3°/3° GAV

ESQUADRÃO FLECHA

MK

ATAQUES CIBERNÉTICOS A AERONAVES DE CAÇA

CAMPO GRANDE – MATO GROSSO DO SUL
2012

MK

ATAQUES CIBERNÉTICOS A AERONAVES DE CAÇA

Adaptação do trabalho apresentado no Curso de Líder de Esquadrilha de Caça no Esquadrão Flecha.

CAMPO GRANDE – MATO GROSSO DO SUL
2012

“Aquele que se empenha a resolver as dificuldades resolve-as antes que elas surjam. Aquele que se ultrapassa a vencer os inimigos triunfa antes que as suas ameaças se concretizem.”

Sun Tzu

RESUMO

Este trabalho busca estudar as vulnerabilidades da aeronave A-29, e de vetores com sistemas similares, a ataques cibernéticos que possam diminuir a confiabilidade e precisão de seu uso em possíveis conflitos futuros, bem como chamar a atenção para a necessidade de preocupação e preparação para esse novo campo da guerra moderna.

Palavras-chave: Guerra Cibernética; Aeronaves de Caça; Sistemas embarcados.

ABSTRACT

This paper explores the vulnerabilities of the aircraft A-29, and vectors with similar systems to cyber attacks that could reduce the reliability and accuracy of its use in possible future conflicts, as well as draw attention to the need for concern and preparation for this new field of modern warfare.

Key-words: Cyber attacks; Fighter aircraft; Airborne systems.

LISTA DE ABREVIATURAS E SIGLAS

CDCiber	- Centro de Defesa Cibernética
CMFD	- Display Multifuncional em Cores
CPU	- Unidade de Processamento Central
DTC	- Cartão de Transferência de Dados
EGIR	- GPS, Inercial e Radar Altímetro Conjugados
EICAS	- Sistema de Indicações do Motor e Alerta à Tripulação
EUA	- Estados Unidos da América
FAB	- Força Aérea Brasileira
GPS	- Sistema de posicionamento global
HUD	- Head-Up Display
IRNA	- Islamic Republic News Agency
MDP	- Processador de Displays e Missão
OFP	- Programa de Voo Operacional
PLC	- Controlador Lógico Programável
SCTIC²	- Sistemas de Comunicações e Tecnologia da Informação para Comando e Controle
VANT	- Veículo aéreo não tripulado
XML	- eXtensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA E PROBLEMA

Nos últimos anos temos percebido uma crescente onda de notícias e preocupação com ataques cibernéticos. A grande maioria voltada a fins criminosos para obtenção de dados pessoais e corporativos, dados bancários e outras formas de se conseguir vantagens financeiras.

No âmbito governamental e militar há grande preocupação na manutenção e proteção dos meios de Comando e Controle e páginas corporativas, especialmente durante eventos de grande vulto, ou situações de agitação social que levem ao aumento dos ataques que têm como objetivo realizar protestos e anarquizar.

Nessa linha de raciocínio podemos destacar a criação em 2010 do Centro de Defesa Cibernética (CDCiber), sob comando do Exército Brasileiro, com participação de militares da Força Aérea e da Marinha e a atualização em 2012 da Doutrina Básica da Força Aérea (DCA 1-1) que entre outras modificações incluem as Ações de Defesa Cibernética.

Segundo o Coronel do Exército Luis Cláudio Gomes Alves, coordenador na implantação do CDCiber, o Centro trabalha em dois níveis: a defesa nacional, no qual as Forças Armadas têm papel preponderante, e a segurança nacional, quando entram como força auxiliar. O Centro irá primordialmente proteger as redes militares e governamentais, e também pode contribuir para proteger as infraestruturas de informação como um todo.

A Doutrina Básica da FAB (Força Aérea Brasileira), ao definir a ação de Defesa Cibernética a divide em Proteção, Exploração e Ataque. A Proteção visa neutralizar ataques cibernéticos e

explorações cibernéticas, a Exploração busca coletar dados de interesse e identificar as vulnerabilidades, e o Ataque tem como objetivo neutralizar e destruir os meios inimigos. Entretanto as 3 subtarefas, bem como a definição da Tarefa, são voltadas para a proteção e a exploração dos meios de SCTIC[2] (Sistemas de Comunicações e Tecnologia da Informação para Comando e Controle)

É perceptível a grande preocupação com as redes e sistemas de informação, entretanto estão se tornando cada vez mais comuns os casos conhecidos de uso organizado e provavelmente governamental de ataques voltados a meios físicos como usinas nucleares e aeronaves não tripuladas, levando-nos a crer que qualquer meio que se utilize de controles eletrônicos pode estar vulnerável a ataques cibernéticos num futuro não muito distante.

1.2 OBJETIVOS

1.2.1 Objetivo geral

Este trabalho objetiva analisar até que ponto as aeronaves de caça com sistemas similares ao do A-29 estão vulneráveis a ataques cibernéticos, de que forma estes poderiam ser realizados, quais suas consequências e formas de precaução.

1.2.2 Objetivos específicos

Realizar pesquisa de notícias a respeito de ataques conhecidos, sistemas embarcados do A-29 e publicações técnicas, analisando-os a fim de verificar as vulnerabilidades de nossas aeronaves de caça.

1.3 JUSTIFICATIVA

Com grandes evidências de que países ao redor do mundo dispõem de armas cibernéticas altamente desenvolvidas, e já em uso, ainda que de forma silenciosa, devemos verificar se estamos preparados para enfrentar esta nova modalidade de guerra.

Estas armas já foram usadas contra usinas nucleares e aeronaves não tripuladas, este trabalho busca analisar o grau de vulnerabilidade das aeronaves de caça da Força Aérea Brasileira

1.4 HIPÓTESES

A aeronave A-29, assim como os caças com aviônicos similares estão vulneráveis a ataques cibernéticos, através de seus sistemas ou equipamentos de auxílio a navegação, podendo até mesmo já estar contaminados por programas ou códigos em espera.

1.5 ESTRUTURA DA MONOGRAFIA

Após analisar os casos conhecidos de uso de armas cibernéticas, e os estudos realizados sobre o tema, vamos pesquisar possíveis brechas nos sistemas do A-29, que poderiam ser utilizados para diminuir sua eficácia e eficiência no combate.

2 ATAQUES CONHECIDOS

Por se tratar de um campo ainda novo, que começa agora a vir à tona (apesar de já estar sendo estudado e desenvolvido pelos países desenvolvidos a mais de 10 anos), as informações relativas às armas cibernéticas existentes são totalmente imprecisas, e muitas delas já podem estar em uso sem o conhecimento da sociedade. Poucas vieram à tona, e somente após terem cumprido total ou parcialmente seus objetivos. Devemos observar também que algumas fontes são discutíveis, e até mesmo a autoria de ataques não é confirmada.

2.1 STUXNET

Este é o caso mais marcante do uso de armas cibernéticas, por ser o primeiro que se tem notícia que não apenas rouba informações, mas causa danos físicos a instalações sensíveis, que não utilizam sistemas operacionais convencionais, como o Windows ou OS X, mas estruturas baseadas no sistema SCADA, desenvolvido pela Siemens para monitorar e controlar partes ou todo um processo industrial.

O Malware Stuxtnet, que tinha como alvo a usina nuclear de Natanz, no Irã, foi descoberto em Junho de 2010 pela empresa bielorrussa de segurança digital Kaspersky depois de ter infectado

computadores fora do complexo de Nanatz, devido a um erro em seu código.

Segundo o jornal New York Times, o desenvolvimento deste vírus se deu ainda durante o governo de George W. Bush (2001-2009), em conjunto com especialistas de Israel, mas o ataque foi autorizado pelo atual presidente dos EUA, Barack Obama.

De acordo com a empresa de segurança Symantec, 60% dos computadores infectados no mundo estavam no Irã, fato que evidencia a tática do ataque. Como a usina não é conectada à internet, a estratégia foi infectar algum dos poucos usuários com acesso às maquinas PLC (Controlador Lógico Programável) para que este infectasse involuntariamente o sistema da usina.

Devido a sua grande especificidade, o malware não causa qualquer problema em computadores normais, tendo como único objetivo nestes sistemas, se disseminar até encontrar a máquina certa.

Uma vez na máquina de controle da usina, após identificar as especificidades do sistema daquela unidade, ele inicia a reprogramação do sistema de controle. No caso de Nanatz fazia com que as centrifugas iranianas girassem 40% mais rápido, o que causava danos estruturais, ao mesmo tempo em que gerava indicações falsas aos sistemas de gerenciamento, fazendo os funcionários acreditarem que tudo estava na normalidade.

A necessidade de informações detalhadas e de difícil acesso aos sistemas da usina descartam a possibilidade de usuários domésticos terem desenvolvido o vírus, voltando as suspeitas para grandes organizações e governos.

.

2.2 FLAME

Descoberto em 2012, após apagar diversos dados importantes e causar problemas de rede no Ministério do Petróleo do Irã, este vírus pode parecer mais convencional que o Stuxnet, devido a sua finalidade, de espionagem em computadores convencionais. Segundo a Kaspersky, o super-vírus, que tem mais de 20 megabytes quando com todos os módulos, impressiona pela complexidade, e pode levar mais de 10 anos para ser completamente desvendado. O programa pode gravar áudio através dos microfones do computador, monitorar telas, atividades e registros de rede e teclado, roubar informações de dispositivos bluetooth próximos, pode copiar, corromper e destruir arquivos específicos. Ele se comunica com servidores ao redor do mundo para repassar informações e aguardar comandos, podendo inclusive receber ordens para se apagar sem deixar rastros.

Utilizando-se de métodos avançados para passar despercebido pelos antivírus, ele possui linhas de código em comum com o Stuxnet, podendo-se dizer que ambos vêm da mesma fonte.

Segundo Eugene Kaspersky, "a localização geográfica dos alvos e a complexidade da ameaça não deixa dúvida sobre a existência de um Estado-nação que apoia o desenvolvimento deste malware.” Quando foi descoberto, os países mais afetados eram o Irã, Israel, Sudão, Síria, Líbano, Arábia Saudita e Egito.

2.3 CAPTURA DO RQ-170 SENTINEL

O RQ-170 Sentinel é um dos VANTs (Veículo aéreo não tripulado) de reconhecimento mais avançados dos EUA, desenvolvido pela Lockheed Martin, está em operação desde 2005, mas pouco se sabe sobre suas reais especificações.

Em dezembro de 2011, a mídia Iraniana divulgou imagens de um RQ-170 em bom estado de conservação, que segundo eles, foi capturado com o uso de modernas técnicas cibernéticas e com o mínimo de danos à aeronave.

De acordo com a IRNA (Islamic Republic News Agency), O VANT foi trazido ao solo com avançados jammeadores eletrônicos, desenvolvidos pela indústria iraniana. Em pronunciamento oficial, o Air Force Chief Gen. Norton Schwartz se recusou a dizer que o RQ-

170 foi derrubado por recursos eletrônicos, e disse temer pela engenharia reversa que pode ser feita na aeronave. Entretanto, Schwartz foi confrontado por Dan Goure, analista do Instituto Lexington, que argumenta que esse tipo de aeronave é programada para retornar à base por meios independentes, caso ocorra qualquer problema na rede de Comando e Controle.

3 ESTUDOS JÁ REALIZADOS

Além dos ataques que vieram à tona, algumas instituições estão se preocupando em estudar as possibilidades e vulnerabilidades dos meios de força aérea. Recentemente, a Marinha Norte-Americana informou que está trocando o sistema operacional que controla suas aeronaves não tripuladas, com o objetivo de evitar ataques de software maliciosos que poderiam acessar os sistemas das aeronaves.

3.1 DRONES VULNERÁVEIS

Em Junho de 2012, a equipe do professor Todd Humphreys, na Universidade do Texas, apresentou um experimento que pode atrasar bastante os planos do Governo Americano de autorizar o voo de aeronaves autônomas em seu próprio espaço aéreo.

Em um estádio, onde um drone cumpria uma rota em pontos programados no GPS, a equipe conseguiu enviar sinais falsos, modificando a sua rota.

Existe uma diferença importante entre o experimento do Prof. Humphreys e os conhecidos Jammeadores de GPS. Enquanto estes interferem nos sinais recebidos pelos navegadores, causando a perda de sinal e incorreções, o aparelho desenvolvido pela equipe do Texas inicialmente envia a cópia dos sinais corretos dos

satélites, porém com mais potência, e quando deseja assumir o controle, começa a modificar os sinais enviados de forma a direcionar o alvo para um novo destino.

Esse experimento demonstra a possibilidade de além de controlar aeronaves não tripuladas, poder enganar o sistema de navegação das aeronaves tripuladas, diminuindo a precisão e consciência situacional dos pilotos.

4 VULNERABILIDADES CONHECIDAS

De acordo com o manual de manutenção da aeronave, a estrutura do sistema aviônico do A-29 está baseada em dois MDPs (Processador de Displays e Missão), um ativo e outro reserva, os quais controlam os CMFDs (Display Multifuncional em Cores) e o HUD (Head-Up Display). Em ambos os MDPs, é executado o OFP (Programa de Vôo Operacional).

Este é responsável pela geração de vídeo, controle de interfaces, gerenciamento de rádios, indicações do motor, gerenciamento de cargas e monitoramento do sistema.

Dentro das análises que vamos realizar vale ressaltar que o MDP provê as funções de cálculos e indicações de navegação e pontaria, geração e controle da simbologia para o HUD e CMFDs, gerenciamento do “data link” e controle de dados, EICAS (Sistema de Indicações do Motor e Alerta à Tripulação) e monitoramento e controle de combustível.

O MDP é um computador com arquitetura modular aberta, baseado em uma CPU (Unidade de Processamento Central). Essa CPU opera como controladora principal do sistema e controla um conjunto de módulos. A CPU possui os seguintes tipos de memória: 66MB Flash (para armazenamento do OFP), 128MB RAM dinâmica (para execução do OFP) e 2MB de RAM estática (para dados suportados pela bateria da aeronave). Estas memórias são

associadas a um processador Power PC 750 RISC, de 300MHz e 64 bits.

Como se pode perceber, todas as informações importantes repassadas ao piloto em voo, como cálculo de impacto de bombas, indicações de navegação e alertas dos variados sistemas são gerenciados pelo MDP, que a grosso modo é um computador, diferenciado dos PCs pela redundância, que o deixa mais confiável, e por contar com um Firmware, também chamado de sistema operacional, ou programa residente, no caso do A-29 o OFP, que promove a integração com os diversos módulos que convertem os sinais digitais e analógicos, enviados e recebidos, fazendo com que através de sinais digitais o piloto consiga operar itens mecânicos, como por exemplo as metralhadoras.

Estes Firmwares são atualizados com certa frequência, sempre que se altera alguma lógica do sistema, ou quando se deseja adicionar novas funcionalidades. As atualizações são realizadas por um notebook, através de um conector de teste ao MDP ou pelo barramento multiplexado. Estas atualizações são colocadas no notebook, de uso exclusivo para manutenção no A-29 , através de CDs entregues pela Embraer.

O sistema é desenvolvido pela Elbit, empresa Israelense, e fornecido à Embraer através da Aeroeletrônica, sua subsidiária no Brasil, e é bastante similar ao encontrado em diversas aeronaves de

caça modernizadas, como é o caso do F-5M da FAB e do IA-63 Pampa da Força Aérea Argentina.

4.1 SISTEMA GPS

O sistema de navegação e pontaria do A-29 é baseado no EGIR (GPS, Inercial e Radar Altímetro Conjugados), e pode-se selecionar entre apenas o GPS, apenas o Inercial, ou o Inercial corrigido pelo GPS.

Operando no modo Inercial+GPS o sistema é mais preciso, porém como não dispomos da mesma precisão e da criptografia utilizada pelos Norte-Americanos o sistema torna-se bastante vulnerável, seja por sinais incorretos enviados pelos satélites americanos, ou pelo uso de Jammeadores.

Este sistema dá brecha também ao uso de equipamentos como o demonstrado pelo Prof Humphreys, onde o sistema seria enganado, e levado a uma coordenada diferente da planejada.

O sistema operando no modo GPS puro fica ainda mais vulnerável, já que não tem auxílios do Inercial.

Levando em conta estas restrições ao uso em um conflito, é prática comum na FAB realizar a maior parte dos treinamentos de Ataque e missões similares com o sistema no modo Inercial puro. Neste modo, são eliminadas as possibilidades de interferências externas em relação à localização da aeronave, porém quanto maior

o tempo de voo, maior será o erro acumulado no posicionamento do sistema de navegação, e os últimos ajustes de pontaria no emprego de armamento devem ser feitos visualmente, de forma a aumentar a precisão dos acertos.

4.2 ATUALIZAÇÃO DE OFP

Esta foi identificada como a fase mais crítica e mais vulnerável a ataques cibernéticos na operação da aeronave A-29.

Como o Sistema do A-29 não se conecta a redes, e tem um Firmware bastante específico, não existem meios diretos para infecção por vírus como o Stuxnet.

Entretanto o notebook que efetua o carregamento dos novos OFPs nas aeronaves, utiliza sistema operacional Windows, bastante vulnerável a programas maliciosos, e apesar de não ter conexão direta a redes, este notebook também é responsável pelo download de dados e parâmetros dos voos, que com frequência são descarregados em pen-drives, abrindo aqui uma brecha para a infecção do sistema.

Como foi visto no caso Stuxnet, um ataque direcionado aos possíveis operadores destes notebooks, poderia lograr sucesso e garantir acesso à maquina que atualiza o OFP.

Um ataque por este meio necessitaria pelo menos de 2 programas distintos.

O primeiro, que rodasse no Windows e se utilizasse de técnicas de rootkit (camuflagem de ações) para quando fosse executado o Software de atualização dos OFPs inserir junto aos pacotes de arquivos enviados à memória Flash do MDP, arquivos de Firmware adulterados.

Estes arquivos de Firmware seriam o segundo programa, muito mais complexo, pois necessita do conhecimento profundo da lógica, caminhos, barramentos e da linguagem de programação utilizada no OFP. Através de sutis modificações no sistema original, poderiam ser adulteradas indicações do sistema de motores, e de panes, minando aos poucos a aeronave, poderiam ser inseridos erros de cálculo para a balística de armamentos específicos, e até mesmo colocar comandos em espera de uma ordem para agir, através dos arquivos do DTC (Cartão de Transferência de Dados), data-link, ou uma data específica, podendo inviabilizar até mesmo o voo da aeronave.

Apesar dos requisitos complexos, que evidenciariam um ataque totalmente estudado e direcionado, esta hipótese é uma realidade, principalmente se levarmos em conta que o sistema do A-29 é desenvolvido por uma empresa israelense, país que tem sido envolvido em todos os casos recentes de ataques cibernéticos e possui o domínio total do sistema, além de o mesmo ser operado por diversas outras Forças Aéreas com aeronaves modernizadas pela Elbit.

4.3 CARREGAMENTO DE MISSÕES POR DTC

Ao contrário da atualização do OFP, não poderiam ser incluídas mudanças no sistema residente da aeronave (OFP), pelo simples carregamento dos dados do DTC, a menos que o sistema já possuísse algum comando embutido que permitisse essa ação.

Entretanto, caso o computador utilizado para planejamento e carregamento das missões esteja contaminado com um vírus com funções de rootkit, este poderia inserir dados incorretos no DTC. Caso não fossem percebidos quando no carregamento dos dados na aeronave, poderiam levar a rotas de navegação incorretas, coordenadas de alvos defasadas e perfis de emprego de armamento adulterados.

Estes vírus teriam também de ser desenvolvidos exclusivamente para este fim, e direcionados aos operadores destas estações, que com frequência conectam pen-drives às mesmas, podendo infectá-las. E o seu desenvolvimento seria menos complexo, uma vez que os arquivos que carregam os dados são XML simples, sem qualquer tipo de codificação ou criptografia.

5 CONTRAMEDIDAS E EXPLORAÇÃO

Dadas as características dos sistemas operacionais das aeronaves de caça da geração empregada pela Força Aérea Brasileira, em linguagens de mais baixo nível, atualizações e instalação de programas adicionais, são difíceis de serem feitas e implantadas, necessitando de conexões específicas para a transferência dos dados. A atenção deve ser voltada principalmente para as máquinas que fazem essas atualizações. A situação ideal seria equipamentos dedicados exclusivamente a esta função, que não tivessem qualquer tipo de contato com outras mídias (pen-drives, disquetes, CDs, etc), exceto os CDs de atualização do Firmware, inclusive com as portas USB desabilitadas, e preferencialmente com sistema operacional Linux.

Nas estações de planejamento de missões, deveria ser estudada a possibilidade de implantação de Linux, como forma de dificultar rootkits, além do isolamento das portas de entrada, deixando habilitada apenas a conexão com o DTC. Para isso todas elas deveriam dispor de impressoras, e como forma de troca de informações uma rede fechada entre as estações.

Os sistemas de navegação, a longo prazo poderiam ser atualizados para utilizar em redundância sistemas paralelos ao GPS, como o Glonass(Russo), Galileo (Europeu), ou o BeiDou(Chinês), de forma a terem dados mais confiáveis. Contudo a solução de utilizar

apenas o Inercial é razoavelmente precisa, e é a única possível atualmente.

A transferência de dados sem fio com a aeronave (Data-link), é bastante limitada, tanto em quantidade de dados como em funções, sendo muito pouco provável que se consiga utilizar este sistema para afetar alguma função do OFP da aeronave. Também deve ser levado em conta que as conexões são criptografadas, o que também dificultaria alguma ação por este meio. Entretanto é uma porta plausível para a possível ativação de comandos maliciosos já implantados por outros meios.

Da mesma forma que ocorre na computação pessoal e corporativa, com o desenvolvimento das aeronaves de caça, seus sistemas tendem a ser cada vez mais interligados e conectados a outras aeronaves e estações em terra. À medida que isto ocorre, estão cada vez mais vulneráveis, e grande atenção deve ser dispensada aos sistemas de proteção das conexões.

A única maneira de não correr riscos deste tipo de interferência é mantendo as aeronaves isoladas de qualquer transmissão de dados, o que cada vez mais se mostra inviável.

A guerra cibernética com objetivos físicos é uma realidade, e muitos países já atuam em armas e defesas relacionadas. O estudo e o desenvolvimento deste campo devem ser iniciados o mais rápido possível, tanto defensiva como ofensivamente, sob pena de, em um

eventual conflito, ver vetores de milhões de reais inutilizados por ameaças cibernéticas.

6 CONCLUSÃO

Pode-se verificar que ataques direcionados a aeronaves A-29, ou que possuam sistemas similares são totalmente plausíveis, como os direcionados recentemente ao Irã, e devemos estar preparados para evita-los.

Extrema importância deve ser dada à proteção dos sistemas digitais como um todo (e não apenas de Comando e Controle), e a verificação constante da integridade dos sistemas operacionais diversos deveria ser uma rotina.

Mais atenção deveria ser dada a este tipo silencioso de guerra, que pode, inclusive, já ter muito mais armas em uso, e é capaz de deixar equipamentos de milhões de dólares inutilizáveis. Através de armas relativamente baratas e muito precisas, perdas importantes podem ser impostas ao inimigo, com o menor dano colateral possível.

REFERÊNCIAS

COMANDO DA AERONÁUTICA. *DCA1-1 DOUTRINA AEROSPACIAL:* Doutrina Básica da Força Aérea / Brasília: MD, 2012.

EMBRAER. *MANUAL DE MANUTENÇÃO DA AERONAVE A-29:* Capítulo 42 – Sistema Aviônico Integrado / São José dos Campos: EMBRAER, 2011.

MAJUMDAR, Dave*. Iran's Captured RQ-170: How Bad Is the Damage?*.Disponível em: <http://www.defensenews.com/article/20111209/DEFSECT01/112090307/Iran-s-Captured-RQ-170-How-Bad-Damage-> Acesso em 28/06/2012

VÁRIOS. *Stuxnet*
Disponível em:< http://pt.wikipedia.org/wiki/Stuxnet>. Acesso em 28/06/2012

LUPION, Bruno. *Exército se arma para defender o espaço cibernético brasileiro.*
Disponível em: <http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm>. Acesso em: 27/08/2012.

ROBERTS, John. *Drones vulnerable to terrorist hijacking, researchers say*
Disponível em:< http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say/>. Acesso em 25/06/2012

BIBLIOGRAFIA CONSULTADA

WOLOSZYN, André Luís. *A espionagem cibernética no século XXI*. Disponível em:< http://www.defesanet.com.br/cyberwar/noticia/7710/A-espionagem-cibernetica-no-seculo-XXI>. Acesso em 18/10/2012

WOLOSZYN, André Luís. *Ciberataques, uma nova ameaça à civilização?*. Disponível em:< http://www.defesanet.com.br/cyberwar/noticia/7411/Ciberataques--uma-nova--ameaca-a-civilizacao-->. Acesso em 23/08/2012

LIMA, Jose Antonio*. Irã divulga imagens de avião espião dos EUA que caiu no domingo* Disponível em:< http://colunas.revistaepoca.globo.com/ofiltro/2011/12/08/ira-divulga-imagens-de-aviao-espiao-dos-eua-que-caiu-no-domingo/>. Acesso em 28/10/2012

WOLOSZYN, André Luís*. O mundo ameaçado pela corrida de armamentos virtuais* Disponível em:< http://www.defesanet.com.br/cyberwar/noticia/6377/O-mundo-ameacado-pela-corrida-de-armamentos-virtuais >. Acesso em 11/06/2012

CANDIDO, Fabiano. *Obama ordenou ataque com o Stuxnet, diz NYT.* Disponível em:< http://info.abril.com.br/noticias/seguranca/obama-ordenou-ataque-com-o-stuxnet-diz-nyt-02062012-0.shl>. Acesso em 28/06/2012

REUTERS. *Flame pode sabotar computadores e atacar Irã.* Disponível em:< http://info.abril.com.br/noticias/seguranca/flame-pode-sabotar-computadores-e-atacar-ira-22062012-9.shl>. Acesso em 28/06/2012

FERRER, Rafael. *Marinha usará Linux para controlar helicópteros não tripulados.* Disponível em:< http://info.abril.com.br/noticias/computacao-inteligente/marinha-usara-linux-para-controlar-helicopteros-nao-tripulados-04072012-24.shl>. Acesso em 28/06/2012

COSTA, Christian. *Drones dos EUA têm sistema vulnerável.* Disponível em:< http://info.abril.com.br/noticias/seguranca/sequestro-de-drone-nos-eua-aumenta-preocupacao-com-seguranca-04072012-35.shl>. Acesso em 28/06/2012

TANJI, Thiago. *Como o exército protege o espaço virtual brasileiro.* Disponível em:< http://info.abril.com.br/noticias/seguranca/como-o-exercito-protege-o-espaco-virtual-brasileiro-16072012-21.shl>. Acesso em 28/06/2012

GARCIA, Augusto. *Kaspersky descobre três vírus relativos ao Flame.* Disponível em:< http://info.abril.com.br/noticias/seguranca/kaspersky-descobre-tres-virus-relativos-ao-flame-17092012-38.shl>. Acesso em 28/06/2012

AFP. *Variante do Flame é detectado no Irã e Líbano.* Disponível em:< http://info.abril.com.br/noticias/seguranca/variante-do-flame-e-detectado-no-ira-e-libano-15102012-48.shl>. Acesso em 28/06/2012

SANTA ROSA, Giovanni. *Kaspersky vai criar seu próprio sistema operacional super seguro voltado para empresas.*
Disponível em:< http://www.gizmodo.com.br/kaspersky-sistema-operacional-seguro-empresas/>. Acesso em 28/06/2012

MCMILLAN, Robert. *Siemens: Stuxnet worm hit industrial systems.* Disponível em: <http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142> Acesso em 28/06/2012

DSOUZA, Larkins. *Iran claims to have captured a RQ-170 Sentinel.*
Disponível em: < http://www.defenceaviation.com/2011/12/iran-claims-to-have-captured-a-rq-170-sentinel.html> Acesso em 29/10/12