Instituto Superior de Ciências Sociais e Políticas
UNIVERSIDADE DE LISBOA

O Ciberataque como Guerra de Guerrilha

O Caso dos Ataques DoS/DDoS à Estónia, Geórgia e ao Google - China

Pedro José Bentes Graça

Orientador: Professor Doutor Pedro Ferraz de Abreu

Coorientador: Professor Doutor António Silva Ribeiro

Dissertação de Mestrado em Estratégia

Lisboa

2013

Índice

INTRODUÇÃO

Problema, Hipótese Método

1 O PROBLEMA

Os ataques cibernéticos são uma realidade cada vez mais comum na atualidade. É uma realidade relativamente nova, para a qual ainda não existe uma resposta global e eficaz de forma a evitá-los. A sua própria natureza heterogénea, as tecnologias que utilizam e o caráter esporádico e imprevisível da sua predação, tornam praticamente impossível organizar uma defesa e prevenção total, bem como estabelecer fundamentos consolidados quanto à forma de reagir operacionalmente e estrategicamente. Como tal, creio que é necessário analisar outros comportamentos de conflito não convencionais. A guerra de guerrilha surge naturalmente, devido à sua natureza não convencional, esporádica e de caráter irregular. Creio que será bastante útil utilizar os ensinamentos estratégicos e políticos da guerrilha, realidade bastante antiga e alvo de estudos aprofundados e tentar aplicá-los à nova realidade dos ciberataques. Para tal, preciso de estabelecer se são realidades comparáveis. Os objetivos deste trabalho são os de tentar retirar ensinamentos decorrentes da guerra de guerrilha e do seu combate, que possam conduzir à prevenção e combate aos ataques informáticos do tipo Denial of Service/ Distributed Denial of Service (DoS/DDoS). Este trabalho tem como objetivo retirar ensinamentos decorrentes da guerra de guerrilha e da aplicação de ciberataques que apresentam uma metodologia muito próxima desta. Tendo em conta esta similitude entre a praxis da guerra de guerrilha e a preparação e o desenrolar de um determinado tipo de ciberataque**.**

2 OBJETO DE ESTUDO E A SUA DELIMITAÇÃO

Irei estabelecer paralelismo entre o desenvolvimento de um ataque de guerrilha convencional e um ataque cibernético específico.

A guerrilha oferece três modalidades de ação: terrorismo, sabotagem, e combate. Esta dissertação individual não visa definir, interpretar ou caracterizar estas três modalidades da guerra de guerrilha, por estas já estarem suficientemente estudadas e divulgadas em estudos e obras nacionais e estrangeiras. Iremos abordar de forma limitada, como se podem tentar reproduzir, na forma de um ataque cibernético (o DDoS), estas três modalidades de ação estratégica características da guerrilha e que se complementam entre si. Para tal, partirei de um conjunto de descrições e ataques de guerrilha levados a cabo desde o começo do séc. XX

até à atualidade. A escolha deste período específico, tem a ver com a multiplicidade de diferentes ataques e do facto de o contexto político, social e tecnológico, mais se aproximar da realidade presente.

No que diz respeito ao universo dos ataques cibernéticos, irei limitar-me a três ataques conhecidos: Estónia 2007; Geórgia 2008 e o ataque ao Google, alegadamente comandado pela República Popular da China em 2010. A escolha destes três ataques, apresenta muitas das características dos ataques DDoS, as suas potencialidades, os danos sofridos. Também os escolho, por os dois primeiros serem, aparentemente, dirigidos a Estados. No caso da Geórgia, por ter acontecido antes de um ataque convencional. O terceiro, é algo mais complexo, dado que, aparentemente, envolve uma empresa privada e um Estado, havendo, ao tempo da sua ocorrência, um considerável historial de conflitualidade entre os dois atores.

3 OBJETIVO DA DISSERTAÇÃO

A dissertação visa contribuir para uma perceção mais apurada das semelhanças entre a guerra de guerrilha e a realidade dos ciberataques. Isso é feito através da identificação de um padrão comum entre os ataques de guerrilha convencional, os seus métodos, objetivos e alvos e os ataques cibernéticos DDoS, levando-nos mesmo a interrogar se, este fenómeno novo no âmbito da conflitualidade, não será mais um ataque a acrescentar ao âmbito da guerrilha, trazendo-a para o virtual e assim atualizando-a e complementando-a. Claramente, estamos dentro do domínio da Estratégia, tal como ela é definida pelo almirante Silva Ribeiro "… como a ciência é a arte de edificar, dispor e empregar meios de coação num dado meio e tempo, para se materializarem objetivos fixados pela política, superando problemas e explorando eventualidades em ambiente de desacordo" (Ribeiro, 2009).

Os objetivos práticos deste estudo visam tentar retirar ensinamentos decorrentes da prática da guerra de guerrilha e de contra-guerrilha que possam conduzir à prevenção e combate de ataques informáticos do tipo DoS/DDoS. É uma nova realidade que se desenrola num meio virtual e, no entanto, partilha muitas táticas e ensinamentos extraídos de conflitos reais passados. Esta similitude é observável sobretudo no conjunto de boas práticas de segurança e de recuperação de incidentes. Para além deste aspeto, existe um outro que também deve ser levado em conta: as realidades políticas, sociais e militares que poderão estar por detrás de um ataque informático. Certamente que será importante aplicar contra-medidas que vão para além do âmbito técnico.

4 QUESTÃO CENTRAL E HIPÓTESE

A minha hipótese inicial era – É possível enquadrar os ataques DoS/DDoS dentro da prática da guerra de guerrilha atual?

Uso a sigla DoS (Denial of Service) com o significado de denegação de serviço de equipamentos conectados à internet. Uso a sigla DDoS (Distributed Denial of Service) a uma escala muito maior , visa restringir, desligar, destruir equipamentos que estejam ligados à internet, provocando grandes perturbações ao normal funcionamento dos serviços disponíveis na internet.

Adoto a definição de guerra enunciada pelo General Cabral Couto no seu livro Elementos de Estratégia "violência organizada entre grupos políticos em que o recurso à luta armada constitui, pelo menos, uma possibilidade potencial, visando um determinado fim político, dirigida contra as fontes de poder do adversário e desenrolando-se segundo um jogo contínuo de probabilidades e azares" (Couto, 1988:53)

A guerra de guerrilha consiste na atuação das forças de guerrilha sempre em desvantagem numérica e em material"… atuam em pequenos destacamentos, por surpresa e com grande rapidez, procurando não se empenhar em combate com as forças da ordem, essencialmente por meio de:

- golpes de mão contra objetivos fixos (povoações, quartéis, fontes de energia, fábricas, etc.);
- emboscadas contra objetivos móveis (pequenas unidades em deslocamento, colunas de reabastecimento militares e civis, etc.):
- ações de flagelação semelhantes às anteriores mas de menor envergadura e sem objetivo determinado, por vezes executadas só pelo fogo, destinadas unicamente a manter um clima de insegurança na população e nas forças da ordem;
- ações de obstrução sobre os itinerários, levados a efeito pelo estabelecimento de obstáculos, passivos ou ativos, ou pela execução de destruições com a finalidade essencial de dificultar os movimentos militares e civis" (Exército, 1966:!8-19)

A guerra de guerrilha só é decisiva quando o lado que a não pratica lhe atribui pouca importância e não empenha todos os seus recursos na luta.

Com a evolução da investigação também a hipótese foi sofrendo alterações A principal evolução foi resultante da evolução das tecnologias e ataques DoS/DDoS do seu alcance e sofisticação que tornam cada vez mais difícil distinguir o grau de conflitualidade entre os

atores. Posto de outra forma, em que ponto poderemos considerar que um ataque desta natureza como sendo um ato de guerra e distingui-los de outras ações maliciosas.

O que me leva diretamente à formulação da hipótese –Até que ponto os ataques DoS/DDoS, não serão formas de luta cibernéticas concorrentes e complementares às operações de guerrilha convencional?

5 CONCEITO DE ESTRATÉGIA

A palavra estratégia serviu para a ciência e a arte do emprego das forças armadas. Muitas foram as definições apresentadas por vários autores estrategos (Clawsewitz, Molteke, Castex e outros) mas todas elas preocupando-se quase sempre com a distinção entre estratégia e a táctica.

Mais recentemente um escritor militar inglês Liddell Hart definiu Estratégia como «a arte de aplicar as forças militares para atingir as finalidades fixadas pela política» De facto, a palavra estratégia no sentido lato, engloba todas as acções que podem ser realizadas para atingir os objectivos fixados pela política, utilizando os meios de que dispõe para esse fim.

Das definições apresentadas, resulta que os seus autores admitem que os únicos meios a que a estratégia pode recorrer são os meios militares. Desta forma, o conceito de Estratégia contido naquelas definições exclui a existência de qualquer estratégia que não seja uma estratégia militar. É de verificar que tal conceito não está actualizado.

Efectivamente, quando a política fixa objectivos e a realização destes encontra oposição interna ou externa de algum adversário, gera-se um conflito que só pode ser resolvido de duas formas: persuasão ou a coacção. Sempre que há necessidade de recorrer à coacção para impor a vontade ao adversário, forçando-o a aceitar objectivos fixados pela política, entra-se no domínio da estratégia.

Tal é demonstrado pela análise dos conflitos mais recentes, há uma extrema diversidade de processos ou formas de coacção que podem agrupar-se em cinco categorias: estratégia psicológica, estratégia diplomática, estratégia política, estratégia económica e estratégia militar. O estudo e o emprego de qualquer destas formas de coacção, visam a imposição da vontade ao adversário, obrigando-o a capitular, quer por meio de esmagamento físico, quer pela estratégia psicológica de capitulação, são sem dúvida do domínio da estratégia.

Desta forma, não pode considerar-se um conceito de estratégia exclusivamente no emprego de meios de acção militar, nem de resto se compreenderia que o fenómeno da coacção, no seu conjunto, não fosse reunido para estudo e aplicação num sistema integrado de pensamento e

de acção. Daqui resulta o conceito actual de estratégia que na definição do General Cabral Couto é a seguinte"«A ciência e a arte de desenvolver e utilizar as forças morais e materiais de uma unidade política ou coligação a fim de atingirem objectivos políticos que suscitam, ou podem suscitar, a hostilidade de uma outra vontade política»"[1] Este conceito de estratégia não é de carácter exclusivamente militar, é hoje geralmente aceite por ser mais conforme com o aspeto total ou global dos conflitos contemporâneos e porque só ele permite explicar e compreender todos os fenómenos ligados a esses conflitos.

Tem-se discutido se a estratégia deve ser considerada ciência ou arte. No conceito de estratégia apresentado ela é apontada, simultaneamente, ciência e arte. Com efeito, a necessidade de o estratego recorrer a conhecimentos acumulados. A utilização de regras e métodos específicos e, a extrema complexidade de factores que integram qualquer estratégia, conferem a esta o carácter de uma verdadeira ciência. Contudo, a conduta puramente «científica» não pode ser normalmente tentada.

Dos factores numerosos que influenciam a solução de qualquer problema estratégico, é necessário discernir quais são, para cada caso, os factores dominantes e limitar o raciocínio aos factores dominantes desse problema.

Assim como o artista não produz obras-primas unicamente porque respeitou uma lista completa de regras teóricas, também o estratego deve possuir qualidades pessoais de intuição, génio e inspiração para escolher os factores essenciais e, com base nestes, conhecer a melhor solução para cada problema. Desta forma, resulta a estratégia ser uma arte além de uma ciência.

Também a guerrilha nas suas múltiplas formas e os ataques DoS/DdoS representam realidades a serem estudados pela estratégia dado serem formas de coacção efectivas e perigosas

6 METODOLOGIA

Depois de termos escolhido o tema, a elaboração de uma pergunta de partida foi uma tarefa que exigiu reflexão, de maneira a revelar com clareza, precisão e interesse do que procurávamos saber. Dessa reflexão resultou a seguinte pergunta: Como poderemos comparar a praxis dos ataques da guerra de guerrilha convencional, com os ataques cibernéticos da atualidade, nomeadamente o DDoS? A resposta a esta pergunta foi a linha de orientação da minha investigação. A metodologia que pretendi adotar, baseia-se na recolha de um conjunto

[1] COUTO, Abel C. *Elementos de Estratégia*: Apontamentos para um curso. Lisboa: Instituto de Altos Estudos Militares 1 v s.d p 209

diversificado de relatos de guerra de guerrilha passadas que cubram um vasto leque de situações e alvos atingidos. Seguidamente, irei compará-los com o conjunto de ataques DDoS (Estónia 2007; Geórgia 2008 e o ataque ao Google, alegadamente comandado pela República Popular da China em 2010) e verificar se há ou não similaridades entre a condução da guerra de guerrilha e um ciberataque DoS/DDoS. Irei identificar as variáveis comuns a ambos, se existirem. Depois, tentarei avaliar o valor conceptual e tentarei aplicá-los à natureza específica dos ciberataques, com vista a identificar padrões que possam contribuir para o combate aos ciberataques.

CAPÍTULO 1

Os ataques Denial of Service e Distributed Denial of Service

A frequência e a sofisticação na internet, dos Ataques de Negação de Serviço (Denial of Service-DoS) e dos Ataques de Negação de Serviço Distribuído (Distributed Denial of Service-DDoS) estão rapidamente a aumentar. Os Fornecedores de Serviço (ISP) estão a sofrer uma pressão crescente para controlarem e mitigarem ataques de DoS e DDoS. A internet é parte de uma infraestrutura internacional, que tem uma característica única, a de não ter fronteiras que a defendam dos ataques. Nos nossos tempos os ataques são quotidianos, sendo eles: ataques diretos, ataques de origem remota, ataques reflexivos, vermes (worms)[2] e virus[3]. Alguns destes tipos de ataques, são bastante nocivos e podem causar extensos apagões na internet.

Os ataques Dos/DDoS, nestes últimos anos, têm-se tornado mais sofisticados, devido ao nível de automação destes. Muitos exemplos de software de ataques prontos a usar em que não é necessário saber como eles funcionam para os utilizar e são passíveis de causar ataques com alguma dimensão, encontram-se facilmente disponíveis na internet. O aparecimento de redes de computadores pirateadas e controladas remotamente (Botnets) têm aumentado a complexidade dos desafios de segurança que os ISP[4] enfrentam. Tem-se assistido a um esforço de otimização das características dos worms, no que diz respeito à sua propagação e rapidez de contágio. Seguidamente apresentarei uma lista, não exaustiva dados eles serem muitos e estarem sempre a surgir novidades - de alguns ataques mais conhecidos de DoS/DDoS e descreverei o seu conteúdo.

1.1 ATAQUES DoS/DDoS

Um ataque DoS/DDoS é um ataque que visa restringir e desligar da internet, equipamento que lhe está ligado. Um ataque deste género, ocorre sempre que várias máquinas saturam a largura de banda da vítima que são geralmente um ou mais servidores, com o de pô-los fora de serviço. O alvo pode ser um servidor, um router ou outro equipamento por vezes, inclusivamente, com a destruição física do hardware visado. Existem várias formas de

[2] Um *worm* é um pedaço de código nocivo que não precisa de intervenção humana, do operador da máquina, para ser executado

[3] Um virus é um pedaço de código nocivo que precisa de intervenção humana, do operador da máquina, para ser executado

[4] *Internet Service Provider* - Fornecedor de Serviço da Internet

conseguir esse corte da rede. Os ataques DoS podem ser classificados de duas formas: ataques lógicos, ou ataques de exaustão de recursos causados por ataques de inundação de pedidos. Os ataques lógicos exploram falhas de segurança que levam a que o servidor ou o serviço em causa, vá abaixo ou se torne substancialmente mais lento. Os ataques lógicos são avaliados pelo impacto que causam na rede e na forma como afetam os serviços disponibilizados por esta (DNS; BGP; RADIUS etc.).

Os ataques por inundação podem ser avaliados pelo seu fator de ampliação. Este fator representa o número de vezes que o pacote original é multiplicado até atingir a vítima. Por exemplo: num ataque de inundação direta, o número de pacotes enviado pelos atacantes, é igual ao número destes recebidos pela vítima. No smurf que é um ataque reflexivo multiplicador, cada pacote é refletido entre um determinado número de máquinas e é mandado para a vítima o número de cópias de cada pacote, igual ao número de reflexões entre as máquinas participantes. Um ataque smurf pode ter um fator de amplificação na casa das centenas. Posto de outra forma - por cada pacote enviado pelo atacante, a vítima recebe centenas.

A velocidade de circulação da informação é altíssima. Senão vejamos; o tempo que vai desde o anúncio de uma vulnerabilidade de hardware/software e o aparecimento de uma forma de tirar dela (exploit) tem vindo a decrescer. Cada vez se assiste mais ao aparecimento de exploits no próprio dia. Um exemplo deste fenómeno foi o anúncio de uma vulnerabilidade no sistema operativo (IOS) da Cisco para o IP V4[5]. O exploit para esta vulnerabilidade era de tal forma óbvio que apareceram logo no próprio dia do anúncio da vulnerabilidade.

1.2 TIPOS DE ATAQUE

Existem 5 grandes tipos de ataques DoS:

1- Ataques de esgotamento de recursos computacionais, tais como largura de banda, espaço no disco ou tempo no processador.

2- Ataques de alteração de informação previamente configurada. Por exemplo: informação de roteamento.

3- Alteração de informação sobre o estado de um determinado serviço. É o caso do encerramento intempestivo de sessões TCP.

4- Ataques de destruição de componentes físicos, na máquina atacada.

[5] Versão mais utilizada do protocolo TCP/IP. Tem-se vindo a implantar cada vez mais o IP V6 que não é directamente compatível com o IP v4

5- Ataques de obstrução efetiva da capacidade de comunicação da vítima com o resto do mundo.

É também conhecido que o DoS pode incluir malware[6] ou, pelo menos, código que o ativa, com vista, entre outros objetivos:

- Por ao máximo o uso do processador, desta forma evitando que a vítima consiga fazer algum trabalho.
- Desencadear erros no sistema operativo da máquina.
- Desencadear erros na ordem de sequência das instruções a serem executadas pelo CPU. Criando assim instabilidade deste ou mesmo, levando-o à paralisia total.
- Criar erros no Sistema operativo de forma a criar falta de recursos e, ou a paralisia total da máquina, de forma que a vítima não possa realizar nenhum trabalho.
- Fazer parar o Sistema operativo.

Passo a descrever alguns dos ataques que se podem efetuar dentro do âmbito destes 5 tipos acima referidos.

O ataque SYN flood

"…A SYN flood ocorre quando uma máquina utilizadora envia uma inundação de pacotes TCP/SYN, com um endereço de remetente forjado. Cada um desses pacotes é tratado como um pedido de conexão, fazendo com que o servidor gere uma conexão semiaberta, enviando de volta uma resposta TCP/SYN-ACK (reconhecimento), e fica à espera de um pacote em resposta a partir do endereço do remetente (resposta ao pacote ACK). No entanto, porque o endereço do remetente é forjado, nunca vem a resposta. Estas conexões semiabertas saturam o número de conexões simultâneas que o servidor é capaz de manter, impedindo assim que responda a pedidos legítimos.

O ataque Teardrop

O ataque Teardrop envolve o envio de fragmentos mutilados de pacotes IP que se sobrepõem uns aos outros. São pacotes de grandes dimensões, o que representa uma carga para a máquina de destino. Isso pode fazer com que falhem os sistemas operativos devido a uma falha no seu processo de fragmentação e remontagem dos pacotes TCP/IP, levando a que o sistema

[6] *Software* com fins maliciosos

operativo da vítima pare. Os seguintes sistemas operativos Windows 3.1x, Windows 95 e Windows NT, bem como as versões do Linux anteriores para as versões 2.0.32 e 2.1 0,63 são vulneráveis a este ataque.

Ataques de baixa taxa de Denial-of-Service

É um ataque que explora o tempo de pedido de retransmissão de pacotes que chegaram com erro. O atacante aumenta e diminui a taxa de envio o que faz com que o protocolo TCP enviado pela vítima vá ficando cada vez mais lento. Este ataque permite que o atacante, na maior parte das vezes passe incólume.

Ataques Peer-to-peer

Os atacantes encontraram uma forma de explorar uma série de erros em servidores peer-to-peer para iniciar ataques DDoS. O mais agressivo é o DC + +. ataques Peer-to-peer são diferentes de ataques com botnetes . No peer-to-peer não há botnet. O atacante não tem que se comunicar com os clientes que subverte. Em vez disso, o atacante age como um "mestre de cerimónias", instruindo os clientes de grandes redes peer-to-peer para se desligarem das suas redes peer to peer e se ligarem ao website da vítima

Resulta que, milhares de computadores tentem ligar-se agressivamente ao dito website. Enquanto um servidor de internet (web) típico pode lidar com algumas centenas de conexões por segundo, antes de o desempenho começar a degradar-se, a maior parte dos servidores web falham quando se atinge cinco ou seis mil conexões por segundo. Num grande ataque peer-to-peer, um site poder ser atingido com até 750.000 pedidos de conexões em curto espaço de tempo…"[7]

Ataques de negação de serviço Permanente

A permanente negação de serviço (PDoS), também conhecido por phlashing, é um ataque que danifica de tal forma um sistema que será necessário substituir o hardware .Ao contrário do ataque distribuído de negação de serviço, um ataque PDoS explora falhas de segurança que permitem a administração remota sobre de hardware da vítima, tais como routers, impressoras ou outro equipamento de rede. O atacante usa essas vulnerabilidades para substituir o firmware de um dispositivo com uma versão corrompida ou com defeito da verdadeira software do fabricante. O dispositivo em causa torna-se imprestável para sua função original até que possa ser reparado ou substituído.

[7] http://en.wikipedia.org/wiki/Denial-of-service_attack

O PDoS é um ataque de hardware puro, pode ser muito rápido e exige menos recursos que a utilização de uma botnet para ataques DDoS. Devido a estas características, e ao elevado número de vulnerabilidades de segurança em dispositivos de rede, a técnica tem chamado a atenção de inúmeras comunidades de hackers.

Ataques de inundação ao nível da Aplicação

Vários DoS exploits tais como o Buffer overflow[8] podem causar confusão no software que está a correr no servidor e escrever no disco rígido interno, ocupando a totalidade do seu espaço ou monopolizando o tempo de CPU.

Outros tipos de DoS baseiam-se principalmente na força bruta, inundando o alvo com um fluxo enorme de pacotes, ocupando toda a largura de banda ou esgotar recursos computacionais da vítima. Ataques de saturação da largura de banda, são possíveis se o atacante tiver maior largura de banda do que a vítima. Uma forma comum de conseguir isto é realizar os DDoS, utilizando uma botnet, de que falarei seguidamente.

O banana attack

Trata-se de outro tipo de ataque DoS. Consiste em redirecionar pacotes à saída do cliente, de volta à sua origem, evitando assim que o cliente tenha acesso ao exterior, bem como inundando-o com os seus próprios pacotes enviados.

O ataque Nuke

É um antigo ataque de DoS que consiste em enviar pacotes ICMP[9] fragmentados ou inválidos. Tal é conseguido através da utilização de uma aplicação que cria e manda continuamente este tipo de pacotes (pings) fazendo assim com que a máquina da vítima vá ficando cada vez mais lenta e chegue mesmo a parar. Um tipo específico do Nuke que atingiu alguma notoriedade é o WinNuk , que explorava uma vulnerabilidade do software de rede do Windows 95 que causava a paragem do sistema operativo e fazia aparecer o ecrã azul da morte, forma como é conhecido, em todos os sistemas operativos Windows, o ecrã de informação que reporta problemas graves de leva ao encerramento compulsivo da máquina.

[8] Excesso de dados para uma determinado endereçamento de memória RAM, ou escrita em endereçamentos de memória que não lhe foram destinados

[9] Internet Control Message Protocol

O ataque Smurf

Num ataque Smurf o atacante inunda com pacotes ICMP o endereço de broadcast da vítima, no entanto, alterou previamente o endereço de retorno dos pacotes (ping) para o endereço de IP do servidor local de acesso à internet. Quando cada um dos computadores responde ao ping, mandam as suas respostas para o servidor da internet que se pretende atacar, fazendo com que ele fique totalmente atolado em tráfego ICMP. No entanto, atualmente, os ataques smurf são facilmente bloqueados através de listas de acesso de ingresso no router, de forma a que neguem a entrada de IP's que não pertençam à rede interna. Se um pacote alterado maliciosamente é detetado é automaticamente descartado pelo router de fronteira

Já vimos que é possível fazer ataques DDoS com várias máquinas operando em peer to peer. No entanto não costuma ser essa a forma de raptar máquinas e pô-las ao serviço de interesses inconfessáveis e, tudo isto, sem que os legítimos proprietários se apercebam ou possam impedir. Estamos a falar das botnets.

1.3 OS DDoS E AS BOTNETS

Botnets

Através das botnets, os atacantes neste caso chamados botherbers, podem reunir milhares de computadores para os utilizarem para o que muito bem entenderem. Um botherber usa um interpretador de comandos (shell) aonde executa um determinado conjunto de comandos e coordena e gere esses milhares de máquinas sequestradas. Não se pode dizer que o software que esta a correr nos botclients, seja um vírus, trata-se antes de um conjunto de software que é utilizado para fins maliciosos. Não é de excluir que esse software não inclua vermes (worms), Cavalos-de-Troia (Trojan) Portas-das-Traseiras (Back-doors) e controles remotos, ferramentas de hacker, tais como rootkits, ferramentas que permitam esconder-se do Sistema Operativo. O facto de o botherber nunca tocar no computador que realiza os atos ilegais tem sido usado, desde há anos, por organizações criminosas.

Uma botnet consiste num servidor bot ou o controlador e um ou mais de botclients. O coração de cada botclient é o interpretador de comandos que é capaz de ir buscar e executar comandos. A botnet atua de forma coordenada e num todo.

Agora que a botnet está criada, lança-se o ataque, temos várias possibilidades:

- Escolher a data e a hora do ataque, para tal coloca-se um worm.

- Pode-se mandar um comando para a botnet, para desencadear o ataque com a possibilidade de determinar a duração e o tipo de ataque. Tal procedimento permite colher informação dos resultados do ataque e planear o passo seguinte.

Só falta saber o que é que se pretendo fazer à vítima. Mais uma vez, abrem-se algumas possibilidades

-Por máquinas fora de serviço – explorando uma vulnerabilidade específica do sistema operativo da máquina alvo, posso fazer com que essa máquina vá abaixo e arranque de novo, o que leva algum tempo, ou obrigá-la a sucessivos arranques. O ataque Teardrop é um exemplo deste tipo de ataques

- **"Estragar" qualquer coisa –** Será também ocasionalmente possível, em alguns casos, corroer o software da máquina de forma que esta não consiga arrancar. A isto chama-se DoS permanente ou phlashing. Se conseguir corroer o firmware - que é o software que a máquina corre para começar a arrancar - ou o setor do disco rígido aonde está guardado o software de onde a máquina arranca, talvez possa avariar temporariamente - até à intervenção de um técnico habilitado - ou mesmo pô-la definitivamente fora de serviço.

1.4 IP SPOOFING

O IP Spoofing consiste em apropria-se de um endereço IP de um utilizador ou de um dispositivo de rede e, fazendo passar-se por ele, aceder a informação confidencial, ou mais simplesmente provocar uma negação de serviço. Cada equipamento de rede encontra-se identificado por um IP único; partindo desta premissa, não podem existir dois equipamentos com o mesmo endereço IP, dado que se criaria um conflito de IP, o que leva a que um dos equipamentos seja desligado, este é o exemplo mais antigo e mais simples de provocar uma negação de serviço, é rápido, efetivo mas muito pouco elegante. Supondo que acontece essa situação, a maior parte dos sistemas operativos avisar-nos –ia com uma mensagem de alarme. Nas redes com servidor DHCP[10], que atribuí endereços IP numa determinada rede é este que se encarrega desta tarefa este procedimento torna-se bem mais difícil.

Vejamos agora uma ataque de IP Spoofing mais sofisticado usando um software que é uma ferramenta complexa que nos permite mudar o pacotes TCP/IP . O ataque consiste em mandar ping (ICMP) com um endereço falseado. A máquina vitima responderá a esse ping o que leva

[10] Dynamic Host Configuration Protocol

a que a maquina a quem usurpámos a identidade (pacotes SYN e ACK) a receber os resultados de um ping que não havia solicitado. Isto tem como resultado que a conexão seja terminada e uma negação de serviço.

Este tipo de ataque deve ser feito a partir de uma máquina que tenha Linux como sistema operativo, dado que este software trabalha em ambiente Linux. O Nome do software é :hping2.

ARP spoofing

Um dos aspetos fundamentais no protocolo TCP/IP é a correspondência entre o endereço IP e o MAC-ADRESS que identificam os equipamentos na Local area network (LAN). O mac - adress vem de fábrica inscrito nas placas de rede. Os seus primeiros três octetos são a identificação do fabricante. Em princípio, não se pode alterar não se pode falsear um Mac Adress. Contudo, a realidade é bastante diferente, já que como veremos seguidamente como se pode alterar esta identificação, o que nos permite passar por outro equipamento, concretamente por outra placa de rede e aceder a outro tipo de serviços. Na realidade este é o tipo de spoofing que funciona ao nível da LAN. Falsear um endereço Mac é interessante dado que se pode "envenenar" a tabela de ARP (Access Resolution Protocol). Estas tabelas são as que fazem a correspondência entre os endereços IP e os Mac Adress. É importante que estas tabelas estejam corretas, dado que se aparecerem dois Mac iguais provoca-se uma negação de serviço. No entanto tudo isto é bastante rudimentar uma vez que se pode fazer bastante melhor. Como disse acima pode-se alterar o mac- address totalmente tanto em ambiente Linux ou Windows.

Existe outro ataque de negação de serviço mais elaborado usando o ARP Spoofing. Começa-se por fazer um ping à máquina que queremos atacar. Seguidamente, na linha de comando do windows verificamos qual é a entrada nova que temos ou se já sabemos o seu IP agora temos o IP associado com o Mac adresss. Então é só trocarmos o nosso MAC pelo Mac Adress da vítima. Depois desta troca feita todos os equipamentos que tenham de fazer uma resolução ARP não conseguem fazê-la nem contactar com o computador vítima. O ataque é verdadeiramente efetivo, no entanto tem uma desvantagem tem de se ter acesso à LAN, algo que poderá ser possível se por exemplo existir um acesso Wi-Fi mal configurado.

Man-In-The-Middle

É o ataque que mais se assemelha a colocar uma escuta nos fios de cobre dos telefones antigos. Não é um ataque de DoS ou de DDoS puro, no entanto pode fornecer informação relevante para os realizar. Quando fazemos a comparação entre este tipo de ataque e uma antiga escuta telefónica, mais nos apercebemos do perigo que este ataque representa. Um dos aspetos que o torna tão perigoso é que não é necessário que haja vulnerabilidades no sistema operativo, nem no software das máquinas que se pretende atacar. Dito de outra forma, a rede alvo pode estar bem protegida e as atualizações de software terem sido feitas, existe sempre a possibilidade de um ataque de Man-in-the-Middle. De facto assim é, por se ligar uma máquina à LAN local. Por definição na LAN circula todo o tráfego gerado nessa rede. Todas as máquinas estão à escuta de tudo o que se passa na LAN; só reagem quando o seu Mac address é utilizado. É também pela LAN que todas comunicam umas com as outras ou enviam tráfego para fora, através do router local. Enfim, quem está na LAN sabe tudo o que se passa naquela rede.

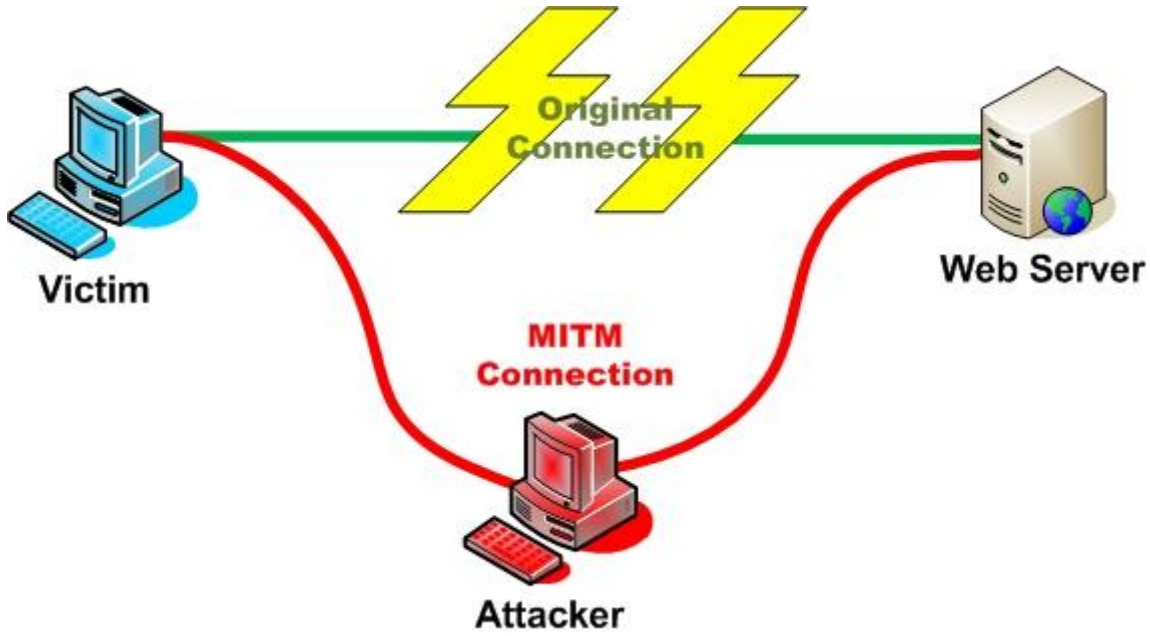

Figura 1[11]
Ataque Man-in-the-Middle

O atacante que desejar efetuar um ataque Man-in-the-Middle, tem um bom entendimento do funcionamento do protocolo de resolução de endereços (ARP)e a disponibilidade de várias ferramentas na internet, para realizar este ataque. Trata-se de um ataque relativamente fácil de

[11] https://www.owasp.org/index.php/Man-in-the-middle_attack

efetuar. De facto, encontram-se na internet, várias ferramentas para fazer o ”envenenamento” da lista ARP, a lista que faz corresponder os IP`s aos endereços Mac. Pode-se, usar por exemplo a Ettercap ou a Cain & Abel Algumas das características destas ferramentas são a descoberta das máquinas da rede, seleção de várias formas de ataque Man-in-the-Middle, snnifing e vários plug-ins que se podem usar durante o ataque . Esta ferramenta pode correr em diferentes ambientes (windows, Linux Apple etc., bem como a utilização em modo gráfico, mais atraente ou por texto (linha de comando). Uma vez estando infiltrado o atacante pode snifar todo o tráfego, desencadear outros tipos de ataques incluindo o Denial of Service. Este ataque é perfeito para roubar informação.

CAPÍTULO 2

A guerra de guerrilha

A expressão "guerra de guerrilha" deriva da ocupação da Península Ibérica durante as guerras napoleónicas, mais concretamente da palavra espanhola "guerrilleros", nome dado aos insurrectos portugueses e espanhóis, que combatiam os franceses através de métodos de guerra não convencionais. A guerra de guerrilha é uma forma de guerra na qual o lado estrategicamente mais fraco empreende ofensivas táticas de acordo com formas, tempos e locais previamente escolhidos. A guerra de guerrilha é a arma do mais fraco. Nunca é escolhida preferencialmente à guerra regular, empregada somente quando as possibilidades de se fazer uma guerra regular não é possível. A guerra de guerrilha só é decisiva quando o lado que a não pratica lhe atribuí pouca importância e não empenha todos os seus recursos na luta.

A guerrilha é um fenómeno de poder subversivo transposto para um nível intranacional. Apesar de muitas não se considerarem marxistas, actualmente a maioria destas seguem os ditames ideológicos e tácticos das doutrinas assim classificáveis. É sim o fenómeno do poder subversivo transposto para nível internacional.

"A guerra revolucionária, pelo contrário desenvolve-se a nível internacional e resulta normalmente da criação de um ou mais grupos, formados dentro das fronteiras de um Estado e à margem da sua lei, que pela via das armas, tenta substituir, através de uma pluralidade de meios de que disponha, o governo e o seu poder na totalidade ou numa parte do respectivo território.

A este tipo de subversão intranacional foram e são dados nomes diversos como «operações paramilitares», «guerra interna», «luta de guerrilhas», «guerra subversiva», «guerra terrorista», actividades «rebeldes», «insurreição armada», «resistência armada», luta «partisan», todas elas utilizadas para rotular o mesmo fenómeno eventualmente com divergências de sentido insignificante"[12]

Uma célula de guerrilha é composta por 20 a 50 homens. Razoavelmente armadas treinadas e endurecidas, actuam nas regiões de origem de modo a tirarem o máximo partido do conhecimento do terreno e população As guerrilhas regionais executam acções ofensivas que flagelam as forças adversas, procuram mantê-las desequilibradas.

[12] Lara, António Sousa. *Ciência Política*: Estudo da Ordem e da Subversão. 6 ed Lisboa, Instituto Superior de Ciências Sociais e Políticas 2011

As acções da guerra de guerrilha são eminentemente tácticas e devido à sua inferioridade numérica episódicas e de curta duração.

Um ciberataque é a exploração de um sistema de computadores e de redes destes. Os ciberataques usam código malicioso para alterar código do computador, a sua lógica ou dados armazenados, resultando em negações de serviço, comprometer informação e conduzir ao crime informático.

Também podemos centrar a questão pela definição de ciberguerra pelo uso da força para causar estragos, destruição ou mortes para obter efeitos políticos por Estados ou grupos.

Como poderemos apreender o significado sociológico dos potenciais efeitos da predação dos ciberataques para lhes dar um carácter subversivo? Esta é uma pergunta importante a que urge responder. Contudo não é nela que está baseada a hipótese desta dissertação e, como tal, foge ao seu âmbito.

2.1 CARACTERÍSTICAS DA GUERRA DE GUERRILHA COMO FORMA DE SUBVERSÃO

O Professor Sousa Lara[13]identifica as seguintes características fundamentais da guerrilha:

a) Intranacionalidade
b) Ilegalidade
c) Partes em conflito: o governo e um ou mais grupos anti-governamentais;
d) Finalidade principal: A substituição do governo em todo ou em parte do território;
e) Utilização dos meios militares entre outros:
f) É uma forma de luta escolhida pelo parceiro estrategicamente mais fraco;
g) O autor da guerrilha dirige a ofensiva tática no que concerne a métodos tempo e locais;
h) É uma forma de combate selecionada perante limitações das forças regulares governamentais, quer em efetivos, quer em capacidade de atuação ou resposta;
i) Exploram habitualmente certas vantagens que jogam espontaneamente a seu favor como:

i.1 – Justas reivindicações sociais e políticas

i.2 – Confusão e identificação dos guerrilheiros com a população civil

i.3 – Auxílio e proteção da população civil voluntária ou compulsivamente obtidos

[13] Lara, António Sousa. *Ciência Política* : Estudo da Ordem e da Subversão. 6 ed Lisboa

i.4 – Conhecimento íntimo da região da operação

i.5 - Informalidade de atuação

J) Estrategicamente a ação da guerrilha inverte a prática normal da guerra procurando evitar o combate e, taticamente, fugindo a qualquer envolvimento onde seja provável sofrer baixas

2.2 A GUERRILHA E OS ATAQUES DE NEGAÇÃO DE SERVIÇO

Passarei a comentar unicamente sob o ponto de vista de ataques de negação de serviço as características acima expostas

a) **Intranacionalidade.** Devido ao funcionamento da internet estar baseado na comutação de pacotes, o mais certo é que haja mais de um caminho para chegar de A a B e que esses pacotes maliciosos atravessem vários Estados
b) **Ilegalidade.** São ilegais
c) **Partes em conflito: o governo e um ou mais grupos anti-governamentais.** Os ataques de negação de serviço podem ter, ou não ter como instigador o governo de um Estado.
d) **Finalidade principal: A substituição do governo em todo ou em parte do território**. Os ataques não têm como finalidade essencial a substituição do governo em todo ou em parte do território
e) **Utilização dos meios militares entre outros.** Esta característica não se aplica aos ciberataques puros.
f) **É uma forma de luta escolhida pelo parceiro estrategicamente mais fraco.** Não é forçoso que assim seja, muitas vezes é o mais poderoso estrategicamente, tal como iremos ver mais adiante.
g) **O autor da guerrilha dirige a ofensiva tática no que concerne a métodos tempo e locais**. De facto assim é
h) **É uma forma de combate selecionada perante limitações das forças regulares governamentais, quer em efetivos, quer em capacidade de atuação ou resposta**. Poderá ser verdade, mas, felizmente ainda não assistimos a uma guerra total que inclua armas cibernéticos. O mais próximo foi o caso da Geórgia e da Rússia a propósito da Ossétia do Sul. Alegadamente, terá sido a Rússia a começar uma série de ataques de Negação de serviço, tal como veremos mais adiante

i) Exploram habitualmente certas vantagens que jogam espontaneamente a seu favor como:

i.1 – **Justas reivindicações sociais e políticas.** É possível que assim seja

i.2 – **Confusão e identificação dos guerrilheiros com a população civil.** Sim, de facto o atacante dissimula-se facilmente na população

i.3 **– Auxílio e proteção da população civil voluntária ou compulsivamente obtidos.** Pode ser que assim seja, no entanto não é necessário, dado que o atacante atua sozinho. O que ele poderá precisar, segundo o ataque a desferir, é de uma multiplicidade de máquinas previamente comprometidas que o ajudem a desencadear o ataque

i.4 **– Conhecimento íntimo da região da operação.** Não é necessário. O que é necessário é um bom conhecimento do protocolo TCP/IP, Conhecimentos profundos de Sistemas operativos (windows, Unix) saber ler e programar em C Java Pearl bem como dos URL`s aonde estão as vulnerabilidades publicadas, bem como dos ataques prontos a usar que existem na internet

i.5 - **Informalidade de atuação**. De acordo, essa é uma das características dos atacantes informáticos.

j) Estrategicamente a ação da guerrilha inverte a prática normal da guerra procurando evitar o combate e, taticamente, fugindo a qualquer envolvimento onde seja provável sofrer baixas. Os atacantes informáticos fazem uma prospeção das vulnerabilidades das redes que pretendem atacar. Só depois planeiam e levam a cabo o ataque, de acordo com a capacidade que têm ,ou não para levar a cabo esse ataque. Certamente não arriscarão atacar redes bem protegidas ou de pouco impacto nos objetivos que os movem.

Antes de continuarmos, torna-se necessário uma clarificação de conceitos que, frequentemente parecem ser sinónimos uns dos outros: guerra revolucionária, guerra psicológica, guerra insurrecional e subversão que foi acima definido:

2.3 CONCEITOS

Guerra de Subversão – O livro, O exército na Guerra Subversiva define subversão como" toda a ação deliberada levada a efeito por qualquer movimento ou organização, recorrendo a formas de atuação extralegais com o objetivo de destruir ou corroer o Poder estabelecido e, em regra a ordem político-social existente." (Exército, 1966) Esta definição parece ser bem

plausível, no entanto a observação dos ataques que têm ocorrido, têm sido dirigidos a entidades económicas, empresas dos mais variados ramos órgãos de comunicação social e também claro dirigidos a governos de Estados.

Guerra Revolucionária – "O conceito de guerra revolucionária foi apresentado pela primeira vez por Marx e depois sucessivamente detalhado por Lenine, Trotsky, Estaline e Mao Tsé Tung, além de outros. Tem simultaneamente dois significados.

- guerra total, levada a efeito pelos países comunistas, com o fim de implantarem o comunismo em todas as nações.
- Doutrina. Estabelecida para conduzir essa guerra.

Comparando-a com a guerra subversiva verifica-se que a guerra revolucionária, tal como aquela pode ser:

- Conduzida no interior de um território
- Por uma parte da sua população
- Apoiada e reforçada do exterior
- Contra as autoridades estabelecidas
- Para paralisar a sua ação

Mas, além disso. A definição de guerra é mais pormenorizada em três aspetos:

- Na doutrina seguida pelos elementos que a conduzem
- Nos objetivos particulares a atingir
- Nos meios e processos a empregar

Quanto à doutrina: enquanto a guerra subversiva pode ser conduzida em conformidade com qualquer doutrina ou, até nenhuma, a guerra revolucionária é regida por uma doutrina própria, rigorosamente estabelecida e constantemente melhorada pela experiência.

Quanto aos objetivos: A definição de guerra subversiva não fixa, como se disse, quais os objetivos particulares a atingir, enquanto que a guerra revolucionária tem, pelo contrário, objetivos perfeitamente definidos - estabelecer o regime comunista no território em questão e converter toda a sua população a este sistema social.

Quanto aos meios e processos: estes podem, na guerra revolucionária, ser todos sem qualquer exceção. A guerra propriamente dita, com meios convencionais ou nucleares, bem como a guerra subversiva, são considerados, portanto, como processos a empregar na guerra revolucionária".

Guerra Psicológica – " O conceito de guerra psicológica está ligado aos meios e processos utilizados. É uma luta levada a efeito por um conjunto de meios e processos que têm por fim influenciar as opiniões, os sentimentos e as crenças dos homens - população, autoridades e forças armadas – e, portanto, as suas atitudes e o seu comportamento. Tem, pois, um caráter restrito, idêntico ao de guerra de gases ou de guerra económica por exemplo. Além disso, é comum a todos os tipos de guerra, convencional, nuclear ou subversiva.

A razão da sua confusão com a guerra subversiva reside no facto de a guerra psicológica encontrar naquela, um campo de ação ideal e de não poder conduzir-se uma guerra subversiva sem ação psicológica. Mas não é realmente mais do que um dos processos empregados para levar a efeito uma guerra subversiva. (Exército, 1966:53)

Guerra Insurrecional – "A expressão guerra insurrecional designa uma luta armada, de caráter político, levada a efeito num dado país com poder político constituído. Em certos aspetos este conceito é, portanto, mais lato que o de guerra subversiva (uma guerra insurrecional não é obrigatoriamente levada a efeito pela população civil, como a subversiva); noutros, porém é mais restrito (uma guerra subversiva pode não ter caráter político, nem ser conduzida contra o poder político constituído mas sim contra autoridades de ocupação). Deste modo; certas guerras insurrecionais serão subversivas, mas outras não.

Um dos exemplos mais característicos de guerra inssurrecional é a «Guerra de Espanha» conduzida contra o governo legal, mas com forças militares organizadas e segundo os moldes de uma guerra convencional." (Exército, 1966:5)

2.4 PRINCIPAIS TEÓRICOS DA GUERRA DE GUERRILHA

Sun Tzu

Não se sabe ao certo se Sun Tzu terá existido ou não. Deveria ter vivido no período clássico chinês (551 a.C – 249 a.C) A sua obra terá sido escrita cerca do ano 500 a.C e tem o título A Arte da Guerra que é o precursor da literatura da arte da Guerra. No que diz respeito à guerra de guerrilha a obra é inovadora dado que ele afirma que a estratégia e tática " … são baseados na deceção na criação de falsas aparências para confundir e iludir o inimigo, na aproximação indireta, na adaptabilidade pronta à situação do inimigo, na manobra flexível e coordenada de elementos de combate separados e na concentração rápida contra pontos fracos" (Lara, 2011:

370-376) São de especial interesse para um atacante de sistemas de informação os ensinamentos contidos na sua doutrina. Entre outros destaco:

- A tese que diz que toda a guerra é baseada na deceção;
- O princípio do ludíbrio do inimigo ("quando capaz finge incapacidade; quando ativo, inatividade; quando faz parecer que está longe, quando longe que está perto; oferece ao inimigo uma isca para o tentar, finge desordem e ataca-o" (Lara, 2011: 373)
- O princípio da guerra psicológica" enfurece o seu (do inimigo) general e confunde-o; mostra inferioridade e encoraja a sua arrogância; mantém-no sob tensão e desgasta-o; quando estiver unido, divide-o"
- O princípio da surpresa no ataque "ataca quando ele não estiver preparado, investe quando ele não te espera" (Lara, 2011: 373)

No capítulo 2 é de reter dois ensinamentos:

- Um ataque pode ser engenhoso, mas deve ser lançado com velocidade sobrenatural
- Não há uma guerra prolongada da qual algum país tenha beneficiado.

Clausewitz via a guerra de guerrilha como uma forma de "desbaste" das forças do inimigo Era vista como uma forma de auxílio à guerra convencional. As suas operações militares deveriam centrar-se em pontos previamente determinados, ao longo dos flancos do dispositivo inimigo (Clausewitz: 1984).

T.E. Lawrance, após a sua experiência de comando de forças não regulares de tribos árabes no médio-oriente, teoriza que é possível que a guerrilha poderia ser bem sucedida se aplicasse operacionalmente determinados princípios que a tornariam uma ciência exata. Segundo Lawrance o que era necessário era a construção ou existência de uma base que fosse inexpugnável e um inimigo com recursos limitados de controlo de determinado território e uma população apoiante da caus a da guerrilha. Nestas circunstâncias o que a guerrilha necessitaria seria de velocidade, perseverança, linhas de apoio logístico autónomas. Equipamento capaz de paralisar linhas de comunicação do exército turco. Na perspetiva da estratégia operacional, o alcance e a velocidade eram mais importantes do que a dimensão e a capacidade da força. Lawrence avançou também com a introdução da ideia da dimensão (Estado Árabe) política das ações levadas a cabo pela guerrilha. Sob o ponto de vista de estratégia operacional, encontro vários pontos de contacto entre as ideias de Lawrence e os

ataques de negação de serviço DoS e DDoS. Podemos dizer que a base inexpugnável é o próprio meio, o ciberespaço, desde que esteja devidamente dissimulado, e atacar de uma forma silenciosa o atacante está virtualmente livre de perigos. Conforme for o ataque que pretenda efetuar, ou que as circunstancias e as defesas da vítima, identifica as vulnerabilidade e daí efetua o ataque que lhe parecer mais eficaz. Pode, inclusivamente, contar com o apoio da "população local" na forma de outras máquinas que o atacante consiga captar para levar a cabo os seus intentos. Estou a falar dos casos dos ataques peer to peer bem como das botnets. Também é possível fazer um paralelo com o princípio da velocidade e perseverança de Lawrence. De facto quando se faz um ataque, este tem de ser forte e rápido, especialmente nos casos de negação de serviço, o atacante está a atacar e a paralisar as linhas de comunicação do adversário.

Lenine - As grandes contributos de Lenine e dos seus seguidores foram de duas ordens: por um lado a adaptação da teoria de guerrilha ao marxismo e por outro lado a exploração de novas técnicas nomeadamente a utilização sistemática do crime e do terrorismo

Mao Tsé Tung - Um dos grandes teorizadores da guerrilha revolucionária. Para ele o conceito de revolução assentava em três princípios: o papel decisivo das forças militares; a importância das bases de guerrilha em áreas rurais; e o caráter de fricção do combate. A guerra de guerrilha era uma componente importante da sua doutrina operacional, mas não era o único aspeto da luta revolucionária; por si só não significava a obtenção do sucesso total.

Não era um fim em si e, como tal, não podia ser divorciada das operações militares das forças regulares. Ainda que pudesse assumir temporariamente uma maior importância no contexto da guerra popular, globalmente falando, as forças regulares eram primordiais na estratégia militar

A guerra de guerrilha, de acordo com a conceptualização maoista era apenas uma das três fases interactuantes da luta revolucionária. Genericamente, na sua ótica as insurreições eram um fenómeno típico dos países subdesenvolvidos e contemplavam três fases:

- Agitação e proselitismo das massas populares, incluindo a criação de um Partido (fase de contenção)
- Violência aberta, operações de guerrilha e estabelecimento de bases (fase do equilíbrio estratégico)

- Guerra móvel, convencional, com grandes unidades de forças insurrectas contra forças governamentais com o objetivo de depor o governo (fase da contraofensiva). Durante esta fase as ações militares respeitantes às duas fases anteriores continuam a ser conduzidas" (Dias, Carriço, 2006:59)

Também são de mencionar outros teóricos marxistas leninistas . Tais como: O General Lin Piao desenvolveu as suas teorias durante a guerra de ocupação japonesa, mais tarde vem a aplicá-las na luta contra o Kuomintang e mais tarde no comando do corpo de voluntários maoístas, na Guerra da Coreia. Ho-Chi-Minh o homem que derrotou os franceses e os americanos no Vietname. Vo Nguyen Giap, Josip Broz Tito, Fidel Castro Che Guevara, Carlos Marighella e o seu livro "Manual do Guerrilheiro Urbano e outros textos" (Marighella, 1975:59) aonde advoga :

a) "A liquidação física dos chefes e dos postos menores das forças armadas e da política."
b) A expropriação (eufemismo de roubo ou furto) do Governo

Marighella aconselha, os assaltos a bancos, a ricos comerciantes e dos grandes proprietários agrícolas, pois tais ações teriam um efeito duplo político: o do financiamento da subversão, bem como, simultaneamente provocariam grandes danos no sistema capitalista: a rede bancária. Este é um dos pontos que vem ao encontro das atuais atividade criminais de muitos hackers, que fazem fraudes com cartões de crédito, obtêm informação bancária através de ataques de phishing e enviam spam tudo com o fito de extorquir dinheiro, transferência clandestina de capitais etc. Existem mesmo algumas zonas de países cuja principal fonte de receita é a fraude e o crime informático. Falo, nomeadamente De algumas províncias da Roménia bem como de certas zonas na Ucrânia e Rússia

CAPÍTULO 3

Apresentação do Estudo de Caso

3.1 INTRODUÇÃO

Na primeira fase do estudo, estudarei 3 tipos de ataques de negação de serviço. A saber:

a) Estónia versus Rússia em 2007

b) Geórgia versus Rússia a propósito da Ossétia do Sul em 2008

c) Google versus República Popular da China em 2010

Creio que estes três casos de ataques informáticos, representam 3 situações diferentes da versatilidade das tecnologias da informação e, da forma como se pode fazer política com eles.

3.2 ORGANIZAÇÃO DO ESTUDO DE CASO

A primeira parte da investigação consistiu em estudar os 3 casos de ataques cibernéticos acima mencionados. Eu pretendia comparar, sobretudo, identificar padrões e comportamentos que pudesse utilizar na segunda parte do trabalho, quando estivesse a comparar esses ditos padrões com episódios passados de guerra de guerrilha Pretendia verificar se a preparação logística, tática, os resultados obtidos eram comparáveis ao processo de preparação dos ataques de negação de serviço e se poderia considerar estes tipos de ataque como mais uma arma no arsenal tático da guerrilha moderna.

Reconhecendo que estava perante um assunto complexo que tocava várias áreas: (informática, telecomunicações, estratégia, história e sociologia), bem como o facto de pretender fazer comparações, levou a que eu optasse pelo Método do Estudo de Caso[14].

3.2.1 CRITÉRIOS USADOS PARA AVALIAÇÃO E COMPARAÇÃO

Escolhi cinco critérios de comparação para o termo de comparação, os ataques DoS DDoS, bem como os mesmos cinco critérios para avaliar as ações de guerra de guerrilha.

<u>Tipo de ataque</u>:

a) Qual o tipo de ataque cibernético

b) Que tipo de ataque guerrilheiro foi executado ou havia capacidade para executar.

Neste ponto pretendo sobretudo comparar a logística e a tática que conduzia aos ataques

[14] YIN, Robert K. *Estudo de Caso*, Planejamento e Métodos: Porto Alegre 2001

Origem Interna/Externa:

a) De aonde parte o ataque, nacional, ou se provem do estrangeiro, ou verificam-se os dois casos.
b) De aonde parte o ataque, em princípio será de dentro do território. A não ser que haja um país limítrofe que sirva de santuário.

Efeito dos Ataques:

a) Qual o efeito obtido está de acordo com os objetivos

Lições Recolhidas:

a) O que correu bem e o que correu mal, como melhorar a eficácia do ataque.

Os dois primeiros requerem alguma clarificação: No que diz respeito ao tipo de ataque informático, é importante saber claramente o que se pretende obter porque é durante a fase de penetração que se descobrem as vulnerabilidade que determinam os ataques que se podem efetuar e dentro destes quais os mais apropriados aos resultados que se pretende obter. Pode ser um simples ataque de negação de serviço, pode ser um ataque de recolha de informação, ou um simples desfiguramento de um site, colocar vírus, ou worms para serem utilizadas mais tarde, colocar um verme (worm) que seja uma back door e assim proporcionar mais visitas aquela máquina.

A origem interna ou externa de um ataque é difícil de determinar dado existir a possibilidade de se estar a usar IP spoofing, no entanto dá-nos algumas indicações, poucas, sobre a origem do ataque e os seus eventuais motivos. Por exemplo: Se estivermos perante um ataque de desfiguração, o motivo e a página aonde foi feita são óbvios.

Foi sempre minha preocupação arranjar um padrão de comparação dos ataques DoS DDoS que fosse amplo e pudesse servir de referência para um grande número de casos. Para a elaboração deste trabalho escolhi os seguintes 3 casos acima referidos: Estónia versus Rússia 2007; Geórgia versus Rússia 2008; Google versus República Popular da China 2010. Estes 3 ataques representam três marcos incontornáveis na história dos ataques cibernéticos, pela sua dimensão, pela conjuntura que levou ao seu desencadeamento, um deles (Geórgia) é uma manobra precursora de uma agressão militar. Por outro lado, cada um deles é um caso diferente, com diferentes motivações e muito possivelmente com diferentes atores. Dois deles poderão estar direcionados contra outros Estados e o terceiro contra uma empresa multinacional privada.

No que diz respeito à guerra de guerrilha, os exemplos que consegui recolher com algum contexto de ordem tática e logística dizem respeito a: Malásia, URSS, R.P. China, Vietname, Argélia, Guiné Portuguesa

3.2.2 ANÁLISE QUALITATIVA

Na elaboração deste estudo tive duas preocupações :

a) Saber se estava a comparar o que é comparável
b) Procurar saber qual o universo para o qual as minhas conclusões, baseadas num universo tão restrito, teriam significado; se é que não eram de todo irrelevantes.

A primeira foi-se resolvendo à medida que escrevia e investigava, procurei sempre manter uma estrutura lógica, em que os vários elementos se suportam conceptualmente entre si. Encontrei eco em Franklin Y Ballau[15] "corroboração estrutural: processo mediante o qual várias partes dos dados / categorias por exemplo) se suportam conceptualmente entre si (mutuamente). Implica reunir os dados e a informação emergente para estabelecer conexões ou vínculos que eventualmente criam um todo, cujo suporte são as próprias peças da evidência que o compõem ".

Tendo inferido uma lógica de comportamento em Yin[16] fiz o tratamento numérico dos parcos dados obtidos . Os "casos" não são amostras estatísticas e que o objetivo da pesquisa pelo método do Estudo de Caso é entender o comportamento lógicos subjacente. Enfim esta é uma resposta parcial de aonde posso inferir unicamente uma determinada lógica de comportamento em determinadas circunstancias.

[15] FRANKLIN , y Balllan. *Reliability and Validity in qualitative research*. Apud SAMPIERI, Roderto, COLLADO;. Collado, LUCIO, Pilar. *Metodologia de la Investigación* 4 ed. Santa Fé 2004 p 666
[16] YIN, Robert K Trad. Daniel Grassi. *Estudo de caso:*Planejamento e Métodos. Belo Horizonte: Bookman, 2001

CAPÍTULO 4

Ciberataques à Estónia 2007

Estou a referir-me a uma série de ataques que ocorreram na Estónia em 2007. Os ataques começaram no dia 7 de abril e afetaram sites de variadas instituições e organizações estónias, tais como: Parlamento. Todos os bancos comerciais, empresas de telecomunicações, jornais e rádios comerciais. "Foi a primeira vez que um ataque de negação de serviço pôs em causa a segurança nacional de toda uma nação"[17]. O acontecimento que desencadeou este ataque informático, tinha ocorrido alguns dias antes, quando o Governo estónio tinha decidido remover uma estátua de bronze, da baixa de Tallin. Os soviéticos tinham construído a estátua em 1947 para comemorar os seus mortos em combate depois de terem expulsado as tropas alemãs no final da Segunda Guerra Mundial. Após a guerra, a Estónia transforma-se numa república soviética dirigida por Moscovo. A polícia secreta instalou-se e, rapidamente, hordas de estónios estavam a ser presos e deportados para a Sibéria. Para muitos estónios, a estátua era um símbolo da ocupação opressiva. Tinham passado 16 anos desde a reconquista da independência, os estónios estavam prontos a não ceder às ameaças e chantagem do governo Russo - que tinha avisado repetidamente, que a remoção da estátua seria "desastrosa" para os estónios - e retiraram a estátua. Foi instalada, três dias depois, num cemitério militar, nos subúrbios.

Mesmo antes de a estátua ser retirada, houve violência nas ruas de Tallin. Vândalos, destruíram montras de lojas, viraram automóveis ao contrário e apedrejaram a polícia de choque. Grande parte dos manifestantes eram de etnia russa[18]. No entanto, os ânimos acalmaram rapidamente, cessaram os combates de rua, centenas de pessoas foram presas. Os estragos foram reparados antes do dia 28 de abril. Tratava-se de uma calma aparente já que nesse dia começaria um dos maiores ataques cibernéticos de negação de serviço que há memória.

A Estónia é um país que apostou e aderiu fortemente às tecnologias da informação: Cerca de 49% da população lê diariamente o jornal online. Mais de 90% das transações bancárias são feitas pela internet. Existem muitos pontos Wi-Fi gratuitos Os telemóveis podem ser usados para pagar parqueamentos ou pagar refeições e o Skype está a arrebatar o negócio das

[17] http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

[18] A etnia russa representa um quarto da população total da Estónia.

chamadas internacionais, à operadora telefónica nacional. Dito de outra forma a Estónia ou e-Stonia, como alguns cidadãos preferem, é uma janela aberta para o futuro.

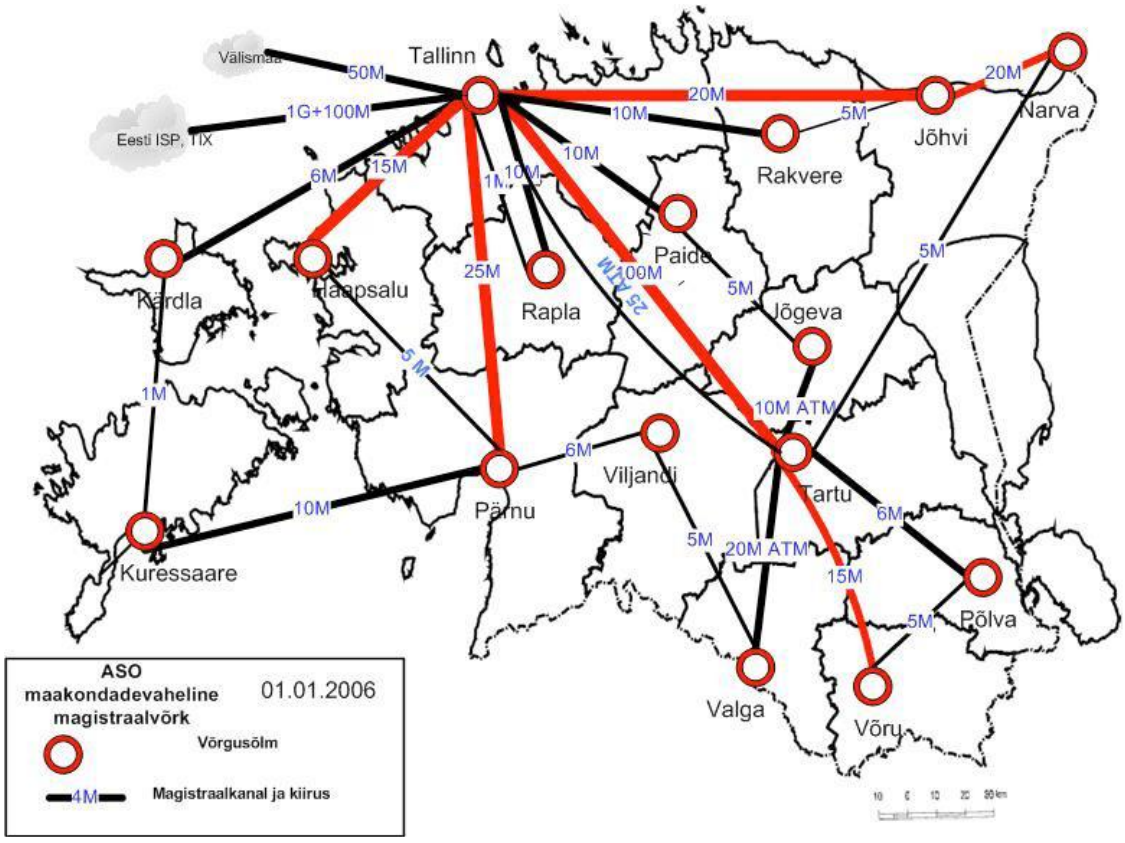

Figura 2
Esquema da rede pública[19]

Alguns dos ataques foram de Distributed Denial of Service (DDoS). Os hackers usaram centenas senão mesmo milhares de máquinas comprometidas "zombie" e inundaram sites estónios com milhares de pedidos por segundo, aumentando enormemente o tráfego. Os ataques à Estónia foram efetuados maioritariamente por Script kiddies, pessoas que copiam linhas de código previamente publicados em sites na internet. Normalmente nem têm conhecimentos para saber os efeitos daquele código. No entanto são úteis dado que dão dimensão ao ataque A sua primeira arma foi o ataque com pings sucessivos repetidos centenas de vezes por segundo, o que pode levar ao encerramento de um servidor. Os Script kiddies reuniam-se em torno de salas de conversação em língua russa. Primeiro foram doutrinados e acossados com a remoção da estátua no dia 27 d abril. Uma semana mais tarde, começaram a

[19] http://www.riso.ee/en/pub/2003it/p15.htm

aparecer mensagens para a coordenação de ataques no dia 9 de maio (Data em que a Rússia comemora a vitória sobre a Alemanha Nazi). De facto no dia 9 de maio aconteceu outro ataque ainda mais intenso. Pensa-se que foram utilizadas cerca de 58 botnets. Alguns dos ataques vinham da Rússia, incluindo um do gabinete administrativo do próprio Presidente Putin. No entanto, é de querer que esses computadores estivessem comprometidos da mesma forma que as máquinas dos EUA estavam. De facto, pelos IP's não se chegava a conclusões seguras. No entanto, existiam muitas provas circunstanciais que apontavam apara a Rússia. De facto o Ministro dos Negócios Estrangeiros estónio acusou a administração de Putin de estar por detrás do ataque. Contudo a Rússia sempre negou que estivesse por detrás destes. A 6 de setembro de 2007 o ministro da Defesa estónio admitiu que não tinha provas que ligassem os ataques às autoridades russas. Finalmente em janeiro de 2008 um estónio de etnia russa foi acusado de ter participado nos ataques e julgado. A 10 de março de 2009 Konstantin Goloskokov um "comissário" da juventude do grupo Nashi, declarou que era responsável pelo ataque. Os peritos estão céticos quanto a estas variadas assunções de responsabilidade por parte de cidadãos russos

Figura 3[20]

28 – 30 de abril de 2007, primeira noite do ataque até segunda-feira

[20] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

Critérios de comparação

Tipo de Ataque- Partindo de uma informação deficiente e muito imprecisa sobre este assunto, encontro 2 géneros de ataque: Negação de serviço distribuída (DDoS) que teria partido de centenas ou mesmo milhares de botnets. Também surgiram ataques de phishing, Spam de E-mail, desfiguração de sites, ataques TCP SYNC. Também há referência a ataques de pings (ICMP) violentos podendo também ter origem em botnets ou autores individuais.

Origem interna/externa do ataque- Este ataque teve claramente origem externa e espalhada pelo planeta, há referências a IP`s dos EUA Europa ocidental, Irão. No entanto estes IP pouco ou nada nos dizem dado que, apesar de poderem ser verdadeiros, muito provavelmente, pertencem a máquinas que estão comprometidas e fazem parte de botnets e, desta forma, nem o seu próprio proprietário sabe. Também houve ataque a partir da Rússia, no entanto sem serem um número expressivo, apesar de antes do segundo ataque (9 de maio) existirem sites de língua russa que incitavam aos ataques e fornecendo ferramentas para os realizar.

Efeitos dos Ataques- Os ataques foram bastante generalizados: o Parlamento estónio, Ministérios, Redações de jornais, os principais bancos comerciais, empresas de telecomunicações, servidores de DNS. Conseguiram parar a quase totalidade dos serviços via internet.

Lições aprendidas- Na ótica dos atacantes o ataque foi bem sucedido e os seus objetivos parecem ter sido atingidos, embora não saibamos quais eles eram. Sob o ponto de vista da Estónia, deu lugar a uma grande reflexão, sobre a segurança da internet e as boas práticas que devem ser seguidas. Claro que há muito mais aspetos que mudaram na rede estónia bem como na sua topologia. Seria interessante verificar que alterações foram feitas para robustecer a rede. No entanto não encontrei dados sobre o assunto e, também, isso escapa ao âmbito deste trabalho

CAPÍTULO 5

Guerra Russo- Georgiana Ataques cibernéticos

A série de ataques cibernéticos que pretendo analisar está inserida num conflito maior, que teve início em agosto de 2008, opondo a Federação Russa à Geórgia, a propósito da Ossétia do Sul, uma região autónoma de jure desde 1992 e desmilitarizada, que se situa na fronteira de Geórgia com a Rússia,

A Ossétia do Sul tornou-se independente "de facto" da Geórgia em 1991, aquando do conflito entre a Geórgia e a Ossétia do Sul. No entanto a comunidade internacional continuou a reconhecer a Ossétia do Sul como parte da Geórgia. Apesar de ter havido um cessar fogo e numerosos esforços de paz, o conflito continuou sem solução.

Figura 4
Mapa da Geórgia e da Ossétia do Sul[21]

Tendo em vista a estabilidade da região depois do conflito de 1991, formou-se , no âmbito da OSCE, uma força de manutenção de paz. Esta força era constituída por russos, georgianos e ossétios. O comando desta força foi confiado à Rússia. Na prática esta força de manutenção de paz falhou e as tensões foram aumentando gradualmente entre a Geórgia e os elementos separatistas ossétios, que por sua vez eram apoiados pela Rússia. No dia 7 de agosto de 2008, depois de provocações separatistas, forças georgianas lançaram um ataque surpresa contra as

[21] http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

forças separatistas. A 8 de agosto a Rússia respondeu ao ataque efetuando operações militares em território georgiano que foi tomado pelas autoridades de Tiblissi como una invasão. No dia 7 de agosto antes da invasão russa ter começado, começaram uma série de ataques cibernéticos dirigidos na sua maioria a sites do governo georgiano. Desta forma tornou-se o primeiro caso em que um conflito internacional político e militar, foi acompanhado, ou mesmo precedido por uma ofensiva de ataques cibernéticos.

A Geórgia e a Sociedade da Informação

Estatísticas referentes ao setor das Tecnologias da Informação mostram que somente 7 em cada 100 georgianos têm ligação à internet. Este número tão baixo de utilizadores reflete bem a capacidade das infraestruturas bem como a falta delas. Por outro lado, mostra também a falta de fiabilidade destas. No entanto, apesar de tudo, o número de utilizadores tem vindo a crescer, de uma forma sustentada.

Têm surgido várias críticas pela dependência que a Geórgia apresenta em relação à Rússia. Temos de ter em consideração a geografia da região, a Geórgia tem poucas possibilidades de ligação terrestre à internet, são elas via: Turquia, Arménia, Azerbaijão e Rússia. É justamente pela Rússia que passa a ligação à Geórgia. A Geórgia tem dificuldade de acessos redundantes à internet, por diferentes países vizinhos Para alterar esta situação, a Geórgia decidiu colocar um cabo de fibra ótica no mar Negro que a ligou diretamente Varna na Bulgária e daí para o resto da Europa. Aquando do começo do conflito de 2008 este cabo estava quase terminado.[22]

Métodos de Ciber-ataques

Os métodos de ataques informáticos utilizados foram vários. Os mais utilizados foram o desfiguramento de websites públicos e a Negação Distribuída de Serviço. O desfiguramento era dirigido a sites políticos, ou do governo, bem como instituições financeiras

[22] http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Figura 5
Um dos desfiguramentos utilizados[23] Alguns sites que foram desfigurados:[24]

As estatísticas do ataque fornecidas pela Arbor Networks[25] mostra uma grande intensidade de ataques com um volume de tráfego a chegar aos 211.66 Mbps como valor médio e 814.33 Mbps como valor máximo. No que diz respeito à duração, o ataque médio teve uma duração de 2 horas e 45 minutos, tendo sido de 6 horas o mais prolongado.

Existe consenso alargado de que os ataques eram ataques coordenados, desde o primeiro momento. Neste ponto existe uma diferença em relação ao caso dos ataques à Estónia, aonde só foi identificável um padrão de coordenação, na segunda fase dos ataques

Origem dos Ataques

Tal como no caso da Estónia, não há provas conclusivas de quem esteve por detrás dos ataques DDoS no entanto é geralmente apontada a Rússia como sendo a origem dos ataques. Há um consenso alargado de que os ataques estavam coordenados e os autores devidamente instruídos do que se ia fazer.

De acordo com a Arbor Networks que efetua análises de tráfego, os maiores ataques observados, tinham origem de todo o mundo, sugerindo assim a existência de uma botnet ou de múltiplas botnets

[23] http://en.wikipedia.org/wiki/Cyberattacks_during_the_2008_South_Ossetia_war
[24] www.president.gov.ge website de Mikheil Saakashvili, Presidente da Republica da Geórgiawww.nbg.gov.ge website of the National Bank da República da Georgiawww.mfa.gov.gewebsite do Ministério dos Negócios Estrangeiros da Republica da Geórgia.
[25] http://www.arbornetworks.com/

Segundo a Shadowserver Foundation[26] desde os primeiros dias do ciber-ataque à Geórgia , existiram pelo menos seis diferentes servidores de comando e controle das botnets implicadas no ataque. Algumas destas botnets são para alugar e praticar ataques DDoS ou para extorsão baseada em DDoS. A botnet de ataques http funcionava com um servidor de comando e controlo que foi identificado como sendo um controlador MachBot que é uma ferramenta frequentemente utilizada pelos botherbers russos.

Existem algumas indicações do envolvimento do RBN[27].O perito em segurança da Shadowserver pensa que o envolvimento não foi além de ter proporcionado alojamento do servidor de Comando e controle e que não foi ele RBN a cometer os ataques de DDoS!

A equipa do projeto Gray Goose, diz que não foi capaz, de encontrar, na pesquisa que fizeram aos sites hackers russos, nenhuma referência a organizações estatais que dirijam ou efetuem os ataques, Tal pode ser por várias razões; Por não haver nenhuma organização estatal relacionada com os ataques, porque os esforços da equipa de pesquisa, não foram suficientemente fundo, ou porque o envolvimento das organizações estatais é feito de forma a que nunca seja possível atribuir-lhe responsabilidades. No entanto, o relatório diz que existe uma tradição de que membros antigos e atuais, delegarem as atividades de guerra cibernética/ ou ciber ataques serem levados a cabo pelos hackers russos

Critérios de comparação

Tipo de Ataque- Partindo de uma informação razoável maioritariamente encontrada na internet, encontro dois géneros de ataque Negação de serviço distribuída (DDoS) que teria partido de algumas botnets bem organizadas e pode-se encontrar um modelo de atuação durante os ataques. O segundo ataque mais praticado foi a desfiguração, sobretudo relacionada com políticos e a associação do Presidente Shaskashevili com Hitler. Há também notícias de ataques a servidores de correio eletrónico

Origem interna/externa do ataque- Este ataque teve claramente origem externa e espalhada pelo planeta, há referências a IP`s dos EUA Europa ocidental, Irão. No entanto estes IP`s pouco ou nada nos dizem dado que, apesar de poderem ser verdadeiros, pertencem a máquinas que estão comprometidas e fazem parte de botnets e, desta forma, nem o seu próprio proprietário sabe. Parece existir uma ligação à RBN Russian Business Network.

[26] http://www.shadowserver.org/wiki/

[27] [51] Russian Business Network. Uma organização de ciber-crime especializada em phishing, código malicioso e comando de botnets .

Depois existem muitas alegações à participação russa no ataque cibernético, tal como no caso da Estónia

Efeitos dos Ataques- Os ataques foram bastante generalizados: A Presidência da Geórgia, o Parlamento georgiano, Ministérios, redações de jornais, os principais bancos comerciais, empresas de telecomunicações, televisão, associação de imprensa Conseguiram parar a quase totalidade dos serviços via internet. Apesar de o ataque ter sido pesado e demorado no tempo, não teve grandes efeitos sobre a vida normal no país devido à pouca expressividade da internet - só 7 habitantes em cada 100 - possuem ligação, ao contrário da Estónia, o dia a dia não está baseado nas Tecnologias da Informação.

Lições aprendidas- Na ótica dos atacantes o ataque foi bem sucedido e os seus objetivos parecem ter sido atingidos, e ao mesmo tempo acompanhados com uma invasão militar. Claramente há uma estratégia de lançar a confusão na internet, cortar serviços vitais, fazer propaganda e ao mesmo tempo que se atua no mundo virtual está-se a atacar com forças militares. Dá a ideia que o ataque cibernético visou também suavizar a resistência georgiana sob o ponto de vista da Geórgia, reforçou a autonomia dos acessos internacionais à internet, daí o ter colocado o cabo submarino para a Bulgária. Verificou que estava demasiado dependente, em termos de internet, da Rússia, o que não é nada bom quando se tem um conflito de disputa sobre um território fronteiriço, a Ossétia do Sul

CAPÍTULO 6

O caso Google – R.P.China

Operação Aurora

Desde meados de 2009 até janeiro de 2010 foi lançado e mantido um ataque contra o Google e mais 20 outras empresas. De acordo com um telegrama diplomático da embaixada dos EUA em Pequim, uma fonte chinesa teria revelado que estes ataques teriam sido dirigidos pelo Politburo. O telegrama sugeria que este tipo de Hacking faria parte de uma campanha coordenada, levada a cabo por funcionários governamentais, peritos em segurança pública e criminosos da Internet recrutados pelo governo chinês. Aurora era o nome da operação e o seu propósito específico era atacar o Google, mais concretamente as contas de Gmail de dissidentes e ativistas dos direitos humanos chineses. Num âmbito mais lato o objetivo do ataque era ter acesso e modificar código fonte[28]de 20 a 34 empresas de alta tecnologia, segurança e de defesa. Os atacantes exploraram uma vulnerabilidade do formato Adobe PDF no browser do Microsoft Internet Explorer. O objetivo era abrir uma porta das traseiras (back door), através da qual o intruso entraria e apoderar-se-ia do código fonte.

Funcionamento do esquema Aurora

A operação Aurora incluía muitos passos que eram invisíveis para o atacado. Como se pode ver pelo esquema abaixo. O ataque dava-se de uma forma totalmente silenciosa sem qualquer pista do ataque malicioso que estava a acontecer. "[29]…A operação Aurora tem 6 passos:

1- A vítima recebe um link num email ou mensagem instantânea de uma fonte em que ele confia.
2- A vítima clica sobre esse link, que a leva a visitar um site instalado em Taiwan que contém também um script malicioso em linguagem Java.
3- O browser do atacado descarrega esse script Java que incluí uma vulnerabilidade desconhecida, ou conhecida por muito poucos do browser Internet Explorer.
4- O código malicioso descarrega código máquina disfarçado numa imagem dos servidores em Taiwan e executa o código malicioso

[28] Código fonte é aquele que está por detrás de qualquer software e que permite que esse software funcione. Muitas vezes esse código está escrito em linguagens de baixo nível. O código fonte pode ser aberto ou fechado.
[29] http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

5- O código malicioso cria uma porta das traseiras (backdoor)que se encontra nos servidores de comando e controle (C&C) localizados em Taiwan.

6- Tudo isto resulta que o atacante tem acesso total à máquina da vítima. Os atacantes chineses pretendiam sobretudo assuntos de propriedade intelectual, configuração e gestão de software. O atacante poderia usar a máquina para explorar mais outras máquinas instaladas na mesma rede…."

Figura 6
Os seis passos do ataque[30]

Desde que o Google chegou à China em 2006, concordou num arranjo em que ele não apresentaria uma lista de assuntos proibidos por Pequim. Por proceder desta forma. a Google foi criticada um pouco por todo o lado. No entanto depois deste ataque sofisticado que visava entre outras coisas ler a correspondência do Gmail, das contas de defensores dos direitos humanos na China, a situação chegou a um ponto em que continuar na China não era possível. A Google saiu da China. Atualmente os seus serviços em língua chinesa, são fornecidos a partir de Hong Kong e de Taiwan

[30] http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

Claramente estamos perante um ataque totalmente diferente, é um ataque de espionagem em larga escala, decidi inclui-lo devido à sua importância e alcance, pelo seu processo engenhoso de propagação, mas sobretudo porque foi um caso que envolve um Estado e uma empresa privada, o que apresenta uma outra vertente da topologia de ataques futuros – um Estado contra uma empresa privada estrangeira – é um ataque diferente dos ataques à Estónia e à Geórgia. É um ataque que apresenta características muito particulares, tanto a nível do alvo ou alvos, a sua concepção e engenharia, o que se pretendia obter com ele.

Tipo de Ataque- Partindo de uma informação razoável sobre o género do ataque. Num primeiro momento parece um simples ataque de verme (worm) no entanto este abre uma backdoor que permite o atacante fazer tudo, inclusivamente roubar código fonte ou alterá-lo. Por outro lado, o ataque é feito a um empresa privada que se encontrava a trabalhar na República Popular da China, Não é um ataque a outro Estado. No entanto a maior parte das outras 30 empresas também eram americanas!

É um ataque que tem como objetivo roubar e passar impune. Não é um simples DDoS que visa somente cortar o acesso e demonstrar poder. É um ataque muito próximo, se não mesmo de espionagem industrial por um lado, por outro lado é um ataque à privacidade do correio eletrónico dos seus cidadãos. Por outro lado este ataque também pode dar origem a botnets

Origem interna/externa do ataque- Este ataque tem uma assinatura. Essa assinatura vem do servidor C&C comando e controlo de Taiwan. Como Taiwan é reconhecido pelas Nações Unidas como um Estado, temos de dizer que o início do ataque é externo, embora no caso do Google o ataque visava claramente máquinas dentro da R.P. China

Efeitos dos Ataques- A Google afirma que Pequim não conseguiu ler o conteúdo das mensagens , só leu os cabeçalhos destas e soube os IP's. Sob o ponto de vista do roubo de código fonte, é muito mais difícil saber quantas foram atingidas: Algumas delas terão sido: Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Grumman, Morgan Stanley e a Dow Chemical.

Lições aprendidas- Na ótica dos atacantes o ataque foi bem sucedido e os seus objetivos parecem ter sido atingidos. Claramente, há uma estratégia de enganar e passar despercebido. O que há de novo, é uma vulnerabilidade praticamente desconhecida no Microsoft Internet Explorer e a sua utilização. Utilizou-se um verme que descarregava o código malicioso de uma imagem de Taiwan, estamos perante um caso de

esteganografia[31]. Esse código visava controlar outras máquinas, podendo assim dar origem a um botnet. A lição a tirar perante um ataque sofisticado como este é: ter sempre as últimas atualizações do software de forma a ser menos suscetível a vulnerabilidades de código. Ter um bom antivírus e deixá-lo atualizar-se. Possuir uma firewall com políticas bem definidas. e em último caso para os documentos altamente sensíveis, utilizar encriptação. Contudo há situações em que uma máquina com conteúdo sensível não deve estar ligada à internet

[31] Processo de encriptação que utiliza os píxeis de uma imagem.

CAPÍTULO 7

Episódios de Guerra de Guerrilha

A Emergência Malaia 1947-1960

O caso da Malásia é, possivelmente um dos mais interessantes de analisar, dado que ele foi um dos poucos casos de derrota da guerra de guerrilha. Durante a ocupação japonesa da Malásia na II Guerra Mundial, a única resistência organizada à ocupação japonesa era a do Exército Anti Japonês do Povo Malaio. O núcleo duro deste exército era constituído por membros do Partido Comunista Malaio, sendo a maioria dos seus membros de etnia chinesa.

Quando a paz chegou, os comunistas possuíam uma organização capaz de travar batalhas e de se opor à dominação britânica. Proclamaram a criação do Exército de Libertação das Raças Malaias (MRLA).

A selva malaia tornou-se o seu refúgio dado que as unidades regulares do exército britânico não os conseguiam apanhar devido à natureza desta. Inicialmente os britânicos tentaram penetrar na selva com os efetivos de um batalhão, mas mesmo que as ações militares fossem realizadas em esquadra, eram constantemente mal sucedidas, porque a informação da sua aproximação chegava bastante antes do que eles. Quando por vezes conseguiam encontrar um acampamento, já há muito os guerrilheiros haviam dispersado para outra posição previamente estabelecida. A perseguição britânica seria inútil, mas. por precaução, os guerrilheiros deixavam ficar para trás uma pequena força para assegurar o atraso dos britânicos

As suas táticas de guerrilha eram baseadas no medo/intimidação, terror, assassinato, fogo posto, raptos de mulheres ou crianças ameaças e chantagens.

Tinham como objetivo cativar as populações asiáticas, especialmente os chineses que constituíam quase metade da população da Federação.

Para manterem a sua organização e a sua existência, a guerrilha precisava de dinheiro, alimentos, armas e munições. No que diz respeito a dinheiro e alimentos eles confiavam no que podiam extorquir à população local. Esta extorsão tornou-se quase numa "arte". Os comunistas tornaram todas as pequenas comunidades responsáveis pelo fornecimento de uma quota em dinheiro dos seus salários semanais e todas as famílias foram encarregadas de fornecer alimentos segundo os seus ditames. Este sistema de fornecimento foi muito facilitado pela presença de uma vasta população de colonos, sendo a maior parte chineses. Estes chineses e os seus antepassados tinham entrado na Malásia, a maior parte ilegalmente, estabeleceram-se numa determinada área aonde as suas casas isoladas, formavam postos

ideais para fornecer dinheiro e alimento à guerrilha comunista. Outros viviam em aldeias de colonos que se tinham desenvolvido com o decorrer do tempo e que estavam distantes das áreas populacionais mais importantes tornando-se unicamente acessíveis aos guerrilheiros.

A partir de 1950 a situação muda com a execução do plano do General Sir Gerald Templar, que consistia numa serie de medidas em relação à população civil bem como à distribuição das forças combatentes.

Todos os colonos isolados foram concentrados em aldeias defendidas por arame farpado, protegidos por postos de polícia. Tendo também centro médico e escola. Estas medidas não se destinavam só a proteger os colonos mas também a darem-lhe um grau de segurança. Com o tempo perderam algum do seu medo e começaram a dar informações à polícia.

Com a finalidade de ter uma melhor compreensão sobre a forma como as atividades comunistas eram assimiladas ao nível mental das populações indígenas, foi estabelecido uma força de pesquisadores/esquadrinhadores composta por ingleses, Malaios, indianos, e chineses - a constituição étnica da Malásia. Esta força destinava-se a efetuar missões de patrulha no interior da selva, obtendo informações da organização comunista. Depois, estas informações eram utilizadas pelas esquadras e pelotões altamente móveis que entravam na selva para lhes dar luta, utilizando as mesmas técnicas e táticas guerrilheiras.

A guerrilha começou a sentir o aperto, A dificuldade de manter as linhas de abastecimento locais, depois da transferência dos colonos que viviam na orla da floresta, obrigou-os a dependerem de culturas feitas nas clareiras da selva. Isto proporcionava bons alvos à RAF para pulverizar essas culturas com veneno ou queimá-las. A Marinha Real também exerceu pressão sobre o MRLA, tornando impossível, por via marítima, a importação de armas ou de alimentos.

Toda esta pressão teria de ter efeito sobre a moral da guerrilha. Então os britânicos decidiram atacar na frente psicológica. Utilizaram helicópteros equipados com altifalantes que pairavam de noite, sobre os acampamentos da guerilha massacrando-os com avisos acerca da sua desastrosa situação e aonde lhes era dado a escolher: deixar os comunistas e ter uma nova vida na Malásia ou; ter uma vida pobre e morrer brevemente.

A parte humorística desta bem sucedida ofensiva de guerra psicológica, foi que muitos dos guerrilheiros que se apressaram a render-se, relataram que a sua maior dificuldade em tirar proveito da oferta da amnistia, consistia em não encontrar meio de saída da densa selva, à noite. Estes guerrilheiros não ousavam movimentar-se durante o dia porque se tornavam vulneráveis ao desagrado do pessoal das suas unidades, normalmente manifestado por uma

saraivada de balas que constituíam o "Boa Viagem" de despedida aos que tentavam escoar-se para o lado dos Britânicos.

Os Ingleses montaram holofotes coloridos e camionetas providas de aparelhagem sonora que serviam de guias até ao posto de polícia ou do exército mais próximo" (Osanka:1963)

Tipo de Ataque- Os tipos de ataques perpetrados pela guerrilha eram: infundir medo, intimidar, terror, chantagem, criação de zonas, na orla da floresta aonde cobravam o imposto revolucionário. Havia possibilidade de executar assassinatos, fogo posto, rapto de mulheres ou crianças, ameaças e chantagens.

Origem Interna ou externa dos ataques- Os ataques são efetuados em pequenas aldeias isoladas na orla da floresta, sabendo-se que as tropas guerrilheiras se acoitam na grande floresta equatorial malaia. A origem dos ataques é nacional .

Qual o efeito dos ataques- O grande efeito obtido por estes ataques foi criar um sentimento de coação, intimidação e de terror (no caso dos assassinatos) que visavam isso mesmo gerar o terror, a intimidação para coagir a população a ajudá-los. Esta ação estava de acordo com os objetivos de criar uma retaguarda de população amedrontada e dócil, que lhes servisse de vetor de fornecimento e, em caso de necessidade, de escudo aonde se pudessem diluir no anonimato.

Lições aprendidas- Desde o final da II Guerra Mundial até 1950, este tipo de operações decorria muito bem e dava aos guerrilheiros : abrigo na floresta, comida, acesso a produtos médicos e medicamentosos, dinheiro, roupas A partir de 1950 a situação muda com a execução do plano do General Sir Gerald Templar, que consistia numa serie de medidas em relação à população civil bem como à distribuição das forças combatentes.

A Guerrilha Partisan Soviética na II Guerra Mundial

A primeira aparição dos partisans na batalha da Rússia verificou-se pouco depois da penetração da Wermacht no país, mas nessa altura mostraram-se ineficazes e denunciaram falta de treino e de organização. Foi só depois de os alemães terem entrado profundamente em território soviético que os partisans iniciaram as suas atividades em grande escala. No espaço de um ano, os bandos combatendo por detrás das linhas alemãs encurralavam os transportes, interrompiam comunicações, destruíam os mantimentos de reserva e causavam pesadas baixas aos alemães. Tão eficazes foram estes guerrilheiros que o exército alemão, de mais de 100.000 homens, foi incapaz de manter limpas as vias principais de abastecimento para a frente.

As forças partisans operando como espiões, sabotadores e soldados atacavam também os pontos de produção de material de guerra. A coordenação dos partisans com o Exército Vermelho era perfeita. Horas antes de se dar o ataque russo, os partisans cortavam as comunicações alemãs, destruíam os seus abastecimentos, desviavam-lhes as suas forças e minavam o ânimo, até ao ponto de se tornarem impossíveis operações bem sucedidas. Os vastos reconhecimentos e a espionagem davam aos partisans detalhes das posições alemãs e até, em alguns casos, o roubo de planos de batalha da Wermacht, raides ao Estado Maior Alemão e interceção de linhas telefónicas alemãs. A enorme quantidade de elementos informativos colhidos em conjunto com outras informações obtidas através de interrogatórios e mesmo de tortura de soldados capturados e de civis russos, depois enviados para o Exército Vermelho. Então, quando o ataque começava, as forças partisans atacavam simultaneamente os alemães pela retaguarda com forças ao nível de regimento. À medida que iam avançando as tropas do Exército Vermelho podiam contar com estradas reparadas e novas, construídas pelos partisans por detrás das linhas alemãs. Pode-se dizer que a guerra partisan realizada pelos russos constituiu grande parte do esforço de guerra soviético. À medida que a guerra prosseguia as forças guerrilheiras partisans, tornavam difícil aos alemães combaterem o Exército Vermelho em igualdade de circunstâncias. Favorecidos pelos invernos rigorosos e pelos erros estratégicos de Hitler, os guerrilheiros eliminaram em primeiro lugar a vantagem inicial alemã e depois passaram das táticas defensivas de resistência para se reunirem e se juntarem ao impulso final para expulsar o invasor do solo russo.

Tipos de Ataques: Cortavam as comunicações alemãs, destruíam os seus abastecimentos, desviavam-lhes as forças, minavam a moral, efetuavam espionagem, interceção de linhas telefónicas, coletavam informação deslocamentos inimigos, recolha de informação através de interrogatórios e torturas. Quando o ataque começava atuavam combatendo na retaguarda do inimigo. Também na retaguarda, melhoravam vias de comunicação para facilitar o deslocamento do exército vermelho.

Origem Interna ou externa das ataques: A origem é interna, se bem que possam existir partisans oriundos de diferentes partes da URSS.

Qual o efeito dos ataques: Desorganização das comunicações e abastecimentos alemães, diminuição da moral. Recolha de informação sensível. Combates na retaguarda alemã. Melhoramentos feitos à rede viária atrás das linhas alemãs, para escoar mais facilmente os deslocamentos soviéticos.

No exército alemão: Desorganização, desalento, sentimento de impotência. Perdas físicas.

No exército Russo: A criação e a atuação do movimento partisan, que não existia no começo da guerra, trouxe importantes benefícios: enquadrar elementos da população e do exército vermelho na luta contra a Alemanha. Recolha de informações sobre o inimigo. Combate na retaguarda deste e melhoria das vias de comunicação

Lições Aprendidas: A principal lição aprendida seria a criação do movimento partisan. Deu um Novo alento à resistência anti-alemã recolha de informações, combater na retaguarda do inimigo. São ações que elevam bastante a moral.

O Exército Vermelho Chinês e a Guerra de Guerrilha

O primeiro chefe do governo comunista chinês Mao Tsé Tung foi também o fundador do exército vermelho chinês. O seu comandante, Chu Teh juntou-se a Mao e tornou-se no seu comandante. É um produto das escolas militares alemãs. No entanto, mais tarde voltou-se para a URSS, cujos interesses ele acreditava serem mais compatíveis com os problemas da China.

Para o general vermelho, a guerra de guerrilha consiste em três fases. Estas três fases mantêm-se imutáveis independentemente do tamanho do objetivo da operação:

- A primeira fase é a das informações. Para as unidades de guerrilha, estas consistem num conhecimento do inimigo. Os seus movimentos, abastecimentos e potenciais. Onde o exército regular usa os seus diversos serviços de informações profissionais, as unidades de guerrilha utilizam os camponeses e os agricultores dentro de determinada área de operações. Estes civis constituem uma rede de espionagem desenvolvida. O seu conhecimento acerca dos movimentos e concentração de tropas é rapidamente transmitido, sem cadeia definida, até chegar ao comandante de uma unidade guerrilheira. Esta fase consiste também em ações por pequenos elementos de guerrilha individual, que se encontram permanentemente em ação – dissimulando, embaraçando e cortando os meios de comunicação e transportes.
- Na segunda fase o comandante de unidade de guerrilhas tem de demonstrar capacidade e ousadia invulgar. A sua unidade deve executar uma série de movimentos para conseguir cortar uma posição temporária para um ataque ou emboscada às forças do inimigo. Aqui, a vantagem é mantida através do conhecimento do inimigo e do terreno e pela mobilidade do grupo. Cada soldado, individualmente, transporta somente o que é absolutamente necessário para uma operação individual como tal podendo-se mover com uma rapidez surpreendente sobre o terreno mais acidentado.

- Na fase final, o combate é um combate de contacto. No entanto a aniquilação e a derrota do inimigo, são assuntos secundários num combate individual destinado à captura de despojos. Na luta defensiva não se pode esboçar uma linha divisória de demarcação entre as forças guerrilheiras e os exércitos maiores. Ambos dependem igualmente um do outro e estão intimamente associados entre si.

Os comunistas chineses distinguem entre uma "força de guerrilha" e um grupo de" camponeses individuais, armados e organizados" Assim sendo, teremos por ordem decrescente:

1 – tropas regulares e unidades de combate;

2 – forças de guerrilheiros;

3– camponeses armados e organizados;

Sob condições satisfatórias, as forças de guerrilha são integradas como mais um membro do exército. O tamanho de cada unidade particular é determinado pela área abrangida e pelos efetivos das forças inimigas nessa área especificada. As unidades de guerrilha são comandadas por oficiais do exército regular especializadas em técnicas de guerrilha. Organizam e dirigem todas as unidades nas mesmas bases que as do exército regular. Desta forma há um enquadramento perfeito da guerrilha no exército vermelho chinês.

Durante a guerra sino-japonesa as lutas de guerrilha podiam atingir proporções que preocupavam o alto comando japonês. Em agosto de 1940, uma destas lutas que passou para a história como a "Batalha dos Cem Regimentos " envolveu uma força de 500 mil homens, ajudados por 159 mil camponeses armados. Destruíram as comunicações e as linhas de transporte de todo o Norte da China. Esta operação combinada, que foi apontada por alguns como sendo uma das maiores ações de guerrilha da história, alcançou um enorme sucesso, desbaratando pessoal militar e civil japonês.

Tipo de ataque: Destruição de linhas de comunicação, linhas de transportes, pontes, vias férreas e estradas destruídas, estações de caminho-de-ferro, túneis fortes de cimento, igualmente destruídos.

Origem interna ou externa dos ataques: Origem interna

Qual o efeito dos ataques: Destruição massiva e generalizada de vias de comunicação.

Lições aprendidas: A importância tática, operacional do enquadramento das forças de guerrilha dentro do exército vermelho chinês.

A importância do enquadramento das forças de guerrilha no Exército Vermelho Chinês As unidades de guerrilha são comandadas por oficiais do exército regular especializadas em técnicas de guerrilha. Organizam e dirigem todas as unidades nas mesmas bases que as do exército regular. Desta forma há um enquadramento perfeito da guerrilha no exército vermelho chinês.

O Exército Vietmine e a Guerra de Guerrilha no Vietname

As duas guerras do Vietname

Em 1950 a República Democrática do Vietname e a República Popular da China iniciaram relações diplomáticas sob o patrocínio da URSS. O governo americano do Presidente Harry Trumann, preferiu apoiar o governo colonial francês da Indochina, sob o pretexto de afirmar que a China transformaria todo o sudeste asiático em regimes comunistas. O apoio Chinês foi muito importante para o sucesso do Viet-minh e do seu líder Ho Chi Minh.

A batalha de Dien Bin Phu em 1954 marcou o fim da presença francesa na Indochina, o Viet-minh (tropas vietnamitas) e o famoso general Vo Nguyen Giap, impuseram aos franceses uma pesada derrota militar. A paz seria negociada em Genebra. Mais de 400.000 soldados de ambos os lados, pereceram em 9 anos de combates. Assim terminou a 1ª guerra do Vietname.

O país foi temporariamente dividido em dois, ao longo do paralelo 17, Em 1965 os EUA enviaram conselheiros militares e mais tarde tropas para ajudar o governo do Vietname do Sul que se via a braços com um movimento insurgente de nacionalistas e comunistas- a Frente Nacional para a Libertação do Vietname (FLN) mais conhecida nos EUA e pelas tropas americanas como vietcongs. Apesar do seu enorme poderio militar, do material, homens e dinheiro investidos na guerra, os EUA falharam os seus objetivos sendo obrigados a sair do país em 1973 Dois anos depois, os dois vietnames foram unificados sob o governo socialista do Vietname do Norte, tornando-se, em 1976, na República Socialista do Vietname.

Apesar de nos dois períodos de guerra, os vietnamitas tenham privilegiado a guerra de guerrilha, vamo-nos ater ao período até 1954, a guerra entre a França e as forças Viet Minh.

As unidades Viet Minh costumavam deslocar-se para o campo de batalha por infiltração, escapando à deteção terrestre e aérea. Muitas vezes infiltravam-se através das unidades francesas a fim de as poderem atacar a partir de duas posições diferentes. Os Viet Minh atacavam de noite dado que esta lhe proporcionava algumas vantagens importantes. Os franceses eram considerados fracos combatentes noturnos e como os vietnamitas não tinham força aérea a escuridão tornava difícil a utilização da artilharia. Um ataque típico teria início

por volta da meia-noite e terminava às 9 horas da manhã. Sempre que possível, os Viet Minhs atuariam tendo o fator surpresa do seu lado, dispensavam de fogos preparatórios para o conseguir. O esforço principal era concentrado numa frente bastante estreita. O resto fazia fintas, sobretudo se não se conseguisse o fator surpresa. O seu poder de fogo seria dirigido somente e massivamente, sobre algumas posições criticas.

Geralmente, quatro grupos de soldados estavam envolvidos no ataque. O primeiro, era o que se encarregava das armas pesadas de apoio (armas automáticas, morteiros, armas sem recuo) cujo objetivo era neutralizar algumas posições do inimigo, tais como o posto de rádio, armas pesadas ou mesmo o posto de comando. Se o ataque fosse mal sucedido, o seu fogo cobriria a retirada. O segundo grupo era constituído pela engenharia de assalto ou dinamitadores. Estes homens que podiam ser uma companhia ou um pelotão, corriam para a linha da frente, infiltravam-se na linha inimiga e faziam explodir dinamite em sítios críticos a fim de criar brechas no forte. É de salientar a extrema coragem destes homens, já que não levavam consigo armas, só transportavam a dinamite, muitas vezes em varas de bambu que podiam ser passadas através de redes de arame. Outras vezes, levavam os explosivos atados ao corpo para lhes permitir atravessar o arame farpado. Uma vez neutralizadas as armas inimigas e criada a brecha pelos dinamitadores, tropas de choque ou infantaria de assalto avançavam sobre uma frente estreita, tentando conquistar a posição. O quarto grupo de soldados era um grupo de reserva que cobria as tropas de choque, explorava o sucesso e cobria a retirada. Depois do ataque terminado as tropas recuperavam material de guerra e escapuliam-se para a selva através de caminhos de fuga previamente estudados. É extremamente difícil combater dentro das posições do inimigo, no entanto os vietnamitas provaram que tal poderia ser feito com sucesso se fossem observados 4 princípios:

1 – Cuidadoso planeamento e treino. O planeamento era normalmente com a utilização de caixas de areia, ou réplicas dos postos franceses, e o ataque era ensaiado múltiplas vezes.

2 – Com o fim de destruir as principais instalações inimigas, as tropas deveriam penetrar tão profundamente quanto possível e não poderiam ficar na periferia do forte.

3 – Tinha de existir uma íntima cooperação entre os dinamitadores, unidades de fogo e de apoio e tropas de choque.

4 – Uma operação de êxito requeria íntima ligação entre a unidade atacante, o seu regimento e as unidades vizinhas.

Tipo de ataque: Ataques noturnos. Destruição, de instalações do inimigo francês

Origem interna ou externa dos ataques: Origem interna

Qual o efeito dos ataques: Destruição das instalações fortes e fortins do inimigo. Captura de armas

Lições aprendidas: Combater dentro das posições do inimigo, o que é muito difícil e corajoso. Os vietnamitas provaram que tal poderia ser feito com sucesso se fossem observados os 4 princípios acima enunciados

A Guerra da Argélia contra a França 1954-1962

Condução da guerra de guerrilha

A guerra desencadeada pelos nacionalistas muçulmanos contra a presença francesa, teve início em novembro de 1954 e prolongou-se até 1962. Iniciou-se com uma série de atentados terroristas. Nos dois primeiros anos do conflito, as ações terroristas tiveram como alvo principal, não só as tropas francesas, mas especialmente, os muçulmanos que se encontravam ligados à França e os colonos europeus instalados na Argélia, os pieds-noirs, como eram designados pelos autóctones. A dura atuação contra a população civil muçulmana era um claro indício que a rebelião ainda não contava com um apoio popular significativo. Do ponto de vista geográfico, a Argélia tem uma superfície 2275033 Km^2; dos quais 1980000 Km^2 fazem parte do deserto do Saara. É de realçar a circunstância de até março de 1956 a FLN (Frente de Libertação Nacional) não dispor de santuários nos países limítrofes - Marrocos e Tunísia, que só neste mês obtiveram a independência da França. A condução de uma guerra de guerrilha na ausência de uma extensa floresta tropical com bons refúgios; tal como sucedia com a Malásia e as colónias portuguesas: Nos primeiros tempos, a guerra fez-se de violentas ações em simultâneo em zonas urbanas e zonas rurais. Esta circunstância tem como consequência 2 efeitos distintos: A subida do grau de violência para níveis preocupantes, e um envolvimento direto e permanente dos diversos setores da população urbanas e rurais. Num lado, situavam-se os autóctones muçulmanos pró-independência, sob a direção da FLN e no campo contrário, os não europeus partidários da Argélia francesa e os colonos de origem europeia.

Sendo este, o enquadramento dos primeiros anos da guerra da Argélia, pretendo realçara algumas vulnerabilidades e táticas usadas pela FLN no meio rural, sobretudo nos ataques às barreiras físicas que existiam ao longo das fronteiras de Marrocos e da Tunísia - linha Morice. Uma das vulnerabilidades era as comunicações da FLN. A morosidade das comunicações, implicava um dispositivo disperso e não coordenado de unidades rebeldes. Desta forma, cada ação da FLN é uma ação de uma ou de muito poucas unidades, com duração e objetivos

limitados, Se, por acaso, se alterassem as circunstâncias, os planos ficavam sem efeito. Do mesmo modo que afeta a flexibilidade e a duração das principais operações rebeldes, o problema das comunicações limita a força que pode ser dirigida contra um único objetivo. Desta forma, raramente, as forças rebeldes atacavam forças superiores a uma companhia. As forças do ALN -Exército de Libertação Nacional - têm de ter sempre em conta a capacidade francesa de contra-atacar rapidamente de dia, com bombardeamento aéreo e artilharia. Desta forma, os rebeldes, com a perfeita noção do facto, limitam as suas ações e manobras de táticas de forças partisans.

A guerra Mosquito é a preferida pelo ALN, especialmente contra guarnições francesas mais afastadas. Trata-se de uma guerra noturna ou de mau tempo em que a eficácia dos carros de combate e da aviação é mínima.

Em cada operação, os argelinos desfrutam de uma vantagem importante, os auxiliares civis que estão sempre em toda a parte e atuam como radares humanos, escutas, agentes informadores e guias. Estes elementos apelidados "moussebelline" infiltram-se nas localidades em poder dos franceses, sondam os terrenos na frente das colunas regulares do ALN.

As Táticas de emboscada variam conforme o tipo e a proximidade de apoio de outras tropas francesas. "Uma técnica consiste em colocar minas nas vias de abastecimento francesas, nos pontos aonde a estrada passa por desfiladeiros, ou no sopé de uma colina. Os exploradores, os moussebelline dão aviso do comboio esperado. Quando o primeiro veículo atinge a área minada, ou quando os detetores franceses localizam as minas, o comboio para, os rebeldes irrompem de ambos os lados, com armas automáticas e granadas, com fogo de enfiada na direção da estrada. Depois, quando possível, um grupo de elementos da emboscada, procura lutar com os sobreviventes que se encontram nos carros estacionados. Objetivo: apanhar as armas, estabelecer maior confusão e destruir o inimigo mesmo com risco de mais pesadas baixas por parte dos rebeldes" (Osanka:1963)

Tipo de Ataque –Ataques de guerrilha urbana, colocação de bombas. Fora da cidade, emboscada a posições e linhas francesas, nomeadamente nas linhas de fronteira entre Marrocos e a Tunísia - linha Morice.

Origem Interna / Externa – Origem interna com santuários em Marrocos e na Tunísia.

Efeitos dos ataques – Destruição de edifícios à bomba, terror generalizado nas cidades. Perca de vidas e de material militar francês. Grandes gastos franceses para continuar a guerra.

Lições aprendidas – Como fazer guerra de guerrilha numa zona desértica, com poucos abrigos de vegetação. Devido às debilidades de comunicação do ALN, a impossibilidade de confrontarem o inimigo com grandes investidas. Esta particularidade é criadora da Guerra Mosquito,: Criação de brigadas de informação dentro do território do inimigo "Mousebellines" bem como o cuidado e rigoroso doseamento de atribuição de recurso que eram de si bastante escassos. Todos estes fatores foram responsáveis de atrito ocasional e mínimo mas de longa duração.

O ataque do PAIGC ao posto de Cantacunda em 11 de abril de 1968

Portugal lutou numa guerra ultramarina de caráter colonial entre 1961-1975 em três teatros de guerra no continente africano. Um dos mais relevantes foi o da Guiné, do qual apresento um relato:

"O PAIGC atacou o destacamento de Cantacunda (Geba) no Leste causando um morto e 11 desaparecidos entre a população. Este tipo de ataques contra destacamentos de pequenos efetivos revelava-se cada vez mais rentável para os guerrilheiros. Os comandos militares portugueses demoraram algum tempo a perceber que a guerra tinha passado a um patamar superior e que estes pequenos postos guarnecidos por uma secção, ou por um pelotão eram incapazes de garantir a sua defesa. Os militares portugueses pertenciam à Companhia de Artilharia 1690. Esta operação do PAIGC foi comandada pelo comandante Gazela. Os militares portugueses foram levados para Conacri. Cantacunda era um dos destacamentos da Companhia de Artilharia 1690 que tinha a sede na tabanca de Geba, na zona do Oio e que se dispersava por vários outros destacamentos entre os quais Sinchã Jobel e Samba Culo. O destacamento de Cantacunda caracterizava-se pelas péssimas condições das instalações do pessoal e pelos deficientes meios e condições de defesa. Ficava a 50 Km da sede da companhia. Sem luz elétrica, não dispunha de um simples gerador, estava junto à floresta e perto da base de Samba Culo, do PAIGC e como armamento dispunha de umas ultrapassadas metralhadoras Dreyse e Breda, morteiros de 81 mm e 60 mm. Os abrigos eram uns buracos de difícil acesso e sem condições interiores. O efetivo era de um pelotão, normalmente, embora no dia deste ataque estivessem lá duas secções de atiradores" (Afonso, 2010:446-447)

Tipo de ataque – Ataque armado do PAIGC ao destacamento da Cantacunda.

Origem interna/externa – Ambas. No entanto é difícil determinar precisamente; dado que os 11 desaparecidos foram enviados para a Guiné Conackri que desempenhava o papel de santuário e refúgio.

Efeitos do Ataque – Um morto e 11 desaparecidos que foram levados para a Guiné Conackri.

Lições aprendidas – O destacamento do exército português era inadequado e insuficiente e localizado na orla da floresta. Foi uma séria advertência aos militares portugueses, para o facto de a guerra se ter tornado mais forte e que os postos guarnecidos por uma secção ou por um pelotão eram incapazes de garantir a sua defesa. Seguidamente, apresento um quadro aonde mostro resumidamente os casos de estudados e os critérios de avaliação

Quadro de comparação

Ataques cibernéticos

	Tipo de Ataque	Origem Interna/ Externa	Efeitos Ataques	Lições aprendidas
Estónia	DDoS phishing, Spam de E-mail, desfiguração de sites, ataques TCP SYNC. Também há referência a ataques de pings (ICMP) violentos podendo também ter origem em botnets ou autores individuais.	Externo	Ataques generalizados. Conseguiram parar a quase totalidade dos serviços via internet.	Reflexão sobre segurança da internet e as boas práticas que devem ser seguidas.
Geórgia	DDoS Desfiguramentos de imagens. Ataques a servidores de correio eletrónico	Externo	Ataques generalizados. No entanto, não teve grande expressividade dado a fraca expressividade da utilização da internet . Só 7 em cada 100 habitantes tinham acesso	Ataques cibernéticos que precederam e acompanharam ações armadas do exército russo
Google	É um ataque que tem como objetivo roubar e passar impune. É um ataque muito próximo, se não mesmo de espionagem industrial por um lado, por outro lado é um ataque à privacidade do correio eletrónico dos seus cidadãos. Por outro lado este ataque também pode dar origem a botnets	Externo	Foi lido correio eletrónico pelas autoridades chinesas.	Importância das atualizações de software. Ter anti vírus atualizado, usar um firewall, utilização de encriptação

Quadro de comparação

Ataques de Guerra de guerrilha

Malásia	Infundir medo, intimidar, terror, chantagem.	Interno	Coação, intimidação e de terror . Luta armada	Serie de medidas em relação à população civil bem como à distribuição das forças combatentes.
URSS	Cortar as comunicações alemãs. Destruir Desvio de forças, Minar a moral. Espionagem, Interceção de linhas telefónicas. Coleta de informação de deslocamentos inimigos, recolha de informação através de interrogatórios e torturas. Combate na retaguarda do inimigo. Também na retaguarda. Melhoramento de vias de comunicação para facilitar o deslocamento do exército vermelho.	Interno	A criação do movimento partisan. Novo alento à resistência anti-alemã. Recolha de informações. Combate na retaguarda do inimigo.	Criação do movimento Partisan
China	Destruição de linhas de comunicação, linhas de transportes, pontes, vias férreas e estradas destruídas, estações de caminho-de-ferro, túneis fortes de cimento, igualmente destruídos.	Interno	Destruição massiva e generalizada de vias de comunicação.	A importância tática, operacional do enquadramento das forças de guerrilha dentro do exército vermelho chinês.
Vietname	Ataques noturnos. Destruição, de instalações do inimigo francês	Interno	Destruição das instalações fortes e fortins do inimigo. Captura de armas	Combater dentro das posições do inimigo.
Argélia	Guerrilha urbana, ataques à bomba, emboscadas, Guerra Mosquito	Ambos	Destruição de edifícios à bomba, terror generalizado nas cidades. Perca de vidas e de material militar francês. Grandes gastos franceses para continuar a guerra	Como fazer guerra de guerrilha numa zona desértica, com poucos abrigos de vegetação. Guerra Mosquito. Brigadas de Moussebellines Doseamento rigoroso dos meios e tropas de combate
Guiné	Ataque armado	Ambos	Um morto e 11 desaparecidos	Deficiência nas instalações e sua localização. advertência para o facto de a guerra se ter tornado mais forte e que os postos guarnecidos por uma secção ou por um pelotão eram insuficientes.

Quadro síntese

Ataques cibernéticos e guerra de guerrilha

	Tipo de Ataque	Origem Interna/Externa	Efeitos Ataques	Lições aprendidas
Estónia	DDoS phishing, Spam de E-mail, desfiguração de sites, ataques TCP SYNC. Também há referência a ataques de pings (ICMP) violentos podendo também ter origem em botnets ou autores individuais.	Externo	Ataques generalizados. Conseguiram parar a quase totalidade dos serviços via internet.	Reflexão sobre segurança da internet e as boas práticas que devem ser seguidas.
Geórgia	DDoS Desfiguramentos de imagens. Ataques a servidores de correio eletrónico	Externo	Ataques generalizados. No entanto, não teve grande expressividade dado a fraca expressividade da utilização da internet . Só 7 em cada 100 habitantes tinham acesso	Ataques cibernéticos que precederam e acompanharam ações armadas do exército russo
Google	É um ataque que tem como objetivo roubar e passar impune. É um ataque muito próximo, se não mesmo de espionagem industrial por um lado, por outro lado é um ataque à privacidade do correio eletrónico dos seus cidadãos. Por outro lado este ataque também pode dar origem a botnets	Externo	Foi lido correio eletrónico pelas autoridades chinesas.	Importância das atualizações de software. Ter anti-vírus atualizado, usar um firewall, utilização de encriptação
Malásia	Infundir medo, intimidar, terror, chantagem,	Interno	Coação, intimidação e de terror . Luta armada	Serie de medidas em relação à população civil bem como à distribuição das forças combatentes.
URSS	Cortar as comunicações alemãs. Destruir Desvio de forças, Minar a moral. Espionagem, Interceção de linhas telefónicas. Coleta de informação de	Interno	A criação do movimento partisan. Novo alento à resistência anti-alemã. Recolha de	Criação do movimento Partisan

	deslocamentos inimigos, recolha de informação através de interrogatórios e torturas. Combate na retaguarda do inimigo. Também na retaguarda. Melhoramento de vias de comunicação para facilitar o deslocamento do exército vermelho.		informações. Combate na retaguarda do inimigo.	
China	Destruição de linhas de comunicação, linhas de transportes, pontes, vias férreas e estradas destruídas, estações de caminho-de-ferro, túneis fortes de cimento, igualmente destruídos.	Interno	Destruição massiva e generalizada de vias de comunicação.	A importância tática, operacional do enquadramento das forças de guerrilha dentro do exército vermelho chinês.
Vietname	Ataques noturnos. Destruição, de instalações do inimigo francês	Interno	Destruição das instalações fortes e fortins do inimigo. Captura de armas	Combater dentro das posições do inimigo.
Argélia	Guerrilha urbana, ataques à bomba, emboscadas, Guerra Mosquito	Ambos	Destruição de edifícios à bomba, terror generalizado nas cidades. Perca de vidas e de material militar francês. Grandes gastos franceses para continuar a guerra	Como fazer guerra de guerrilha numa zona desértica, com poucos abrigos de vegetação. Guerra Mosquito. Brigadas de Moussebellines Doseamento rigoroso dos meios e tropas de combate
Guiné	Ataque armado	Ambos	Um morto e 11 desaparecidos	Deficiência nas instalações e sua localização. advertência para o facto de a guerra se ter tornado mais forte e que os postos guarnecidos por uma secção ou por um pelotão eram insuficientes.

Os ataques cibernéticos podem ter características e causar danos equivalentes aos ataques de guerrilha. Seguidamente, irei tentar fazer uma correspondência por comparação entre os

ataques cibernéticos descritos e os ataques de guerrilha acima relatados. Para tal, utilizarei os critérios de comparação estabelecidos.

Ciberataques à Estónia 2007

Os tipos de ataques efetuados foram essencialmente os seguintes: DDoS, botnets, phishing, spam, desfiguração de sites, ataques tcp syn, ping storms. A maior parte dos ataques visavam impedir o estabelecimento de comunicações. O equivalente em guerrilha seria o corte de linhas de comunicação (telefone, telégrafo) tal como aconteceu como no episódio de "Guerrilha Partisan Soviética na II Guerra Mundial" acima mencionado. O equivalente ao phishing seria formas de engenharia social[32], espionagem. O spam e a desfiguração; o primeiro, pode ser utilizado para dois grandes fins: enganar, criar instabilidade através da circulação de boatos ou, sob a forma de mail bombing, esgotar o espaço de memória no servidor de correio atribuído a cada utilizador e, enchendo-lhe a caixa do correio, evitar que essa ou essas pessoas recebessem e-mail. Uma atividades de guerrilha o equivalente seria: espalhar boatos, ação psicológica, roubo, desvio ou retenção de correio. As botnets são em si mesmo uma forma de ataque, dado que alguém sequestra máquinas e, sem conhecimento do seu proprietário, forma redes para se dedicar a atividades maliciosas. O equivalente em guerrilha com o mesmo efeito seria o aumento de efetivos e material para aumentar a amplitude do esforço guerrilheiro.

Ataques cibernéticos na Guerra Russo-Georgiana

Os tipos de ataques praticados foram os seguintes: DDoS, botnets, defacement, ataques a servidores de e-mail. È o primeiro caso em que um conflito internacional político e militar foi precedido e acompanhado por uma ofensiva de ataques cibernéticos. Estes ataques destinavam-se a lançar confusão e diminuir a capacidade de defesa militar. A origem dos ataques é inconclusiva, dado que, certamente devido às botnets e a várias formas de IP spoofing, não se consegue determinar com segurança a origem destes. Este caso tem um ponto de contacto com o episódio "Guerrilha Partisan Soviética na II Guerra Mundial", é uma forma de trabalhar na retaguarda da Geórgia. O defacement que foi praticado teria o seu equivalente em guerrilha, na publicação de caricaturas e imagens pouco abonatória dos líderes georgianos na imprensa estrangeira e a circulação, na Geórgia, de panfletos de propaganda.

[32] Utilização das relações humanas e dos laços sociais para obter informação confidencial sobre sistemas e redes.

O caso Google - R.P. China

Exploração de uma vulnerabilidade pouco conhecida do programa de browsing "Internet Explorer". O seu equivalente em guerrilha seria um ataque a uma posição com vulnerabilidades, tal como foi o caso de " Cantacunda Guiné 1968" O ataque teria consistido possivelmente na introdução de um worm ou rootkit com código malicioso nas máquinas alvo, o que teria o seu equivalente em guerrilha na introdução de agentes sabotadores dentro das forças inimigas. A maneira de o introduzir é bastante rebuscada, contudo eficaz, trata-se de um ataque muito próximo da espionagem tanto industrial (ataques a empresas tecnológicas americanas), como política (leitura de correio eletrónico de cidadãos dissidentes chineses).

A Emergência Malaia 1948 – 1960

Os tipos de ataques efetuados de guerrilha visavam; infundir medo, intimidar, terror, chantagem, extorsão através de imposto revolucionário, execução de assassinatos, fogo posto, rapto de mulheres e crianças, ameaças e chantagens. No que diz respeito a infundir medo e intimidar, o equivalente cibernético poderá encontrar-se em vírus que falsamente fazem crer que aquela máquina está a ser vigiada e que a pessoa vai ser punida. É deste género os exemplos dos vírus PSP Polícia de Segurança Pública bem como o vírus SPA Sociedade Portuguesa de Autores, estes dois vírus bloqueiam o pc e reclamam uma determinada quantia de dinheiro a ser enviada imediatamente para o desbloquear. Neste caso há um elemento de medo, dado que se tratam de entidades oficiais e também de que pode ser algo embaraçoso para o proprietário da máquina, revelar o conteúdo que estava a visionar. A chantagem, infelizmente é bastante corrente na internet, desde o cyberbulling até à ameaça de revelação de dados pessoais, ou de listas confidenciais. Neste caso, a maior parte das técnicas intrusivas de malware que tenham acesso a outras máquinas poderá ser usada para efetuar a chantagem (vírus, worms, de uma forma mais sofisticada, rootkits. Este comportamento tem bastante em comum com o caso Google – R.P. China no que diz respeito à leitura indevida de correio eletrónico de cidadãos chineses. A extorsão ocorre diariamente na internet e aparece sob uma miríade de formas, desde spam, ofertas pretensamente gratuitas, anúncios enganosos até à fraude bancária com cartões de créditos em que mais uma vez se podem empregar muitas técnicas de ataque para aceder à máquina visada. São especialmente perigosas as botnets dado que as máquinas que as compõem, estão dominadas por alguém que detém o controle sobre elas e, conforme a natureza do agente de malware, podem tornar-se totalmente transparentes para este. Devido à natureza igualitária da internet cada pessoa tem sempre a possibilidade

teórica de praticar atividades maliciosas online, dependendo a sua força destrutiva dos seus conhecimentos ou dos que consiga reunir em seu favor. O problema põe-se ao nível do utilizador individual e da sua falta de recursos em conhecimentos informáticos que lhe permitam defrontar a situação e resolvê-la da melhor maneira. A credibilidade a ingenuidade e a incúria do utilizador mais acrescentam a este estado de coisas.

A Guerrilha Soviética na II Guerra Mundial

Os tipos de ataques levados a cabo pelos Partisans eram: Cortavam as comunicações alemãs, destruíam os seus abastecimentos, desviavam-lhes as forças, minavam a moral, efetuavam espionagem, interceção de linhas telefónicas, coletavam informação de deslocamentos inimigos, recolha de informação através de interrogatórios e torturas. Quando o ataque começava atuavam combatendo na retaguarda do inimigo. Também na retaguarda melhoravam vias de comunicação para facilitar o deslocamento do exército vermelho. Minar a moral e desorganizar o inimigo pode ser conseguido com o isolamento intermitente de máquinas, Spam aonde se divulga propaganda e mensagens derrotistas. A interceção de linhas telefónicas é uma atividade que se pode efetuar com o ataque Man-in-the-Middle, se tivermos acesso à LAN ou à WLAN. No caso de não se possuir, este acesso, pode-se optar por uma grande variedade de vírus, worms rootkits que nos dão acesso às máquinas pretendidas através de backdoors criadas expressamente pelo código malicioso. A vantagem das backdoors é permitirem múltiplas entradas secretas na máquina e ir efetuando um trabalho de reconhecimento do conteúdo desta. As backdoors também são muito úteis para os programadores, dado que lhes permitem um acesso direto ao código do programa e reparar erros ou acrescentar funcionalidades. Claro que todos estes recursos podem ser utilizados para atividades de espionagem. A construção de estradas por detrás das linhas inimigas apresenta algumas características semelhantes às botnet. Criar botnets com máquinas do inimigo, para atacar mais máquinas deste.

O Exército Vermelho Chinês e a Guerra de Guerrilha

Os tipos de ataques efetuados foram: Destruição de linhas de comunicação, linhas de transportes, pontes, vias férreas e estradas destruídas, estações de caminho-de-ferro, túneis fortes de cimento, igualmente destruídos.

Este tipo de ataques estão vocacionados para a destruição física de infra estruturas. Também é possível destruir fisicamente com um ataque cibernético, basta utilizar algumas técnicas para

que isso aconteça, como o ataque Teardrop que leva a máquina a arrancar sucessivas vezes até à exaustão. Ou então alguma técnica de plashing em que se altera o software de arranque da máquina. No entanto existem outras técnicas de ataque que, se a segurança, podem causar verdadeiros desastres físicos tais como cortes de eletricidade, desregulação da sinalética das vias férreas, abertura inopinada de comportas de barragens e muitas outras: Tudo isto pode acontecer devido ao facto de muitos dos nossos sistemas tecnológicos serem controlados à distância através da internet. Tudo depende da confidencialidade e do nível de segurança dessas mesmas instalações e dos seus funcionários. O caso Stuxnet[33], descoberto em 2010, Consistia na introdução de um worm que destruía as centrifugadoras da central de pesquisa nuclear de Natanz. Este worm fazia com que as centrifugadoras da marca Siemens trabalhassem 40% mais rápido durante 5 minutos de cada vez, desta forma leva-as à destruição. O worm foi feito de maneira a funcionar com o sistema operativo de um determinado modelo de centrifugadoras Siemens. A paternidade deste worm é atribuída a Israel e aos EUA.

O Exército Vietmine e a Guerra de Guerrilha

No Vietname

Os tipos de ataques efetuados foram essencialmente os seguintes: Ataques noturnos. Destruição, de instalações do inimigo francês. As lições aprendidas neste caso são bastante relevantes para o entendimento do que são os ataques cibernéticos que não se limitam só a cortar as comunicações. Qualquer forma de ataque que aceda a máquinas inimigas - vírus, worms rootkits e outros - e processe informação, ou a recolha ilegalmente entra dentro desta categoria. O caso das botnets é ainda mais exemplificativo do que digo, dado que se assume o controle das máquinas, os seus legítimos proprietários não dão por nada e criam-se redes para atacar outras máquinas inimigas. É o perfeito exemplo de usar meios do inimigo contra este.

A Guerra da Argélia contra a França 1954 –1962

Os tipos de ataques efetuados foram essencialmente os seguintes: Ataques de guerrilha urbana, colocação de bombas. Fora da cidade, emboscada a posições e linhas francesas, nomeadamente nas linhas de fronteira com Marrocos e a Tunísia - linha Morice. Os tipos de ataques não diferem muito dos acima abordados. O que é diferente é a forma de fazer a guerra numa geografia desértica com poucos abrigos para as forças de guerrilha. Nos ataques

[33] http://en.wikipedia.org/wiki/Stuxnet

cibernético, por mais encoberto e silencioso ficam traços da intromissão que é necessário apagar. Desta forma quem perpetua um ataque tem sempre a preocupação de apagar as suas ações, dado se não o fizer, estará exposto, tal como as forças de guerrilha no deserto. A rigorosa adequação dos meios à dimensão do ataque que a FLN sempre demonstrou. Também num ataque cibernético isso é verdade, tem de se adequar as máquinas, o software ou softwares utilizados de acordo com o tipo de máquina a ser atacada, bem como o género de ataque que se pretende efetuar. Um outro aspeto que é relevante da organização do ALN, é a sua preocupação com a informação, criando para o efeito brigadas de informadores que atuavam dentro das forças inimigas. A necessidade de informação fiável é um dos aspetos mais importantes em ataques cibernéticos para além da mera utilização de scripts publicados na net. Num primeiro momento, fazer o levantamento é preciso fazer o levantamento exaustivo da rede que se pretende atacar e conhecer as suas vulnerabilidades de topologia bem como de software utilizado aonde se irão procurar fraquezas pouco conhecidas, não cobertas por atualizações do fabricante do software. Essas fraquezas é que muitas vezes determinam a natureza do ataque. Para tudo isto é necessário informação que pode ser obtida diretamente através da rede, com a utilização de ferramentas e programas tais como: ipconfig, ping, traceroute (windows) netstat, Nmap, Zmap Hping e outros. Outra forma de obter informação valiosa do alvo a atacar é utilizando técnicas de engenharia social, criando situações em que os utilizadores, de forma voluntária ou involuntária, forneçam elementos facilitadores do acesso às redes alvo.

Ataque Armado do PAIGC ao Destacamento de Cantacunda 1968

O tipo de ataque realizado foi um ataque armado ao destacamento de Cantacunda aonde houve um morto e 11 desaparecidos. A nível informático poderemos considerar dois tipos de ataques o Teardrop e o phlashing efetuados por uma botnets, criar máquinas reféns que ficam sujeitas às ordens de outrem, que não o seu legítimo proprietário. Por outro lado, no que diz respeito a uma das lições recolhidas, a insuficiência da guarnição e das instalações de Cantacunda, recorda-nos a incessante batalha da segurança no mundo cibernético. Os meios físicos e o software devem estar sempre à altura dos desafios de segurança. Daí a importância da renovação dos equipamentos e, sobretudo, da atualização do software que neles corre.

CAPÍTULO 8

Discussão de Resultados

8.1 Discussão de Resultados

A pesquisa por mim efetuada para esta dissertação foi vasta, proporcionadora de desafios e gratificante

Foi vasta devido à incorporação de vários ramos do conhecimento: informática, telecomunicações, história, ciência política e estratégia. Visitei as principais escolas de teorização da guerra de guerrilha. Inteirei-me dos últimos avanços em técnicas de Dos/DDoS e expliquei como atuam.

Foi um projeto desafiante, porque me fez enfrentar um estudo de caso complexo, multifacetado que vai muito para além da realização e eficácia de ataques informáticos,

Por fim, foi gratificante, dado que consegui encontrar elementos de comparação, não tanto em quantidade determinística de causa efeito, mas sim entender o comportamento subjacente à amostra observada. Foi importante porque permitiu obter comparações entre os ataques informáticos e os ataques de guerrilha convencional, efetivamente, nos casos apresentados foi possível apresentar propostas de ataques informáticos que tivessem um efeito idêntico, ou aproximado ao dos ataques de guerrilha convencional.

Na tecnologia dos ataques utilizados

No que diz respeito aos DoS/DDoS, são instrumentos muito poderosos e disruptivos do funcionamento de serviços baseados na internet. Visam restringir, desligar, destruir equipamentos que estejam ligados à internet. Para além da destruição física das linhas e dos equipamentos que a compõe, esta é a forma mais eficaz de cortar comunicações.

O uso de botnets é uma forma de ampliar o alcance dos ataques bem como a forma de esconder a origem dos ataques (IP Spoofing).

A desfiguração que foi repetidamente utilizada no ataque à Geórgia, como uma forma de ridicularizar os atores e as instituições políticas.

O problema da dependência das ligações internacionais e da sua redundância física. Este foi o caso da Geórgia, que só possuía um acesso internet internacional, através da Rússia. Mais tarde foi concluído um cabo submarino para a Bulgária.

A operação Aurora que parece ser um caso que nada tem a ver com a interrupção de comunicações. Pelo que me foi possível apurar é um caso muito sofisticado de espionagem industrial e de violação de correio eletrónico de possíveis dissidentes da R.P. China. No entanto é de salientar a sofisticação e o tipo de informações que se podem obter na net através de meios ilegais. O que me levanta a seguinte pergunta: será que não estamos a confiar informações demasiado importantes para a própria internet e, designadamente, os protocolos que lhe dão vida: não consigo esquecer um dos princípios fundadores da internet, a confiança entre os utilizadores…!

Tal como na guerrilha o alvo do ataque é escolhido, procuram-se vulnerabilidades que são exploradas e ataca-se. Podemos dizer que tal com na guerrilha o ataque é oportunista.

Na estratégia/Tática da Guerra de Guerrilha

Para além das características fundamentais da guerrilha vistas à luz dos ataques de negação de serviço mencionadas, importa acrescentar as seguintes:

A guerrilha é uma forma de guerra que comporta sempre um potencial possibilidade de luta armada. A pergunta que se coloca é saber qual o ponto de violência a partir do qual se considera guerra. Esta situação é-nos apresentada no caso da Geórgia. Sem dúvida que os ataques informáticos podem ser recursos ofensivos da guerrilha.

Os ataques informáticos são também formas de pressionar acontecimentos e reações públicas favoráveis às posições defendidas pelos seus perpetradores, tal como podemos observar no caso da Estónia.

Acredito que é de todo o interesse reter as lições da guerra contra-subversiva, sobretudo no que diz respeito à liderança das populações. A análise pós ataque dá-nos indicações sobre a forma como o autor do ataque pretendia manipular as populações. Exemplos: caso da minoria russa na Estónia e da população da Ossétia em relação à Geórgia e á Rússia.

Devido às características verdadeiramente transnacionais e de cooperação da internet – no sentido em que nenhum Estado é possuidor de todas as infraestruturas – é extremamente difícil retaliar uma ataque, dado que se está a lidar com algo muito complexo e que tem uma multiplicidade de proprietários tanto das estruturas físicas bem como do bem mais precioso a informação.

A internet e os protocolos TCP/IP são protocolos voltados para a conexão. A regra fundamental é a da confiança, de outra forma seria impossível o sistema funcionar, uma vez que não haveria a certeza de chegada dos pacotes ao destino. Um dos aspetos que realço é o

caráter verdadeiramente internacional que a internet tem, devido ao facto de todos usarem o protocolo TCP/IP e também à comutação de pacotes, e protocolos de routing. É caso para dizer que a internet pertence a todos. Nem todos os pacotes seguem o mesmo caminho de A para B. Também sabemos que a internet funciona num esquema de malhas que se conectam em vários pontos com outras, dando assim redundância às comunicações. Mesmo que uma parte da internet pare, por qualquer razão, as demais continuam a trabalhar. Como tal é praticamente impossível desligar a rede a nível mundial. No entanto, também vimos como se podem atacar máquinas conectadas, pará-las ou mesmo danificá-las fisicamente. Se há ataques na internet e há defesa, então é porque que estamos num meio de conflitualidade e eventualmente mesmo de guerra.

Apesar de os EUA terem criado um comando estratégico para a guerra cibernética (USCYBERCOM) que já se encontra em atividade desde 2011 terem um conjunto de 5 iniciativas estratégicas aprovadas, continuam a não ter regras de ação, isto é, saber qual é o ponto em que devem atuar, dado ser difícil estabelecer de aonde partiu o ataque, tal como vimos no capítulo 1 (O IP spoofing). O fracasso que os governos, bem como os especialistas em segurança de redes, têm em identificar a origem dos ataques é desafiante dado que lidam com questões delicadas tratadas pelos serviços de informação. Atualmente com as infraestruturas físicas e os protocolos da internet que temos, é muito difícil dizer, só por meios técnicos de aonde partiu determinado ataque. A questão vai muito para lá, do que saber que máquinas estiveram ligadas a outras máquinas. Atualmente os ataques dão-se a vários níveis (pensemos no caso de um verme por exemplo). Quase sempre os computadores que iniciam o ataque estão no estrangeiro, como tal é difícil obter os relatórios dos ISP’s.

CONCLUSÕES

A pesquisa efetuada produziu algumas conclusões e indícios que ajudam não a dar uma resposta cabal à pergunta da hipótese, contudo, com algumas limitações, contribuem para o seu aclaramento:

- Os ataques DoS/DDoS podem e têm sido usados como vetores de agressão contra outros Estados ou outras entidades de direito privado.
- Os ataques DoS/DDoS são uma forma moderna de luta concorrente e complementar às operações de guerra de guerrilha.
- Os ataques DoS/DDoS são formas de sabotagem a nível físico(corte de comunicações), conjuntamente com outros tipos de ataques cibernéticos, como por exemplo o defacement e a alteração de conteúdos, são afirmações de força, afirmações políticas e ideológicas.
- Este tipo de ataque, tal como a guerrilha, tira partido das vulnerabilidades do adversário e exploram-nas em seu benefício.
- Os ataques DoS/DDoS, apesar de tirarem partido das oportunidades oferecidas, são cuidadosamente planeados e implementados, tal como as ações da guerra de guerrilha.
- É possível fazer alguma correspondência limitada, entre os efeitos dos ataques de guerrilha que apresentei e ataques cibernéticos capazes de desencadearem efeitos análogos.
- Os ataques físicos de guerra de guerrilha e os ataques cibernéticos são ambos destrutivos nos seus campos de atuação. No entanto não são ainda intermutáveis. Com a progressão da sociedade de informação e da digitalização de muitas atividades, o seu potencial destrutivo aumentará
- Os ataques DoS/DDoS são maioritariamente, de origem externa
- Os ataques de guerra de guerrilha são maioritariamente de origem interna ou com recurso a um terceiro Estado que atua como santuário.

Siglas e Acrónimos Utilizados

ALN	Armeé de Liberation National
ARP	Access Resolution Protocol
BGP	Border Gateway Protocol
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
ICMP	Internet Control Message Protocol
IOS CISCO	Internetwork Operating System
IP	Internet Protocol
IP v4	Internet Protocol version 4
ISP	Internet Service Provider
LAN	Local Area network
PING	Packet Inter Net Groper
RADIUS	Remote Authentication Dial In User Service
SYNC-ACK	Syncronization – Acknowledgement
TCP/IP	Transfer Control Protocol / Internet Protocol
URL	Uniform Resource Locator
WLAN	Wireless Local Area Network

Bibliografia

AFONSO, Aniceto, GOMES, Carlos de Matos. *Os anos da Guerra Colonial* : 1961-1975. Lisboa Quidnovi: 2010, pp 446-447

BEAUFRE, G *Introduction a la stratégie* : Paris 3 edição Librarie Armand Colin 1965

BRAU, Jean- Louis, *Armas da Guerrilha.* Trad. Zarco Moniz Ferreira. Vendas Novas. d. Versão francesa: Paris Balain, 1974

ClAUSWITZ, Carl von*; On War*., Princeton; Princeton University Press, 1984

CONKLIN, Wm. Arthur, WHITE, Gregory B., COTHERN, Chuck, WILLIAMS, Dwayne, DAVIS, Roger L., *Principles of Computer Security Security+ and Beyond.* Burr Ridge, Illinois Mc Graw Hill tecnology Education, 2004

COUTO, Abel C. *Elementos de Estratégia:* Apontamentos para um curso. Lisboa: Instituto de Altos Estudos Militares, 1v s.d

DIAS, Carlos, CARRIÇO, Alexandre. *Vo Nguyen Giap*: O Homem que derrotou os franceses e os americanos. Lisboa: Prefácio, 2006 p205

GARCIA, Maria Teresa Jimeno, PÉREZ, Carlos Miguez, GARCIA, Abel Mariano Matas, AGUDÍN, Justo Pérez, *Hacker Edición 2009.* Madrid: Anaya Multimédia, 2009

GODET, Michel. *Manual de Prospetiva Estratégica*: Lisboa: Publicações Dom Quixote, 1986

HALSALL. Fred, *Computer Networking and the Internet.* 5 ed. Essex: Addison-Wesley, 2005

LAMMLE, Todd. *CCNA Cisco Network Associate Study Guide*. 6 ed Indianapolis**:** Willey Publishing Inc, 2007

LARA, António de Sousa, *Subversão e Guerra Fria*: Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2011

LARA, António Sousa. *Ciência Política:* Estudo da Ordem e da Subversão. 6 ed. Lisboa . Instituto Superior de Ciências Sociais e Políticas 2011

LAUDON, Kenneth C., LAUDON, Jane P., *Management Information Systems*, Managing the Digital Firm, 12 edição Pearson, Harlow England 2012

MARCONI, Marina de Andrade, Lakatos, Eva Maria. *Metodologia do Trabalho Científico.* 6 ed. São Paulo: Atlas

MARIGHELLA, *Manual do Guerrilheiro Urbano.* E outros textos. Lisboa: Assírio & Alvim 1975 p 59

MINISTÉRIO DO EXÉRCITO. *O Exército na Guerra na Guerra Subversiva.* Lisboa 1966

OSANKA, Franklin Mark.Trad. Gabinete de estudos e traduções. *A Guerra Irregular em Transição.* Moçambique 1963(A moderna Guerra de Guerrilhas Publicação nº 6 1 volume parte I 2 edição) RMM Quartel General, Gabinete de estudos e traduções

PINHEIRO, J.A, Franco. Estratégia. Em *Verbo Enciclopédia Luso Brasileira de Cultura:* Lisboa v.7 p.1574-75, 1968

RIBEIRO, ANTÓNIO Silva, *O Essencial ao Processo Estratégico Teoria Geral da Estratégia*: Almedina Coimbra, 2009

SANTOS, Paulo, BESSA, Ricardo, PIMENTEL, Carlos, *Cyberwar:* O Fenómeno, as Tecnologias e os Actores: FCA Editora de Informática, Lisboa 2008

TABER, Robert, *Teoria e Prática da Guerra.*Trad. Isabel Araújo. Lisboa s.d. Versão original em língua inglesa: Lyle Stuart Inc. ,1965

VENTRE, Daniel, *Information Warfare*: Wiley, Hoboken USA, 2009

YIN, Robert K. *Estudo de Caso,* Planejamento e Métodos: Porto Alegre 2001

Recursos da Internet Consultados

China's ciberwar goes beyond Google, in
http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/13/google-china-cyber-war-security consultado em 12/4/2012

China`s Cyber Warfare capabilities, in
http://www.securitychallanges.org.au/ArticlePDFs/vol7no2Ball.pdf

Department of Defense, *Departement of Defense Stategy for Operating in Cyberspace July 2011*, in
http://www.defense.gov/news/d20110714cyber.pdf consultado em 20/5/2012

House of Lords, *Protecting Europe against large-scale cyberattacks*, in
http://www.publications.parliament.uk/pa/ld200910/Idselect/Ideucam/68/68.pdf,consultado em 20/5/ 2012

China`s cibewar goes beyond Google, in
http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/13/google-china-cyber-war-security consultado em 12/4/2012

McAfee, *Protecting your Critical Assets,* in http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf Consultado a 25/4/201

Scientific American, *The Fog of Cyberwar: What are the Rules of engagement,* in
http://www.scientificamerican.com/article.cfm?id=fog-of-cyber-warfare Consultado em 23/5/2012

Ataque à Estónia

http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all Consultado em 14/4/2012\

http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia Consultado em 14/4/2012\

http://www.riso.ee/en/pub/2003it/p15.htm Consultado em 14/4/2012

Ataques à Georgia

http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

http://en.wikipedia.org/wiki/Cyberattacks_during_the_2008_South_Ossetia_war

www.president.gov.ge

www.nbg.gov.ge

www.mfa.gov.ge Consultados em 15/4/2012

http://www.arbornetworks.com/

http://www.shadowserver.org/wiki/Consultados em 15/4/2012

Caso Aurora

http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf Consultado em 17/4/2012

Man-in-the-Middle attack

https://www.owasp.org/index.php/Man-in-the-middle_attack Consultado em 12/4/2012

South Ossetia: The First Cyber/Physical War, in

http://www.loosewireblog.com/2008/08/south-ossetia-t.html consultado em 24/5/2012

STALLINGS, William, *Computer Networking with Internet Protocols http://ww1w.defense.gov/news/d20110714cyber.pdf and Technology*: Pearson Education Inc., Upper Saddle River, NJ USA Consultado em 12/4/2012.

Stuxnet

http://en.wikipedia.org/wiki/Stuxnet Consultado em 17/4/2012

Wikipedia, *2007 cyberatttackson Estonia*, in

http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia Consultado em 14/6/2012

Wikipedia, *Cyberattacks during the 2008South Ossetia war*, in

http://en.wikipedfia.org/wiki/Cyberattacks_during_the_2008_South_Ossetian_war

consultado em 20/6/2012

Wikipedia, *Cyberwarfare, in*

http://en.wikipedia.org/wiki/Cyberwarfare Consultado em 14/6/2012

Wikipedia, *Operation Aurora,* in

http://en.wikipedia.org/wiki/Operation_Aurora Consultado em 17/6/201