# ASPECTOS DA DEFESA CIBERNÉTICA

*Palavras do ministro da Defesa, Celso Amorim,*
*na abertura do III Seminário de Defesa Cibernética*

**Brasília, 24 de outubro de 2012**

Senhoras e senhores,

O alto número de inscritos neste III Seminário de Defesa Cibernética atesta a importância do diálogo que o Ministério da Defesa tem buscado entabular com os setores acadêmico, empresarial, com outras áreas do governo e da sociedade sobre essa senda verdadeiramente inovadora.

O objetivo desta iniciativa é fomentar a discussão, a reflexão e a troca de experiências sobre a temática da defesa cibernética entre instituições públicas, organizações militares e civis, além de integrantes do meio acadêmico – nos âmbitos nacional e internacional – que tenham relação com o tema.

Algumas das questões a serem discutidas são a estratégia de segurança e defesa cibernética, sua aplicação aos grandes eventos, a capacitação de recursos humanos na área e os investimentos do setor empresarial nesse segmento.

★ ★ ★

A internet alterou os parâmetros de ação humana.

O próprio conceito de realidade foi expandido pelo espaço digital.

A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, à terra, ao ar e ao espaço.

Aberto à ação humana, o domínio cibernético abre-se também ao conflito.

A expansão do espaço digital suscita, desde logo, a problemática da proteção das redes.

Há poucos dias, o secretário de Defesa dos Estados Unidos, país mais poderoso do mundo, Leon Panetta, tornou a mencionar a possibilidade de um "Pearl Harbor cibernético".

Embora seja preciso tomar afirmações muito extremadas com um grão de sal, não há dúvida a respeito de estar em curso o desenvolvimento de meios virtuais para emprego como armamentos ou como instrumentos de inteligência – um emprego sujeito não só aos interesses de atores não estatais como também à lógica competitiva do sistema de estados nacionais.

Os ataques produzidos pelos vírus "*Stuxnet*" (utilizado contra o programa nuclear do Irã) e "*Flame*" (que se alastrou no Oriente Médio) apontam nessa direção.

Esse processo importa em sérios desafios para o cumprimento, pelo Ministério da Defesa e pelas Forças Armadas, do mandamento constitucional de defesa da pátria.

A incerteza emanada dessa nova realidade motiva indagações a respeito das vulnerabilidades de nosso país.

Atualmente, quase todos os sistemas de armas funcionam com componentes de tecnologia da informação.

O comando e controle e o apoio logístico dependem pesadamente de sistemas digitais.

As consequências de um ataque, longe de limitar-se ao espaço cibernético, alcançariam a sociedade como um todo.

Um ataque cibernético teria o potencial de desorganizar a sociedade de várias maneiras: materialmente, por perdas econômicas como, por exemplo, o prejuízo causado pela queda de um sistema bancário; psicologicamente, pelo medo, pelo pânico e pela possível paralisia frente a um agressor que possa sabotar sistemas críticos em larga escala.

Tais hipóteses teriam, caso concretizadas, um custo inaceitável para a soberania, a integridade e o bem-estar do país.

Há ainda pouca nitidez no que concerne à natureza dos ataques cibernéticos, mas é evidente que a ameaça digital é real e grave.

Estado e sociedade devem estar prontos para enfrentá-la.

Mas como o Estado e a sociedade desempenharão suas tarefas e responsabilidades no espaço cibernético?

Qual a fronteira entre o crime e o conflito cibernético, e que tipo de regulamentação pode decorrer dessa distinção?

Quais nossas vulnerabilidades e forças nesse campo?

O que sabemos sobre o desenvolvimento de outros países nessas áreas?

A busca de respostas para essas e tantas outras questões torna este seminário pertinente e oportuno.

Nas palavras de Olivier Kempf, membro do corpo editorial da conceituada *Revue Défense Nationale*, da França, o espaço cibernético incontestavelmente representa um novo domínio para o pensamento estratégico.

Vivemos o início de uma importante revisão do paradigma de utilização dos meios militares.

Decidido a participar do estado da arte dessa transformação tecnológica, o governo brasileiro elencou a área cibernética como setor estratégico.

E conferiu ao Exército a responsabilidade primordial pela condução dos programas relativos a ela. Reforços orçamentários razoáveis, embora longe do ideal, foram consignados ao setor – e estão possibilitando seminários como este.

Uma política de defesa cibernética que forneça orientação, coerência e foco para o desenvolvimento do poder militar nacional nesse domínio é absolutamente essencial.

De caráter multidisciplinar, a defesa cibernética abrange um grande número de áreas, elementos intra e interorganizacionais, além de produtos e serviços tecnológicos diversos.

Essa complexidade requer a criação de estruturas e processos de defesa flexíveis, orientados por visão estratégica, capazes de realizar, de forma eficaz, a coordenação, integração e execução de atividades.

Com a criação do Centro de Defesa Cibernética no Exército Brasileiro, o Estado passou a contar com um elemento catalisador.

O CDCiber investe-se de credenciais para participar de discussões nacionais e internacionais sobre sua atividade-fim e para adensar a relação com diversos órgãos governamentais e entidades civis.

Esse adensamento foi posto à prova com êxito em junho de 2012, quando o Centro de Defesa Cibernética coordenou as ações de segurança digital em apoio à Conferência das Nações Unidas para o Desenvolvimento Sustentável (a Rio+20), e o fez utilizando em grande medida *softwares* nacionais – o que demonstra a capacidade de nossa indústria.

As experiências adquiridas naquele evento serão apresentadas nesse encontro.

★ ★ ★

A autodefesa digital requer a proteção de redes, o monitoramento e a análise do tráfego de dados, a identificação de ataques cibernéticos e a consequente resposta contra eles.

Nesse campo, a responsabilidade individual no que concerne à segurança orgânica da informação tem papel de relevo.

Sérias vulnerabilidades, relacionadas à perda ou fuga de informações, estão frequentemente relacionadas a ações não intencionais, tais como o uso descuidado e impróprio da tecnologia da informação.

Ao mesmo tempo que se vale da tecnologia da informação para ampliar os espaços da comunicação e da criatividade, é essencial que a população tome consciência dos riscos associados com os meios digitais.

O reforço, na sociedade, do conhecimento e do poder inovador no ambiente digital será uma ação prioritária, assim como a capacitação e gerência de talentos.

Essas iniciativas devem ser conduzidas de modo a estimular o investimento na tecnologia digital, na pesquisa e na inovação.

Deve também fomentar o intercâmbio de ideias relacionadas ao setor cibernético junto à sociedade brasileira.

A intensificação da cooperação em nível nacional e internacional é outro desafio a ser superado.

No contexto internacional, a Defesa deve buscar a cooperação com as nações que adotam uma abordagem semelhante à de nosso país e enfrentem desafios semelhantes.

Estaremos orientados pela troca de conhecimentos e o desenvolvimento colaborativo da capacidade.

Mas esse intercâmbio, sobretudo quando se tratar de países mais avançados nesse setor e quando houver grande assimetria entre eles, deve ser acompanhado dos cuidados indispensáveis em área de tão grande sensibilidade e com tanto potencial de expor nossas capacidades e vulnerabilidades. Aqui, cooperação e prudência devem andar lado a lado.

Uma discussão conceitual importante, que não me atrevo ainda a propor, é a da distinção e eventual superposição entre defesa e segurança cibernéticas, na linha das diferenças que separam, de forma nem sempre nítida, os temas de defesa dos de segurança pública.

Uma coisa é um grupo querendo atingir nossos interesses. Outra, é outro estado querendo nos prejudicar.

Não tenho dúvidas, por exemplo, de que a proteção das estruturas críticas do país – usinas hidroelétricas, linhas de transmissão, bases de dados do sistema financeiro, para não falar dos próprios meios das Forças Armadas – pertencem à Defesa.

A identificação e perseguição de *hackers* ou *crackers* é tarefa da segurança. Mas há muitas áreas cinzentas entre uma e outra.

Essa questão seria, por si mesma, matéria para um seminário. Mas não quero precipitar discussão que chegará a seu tempo.

★ ★ ★

Maquiavel, no clássico *O Príncipe*, adverte ser erro comum "não levar em conta a tempestade durante a bonança". E, em nosso país pacífico, vivemos prolongada bonança.

Ainda não conhecemos de forma sistemática a "tempestade" no domínio cibernético, mas já vislumbramos com nitidez as formações sombrias que já se acumulam no horizonte.

É causa de especial receio a rapidez com que se condensam e difundem novas ameaças.

Debates como os que se iniciam hoje nos ajudam a construir os abrigos nos quais nos protegeremos contra esses novos riscos.

Dando novamente as boas vindas a todos os participantes, declaro aberto o III Seminário de Defesa Cibernética do Ministério da Defesa.

Muito obrigado.