exercer o seu Poder Nacional neste ambiente virtual. Mas antes de pensarmos em como exercer esse poder, é necessário primeiro delimitarmos o escopo dessa ação, e por isso torna-se necessário, em nossa opinião, a criação de uma nova expressão do Poder Nacional: o Poder Cibernético.

Poder Cibernético

O termo de Poder Cibernético não existe, pelo menos não no sentido proposto por este autor. O que vemos na literatura com frequência considerável são definições com uma abordagem focada em ação no ciberespaço, ou seja, na Internet:

- Estratégia de Segurança Cibernética “... A arte prática de garantir a existência e manutenção da sociedade da informação em uma nação, um d de garantir e proteger, no ciberespaço, seus ativos de informação e estruturas críticas.” (Mandarim JUNIOR, 2010),
- Cyberwar “... As ações de um Estado-nação para penetrar computadores ou redes de outra nação com a finalidade de causar danos ou interrupção.” (Clarke e Knake, 2010),
- Ciber Power “... É a capacidade de usar o ciberespaço para criar vantagens, influenciar os acontecimentos em outros ambientes operacionais e utilizando instrumentos de poder.” (Ventre, 2011),
- Cyberwar “Conjunto de ações para o uso ofensivo e defensivo da informação e informação para impedir, explorar, corromper ou destruir os valores do oponente com base em informação, sistemas de informação e sistemas de rede de computadores.” (MD, 2007),
- Cyberdeterrence “... A capacidade no ciberespaço fazer aos outros o que os outros podem querer para ungi um de nós.” (LIBICKI, 2009).

O conceito de que talvez mais se aproxime da proposta apresentada está contido na doutrina militar de Operações Conjuntas escreveu pelo Departamento da Defesa do Brasil, onde Poder Cibernético é definido como “capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e de outros instrumentos de poder.”

Mas, no mesmo documento, quando olhamos para a definição de ciberespaço, mais uma vez, notamos que só são considerados os ambientes virtuais onde os dados são transmitidos, processados e/ou armazenados (MD30-M-01, 2011). Contudo acreditamos que o alcance desse conceito não é o suficiente uma vez que ele não considera o indivíduo (humanware) e os equipamentos (hardware), elementos chaves na nossa definição de Poder Cibernético..

Percebemos, então, que os conceitos atualmente ligados à Defesa e assuntos cibernéticos estão em fase de pré-pragmática que a estrutura descrita por Thomas Kuhn (Kuhn, 1991). Isso porque não há consenso sobre a essência de como a questão deve ser percebida: através de uma visão filosófica, através de uma visão cultural, militar, econômica?

Assim, percebemos hoje que o Estado brasileiro está agindo em resposta a situações que estão acontecendo ao invés de planejar o futuro por meio de um planejamento estratégico orientado. Isso resulta em um esforço capilar, considerando que cada ente estatal afetado tentou encontrar uma solução que satisfizesse suas próprias necessidades.

Um exemplo de tal divisão está nas estruturas responsáveis pela manutenção da Segurança (no conceito apresentado pelo ESG) do ciberespaço no Brasil. Haviam, no Brasil, em 2010, dezesseis instituições responsáveis pela segurança cibernética do Poder Executivo brasileiro (MANDARINO JUNIOR, 2010). Porém apesar desse elevado numero de atores não existe a definição de ações no nível estratégico (quais os objetivos a serem alcançados, definidos por uma Política de Segurança Cibernética brasileira), e, no nível tático (por exemplo, a resposta a um ataque cibernético), ocorre uma sobreposição de responsabilidades uma vez que não existe um órgão superior responsável pelo Poder Cibernético Nacional.

A Política Nacional de Defesa (PND), aprovada pelo Decreto nº 5.484, de 30 de junho de 2005, foi formulado com o objetivo de proteger o Brasil principalmente contra inimigos externos. Ela estipula três áreas estratégicas como prioridades: a nuclear, a espacial e a cibernética (MD, 2005).

Dada a definição de Nelson Jobim (El País, 2009), Ministro da Defesa no período de 2007-2011, de que “ter uma boa defesa é ter a capacidade de dizer não quando precisamos dizer não”, conclui-se que é uma condição de Defesa no Brasil a capacidade de exercer o seu poder nacional nas três áreas estratégicas citadas para garantir seus interesses na arena internacional, o principal cenário focado no PND.

Se olharmos para a área nuclear, temos uma Comissão Nacional de Energia Nuclear (CNEN), órgão federal responsável pela:

- a) Auxiliar na preparação dos programas de Energia Nuclear Nacional;
- b) Ações de investigação de conduta, de desenvolvimento e de promoção relacionada com a energia nuclear, e;
- c) Prover serviços no domínio da tecnologia nuclear e suas aplicações para fins pacíficos além regular, licenciar, autorizar, fiscalizar e controlar a sua utilização.

A CNEN atua no mercado civil e de acordo com as necessidades militares, especificamente no projeto do submarino nuclear brasileiro (CNEN, 2014).

No setor aeroespacial, temos outra agência federal, a Agência Espacial Brasileira (AEB), que é responsável pela formulação e coordenação da política espacial brasileira no sentido de uma autonomia no setor aeroespacial trabalha em colaboração com parceiros de militares e civis. (Brasil, 1994).

No entanto, quando olhamos para o campo de defesa cibernética, temos uma vasta gama de agências envolvidas no Poder Executivo. Podemos citar alguns, como o Centro de Gestão de Incidentes de Segurança em Redes de Computadores criada em 2006 (GSI, 2006), o Centro de Defesa Cibernética do Exército criado em 2010 (EB 2010) e do Escritório de Crimes Cibernéticos da Polícia Federal criado em 2011 (MJ, 2011).

No entanto, não existe uma única agência federal com plena autoridade para coordenar e formular questões sobre todo o setor cibernético federal, com a responsabilidade única e exclusiva de assegurar a utilização do poder nacional no domínio cibernético. Portanto, podemos dizer que as ações no domínio cibernético estão agora relegadas para atores responsáveis pelas ações de outras expressões do poder nacional (como o Exército Brasileiro, que é parte da expressão militar), mas não há nenhum órgão central para agir em nome do Poder Cibernético especificamente.

Outro obstáculo é que as ações observadas concentram suas ações no uso seguro da rede mundial como a principal linha de defesa e a preocupação em garantir o acesso às tecnologias que nos permitem acessar as redes de comunicação existentes (por exemplo, processadores e memória para computadores), o que certamente levar a um enfraquecimento do Poder Nacional e na incapacidade de fornecer a Segurança necessária conforme estipulado na PND.

Por isso, acreditamos que uma reestruturação do sistema atual é necessária para que possamos utilizar os conceitos discutidos acima não de forma compartimentada, mas com uma visão holística do assunto, a fim de iniciar uma gestão estratégica sobre essa área. Para que isso aconteça o primeiro passo é a classificação dos assuntos relacionados sob uma nova expressão de Poder Nacional para que, desta forma, tenhamos um escopo definido do ambiente para iniciar o nosso planejamento estratégico.

A nossa explicação para a criação de um novo poder reside no fato de que, ao contrário de outros meios tais como aéreo e o naval, o ciberespaço é um ambiente criado, desenvolvido, mantido e controlado por seres humanos. Por conseguinte, a interação humana é necessária para a existência desse ambiente.

Então chegamos à conclusão de que este ambiente, tão importante para a civilização, só pode ser acessado através dos mecanismos criados pelo homem, e é nesta realidade que reside a fraqueza já que são poucos os países no controle desse processo de criação.

Se seguirmos o modelo proposto por John A. Warden III e tivermos a intenção de causar uma paralisia estratégica por um ataque paralelo ou tenhamos que nos defender de um ataque (WARDEN III, 1995), temos estar ciente de que só se preparar para uma luta no ciberespaço (considerando uma rede virtual como o campo de batalha) é uma visão estreita do problema, porque não adianta termos excelentes proteções virtuais no ciberespaço se nos for negada a possibilidade de acessá-lo. Todo o nosso planejamento terá sido inútil.

Warden também nos ensina que no conflito não devemos buscar a batalha, pelo contrário, é inteligente evitá-la ao máximo. Podemos fazer isso identificando primeiro os Centros de Gravidade do inimigo, sendo estes os elementos de uma sociedade que afetam diretamente a capacidade de combate do Estado. Após fazer isso, devemos atingi-los com força total e então a luta será breve. Para maximizar o esforço não devemos atacá-los de maneira isolada, mas sim por meio de ataques paralelos que levem à incapacidade do inimigo de continuar lutando e sua capitulação em uma luta rápida e eficaz.

Sob essa lógica, muito mais eficazes do que realizam ataques na Internet seria através de engenharia social atacar o humanware na expressão política ou explorar dependência externa total do Brasil sobre o hardware para explorar todas as expressões do Poder Nacional em apenas um golpe.

Portanto, o que propomos como do Poder Cibernético é um conceito que engloba não só o ciberespaço, mas também a capacidade de acessá-lo e os indivíduos que interagem neste ambiente. Isso só será possível se nós controlarmos a produção de equipamentos (hardware), as ferramentas utilizadas (software) e treinarmos aqueles que irão trabalhar com esses dois elementos (humanware).

Considerando-se que em 2010 tínhamos 16 instituições atuando nessa questão (segurança cibernética), talvez tenhamos sentido que estamos bem protegidos. No entanto, o entendimento desse autor é exatamente o oposto.

Esta conclusão baseia-se em algumas premissas. A primeira é a de que não se definiu um único responsável pelo desenvolvimento da Política Nacional de Defesa Cibernética, com a autoridade para delegar tarefas, direcionar esforços e projetar cenários futuros com autoridade sobre outras organizações públicas e privadas nesse campo. Portanto, existe uma falta de liderança no nível mais alto de decisão Política Nacional Cibernética.

Outra questão é a atual falta de definição de responsabilidades. Por exemplo, se um ataque cibernético atinge a rede elétrica em uma determinada região do país, quem é responsável pelos procedimentos de contenção, de identificação dos autores e (se for o caso) de retaliação? Porque se estamos falando de um crime que você poderia dizer que caberia à Polícia Federal, mas se estamos falando de um ato de guerra a responsabilidade seria do Exército. Este exemplo traz muitas outras questões técnicas:

- Criminalizado o ato, podemos identificar com precisão um indivíduo ou organização como responsável?
- Criminalizado o ato, que lei se aplica se o ilícito foi praticado em outro país?
- Qual a legitimidade do Marco Civil Internet brasileiro no contexto internacional?
- Quem seria responsável por negociar os termos de tal Marco na comunidade internacional?
- Se classificarmos o ataque como um ato de guerra, mais problemas irão aparecer:
- Que regras se aplicam na comunidade internacional para justificar o nosso direito de declarar guerra (*Jus ad bellum*) sobre a base de um ataque virtual?
- Quais são as normas que legitimar nossas ações no ambiente cibernético respeitando as convenções internacionais (*jus in bello*)?
- No caso de um ataque cibernético embebidas em um conflito convencional, quem seria responsável pela realização de ações (exploração, defesa e ataque) no ciberespaço: o Exército Brasileiro, que também estaria envolvido na realização de operações em terra, ou uma outra organização que teria a responsabilidade exclusiva sobre o Poder Cibernético?

Nos exemplos acima, estamos vendo apenas as implicações em nível estatal, mas se nós nos movemos para o setor privado, a pergunta é quem deve proteger as transações financeiras, redes de comunicação de dados, rede de telefonia e indústrias de alta tecnologia de infra-estrutura crítica? Será que o Estado têm esta responsabilidade, e, mais ainda, a capacidade de estender a Segurança para essas áreas?

Estes desafios não são novos e, certamente, não são fáceis de resolver porque envolvem muitas variáveis. Como um exemplo de como devemos olhar para o problema, temos o pensamento de Harold Valadão em seu trabalho sobre o direito aeroespacial:

Nenhum poder ao homem, sem um imediato controle jurídico. Cabe ao Direito proteger o homem contra os desmandos do próprio homem. A cada novo progresso social, econômico ou técnico, outra cobertura jurídica à pessoa humana. No limiar de uma nova era, o alvorecer de um novo direito. (1957, apud FILHO, 2007)

Quanto ao planejamento estratégico do Estado no que diz respeito à questão da segurança cibernética, quem vai definir se:

- Independência Tecnológica é possível neste sector?
- Se não for possível a independência, quais as alternativas temos para manter a Segurança e a Defesa do país?
- Se buscamos a independência, quais equipamentos e sistemas devem ser desenvolvidos e fabricados no país?
- Quais são as competências esperadas dos indivíduos que irão trabalhar nesse setor?
- Qual é o papel do governo e da iniciativa privada nesse processo?

Na Figura 1, podemos ver um exemplo de um sistema unificado e interdependente:

3: U.S. Government: Overview

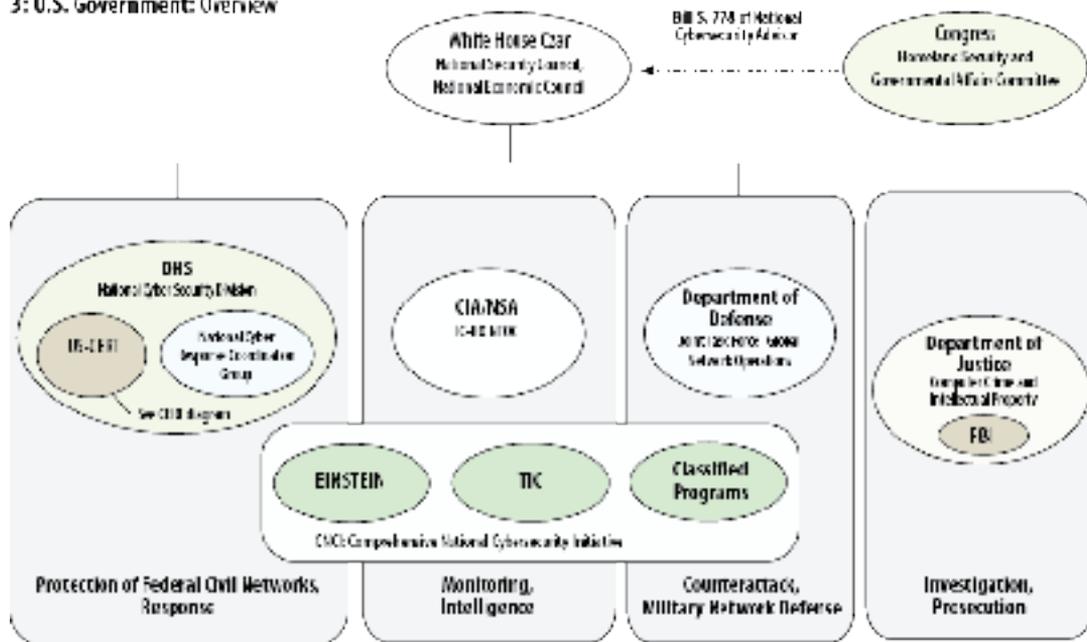


Figura 1 estrutura proposta para os Estados Unidos

Fonte: "Institutions for Cyber Security: International Responses and Global Imperatives," Information Technology for Development .Choucri, Madnick e Ferwerda (2013).

Talvez esta estrutura seja montada para coordenar esforços em consonância com a definição do Departamento de Defesa dos Estados Unidos sobre o que é ciberespaço (DOD, 2014): "uma infra-estrutura de rede interdependente de tecnologia da informação e conteúdo de dados, incluindo a Internet, redes de telecomunicações, informática, comunicações e sistemas de informação, bem processadores e controles embutidos".

Em nossa definição de Poder Cibernético poderíamos acrescentar a isso as organizações que promovem pesquisa e desenvolvimento bem como a regulamentação das atividades cibernéticas (incluindo a defesa) no ambiente interno e externo, tanto no setor privado como estatal.

Corroborando as idéias apresentadas acima, este autor acredita que a definição de um ator responsável pela gestão das políticas estratégicas cibernéticas parece ser não só desejável, mas uma solução inevitável. E então para definir que tipo de ator precisamos primeiro devemos definir qual sua área de responsabilidade.

Na metodologia usada, nós decidimos delimitar esta área de Poder Cibernético, sendo esta uma nova expressão de Poder Nacional utilizando o conceito da ESG. Acreditamos que esta ação ajudaria futuros estudos na criação de paradigmas para que possamos passar para a fase de ciência normal (Kuhn, 1991), ou seja, com conceitos definidos em que uma ou mais áreas poderiam explorar a questão de forma interdisciplinar.

Seguindo então a formulação definida pela ESG, sustentamos nossa nova expressão de poder em três pilares:

Homem: seria o ou indivíduo grupo de indivíduos com a habilidade para usar um dispositivo eletrônico para interagir em uma rede pública, privada ou mista sendo capaz de interagir com outra membros desta rede em uma relação de poder;

Terra: seriam os equipamentos e os sistemas operacionais que permitiriam o indivíduo ou grupo de indivíduos interagir em um ambiente de rede pública, privada ou mista sendo capaz de se relacionar com outros membros em uma relação de poder, e;

INSTITUIÇÕES: seriam as entidades públicas, privadas ou mistas responsáveis pela sustentabilidade (no sentido de sustentar: sustentar, defender, apoiar, manter) das redes públicas, privadas ou mistas permitindo que o HOMEM (como definido acima) possa influenciar as expressões do poder nacional por meio da TERRA (como definido acima).

Assim podemos concluir que o Poder Cibernético é a expressão do Poder Nacional que procura regular, controlar e desenvolver (de acordo com os princípios morais da sociedade), a transmissão de informações entre os indivíduos e / ou grupos sociais bem como os efeitos destas relações de poder a fim de atingir e manter os Objetivos Nacionais.

CONCLUSÃO

Chegamos à conclusão de que, na sociedade de hoje, relações de poder estão mudando devido a transformação dos conceitos de espaço e tempo, bem como a substituição da presença física do indivíduo pela presença virtual sem uma perda de influência nas relações sociais.

Assim, a relação é agora cada vez mais fluida e capaz de adaptar-se ao ambiente que a rodeia, mas tal mudança implica em uma maior dependência de acesso a equipamentos tecnológicos, já que eles são a única maneira de acessarmos um ambiente totalmente artificial criado pelos seres humanos: o ciberespaço.

Considerando-se os conceitos da ESG percebemos que, no mundo de hoje, não podemos discutir Segurança e Defesa sem termos a capacidade de projetar o nosso poder nacional no ambiente virtual (privado ou público), e, portanto a sociedade brasileira não vai ter a sensação de Segurança se não há confiança de que a nossa integração na Era da Informação é garantida por meio da ação de Defesa para garantir esse acesso.

Torna-se necessário, então, termos capacidade de planejar a nossa defesa na expressão de poder nacional por nós definida como Poder Cibernético para garantir a segurança de nossa nação, levando em conta o fato de que um ataque focado nessa setor poderia causar uma paralisia estratégica, e que nossas defesas devem ir além ciberespaço para que o nosso acesso a este mundo virtual não seja negado.

Então entendemos que uma boa solução seria a criação de uma nova expressão do Poder Nacional a fim de facilitar o desenvolvimento de estudos, ações e conceitos doutrinários com uma visão holística da situação.

Esta congregação de conceitos existentes não é uma evolução dos conceitos atuais, mas uma quebra do atual sistema reativo mudando para um sistema preventivo. Tal ruptura poderia ocorrer através da adoção de um ponto de vista dedutivo, com a assimilação dos conceitos de relações de tempo e espaço e energia dos adotados hoje, com a intenção de proporcionar uma melhor capacidade Defesa para o Brasil.

Referências

- Bauman, Zygmunt *Modernidade Líquida* Rio de Janeiro: Jorge Zahar Editor de .. de 2001.
BRASIL. Constituição Federal. Brasília, 1988.
BRASIL . Lei No. 8854, de 10 de fevereiro de 1994 Brasília, Disponível em:
<[Http://www.planalto.gov.br/civil_03/Leis/L8854.htm](http://www.planalto.gov.br/civil_03/Leis/L8854.htm)>. Página visitada em 20 de julho de 2014.
Choucri, Nazli *Ciberpolitics in International Relations*. Cambridge: MIT Press .. 2012.

Choucri, Nazli; Madnick, Stuart; Ferwerda, Institutions for Cyber Security: International Responses and Global Imperatives,” Information Technology for Development Disponível em: <http://ecir.mit.edu/images/stories/website%20photos/ECIR%20website%20staff%20pics/ECIR%20website%20staff%20pics/choucri%20madnick%20ferwerda_institutions%20for%20cyber%20security_published.pdf> acesso em 05 de julho de 2014.

CLARKE, Richard; Knake S, CyberWar New York:. HarperCollins, 2010.

Comando do Exército -. EB Portaria nº 666, de 4 de agosto de 2010.

Brasília, Disponível em:

<[Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C BwQF-jAA](http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C BwQF-jAA) e url = <http://www.sgex.eb.mil.br/sistemas/ser/copiar.php?codarquivo=ac=824&t=&ei=bre meLYU7DOLpLmsATi->

YDYCA e usg = AFQjCNEmEuRHQuBtjgQJGYwSIANIM7sjNA e bvm = bv.71778758, .cWc d>. Acessado em: 22 de julho Em 2014.

.. Comissão Nacional de Energia Nuclear - CNEN Institucionais Disponível em: <<http://www.cnen.gov.br/acnen/inf-competencias.asp>>. Acessado em: 15 de julho Em 2014.

Departamento de Defesa - DOD. DOD Dicionário de Termos Militares Disponível em: <http://www.dtic.mil/doctrine/dod_dictionary/tm> Retirado 17 de junho de 2014.

Drucker, A Sociedade Pós-Capitalista . 7.ed. Rio de Janeiro: Campus, 1999.

O PAIS In: “Uma boa defesa é ter a capacidade de dizer não quando é preciso dizer não” Madrid, 28 de outubro .. 2009 Disponível em:

<[Http://internacional.elpais.com/internacional/2009/10/28/actualidad/1256684401_850215.html](http://internacional.elpais.com/internacional/2009/10/28/actualidad/1256684401_850215.html)>. Retirado 10 de julho de 2014.

Escola Superior de Guerra - ESG Guia Básico: elementos Fundamentais .. vol.I .Rio janeiro 2011

FILHO, José Monserrat A Magna Carta do espaço exterior Disponível em: .. <<http://www.sbda.org.br/artigos/anterior/37.htm>> Retirado 04 julho de 2014.

Gabinete de Segurança Institucional - GSI Portaria nº 13 de abril agosto de 2006, Brasília, Disponível em: <<http://www.ctir.gov.br/sobre-CTIRgov.html#quemsomos>> .. Acesso em: 22 de julho de 2014.

GALBRAITH, Kenneth J. Anatomia de poder São Paulo:. Pioneira, 1986.

. HARVEY, David Condição da pós-modernidade: Cambridge. Blackwell Publishers, 1989.

KUHN, Thomas. A Estrutura das revoluções científicas São Paulo Outlook 1991.

LIBICKI, Martin C .. Cyberdeterrence and Cyberwar. Santa Monica: Rand de 2009.

MANDARINO JUNIOR, Raphael. Segurança e defesa do espaço cibernético brasileiro. Recife: Cubzac, 2010.

. Ministério da Defesa MD35-01-G . Brasília, 2007.

Ministério da Defesa. MD30-M-01 . Brasília, 2011.

Ministério da Defesa. MD51-M-04 Brasília, 2007.

Ministério da Defesa. Política de Defesa Nacional. Brasília, 2005.

Departamento da Justiça -. MJ Portaria nº 2.877, de 30 de Dezembro de 2011.

Brasília, Disponível em:

<[Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C B4QF-jAA](http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C B4QF-jAA) e url = http://www.dpf.gov.br/acessoainformacao/http___intranet.dpf.gov.br_le_gislacao_regimento_interno_portaria_n_2-877-2011-

MJ.pdf e ei = qOTYU6LoM8bnsATiIqKACA e usg = AFQjCNG5TOa0NE6nSrVdN52c3icj-c74XA e bvm = bv.71778758, d.cWc>. Página visitada em 24 de julho de 2014.

. Raffestin, Claude . Por uma geografia do poder São Paulo: Editora Ática, 1993.

VENTRE, Daniel . Cyberwar and Information War London: Iste 2011.

WARDEN III, John A.O inimigo como sistema. Disponível em:

<[Http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm](http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm)>
Retirado 20 de junho de 2014.

WEBER, Max Ciência e política: duas vocações. São Paulo: Martin Claret, 2001.



O Major Aviador Luis Eduardo Pombo Celles Cordeiro, da Força Aérea Brasileira (FABRA), é especializado em MBA em Gestão Pública na Universidade da Força Aérea e responsável pela disciplina do Emprego da Força Militar pela Escola de Oficiais do Esquadrão da Força Aérea Brasileira, no Rio de Janeiro. Ensina a Doutrina Básica da Força Aérea e prepara planos de estudos para cursos. Antes de ocupar seu posto atual, desempenhou o cargo de Oficial de Administração de Pessoal do 5/8 Esquadrão na Base Aérea de Santa Maria. Graduou-se com distinção na Escola de Oficiais de Esquadrão em Maxwell AFB, Alabama. O Major Pombo Celles é piloto com mais de 3.500 horas de voo em T-25, AT-26, AT-27, C-97 C-98, L-42, H-50 H-1 e H-H 60L.

