CIBERGUERRA, INTELIGÊNCIA CIBERNÉTICA E SEGURANÇA VIRTUAL: alguns aspectos

Emerson Wendt*

"Se tutto deve rimanere com'è, è necessario che tutto cambi.
Se tudo deve permanecer como é, é necessário que tudo mude."

Giuseppe Tomasi di Lampedusa

Resumo

A Internet trouxe melhorias na comunicação e na interação social jamais imagináveis. Com esse advento, também vieram as situações incidentes, de vulnerabilidades de segurança e exploração de suas falhas. Grande parte dos serviços essenciais estão disponíveis graças às redes de computadores, interligados e gerenciados remotamente. A vulnerabilidade desses serviços frente à insegurança virtual é uma preocupação, somente combatida com ações proativas e de controle/monitoramento por meio de análise de Inteligência. Insere-se aí um novo conceito, de Inteligência cibernética, com o objetivo de subsidiar decisões governamentais ou não nas ações preventivas de segurança no mundo virtual e de repressão aos delitos ocorridos.

Introdução

Os ataques cibernéticos e as falhas de segurança nas redes, públicas e privadas, e principalmente na web são um problema de constante preocupação para os principais analistas mundiais e as empresas/profissionais de segurança da informação e *web security*.

Neste diapasão é que se insere o presente trabalho, cujo objetivo é avaliar a importância quanto à análise do cenário internacional e brasileiro relativo à segurança virtual, e a observação de aspectos relativos às análises de incidentes de segurança, aos mecanismos de detecção das ameaças virtuais, às políticas públicas e/ou privadas aplicadas e à estipulação de um método, baseado na atividade e nas ações de Inteligência, de obtenção, análise e produção de conhecimentos.

Este processo proposto tem por objetivo principal a utilização de um método de avaliação do cenário atual brasileiro quanto à "guerra cibernética" e seus efeitos, com uma análise conteudista que deve in-

* Delegado da Polícia Civil do RS e atuante em investigações de crime organizado, crimes cibernéticos, interceptação de sinais e telefonia. Foi administrador do Sistema Guardião e Coordenador do Serviço de Interceptação de Sinais da SENASP/RS (2007 a 2009). Coordenador e docente de cursos no CGI/SENASP e na Academia de Polícia Civil/RS.

cluir os principais e mais graves incidentes reportados aos órgãos públicos e privados envolvidos[1], verificação das eventuais sub-notificações, efeitos sociais e repercussões quanto à (in)existência de políticas públicas de detecção e resposta às ameaças virtuais.

Esse método de avaliação e resposta podemos, pois, denominar de Inteligência Cibernética ou *cyber intelligence*, cujo conteúdo e abrangência serão explicados no decorrer deste estudo prévio.

Este trabalho abordará, então, a Inteligência Cibernética como processo de produção de conhecimentos vinculados ao ciberespaço, enfocando e objetivando a segurança virtual necessária, tanto no aspecto macro e/ou coletivo, quanto no individual ou micro.

Em busca de um conceito de Inteligência Cibernética

Não é fácil começar a falar de um tema, cujo referencial teórico é escasso e existem apenas anotações genéricas, ao menos no Brasil. Vários países, em cujo território há preocupação com atos terroristas, já estão atentos à Segurança Cibernética (*Cybersecurity*) e, por consequência, à Inteligência cibernética (C*yber Intelligence*). O melhor exemplo é os Estados Unidos, cujo Presidente Barack Obama lançou recentemente o prospecto Cybersecurity (ESTADOS UNIDOS, 2010) com várias medidas prioritárias, incluindo a criação de um Comando Cibernético nas Forças Armadas americanas.

Afinal, o que é Inteligência Cibernética? O assunto não pode ser tratado em separado e sem passarmos, preliminarmente, pelo tema da Guerra Cibernética ou Ciberguerra (termo também escrito com 'y' – Cyberguerra – ou mencionado como no vocabulário na língua inglesa – *Cyber war)*. Para efeitos deste trabalho usaremos ou o termo Guerra Cibernética ou o termo Ciberguerra.

Fernando G. Sampaio (2001) refere que a Ciberguerra tem suas origens e conceito vinculados ao que é a "técnica cibernética", pois a palavra tem origem grega, "*kybernetiké* e significa a arte de controle, exercida pelo piloto sobre o navio e sua rota". E continua: "E, sendo a cibernética a arte de comandar ou controlar, sua forma primordial de agir é pelo comando ou controle de **todo ciclo de informações**." (grifo nosso.)

Em definição simplista, a 'Guerra Cibernética' é uma ação ou conjunto associado de ações com uso de computadores ou rede de computadores para levar a cabo uma guerra no ciberespaço, retirar de operação serviços de internet e/ou de uso normal da população (energia, água, etc.) ou propagar códigos maliciosos pela rede (vírus, *trojans, worms* etc.).

O conceito acima para ser bem compreendido tem de ser, necessariamente, analisado de forma particionada. Então, vejamos:

[1] Por exemplo, os Centros de Resposta e Tratamento de Incidentes de Segurança de Universidades (CSIRT's) e/ou empresas. CSIRT significa *Computer Security Incidente Response Team* ou Grupo de Resposta a Incidentes de Segurança em Computadores.

- **uma ação ou conjunto associado de ações**: revela que um ataque cibernético pode ser praticado por um indivíduo, um grupo de indivíduos, uma organização específica ou um Estado, usando apenas uma máquina ou um conjunto de máquinas, remotas ou não, mas que têm um fim determinado ou determinável, que pode ser por pura necessidade de reconhecimento, pelo desafio imposto (por si, pelo grupo ou pela sociedade), tais como político-ideológico, financeiro e/ou religioso (*v.g.* o grupo terrorista *al Qaeda)*. Pode ter consequências criminosas ou não, dependendo da legislação de cada país;

- **uso de computadores ou rede de computadores**: os ataques podem ser planejados e executados de um local específico ou através de uma rede de computadores (logicamente, qualquer dispositivo ou grupo de dispositivos que possam se conectar à internet), como ocorre no caso das chamadas *botnets*, quando milhares de máquinas podem ser executadas remotamente pelos criminosos;

Segundo J. M. Araújo Filho (2010, pt. 2), no artigo "Ciberterrorismo e Cibercrime: o Brasil está preparado?" as *botnets* têm se tornado

> [...] *uma ferramenta fundamental para o "cibercrime", em parte porque elas podem ser projetadas para atacar diferentes sistemas de computadores de forma muito eficaz e porque um usuário mal-intencionado, sem possuir fortes habilidades técnicas, pode iniciar estes ataques a partir do ciberespaço, simplesmente alugando serviços de "botnet" em parceria com um "cibercriminoso", tal como vem ocorrendo na atualidade, principalmente envolvendo a máfia russa.*

O mesmo autor define *botnets* ou "redes bot":

> [...] **são constituídas por um grande número de computadores infectados com algum tipo de código malicioso, e que podem ser controlados remotamente através de comandos enviados pela Internet**. Centenas ou milhares de computadores infectados por estes códigos podem funcionar em conjunto para interromper ou bloquear o tráfego da Internet para as vítimas-alvo, coletar informações, ou para distribuir spam, vírus ou outros códigos maliciosos. (grifos nossos)

- **guerra no ciberespaço:** uma definição trazida por Duarte (1999) refere que o ciberespaço é "a trama informacional construída pelo entrelaçamento de meios de telecomunicação e informática, tanto digitais quanto analógicos, em escala global ou regional". Este conceito abrange, portanto, todos os meios onde pode ocorrer a ciberguerra, como, por exemplo onde ocorrem as CMCs (Comunicações Mediadas por Computadores);

- **retirando de operação serviços de internet**: significa que a ação desenvolvida pelos *hackers* tem por objetivo a retirada de um determinado site e/ou serviço dos provedores de internet, como o que ocorreu com o provedor *Speed***,** da Telefônica de São Paulo, quando houve um envenenamento de DNS[2].

[2] Informações sobre: COMO funciona o envenenamento de DNS. Computerword, São Paulo, 2010. Disponível em: <http://computerworld.uol.com.br/slide-shows/ como-funciona-o-envenenamento-de-dns/>. Acesso em 10 dez 2010.

Alguns aspectos são importantes, visando a diferenciação de algumas ações criminosas, o procedimento de ação de um envenenamento de DNS é o seguinte: o servidor do criminoso injeta um endereço falso dentro do servidor de DNS e; 1. O criminoso intervém entre o servidor de cache, o servidor de autorização e o usuário; 2. O criminoso é mais rápido do que o servidor de DNS de autorização, tentando dar ao servidor de cache uma resposta falsa; 3. Para que o servidor DNS aceite a resposta falsa, ela precisa ter os mesmos parâmetros de *query* da resposta legítima. O envenenamento de DNS, portanto, funciona diferenciado do ataque de negação de serviço, pois naquele o serviço não é negado e sim há um redirecionamento a uma página falsa e/ou com conteúdo malicioso.

Importante observar que o ataque de negação de serviço (DoS ou *Denial of Service*) (ATAQUE..., 2010):

> [...] é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Alvos típicos são servidores web, e o ataque tenta tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. Os ataques de negação de serviço são feitos geralmente de duas formas: 1) Forçar o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento por exemplo) de forma que ele não pode mais fornecer seu serviço; 2) Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não comunicarem-se adequadamente.

Ambos diferem do ataque de negação de serviço distribuído, também conhecido por ataque DDoS, quando (ibidem):

> Um computador mestre ("Master") pode ter sob seu comando até milhares de computadores zumbis ("Zombies"). Nestes casos, as tarefas de ataque de negação de serviço são distribuídas a um "exército" de máquinas escravizadas.

- **serviços de uso normal da população (energia, água, etc.) e do Estado**: revela que uma ação hacker pode atingir as chamadas infraestruturas críticas de uma região e/ou país e redundar em resultados catastróficos e imensuráveis quando, *v.g.*, provocar um colapso na rede de transmissão de energia, causando apagão e/ou retardando o retorno do serviço[3]. É claro que esses serviços serão afetados porquanto usem o computador como forma de apoio, execução e controle. Da mesma forma, o ataque pode ocorrer aos órgãos de um país, atingindo sua soberania e segurança;

Sampaio (2001), sobre alvos preferenciais da Ciberguerra, menciona que são aqueles que se baseiam em

> [...] programas de computadores ou gerenciam os seguintes aspectos: 1. comando das redes de distribuição de energia elétrica; 2. comando das redes de distribuição de água potável; 3. comando das redes de direção das estradas de ferro; 4. comando das redes de direção do tráfego aéreo; 5. comando das redes de informação de emergência (pronto-socorro, polícia e bombeiros). 6. comando das redes

[3] Segundo pesquisadores do instituto de pesquisa SINTEF as plataformas de petróleo "operando em alto mar têm sistemas inadequados de segurança da informação, o que as deixa altamente vulneráveis aos ataques de hackers, vírus e vermes digitais". (PLATAFORMA..., 2010).

> bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registrado em nome dos cidadãos (o potencial para o caos e a desmoralização de um país embutido neste tipo de ataque é por demais evidente); 7. comando das redes de comunicações em geral, em particular (redes de estações de rádio e televisão); 8. comando dos "links" com sistemas de satélites artificiais (fornecedores de sistemas telefônicos,de sistemas de sinais para TV, de previsão de tempo, e de sistema GPS); 9. comandos das redes dos Ministérios da Defesa e, também do Banco Central e outros ministérios chave (Justiça, Interior etc); 10. comandos dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral.

- **propagando códigos maliciosos pela rede**: uma ação no ciberespaço, em grande escala e bem planejada, pode fazer com que cavalos de tróia, vírus, *worms* etc. possam ser espalhados pela rede através de páginas web, de e-mails (*phishing scam*), de comunicadores instantâneos (*Windows Live Messenger, Pidgin, GTalk* etc.) e de redes sociais (*Orkut, Twitter, Facebook* etc.), entre outras formas possíveis.

Cavalos de Tróia ou *trojans* são programas que, aparentemente inofensivos, são distribuídos para causar danos ao computador ou para captura de informações confidenciais do usuário. Ao criminoso virtual já não importa causar dano à máquina do usuário, pois isso não lhe traz recursos financeiros, fazendo com que a principal meta dos *trojans* seja a coleta anônima e/ou invisível de informações dos internautas.

A diferença entre os *trojans* dos vírus é que estes programas têm a finalidade destrutiva, com características que se agregam ao código de outros programas, principalmente do sistema operacional, causando modificações indevidas no seu processamento normal, causando danos leves e inoportunos até destrutivos e irreparáveis.

Segundo o site da Microsoft (2004) o *worm* é uma subclasse dos vírus e

> [...] cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente. Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que o *worm* contamina o sistema, ele se desloca sozinho. O grande perigo dos *worms* é a sua capacidade de se replicar em grande volume. Por exemplo, um worm pode enviar cópias de si mesmo a todas as pessoas que constam no seu catálogo de endereços de email, e os computadores dessas pessoas passam a fazer o mesmo, causando um efeito dominó de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a Internet como um todo. Quando novos *worms* são lançados, eles se alastram muito rapidamente. Eles obstruem redes e provavelmente fazem com que você (e todos os outros) tenha de esperar um tempo maior para abrir páginas na Internet.

Phishing Scam são e-mails fraudulentos que convidam os internautas a recadastrar dados bancários, a confirmar números de cartões, senhas, a informar outros dados confidenciais em falsas *homepages*, a instalar um novo aplicativo de segurança, usando para tanto de engenharia social (meio empregado para que uma pessoa repasse informações ou execute alguma ação).

Para melhor entendimento, seguimos quanto à análise do tema.

Analisando a Guerra Cibernética e a Inteligência Cibernética

O tema da *Guerra Cibernética* é, portanto, bastante abrangente. Atinge circunstâncias antes tidas apenas no mundo real, incluindo a ameaça à soberania de um país que, a par da tecnologia e das evoluções constantes dos mecanismos de tráfego de dados e voz, tenderia a evoluir e a aprimorar mecanismos protetivos.

Em outras palavras, uma vez ocorrendo ameaça à soberania, a tendência lógica é de criação de mecanismos de defesa e reação, caso necessários. No entanto, não é o que se observa! Da mesma forma que os setores públicos, o setor privado também sofre os efeitos dessa guerra e da espionagem industrial, cada vez mais realizada através dos meios tecnológicos, pois é feita com menor risco e um custo operacional aceitável.

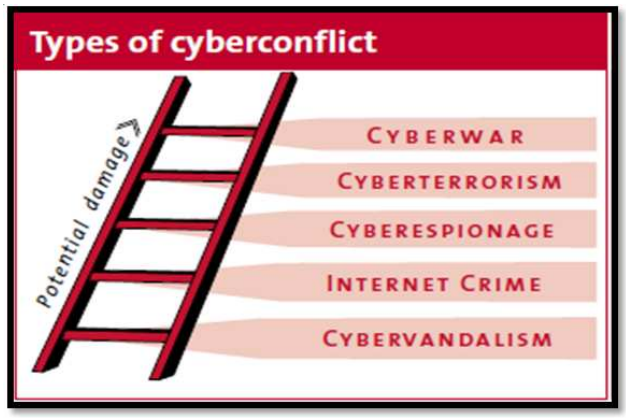
...'Inteligência Cibernética', capaz de propiciar conhecimentos necessários à defesa e otimização da capacidade proativa de resposta(s) em caso de uma ameaça virtual iminente/em curso.

Tido como necessário, um ou vários mecanismos de defesa, similares aos existentes no mundo real, não se pode vislumbrá-lo(s) sem uma prévia análise e/ou atitude proativa. E é esse o propósito de uma *Inteligência cibernética,* capaz de propiciar conhecimentos necessários à defesa e otimização da capacidade proativa de resposta(s) em caso de uma ameaça virtual iminente/em curso.

No entanto, as ameaças no mundo virtual tendem a ser mais rápidas e sofisticadas que as do mundo real, o que gera um tempo menor de reação por parte do alvo a ser atingido. Por isso, ações de Inteligência, baseadas em mecanismos específicos de hardware e software (TI), aliados ao conhecimento humano, podem ser fundamentais à perfeita defesa e à melhor reação, fazendo com que países e organizações públicas e privadas posicionem-se ou não adequadamente em relação à sua segurança na rede (*cyber security*).

'Adequadamente ou não' significa dizer que nem sempre os países e/ou empresas dão a real dimensão ao problema e, por conseqüência, à resposta a ele. Os investimentos são extremamente baixos, o que torna as (re)ações restritas, isso para não dizer minúsculas. Importante referir que não há propriamente distinção entre alvos civis e militares numa eventual *Guerra Cibernética,* o que exige um constante acompanhamento e análise dos fatores, pois as infraestruturas críticas estão expostas às ações, tanto no mundo real quanto no virtual.

Complementando, conforme o CSS (CAVERTY, 2010), a ordem de observação e importância para análise do tema da segurança virtual ou cibernética pode ser caracterizada de acordo com a potencialidade do perigo. Vejamos:



De acordo com o infográfico acima, dentro dos temas tratados, em potencialidade, estão, em uma escala ascendente:

1) **cibervandalismo**, caracterizado pelas ações hackers motivadas pelo desafio, pela brincadeira e/ou desprezo[4];

2) **crime cibernético** ou **cibercrime**, onde a motivação ultrapassa o simples desafio e acarreta algum tipo de dano tutelado penalmente, caracterizando-se, portanto, em um crime;

3) **ciberespionagem**, que não deixa de ser necessariamente um crime cibernético, porém com motivações específicas e voltadas à obtenção de segredos comerciais, industriais e governamentais, cuja detecção é sensível e depende de vários fatores[5];

4) **ciberterrorismo**, com objetivos também específicos de ataques virtuais às infraestruturas críticas de uma região e/ou um país, capazes de ocasionar um colapso nos serviços básicos afetados. Ou, no dizer de Dorothy E. Denning, citado por Araújo Filho (2010), ciberterrorismo são "operações praticadas por especialistas em recursos informáticos e com motivações políticas, destinadas a causar graves prejuízos, como perda de vida ou grave dano econômico"; e,

5) **ciberguerra**, quando os objetivos vão além de um ataque cibernético às infraestruturas críticas, afetando a soberania da nação atacada.

Aliás, sobre o tema**,** Santos e Monteiro (2010) enfatizam que:

> [...] a segurança global está se tornando mais vulnerável e mais exposta. Essa inexorável tendência para a eficiência reduz a robustez dos sistemas, através da eliminação de redundâncias (métodos de backup) e degradando resistências (longevidade dos instrumentos), resultando numa fragilidade destes, inclusive em suas engenharias, o que significa que eles estão sujeitos a desastrosas falhas sistêmicas devido a ataques em pontos críticos.
>
> Falhas em cascata podem ocorrer quando vulnerabilidades individuais, que podem ser inócuas ou manejáveis isoladamente, mas com o potencial para iniciar efeitos dominó através de complexos sistemas interdependentes entre si, são atingidas.

[4] Importante referir que algumas condutas hoje tidas como cibervandalismo não são previstas, na legislação brasileira, como crimes, ficando sua apuração, quando necessária, apenas na seara administrativa e/ou cível. O exemplo é o *defacement*, que é a desconstrução de uma página web que apresenta uma falha de segurança ou vulnerabilidade não corrigida pelo seu administrador. Mais detalhes conceituais em: DEFACEMENT. In: Wikipedia. Disponível em: <http://pt.wikipedia.org/wiki/Defacement>. Acesso em: 05 nov. 2010.

[5] Eventual caso de espionagem através da web pode ser configurado como crime de interceptação ilegal de dados telemáticos, previsto no art. 10 da Lei 9296/96, com a seguinte redação: "*Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa".*

> Por exemplo, um bem sucedido ataque ao aparato computacional de um porto doméstico pode ter um impacto global no comércio internacional, no fornecimento de energia e produção, devido à interdependência do sistema global de navegação. Da mesma maneira, um ataque cibernético ao sistema de controle de tráfego aéreo colocaria não só vidas em risco, mas ameaçaria debilitar uma miríade de atividades econômicas dependentes do funcionamento do transporte aéreo.

Em uma reportagem Shanker (2010), afirma que Keith Alexander, comandante escolhido por Barack Obama, para o Comando Cibernético das forças armadas americanas, em resposta ao Congresso daquele país, delineou *o* "amplo campo de batalha pretendido para o novo comando de guerra computadorizada, e identificou a espécie de alvo que seu novo quartel-general poderia ser instruído a atacar". Na opinião do autor:

> As forças armadas estão penetrando em território incógnito, no seu esforço para defender os interesses nacionais e executar operações ofensivas em redes de computadores [...] e os países do mundo nem mesmo concordam com relação ao que constitui um ataque cibernético, ou quanto à resposta adequada.

O Brasil recentemente tem buscado estudar o tema, também enfocando sua estratégia nos órgãos militares[6]. O Gabinete de Segurança Institucional, vinculado à Presidência da República, terá um papel fundamental, visando a análise de todo o contexto da segurança virtual no Brasil, pois é o órgão de Inteligência que poderá avaliar todas as circunstâncias relacionadas às redes privadas e públicas.

Alguns setores precisarão modificar 'os papéis' atualmente desempenhados no contexto nacional da segurança cibernética, como é o caso do Comitê Gestor da Internet (CGI.br), que como mero recebedor de informações sobre os incidentes na internet brasileira, mantém-se neutro e não repassa avaliações a respeito do conteúdo dos problemas a ele relatados (ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br)[7].

Assim, quais os fatores fundamentais e que devem sofrer análise? O que pode auxiliar uma ação de defesa e pró-ação eficaz? Quais são as principais vulnerabilidades virtuais? Quais as características dos códigos maliciosos distribuídos na web? Como funciona e o que é a ciberespionagem? Qual a quantidade de movimentação financeira clandestina no mundo virtual? Quais os métodos de detecção de ameaças? E, finalmente, quem pode responder a essas questões?

Como visto, vários questionamentos exigem resposta e aí é que está o trabalho da *Cyber Intelligence* ou da Inteligência Cibernética. Serve ela para orientar os organismos públicos e privados no sentido de acompanhar, detectar e analisar as ameaças virtuais, sugerindo ações proativas e abrangentes, de maneira constante, onde as máximas estão na resposta e na solução rápida.

---

[6] Segundo Gen. Antonino dos Santos Guerra Neto, do Centro de Comunicações e Guerra Eletrônica (CCOMGEX), há um trabalho em andamento para desenvolver toda a camada legal do núcleo de guerra cibernética. "Ele servirá para o centro de guerra cibernética do Exército. Já há uma área cuidando de ferramentas, outra de treinamento, uma para defesa de redes e outra para desenvolvimento de formas para a parte ofensiva."

[7] O CERT.br cataloga, coleta e divulga estatísticas sobre os incidentes na internet do Brasil (www.cert.br).

A bem da verdade, essas respostas servirão não só para orientar as medidas administrativas e preventivas, mas também para delinear os aspectos repressivos, a cargo das policiais judiciárias brasileiras: Polícias Civis e Federal.

Com isso, a Inteligência Cibernética nada mais é do que um processo que leva em conta o ciberespaço, objetivando a obtenção, a análise e a capacidade de produção de conhecimentos baseados nas ameaças virtuais e com caráter prospectivo, suficientes para permitir formulações, decisões e ações de defesa e resposta imediatas visando à segurança virtual de uma empresa, organização e/ou Estado.

Concluindo este raciocínio introdutório ao tema, os conteúdos de abrangência da Inteligência Cibernética são:

1. Os ataques às redes, públicas ou privadas, e às páginas web.

2. Análise das vulnerabilidades sobre as redes, sistemas e serviços existentes, enfocando o entrelaçamento à teia regional, nacional e/ou mundial de computadores.

3. Constante análise e acompanhamento dos códigos maliciosos distribuídos na web, observando padrões, métodos e formas de disseminação.

4. Enfoque na engenharia social virtual e nos efeitos danosos, principalmente nas fraudes eletrônicas.

5. Mais especificamente, monitorar as distribuições de *phishing scam* e outros códigos maliciosos (*malwares*), tanto por web sites quanto por e-mail e as demais formas de disseminação, com atenção especial para as redes sociais e os comunicadores instantâneos de mensagens.

6. Observação e catalogamento dos casos de espionagem digital, com abordagem dos casos relatados e verificação dos serviços da espécie oferecidos via internet.

7. Intenso monitoramento a respeito de *adwares*, *worms*, *rootkits*, *spywares*, vírus e cavalos de tróia, com observância do comportamento, poliformismo, finalidade e forma de difusão.

8. Detectar e monitorar os dados sobre fraudes eletrônicas e o correspondente valor financeiro decorrente das ações dos criminosos virtuais.

9. Monitoramento da origem externa e interna dos ataques e da distribuição dos códigos maliciosos, possibilitando a demarcação de estratégias de prevenção e/ou repressão.

10. Verificação e catalogamento das ações e dos mecanismos de hardware e software de detecção de ameaças e de respostas imediatas às ameaças virtuais.

11. Ao final, proposição de políticas de contingência para os casos de ciberterrorismo, preparando os organismos públicos e privados em relação às ameaças existentes e, em ocorrendo a ação, procurando minimizar os efeitos decorrentes por meio do retorno quase que imediato das infraestruturas atingidas.

Em suma, a guerra cibernética, em seu aspecto amplo e, mais especificamente, o ciberterrorrismo tornam-se uma pre-

ocupação constante e que está em nosso meio, o que enseja a adoção de medidas fundamentais e proativas de detecção e reação eficazes.

No Relatório de Criminologia Virtual de 2009, da empresa *McAfee*, citado por Santos e Monteiro (2010), consta que "O conflito cibernético internacional chegou ao ponto de não ser mais apenas uma teoria, mas uma ameaça significativa com a qual os países já estão lutando a portas fechadas".

... a Inteligência Cibernética pode propor soluções tanto do ponto de vista tático (em casos específicos) quanto do ponto de vista estratégico (análise macro/complexa)

Conclusão

Acredita-se, assim, que a Inteligência Cibernética pode propor soluções tanto do ponto de vista tático (em casos específicos) quanto do ponto de vista estratégico (análise macro/complexa), situações estas em que o poder público ou as organizações privadas poderão antecipar-se aos eventos cibernéticos ou reagir adequadamente frente às questões detectadas, tratadas e direcionadas.

Não se pode ignorar que estamos diante de problemas sérios de segurança virtual, principalmente em nosso país, que é desprovido de regras mais claras quanto à organização, o funcionamento e o controle da internet. Casos menos complexos de ataques virtuais e/ou fraudes eletrônicas, embora facilmente resolvidos, não são analisados conjuntamente com outras circunstâncias similares, o que poderia redundar em uma grande resposta, tanto do ponto de vista preventivo quanto repressivo.

Percebe-se, de outra parte, que a população brasileira não está adaptada e devidamente orientada em relação aos problemas de segurança virtual, necessitando de campanhas oficiais e direcionadas aos problemas existentes e sua prevenção.

Não diferente e preocupante são os casos de maior complexidade e gravidade – que conceitualmente podem ser tidos como crimes de alta tecnologia -, derivados de constante exploração de vulnerabilidades de sistemas e redes, públicas e privadas, mas fundamentais ao bom andamento de serviços, essenciais ou não. Nesse diapasão, um estudo aprofundado e metódico de Inteligência, principalmente quanto aos fatos reportados e àqueles que, por uma razão ou outra, deixaram de sê-lo, pode dar um direcionamento quanto às ações preventivas e reativas necessárias.

É extremamente importante o trabalho que o Exército Brasileiro vem fazendo em relação ao assunto. Porém, no Brasil existem inúmeras empresas privadas atuando onde o poder público não atua, ou seja, nos serviços essenciais, e o questionamento é, justamente, se existe um controle de segurança orgânica e/ou virtual em relação a elas.

Exemplo claro desta preocupação é o chamado vírus *Stuxnet*, descoberto em junho de 2010 pela empresa bielorrussa de antivírus *VirusBlokAda*, sendo o pri-

meiro *worm* que espiona e reprograma sistemas industriais. Ele foi especificamente escrito para atacar o sistema de controle industrial *SCADA*, usado para controlar e monitorar processos industriais, tendo como características diferenciadoras: 1) primeiro *worm* conhecido a ter como alvo infraestrutura industrial crítica; 2) o primeiro *worm* de computador a incluir um *rootkit* de CLP; 3) o alvo provável do *worm* foi a infraestrutura do Irã, que utiliza o sistema de controle da Siemens, mais especificamente as instalações nucleares iranianas; 4) além do Irã, também teriam sido afetados pelo *worm* Indonésia, Índia, Estados Unidos, Austrália, Inglaterra, Malásia, e Paquistão (STUXNET, 2010).

O *case Stuxnet* tornou-se uma coerente preocupação aos governos e empresas de segurança. Tanto que a Kaspersky Labs[8], empresa antivírus, anunciou que o *worm* é "um protótipo funcional e temível de uma cyber-arma que dará início a uma nova corrida armamentista no mundo".

Portanto, há muito que ser feito. Propõe-se apenas que o debate seja iniciado acerca da Inteligência cibernética, incluindo todos os setores encarregados e/ou que podem ser afetados pelos incidentes na internet brasileira.

Referências

ARAÚJO FILHO, José Mariano. *Ciberterrorismo e Cibercrime:* o Brasil está preparado? Parte 1 e 2. Disponível em: <http://mariano.delegadodepolicia.com/ ciberterrorismo-e-cibercrime-o-brasil-esta-preparado-parte-2/>. Acesso em: 18 mar. 2010.

ATAQUE aos servidores. Comfrong.blog. Disponpível em: <http://comfrong.br/blog/ataque/>. Acesso em: abr. 2011.

CAVALCANTI, Vitor. Brasil prepara centro de guerra cibernética. *It Web,* 16 set 2010. Disponível em: <http://www.itweb.com.br/noticias/ index.asp?cod=71857>. Acesso em: 07 nov. 2010.

CAVERTY, Myrian Dunn. Cyberwar: concept, status quo, and limitations. *CSS Analysis in Security Policy.* Zurich, n. 71, april 2010. Disponível em: <http://xa.yimg.com/kq/groups/25230945/1232123509/name/CSS_Analysis_71.pdf>. Acesso em: 19 abr. 2010.

COMO funciona o envenenamento de DNS. *Computerword*, São Paulo, 2010. Disponível em: <http://computerword.uol.com.br/.../como-funciona-o-envenenamento-de-dns/>. Acesso em: 19 abr. 2010.

DUARTE, Fábio. Inteligência Cibernética: introdução ao assunto. *Revista Comunicação e Educação*, São Paulo, ano V, n. 14, jan./abr. 1999.

ESTADOS UNIDOS. White House. Executive office. *The Comprenhensive National Cybersecurity Initiative.* Disponível em: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>. Acesso em: 08 mar. 2010.

[8] Mc-MILLAN, Robert. *Siemens: Stuxnet Worm Hit Industrial Systems.* Pc Word, 14 sep 2010. Disponível em: <http://www.pcworld.com/businesscenter/article/205420siemens_stuxnet_worm_hit_industrial_systems.htm>. Acesso em: 05 nov. 2010.

GUIMARÃES JR., Mário J. L. *O Ciberespaço como Cenário para as Ciências Sociais*. Florianópolis, 1999. Disponível em: <http://www.cfh.ufsc.br/~guima/papers/ciber_cenario. html>. Acesso em: 8 mar. 2010.

MICROSOFT. O que são Virus, Warms e Cavalo de Tróia? 9 mar. 2004. Disponível em: <http://www.microsoft.com/brasil/athome/security/viruses/virus101.mspx>. Acesso em: 08 mar. 2010.

PLATAFORMAS de petróleo estão vulneráveis ao ataque de hackers. Blog Cienteca. Disponível em: <http://cienteca.wordpress.com/2009/08/21/ plataformas-de-petroleo-estao-vulneraveis-ao-ataque-de-hackers/>. Acesso em: 03 maio 2010.

SAMPAIO, Fernando G. *Ciberguerra, Guerra Eletrônica e Informacional:* Um novo desafio estratégico. Porto Alegre: Escola Superior de Geopolítica e Estratégia, 2001. Disponível em: <http://www.defesanet.com.br/esge/ciberguerra. pdf>. fls 3-4. Acesso em: 10 out. 2010.

SANTOS, Coriolano Aurélio de Almeida Camargo; MONTEIRO, Renato Leite. *Estruturas Críticas:* o próximo alvo. São Paulo: OAB/SP, 2010. Disponível em <http://www2.oabsp.org.br/asp/comissoes/crimes_eletronicos/noticias/proximo_alvo. pdf >. Acesso em: 15 abr. 2010.

SHANKER, Thom. *Comando de guerra cibernética americano vê lacunas nas leis*. Portal Terra, 15 abr 2010. Disponível em: <http://tecnologia.terra.com.br/interna/0,,OI4383762-EI4802,00.html>. Acesso em: 16 abr. 2010.

STUXNET. In: Wikipedia. Disponível em <http://pt.wikipedia.org/wiki/Stuxnet>. Acesso em: 05 nov. 2010.