O USO DA TECNOLOGIA DA INFORMAÇÃO COMO ARMA DE ATAQUE.

Paulo Sérgio de Araújo[1]

FATEC OURINHOS – Faculdade de Tecnologia de Ourinhos
Av. Vitalina Marcusso, 1400 – Campus Universitário
CEP 19910-206 – Ourinhos, SP – Brasil
Orientadores: Sérgio Duque Castilho, Paulo Roberto Galego Hernandes Júnior.
Novembro/2011

RESUMO

O objetivo deste artigo é abordar os avanços tecnológicos na área da tecnologia da informação sofridos nos últimos tempos e seus reflexos na sociedade atual. Apontar o crescimento dos crimes virtuais e a dificuldade da aplicação de leis para a punição dos infratores que muitas vezes se escondem por detrás de leis que os privilegiam. Apresentar uma breve definição do termo Crime Cibernético e fazer uma análise dos principais conceitos envolvidos no tema Guerra Cibernética.

Palavras chave: avanço tecnológico, Crime Cibernético, Guerra Cibernética.

1. INTRODUÇÃO

O constante avanço tecnológico tem mudado a forma de inter-relacionamento da sociedade moderna nas últimas décadas, atualmente a facilidade de acesso à informação através das mídias é dinâmica. Isto faz com que o fato seja revelado no momento que ocorre, não mais importando onde ocorra. A diminuição do tamanho e do valor dos equipamentos fez com que grande parte da população se mantenha a par das novidades da tecnologia.

Com a disseminação destes equipamentos, fez-se necessário a criação de redes que pudessem interligá-los, e hoje, dispositivos como computadores pessoais, *smartphones*, *tablets* entre outros traz ao cidadão a disponibilidade de recursos que lhe permitem desde efetuar transações bancárias a facilidade das compras sem sair de casa.

[1] Graduando em Análise de Sistemas e Tecnologia da Informação com habilitação em Tecnólogo em Segurança da Informação.
paulo-araujo@msn.com

Esta vasta gama de conectividade possibilitou a criação de novas ferramentas como as redes sociais, espaços virtuais onde é possível encontrar uma enorme diversidade cultural e política. Atualmente essas redes apresentam um papel de grande importância na sociedade, pois através delas já se organizam movimentos capazes de derrubar o poder de governos ditadores ao redor do mundo.

Mas nem tudo é utilizado para o bem, com o advento da conectividade também surgiram os crimes virtuais, a pedofilia, roubos e exposição de informações sigilosas, etc.

Muitas vezes a falta de conhecimento do usuário ou a má utilização das politicas de segurança nas corporações, tornam informações sigilosas acessíveis a qualquer pessoa que queira se utilizar de dados de terceiros para cometimento de crimes ou fraudes.

O crescente acesso à internet pelos países do Oriente Médio demonstra o crescimento vertiginoso do acesso a este tipo de mídia na última década (EL-GUINDY, p16, 2008).

Dados recentes (*INTERNET WORLD STATS*) apontam um crescimento de 1.825,3% no número de usuários de Internet em uma década, em uma região que representa apenas 3,1% da população mundial. Vale ressaltar que neste mesmo espaço de tempo, o crescimento mundial foi de 444,8%.

Com todo este crescimento, os países do oriente médio vêm sofrendo constantes ataques cibernéticos devido à dificuldade de implantação de políticas de segurança da informação; em grande parte devido ao fato das documentações estarem em inglês, o que apresenta um enorme entrave a sua implantação (EL-GUINDY, p17, 2008).

Com a massiva utilização dos computadores e suas redes de informações não só o usuário doméstico ou as grandes corporações passaram a se tornar dependentes destes serviços, secretarias e departamentos governamentais interligam-se e utilizam redes para a troca de informações, muitas vezes sigilosas; processos administrativos que gastavam longo tempo em transito entre departamentos ou unidades da federação hoje estão a um clique do *mouse*. Toda essa informação transitando pela *Internet* torna-se uma ameaça potencial para as nações. Tornou-se evidente que se dois países possuem divergências e/ou hostilidades, a exploração da rede do oponente constitui uma forte ferramenta para obtenção de vantagens estratégicas ou até mesmo a destruição de informações ou equipamentos. A este tipo de ataque dá-se o nome de Guerra Cibernética.

2. CRIME CIBERNÉTICO

A cada dia a *Internet* apresenta ao usuário um mundo de possibilidades, e as facilidades de acesso aos serviços disponibilizados tornam os usuários dependentes dos mesmos. A facilidade em fazer compras, efetuar pagamentos, acessar redes sociais e uma gama inimaginável de serviços e informações ao alcance dos dedos tornam a *Internet* uma grande fonte de pesquisa para pessoas que buscam cometer crimes.

O crime cibernético baseia-se na falta de conhecimento das pessoas em relação aos procedimentos de segurança que devem ser tomados quando disponibilizam seus dados na rede. A falta de programas de proteção nos computadores, ou a não atualização dos mesmos aliados ao uso de engenharia social contribuem para o aumento desta modalidade criminal.

> A Convenção sobre Cibercrime do Conselho da Europa é o primeiro trabalho internacional de fundo sobre crime no ciberespaço. Foi elaborado por um comitê de peritos nacionais, congregados no Conselho da Europa e consiste num documento de direito internacional público. Embora tenham na sua origem, sobretudo, países membros do Conselho da Europa, tem vocação universal. Na sua elaboração participaram vários outros países (Estados Unidos da América, Canadá, Japão e África do Sul) e pretende-se que venha a ser aceite pela generalidade dos países do globo (VERDELHO, et al.,p10, 2003).

O objetivo deste documento é o nivelamento das várias legislações nacionais sobre o tema, propiciar e facilitar a cooperação internacional e facilitar as investigações de natureza criminal. Pois muitos criminosos virtuais se aproveitam de brechas nas leis de alguns países para cometerem seus crimes e escapar da punição.

Segundo o GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS do MINISTÉRIO PÚBLICO FEDERAL, os Estados são obrigados a tipificar as seguintes condutas:

1. Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:

a) acesso doloso e ilegal a um sistema de informática;

b) interceptação ilegal de dados ou comunicações telemáticas;

c) atentado à integridade dos dados;

d) atentado à integridade de um sistema;

e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados;

2. Infrações informáticas:

a) falsificação de dados;

b) estelionatos eletrônicos;

3. Infrações relativas ao conteúdo:

a) pornografia infantil (produção, oferta, procura transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);

b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);

4. Atentado à propriedade intelectual e aos direitos que lhe são conexos.

Um dos crimes cibernéticos de grande repercussão na atualidade é o caso do *site Wikileaks*, que ganhou destaque mundial após divulgar um vídeo de um ataque norte-americano ao Iraque. Segundo noticiou o jornal *The New York Times* (2011), o site divulgou na *Internet* aproximadamente 391.832 documentos secretos sobre a guerra do Iraque, 77 mil documentos confidenciais do Pentágono sobre a guerra do Afeganistão, além do trafego de informações entre o Departamento de Estado Americano e mais de 270 postos diplomáticos americanos ao redor do mundo.

Apesar dos fatos divulgados refletirem informações confidenciais de uma nação, esta ocorrência não configura necessariamente um evento de Guerra Cibernética, pois não há indícios de que o *site* contou com o auxilio de outra nação (fator primordial para que haja evento de Guerra Cibernética) na obtenção e divulgação dos dados.

3. GUERRA CIBERNÉTICA

O termo “Guerra”, desde os primórdios da humanidade se refere a embates onde povos e, posteriormente, nações colocam a prova todo o seu poder destrutivo, seja ele humano, bélico ou tecnológico, com o objetivo único de dominar e subtrair vantagens do inimigo dominado.

Para Lewis (2011), “A guerra é o uso da força militar para atacar outra nação e danificar ou destruir a capacidade e a vontade de resistir. A Guerra Cibernética implicaria um esforço por outra nação ou um grupo politicamente motivado para usar ataques cibernéticos para atingir fins políticos”.

A Guerra Cibernética nada mais é que a evolução do modo de batalha que a humanidade vem aprimorando com o decorrer dos tempos. Esta nova batalha se destaca pelo aparato tecnológico, onde o objetivo principal da nação envolvida é dominar, controlar ou destruir a força do inimigo, através da invasão de seus sistemas de controle informatizados.

Segundo Andress e Winterfeld (2011, p.5) as redes de infraestrutura crítica são os principais alvos de ataque cibernético porque concentram sistemas de comando, controle, gestão e logística, possibilitando o planejamento de pessoal e operações, são, portanto a espinha dorsal da inteligência de capacidades. Atualmente os sistemas de comando e controle, como os controles de armas são ligados à Rede Global de Informações ou possuem *chips* de computadores. Defesa aérea e artilharia atiram munições inteligentes, guiadas por computadores que são capazes de ajustar sua trajetória de voo com base em dados de sistemas de posicionamento global (GPS), permitindo a correta localização do alvo. A nação que detém este forte poder tecnológico certamente possui grande vantagem em relação ao oponente, porém, se seus sistemas forem invadidos, este poder se torna sua maior fraqueza.

Em uma guerra convencional, as ações táticas demandam tempo, pois há a necessidade da movimentação de tropas, equipamentos e uma série de aparatos de infraestrutura. Em um ataque cibernético, bastam apenas algumas pessoas e computadores para desencadear uma ofensiva contra o inimigo.

4. A GUERRA CIBERNÉTICA COMO UMA REALIDADE

Nenhuma nação do mundo teve seu nome envolvido com o fato até o momento, porém recentes acontecimentos nos levam a crer que estamos vivendo uma guerra fria cibernética, onde os atacantes tentam descobrir as vulnerabilidades e poder de ataque do inimigo, evitando ao máximo que o fato se torne público e também temendo uma represália do atacado. Este cuidado se dá ao fato de que diferentemente de um arsenal nuclear ou bélico, é praticamente impossível mensurar a força computacional de uma nação e um ataque deliberado poderia trazer consequências devastadoras ao atacante.

O crescente interesse das nações em busca de formas de ataque e defesa cibernética tem alcançado avanços até então inimagináveis, como o desenvolvimento de algoritmos capazes de causar destruição não só no mundo cibernético, mas também no mundo real.

Nos últimos dois anos, o complexo de Dimona, no deserto do Negev em Israel abriga um projeto ultrassecreto de ensaio crítico visando minar os esforços iranianos de construir armas nucleares. Trata-se de um esforço conjunto entre americanos e israelenses que, segundo informações, teriam construído um *site* de armas nucleares que contém uma série de réplicas das plantas de enriquecimento de urânio iranianas, que serviram de insumo para a criação do software de ataque *Stuxnet* (BROAD; MARKOFF; SANGER, 2011).

Especialistas de segurança europeus alegam que o desenvolvimento deste tipo de ameaça seria inviável sem o auxilio de uma nação. Se desenvolvido por um programador, o vírus levaria aproximadamente 10 anos para ser finalizado, a um custo superior a $10.000.000. A *Symantec* afirma que somente os testes no vírus teriam ocupado de cinco a dez especialistas, por seis meses (SPIEGEL; STARK, 2011).

Em novembro, o jornal *The New York Times* (2010) noticiou que o presidente iraquiano Mahmoud Ahmadinejad se pronunciou sobre o ataque do *Stuxnet* ao programa de enriquecimento de urânio, dizendo que um ataque cibernético havia causado "pequenos problemas com algumas de nossas centrífugas." Felizmente, ele acrescentou, "nossos especialistas descobriram". Dados do Instituto para Ciência e Segurança Internacional, um grupo privado de Washington dão conta de que uma série de falhas ocorridas no complexo de Natanz no Irã, em meados de 2009, tirando de funcionamento 984 centrífugas de urânio.

5. CONSIDERAÇÕES FINAIS

Com este estudo foi possível observar que a *Internet* tornou-se uma ferramenta cotidiana, tanto para uso pessoal quanto profissional. Seus serviços possibilitam, quando utilizados de maneira correta, diversão, informação, comunicação e agilidade no trabalho. Verificou-se que o crescimento das redes de informações e o aumento no tráfego de informações sigilosas trouxeram à tona a modalidade dos crimes virtuais.

Esta dependência das redes de comunicação despertaram as nações para um novo campo de batalha, onde invadir, obter acesso indevido ou controlar infraestruturas se tornou vantagem estratégica no campo de batalha. A Guerra Cibernética sem dúvidas será uma estratégia de grande valia para o futuro militar. Por se tratar de um assunto recente e que o sigilo constitui vantagem estratégica, pouco se divulga sobre o tema e o que se tem acesso, muitas vezes é controverso.

Baseando-se em fontes altamente competentes, o presente estudo busca atingir o objetivo a que se propõe: apresentar as mudanças no modo de vida da população com a popularização dos meios de comunicação e abordar os temas Crime Cibernético e Guerra Cibernética, apresentando suas bases ideológicas, ações e objetos propostos.

6. REFERÊNCIAS

ANDRESS, Jason; WINTERFELD, Steve. Cyber Warfare - **Techniques, Tactics and Tools for Security Practitioners**. Waltham: Elsevier, 2011.

BRASIL. MINISTÉRIO PÚBLICO FEDERAL. PROCURADORIA DA REPÚBLICA NO ESTADO DE SP. GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **CRIMES CIBERNÉTICOS -** Manual Prático de Investigação. Disponível em: <http://www.mpdft.gov.br/portal/pdf/unidades/promotorias/pdij/TAC/Manual_de_Crimes_de__Inform%C3%A1tica_-_vers%C3%A3o_final2.pdf > Acessado em: 09 de abril de 2011.

BROAD, William J.; MARKOFF John; SANGER, David E. Israeli. Test on Worm Called Crucial in Iran Nuclear Delay. **THE NEW YORK TIMES**, Nova Iorque, 15 de janeiro de 2011. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=1&ref=science > Acessado em: 12 de março de 2011.

El-GUINDY, Mohamed N. Cybercrime in the Middle East. **ISSA Journal,** junho de 2008. Disponível em:< http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf> Acesso em: 13 mar 2011.

INTERNET WORLD STATS. **Internet Usage in the Middle East** - Middle East Internet Usage & Population Statistics. Disponível em: <http://www.internetworldstats.com/stats5.htm> Acesso em: 08 abr 2011.

LEWIS, James A. The Cyber War Has Not Begun **Center for Strategic and International Studies**, Washington D.C, 2010. Disponível em: <http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf > Acessado em: 16 de março de 2011

SPIEGEL, Der; STARK, Holger. **STUXNET**. Disponível em: < http://politicageral.wordpress.com/2011/08/09/stuxnet/>. Acesso em: 06 mai. 2011.

Times Topics: PEOPLE>A> ASSANGE, JULIAN P. **The New York Times**, 24 de fevereiro de 2011. Disponível em: < http://topics.nytimes.com/top/reference/timestopics/people/a/julian_p_assange/index.html?scp=10&sq=wikileaks&st=cse > Acessado em: 06 de maio de 2011.

VERDELHO, Pedro, et al. **Leis do Cibercrime**. Vol.1. Lisboa: Centro Atlântico, 2003. 28p.