ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

TEORIA RELATIVISTA DO CIBERTERRORISMO

Marco Aurélio Gonçalves Pinto

Dissertação para a obtenção do grau de

Mestre em Guerra da Informação

Lisboa

2011

ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

TEORIA RELATIVISTA DO CIBERTERRORISMO

Marco Aurélio Gonçalves Pinto

Dissertação de Mestrado em Guerra da Informação

Trabalho realizado sob a supervisão:

Orientador Professor Doutor Fernando Carvalho Rodrigues

Co-Orientador Professor Doutor João Pedro da Cruz Fernandes Thomaz

Lisboa

2011

DEDICATÓRIA

Dedico este trabalho a todos aqueles que acreditaram em mim dizendo para ir em frente pois, com o devido esforço, tudo era alcançável.

Dedico também aos meus amigos de infância, Carlos César e Jorge Canelhas, que tiveram um enorme papel no meu desenvolvimento de carácter e académico.

Dedico também aos meus três mentores: o Bryon Smith (EUA), o Jaban David (Canadá) e o Glenn Steckling (EUA). Ao longo dos mais de dez anos que nos conhecemos, eles tornaram-me uma pessoa mais madura, mais responsável e mais perfeccionista, procurando sempre alcançar "refinement and betterment".

AGRADECIMENTOS

Aos Professores Fernando Carvalho Rodrigues e João Pedro da Cruz Fernandes Thomaz por terem aceitado orientar a minha dissertação, quando todos os outros Professores que contactei não se encontravam disponíveis.

Ao Coronel Vilas Leitão, Coronel Fernando Freire e à Gertrudes Pires por terem entrado na minha vida, pois são as pessoas que conheço há mais tempo na AM e por quem nutro um grande respeito e foram uma força inspiradora para prosseguir o curso.

Ao meu tio Edmundo e tia Edma que sempre me apoiaram no mestrado e disseram para eu ir em frente seguindo o meu coração pois eu era capaz de realizar tudo aquilo a que me propunha, bastando estar mentalizado para tal.

À minha chefia no JUMBO, onde trabalho há quase onze anos, pelo apoio que me deram relativamente ao mestrado e por terem compreendido o quanto importante ele era para mim. Tanto que ofereceram-me dias de dispensa para estudar e alteraram o meu horário para estar sincronizado com as aulas.

Aos meus "irmãos" Nuno Góis, António Guerra, Carlos Silva, Rogério Bravo, Marcelo Borges e Maria Vasconcelos que, além de colegas excelentes, também muito aprendi com o contacto que tive com eles.

À Eduarda Guimarães dos CTT pelas dicas, apoio moral e psicológico que me deu durante a parte lectiva do Mestrado.

Por fim, a todos os meus Professores do passado e do presente por todo o conhecimento que verteram em mim e que se tem mostrado útil nas mais diversas ocasiões.

RESUMO

Esta dissertação procura conseguir minimizar ataques ciberterroristas que usam meios electrónicos, acessíveis a todos, mensurando o grau de severidade e transformando dados em Informação

Aborda a globalização, possibilitando lesar interesses estrangeiros em qualquer parte do mundo usando meios electrónicos. Ao cessar a guerra-fria surgiram novas ameaças sendo necessário detectá-las e impedi-las, estimar a máxima verosimilhança, definir Informação e os níveis, mensurar a quantidade de Informação e certeza associada aos eventos, as dinâmicas humanas e sociais e que os sistemas de crenças são importantes. Define Terrorismo e Ciberterrorismo e as razões atrás dos actos criminosos, as dimensões em que os grupos se encaixam, as diferenças entre suporte e ataques, os graus de ameaça e exemplos de ataques. Aborda também as principais ferramentas dos criminosos.

Explica a relação existente entre as *Botnets* e o Ciberterrorismo, sendo computadores comprometidos, vendidos ou alugados para ataques em grande escala. Explica como se propagam, operam, formas de detectá-las e enfrentá-las.

Conclui que tudo é relativo dependendo de cada indivíduo e cada computador, tendo-se de trabalhar os sistemas de crenças para fazer face às ameaças e desafios, pois o ataque ou a defesa vence dependendo da complicação ou simplicidade dos dados que afectam a quantidade de Informação.

Palavras-chave: Ciberterrorismo, Internet, Informação, Teoria Relativista, Fisher;

ABSTRACT

This dissertation tries to be able to minimize cyberterrorism attacks using electronic means, available to everyone, by measuring the severity degree and transforming data into Information.

It addresses globalization, allowing to affect foreigner interests in any part of the world using electronics means. By ceasing the cold-war, new threats appeared needing ways to detect and prevent them, estimate the maximum likelihood, define Information and its levels, measure the amount of Information and the certainty associated with events, the social and human dynamics and that belief systems are important. Defines Terrorism and Cyberterrorism and the reasons behind terrorist acts, the dimensions in which the groups fit in, the differences between attacks and support, the degrees of threats and examples of attacks. It addresses the main criminals' tools.

It explains the relationship between Botnets and Cyberterrorism, being compromised computers, sold or rent for mass attacks. It explains how they spread, operate, detecting them and ways of facing them.

It concludes that everything is relative depending on each individual and each computer, having to work on the belief systems to face threats and challenges, because the attack or defence wins depending on the complexity or simplicity of data affecting the quantity of Information.

Key-Words: Cyberterrorism, Internet, Information, Relativist Theory, Fisher;

LISTA DE ABREVIATURAS

AC – Análise Combinatória

AM – Academia Militar

C&C – *Command and Control* (Comando e Controlo)

C2 – *Command and Control* (Comando e Controlo)

C2W – *Command and Control Warfare* (Guerra de Comando e Controlo)

C4I – *Command, Control, Communications, Computers, and Intelligence* (Comando, Controlo, Comunicações, Computadores e Inteligência)

CNA – *Computer Network Attack* (Ataque Informático em Rede)

DoD – *Department of Defense* (Departamento de Defesa dos EUA)

DDoS – *Distributed Denial of Service* (Ataque distribuído de Negação de Serviço)

DoS – *Denial of Service* (Ataque de Negação de Serviço)

EA – *Electronic Attack* (Ataque Electrónico)

EPI – *Extreme Physical Information* (Informação Física Extrema)

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation* (Polícia Federal dos EUA)

HSD – *Human and Social Dynamics* (Dinâmicas Humanas e Sociais)

IDNS – *Internationalized Domain Names* (Nomes de Domínios Internacionalizados)

IRC – *Internet Relay Chat* (Protocolo de Comunicação na Internet usado para *chat*)

ISP – *Internet Service Provider* (Fornecedor de Acesso à Internet)

JP – *Joint Publication* (Publicação Conjunta)

MLE – *Maximum Likelihood Estimation* (Estimação de Máxima Verosimilhança)

NATO – *North Atlantic Treaty Organization* (Organização do Tratado do Atlântico Norte)

NSA – *National Security Agency* (Agência Nacional de Segurança dos EUA)

ONG – Organizações não-governamentais

ONU – Organização das Nações Unidas

SI – Sistemas de Informação

TLD – *Top-Level Domain* (Domínio de Topo)

UC – Unidade Curricular

U.S. – *United States* (Estados Unidos)

CORPO DE CONCEITOS

- ***Agressão:*** Pode ser física, mental, psicológica ou verbal. É o acto ou a intenção com o objectivo de causar danos a Estados soberanos, forças armadas, ou simplesmente civis, não esquecendo também as infra-estruturas. Está presente em todos os conceitos, excepto nos crimes que não envolvam o uso ou ameaça da força e depende dos alvos e dos motivos por detrás da agressão.
- ***Crime:*** A violação intencional de um estatuto criminal por um ou mais indivíduos (em grupo). Os departamentos estatais e locais são responsáveis por proteger as comunidades contra todos os tipos de crimes. No crime vulgar, os criminosos tentam minimizar a exposição dos seus actos para não serem detectados, ao contrário do terrorismo que tenta maximizar a exposição dos actos para que todo o mundo saiba que eles existem, são perigosos e ninguém está seguro.
- ***Guerra:*** O uso sistemático da agressão ou da contra agressão por parte de uma nação soberana contra outra, após uma declaração formal de guerra por parte do líder de uma delas, de forma a legitimar a ofensiva. A guerra distingue-se do terrorismo por estar relacionada com assuntos formais entre nações soberanas e por o tipo de equipamento militar ser mais pesado. Podem existir guerras civis que são guerras internas dentro de nações soberanas, onde grupos rebeldes combatem as forças governamentais de forma a tentar conseguir o controlo do poder, ocorrendo normalmente em países do terceiro mundo por serem países com governos instáveis e fracos (regimes ditatoriais e monárquicos normalmente).
- ***Terrorismo:*** É o uso premeditado, ilícito e a ameaça de violência contra civis ou alvos que tenham significado simbólico com objectivos ideológicos, políticos, religiosos ou outros, através da intimidação ou da aniquilação de uma população identificada como o inimigo. É uma forma extrema da agressão e do crime com custos sociais e consequências superiores aos actos severos de crime de rua e da agressão violenta. Em algumas ocasiões o terrorismo assemelha-se mais à guerra do que ao crime, face aos grandes recursos financeiros que consegue para comprar armamento militar e até mesmo armas de destruição maciça.

- ***Cibercrime:*** Acto baseado ou que tem como alvo os sistemas informáticos. Pode envolver o roubo de propriedade intelectual, violação de patentes, roubo de segredos de comércio, violação das leis de direito de autor e a usurpação de identidade. Inclui o ataque a sistemas informáticos com o objectivo de disruptir o processamento, a espionagem industrial, etc. Um ciberataque para infligir danos pode ser um cibercrime, pois depende das intenções dos atacantes. Os sistemas informáticos são usados como armas e esse tipo de actividade pode-se chamar de Guerra da Informação ou Cibercrime.
- ***Ciberterrorismo:*** Actos fundados em motivações políticas, ideológicas ou sociais e em operações de *hacking* com o objectivo de causar prejuízos severos (perda de vidas humanas, prejuízos económicos, ataques ou ameaças contra sistemas informáticos, redes e a respectiva Informação neles armazenada) de forma a intimidar ou coagir um governo. Pode chegar a ser um ataque físico com o objectivo de destruir nós computorizados de infra-estruturas críticas (Internet, telecomunicações) ou a grelha eléctrica de um país ou de uma cidade. O Ciberterrorismo é semelhante ao cibercrime mas é uma versão mais extrema do cibercrime, com consequências piores.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

Capítulo I

Introdução e Metodologia

I.1. Introdução

Vivemos num mundo cada vez mais perigoso e hostil. Enquanto no passado todos os ataques eram físicos e havia fronteiras delimitadoras dos Estados, hoje assiste-se a uma globalização do mundo onde já não existem fronteiras físicas no sentido clássico. O mundo tornou-se uma pequena aldeia onde o que acontece num local é logo conhecido nos locais mais remotos.

Uma pessoa pode estar em qualquer parte do mundo e, através de meios electrónicos, conseguir acesso e/ou afectar infra-estruturas em qualquer outra parte do mundo. Por exemplo: podemos estar na China e lesar infra-estruturas nos EUA. A Internet veio tornar isto possível. O Ciberterrorismo é então o uso da Internet e de meios electrónicos para fins terroristas ou o ataque a infra-estruturas electrónicas também elas ligadas à Internet.

Com o fim da bipolaridade (LEBOW e RISSE-KAPPEN, 1996) mundial no século XX com origem no colapso da União Soviética, através da queda do muro de Berlim e o fim da Guerra Fria entre a União Soviética e os EUA, surgiram outros tipos de ameaças transnacionais. O ataque terrorista de 9/11 marcou uma nova era de guerra mundial em que os Estados civilizados já não são os actores principais, mas sim os grupos organizados vulgarmente conhecidos por terroristas, pelo crime organizado e pelos Estados párias. Estes, por motivos políticos, religiosos, financeiros, ou meramente pelo gozo causam danos enormes em infra-estruturas e na economia dos Estados.

Antes do 9/11 já existia o problema de ataques terroristas internacionais. Mas, o que aconteceu em 9/11 superou tudo até então pois atingiu o coração da "Polícia do Mundo" e teve enormes repercussões e efeitos psicológicos, sociais e políticos em todo o mundo, acordando o planeta para o que ir-se-ia tornar a guerra do século XXI: o combate a uma

nova era de terroristas, capazes de sacrificar a própria vida e a dos outros para alcançar os seus fins. Devido à desanexação da União Soviética e de outros países, surge cada vez mais a ameaça dos criminosos conseguirem armas de destruição maciça: químicas, biológicas e nucleares. Isto é de uma perigosidade aterrorizadora se postas em acção.

Com o início do século XXI tem havido um declínio naquilo que chamamos terrorismo tradicional como é o caso de raptos, desvio de aviões, ataques suicidas, etc. Agora temos de lidar com terroristas "silenciosos" que usam a tecnologia informática e que têm uma capacidade assustadora na destruição de sistemas humanos e, o mundo dito civilizado, já não tem a vantagem que tinha no passado pois os ciberterroristas, mesmo sem recursos financeiros elevados, conseguem infligir danos em Estados soberanos.

Nos dias actuais o tema do Ciberterrorismo é cada vez mais pertinente pois tudo está ligado através de canais electrónicos. Segundo Mark Sunner (2006), director de tecnologia da MessageLabs, qualquer pessoa pode fazer ataques DDoS (*Distributed Denial of Service attacks*) usando *botnets* que são computadores comprometidos também conhecidos por "computadores Zombies", e entrar em computadores para roubar, adulterar ou destruir Informação, e atacar servidores internacionais pertencentes a entidades estatais ou supranacionais. Isto significa que os terroristas actuais podem fazer pior que as pessoas comuns (amadores). Não esquecer que os ciberterroristas possuem conhecimentos de informática para os seus ataques que os terroristas clássicos desconhecem.

Na verdade, os terroristas só precisam vencer uma vez, enquanto os Estados precisam vencer sempre (NUNES, 2010). Daí existir uma assimetria entre forças amigas e forças hostis, pois as amigas têm de dedicar mais esforços na prevenção. Caso não se consiga uma prevenção, deve-se tentar neutralizar e minimizar ao máximo os possíveis danos colaterais. É preciso toda uma política de coordenação de esforços para lidar com esta ameaça.

A globalização agravou em muito os problemas do Ciberterrorismo e, para combater e precaver os actos hostis cometidos e/ou tentados cometer pelos "Terroristas Cibernéticos", existe um, cada vez maior, intercâmbio entre os países ditos democráticos, de forma a

tentar detectar antecipadamente todos os movimentos desencadeados pelos terroristas com recurso à espionagem, como é o caso de elementos infiltrados junto dos terroristas.

Veja-se o Projecto Echelon que, de acordo com a descrição da NSA (2010) constitui à escala mundial uma rede electrónica de vigilância para interceptar as comunicações telefónicas, *faxes* e correio electrónico e torna-los disponíveis aos países do acordo original UKUSA[1]. Actualmente defende-se que o Projecto Echelon não tem apenas como objectivo detectar os criminosos mas serve também para fazer espionagem industrial internacional de forma a beneficiar os membros do acordo. Existe então no Ciberespaço um "Big Brother" a observar e a controlar todos os utilizadores que pensam que ninguém está a ligar ao que estão a fazer.

Colocou-se a problemática de saber quem manda na Internet que no início tudo apontava para um só, os EUA, como durante tempos se admitiu (WACKS, 2010). Actualmente diz-se que ninguém manda devido ao carácter fragmentário da Internet, por esta ser constituída por uma pluralidade de meios de comunicação (redes ligadas umas às outras) e a variedade de utilidades ou meios de comunicação que proporciona, as centenas de milhões de sítios electrónicos, do lado dos fornecedores de Informação e dos utilizadores. Tudo isto coloca a capacidade de deter e comunicar nas mãos de todos.

É pouco provável a concentração absoluta do poder de governação da Internet numa só autoridade, pois esta ficaria com o monopólio virtual da Informação. Mas, é tendencialmente aproximável, se tivermos um único poder ou federação de poderes que consiga observar e controlar todos os demais intervenientes, visto que cada utilizador do Ciberespaço tende a guardar, disponibilizar e comunicar uma cada vez maior quantidade e variedade de Informação, disponível em localizações e ambientes adequados para observação e controlo. Veja-se por exemplo as redes sociais em que as pessoas e organizações partilham Informação pessoal e privada em excesso e que se alguma entidade governamental pretender aceder, poderá fazê-lo de forma fácil.

[1] O Acordo original UKUSA começou em 1947 aquando de um acordo de cooperação estabelecido entre os serviços secretos dos EUA e do Reino Unido durante a 2ª Guerra Mundial, com o objectivo de prosseguir actividades conjuntas de "inteligência". Isto foi conhecido como "Acordo UKUSA" ao qual mais tarde aderiram o Canadá, Nova Zelândia e Austrália.

Tanto na Internet como no mundo físico é-se constantemente inundado com dados, mas isto não significa que na realidade se tem Informação. Surge-nos então o problema de como transformar dados em Informação útil. Os dados são meramente um fluxo fragmentado de eventos ou transacções e que só por si têm pouca utilidade. Os dados para serem transformados em Informação útil, ter-se-á de fazer uso de técnicas de análise de dados que englobam a: (1) Organização dos dados; (2) Descrição dos dados e (3) Interpretação dos dados.

A Teoria da Informação de Fisher aparece-nos então como fundamental para ajudar a efectuar esta análise de dados, pois as Leis fundamentais da Ciência têm a ver com o conceito de Informação, desde a mais pequena escala até à maior, envolvendo também as actividades humanas como é o caso da economia e a organização sociocultural. Essas Leis derivam de um princípio (WordIQ.com, 2010) denominado *Extreme Physical Information* (EPI).

A Informação Física tem a ver com a Informação que é perdida ao observar um efeito físico, devido ao facto de qualquer que seja o canal de onde provém a Informação, este é geralmente imperfeito. O procedimento matemático de extremar a Informação Física através da variação das amplitudes de probabilidade do sistema é denominado de EPI e baseia-se no facto de que a observação da origem de um fenómeno nunca é totalmente preciso e que Informação é perdida durante a passagem da origem para a observação, e esta perda pode ser um valor extremo. Como exemplo: se o nível de Informação de Fisher nos dados tem um valor **I** e o nível de Informação de Fisher na origem tem um valor **J**, a EPI será calculada da seguinte forma: **I – J = Extremo**. Este Extremo é normalmente o mínimo em grande parte dos problemas, existindo uma tendência para qualquer observação descrever a origem de forma fiel o que é bom.

Quando temos de lidar com muitos elementos (dados), torna-se difícil o recurso a diagramas ou tabelas para efectuar uma contagem, pelo que se recorre à Análise Combinatória que parte de um número finito de elementos/dados para formar sequências. Deve-se quantificar os dados e a Informação e estes devem ser os mais simples possíveis e em menor quantidade, de forma a conseguir tornar possível uma melhor avaliação.

I.2. Metodologia da investigação

Neste subcapítulo será apresentada uma delimitação e enquadramento conceptual do tema da dissertação.

I.2.1. Objectivos da Investigação

O objectivo central desta investigação é detectar e impedir/minimizar os ataques dos ciberterroristas transformando dados em Informação. Procuramos pois melhorar e conhecer melhor o mundo em que vivemos e como ele pode ser perigoso devido a grupos extremistas, conhecidos por terroristas, que tudo fazem para causar o caos e a destruição em seu redor.

Ao longo desta dissertação procura-se descrever o que é o Ciberterrorismo, como ele é perigoso, como actuam os criminosos, os diferentes tipos de ataques e como tentar detectá-los de forma a evitar repercussões graves. Caso estes não sejam detectados a tempo dever-se-á tentar minimizar as consequências.

A investigação produzida demostra como é possível detectar uma ameaça ao transformar dados brutos em Informação útil. O mundo poderá ser um local melhor para as gerações actuais e vindouras, se conseguirmos detectar/impedir/travar/minimizar o impacto de ataques ciberterroristas.

A Teoria da Informação de Ronald Fisher desenvolvida a partir de 1925 vem ajudar neste processo pois ajuda a transformar dados brutos em Informação. A Análise Combinatória, Bayesiana, e a Teoria da Informação podem ajudar a detectar e prevenir eventuais ataques de Ciberterrorismo. Também serão descritos exemplos de diferentes formas de Ciberterrorismo e os respectivos impactos causados.

A proposta de valor que se pretende apresentar é uma melhoria da segurança global fazendo face a ciberterroristas e compreendendo como e porquê estes operam, e tornar o

ciberespaço um local e um instrumento de comunicação mais seguro com vista a alcançar um maior desenvolvimento económico, comercial e social a nível global.

I.2.2. Formulação do Problema

A Pergunta de Partida é: "*Como minimizar ataques ciberterroristas que usam meios electrónicos, acessíveis a toda a população, através da mensuração do seu grau de severidade e da transformação de dados em Informação?"*

Questões Derivadas:

Q1 – Qual a ligação entre o terrorismo tradicional e o Ciberterrorismo?

Q2 – Quais as motivações e como actuam os ciberterroristas (métodos e perfis-psicológicos)?

Q3 – Até que ponto será possível anular as repercussões dos ataques, detectando-os atempadamente através de técnicas combinatórias, designadamente, da Teoria da Informação de Fisher?

Q4 – Onde actuam os ciberterroristas, dentro dos Estados ou além-fronteiras?

Q5 – Como irão os ciberterroristas incrementar o grau de severidade dos seus ataques produzindo danos cada vez maiores?

Hipóteses:

H1 – Se utilizarmos técnicas combinatórias que transformam dados em Informação, então poderemos detectar os ataques ciberterroristas e assim proceder à sua monitorização.

H2 – Se o Ciberterrorismo permanecer, então causará danos cada vez maiores.

H3 – Se o Ciberterrorismo prevalecer, então será o principal conflito do século XXI.

H4 – Se os ciberterroristas não têm rosto nem um país certo de origem dos ataques, então a utilização de técnicas de detecção e de monitorização são essenciais para a manutenção da Segurança.

I.2.3. Limitações e Dificuldades

A principal limitação e dificuldade encontrada ao longo do tratamento do tema e da própria investigação foi, desde o início, derivada do tema escolhido, sensível e novo, onde as pesquisas já efectuadas estão pouco divulgadas e os livros são de difícil acesso.

Outra dificuldade encontrada foi na reunião com os orientadores, devido essencialmente a problemas de localização física e de agenda. No entanto, foi possível, através do uso de correio electrónico, a troca de Informação e *feedback* de uma forma rápida, fácil e sem quaisquer encargos.

Sendo a dissertação um desafio, onde existe a satisfação de encontrar soluções para problemas que parecem insolúveis, requer uma metodologia de trabalho bem definida e elaborada que considere a revisão da literatura, as hipóteses e métodos, os resultados e a sua discussão, a análise das implicações e limitações observadas.

Não existem trabalhos perfeitos e há sempre algo que pode ser melhorado, por isso devemos estar conscientes das limitações do trabalho desenvolvido e sugerir formas para as ultrapassar ou diminuir.

Capítulo II

Informação e Teoria da Informação

Neste capítulo aborda-se a Teoria da Informação de Fisher e procura-se explicar como transformar dados em Informação, usando a Estimação de Máxima Verosimilhança, define-se a Informação, como mensurá-la e os diferentes níveis existentes. Descreve-se as diferenças entre adivinhar, prever e ter a certeza. Depois temos as Dinâmicas Humanas e Sociais com vista a prever e impedir catástrofes naturais e humanas. Depois temos o comportamento emergente sendo o processo de formação complexa de padrões onde se apresentam várias figuras e as respectivas descrições. Depois falamos do Interior e Exterior e da Ilha de Resiliência onde se explica como manter a simplicidade de dados na tomada de decisões mencionando três métricas importantes. Por último temos a Pirâmide Cognitiva com os três domínios existentes: o físico, o da Informação e o cognitivo.

Segundo (DREKSTE, 1999) a *Teoria da Informação* é um ramo da teoria da probabilidade e da matemática estatística que identifica a quantidade de Informação associada ou gerada pela ocorrência de um evento, ou a realização de um estado de coisas, com uma redução da incerteza e uma eliminação de possibilidades, representada pelo evento ou estado de coisas em causa. Relativamente à Informação é sempre mencionado "escolha" e "quantidade" e como mensurar a Informação.

Sir Ronald Fisher (1890-1962), cientista de renome do século XX com enormes contribuições para a Estatística, Biologia Evolucionária e Genética, introduziu em 1925 o conceito de *Fisher Information*, muito antes da noção de *entropia* de Claude E. Shannon (1916-2001), com as técnicas de *máxima probabilidade* e da *análise de variâncias*.

II.1. Estimação de Máxima Verosimilhança

A estimação de máxima verosimilhança (MLE) é uma aproximação criada por Fisher em 1922, usada para resolver os problemas (STOICA, VIKALO e HASSIBI, 2003) de processamento de sinais/dados em sistemas de comunicação, nos quais o transmissor usa apenas uma antena e o receptor usa várias, de forma a conseguir uma grande fiabilidade na transmissão.

Devido ao facto de grande parte desses problemas não poderem ser resolvidos de forma analítica, são aplicadas técnicas numéricas como é o caso da atribuição de pontuação ao analisar os dados. Em muitos cenários torna-se ainda necessário alterar a aproximação incluindo Informação lateral adicional que a MLE deverá satisfazer.

De acordo com o sítio electrónico do National Institute of Standards and Technology (2010): a estimação de máxima verosimilhança é um procedimento totalmente analítico de maximização que se aplica a todas as formas de dados, sendo até possível ser usada em várias células de tensão e estimar os parâmetros de modelos de aceleração ao mesmo tempo que os parâmetros de distribuição de existência.

A MLE tem as seguintes propriedades de amostragem:

- Torna-se um estimador imparcial da variância mínima quando o tamanho da amostra aumenta;
- Tem distribuições aproximadas da normal e variâncias amostrais aproximadas, podendo ser calculadas e usadas para produzir limites de confiança;
- As funções MLE podem ser usadas para testar hipóteses relativas a modelos e a parâmetros.

Existem apenas dois pontos negativos, mas de enorme importância:

- Com um pequeno número de insucessos (menos de 5 ou 10) a MLE pode ficar enviesada e as propriedades óptimas de amostras grandes não se aplicam;
- O cálculo da MLE normalmente requer *software* especializado de forma a resolver equações não-lineares complexas, mas o *software* vai sendo melhorado ao longo dos anos de forma a tornar-se cada vez melhor.

O método da máxima verosimilhança (Universidade de Aveiro, 2003) consiste em admitir que uma amostra é a mais provável ou de maior densidade de probabilidade, tendo como estimativas dos parâmetros, os valores que maximizam a probabilidade (variável aleatória discreta) ou a densidade de probabilidade (variável aleatória contínua) da amostra.

Chama-se verosimilhança da amostra à probabilidade de ocorrência desta (dados discretos) ou à função de densidade de probabilidade conjunta desta (dados contínuos).

Este método consiste em seleccionar, entre todos os valores possíveis dos parâmetros populacionais, aqueles que tornem mais verosímil à ocorrência de uma amostra idêntica àquela que efectivamente se obteve. A estimação dos parâmetros deve usar o método de máxima verosimilhança, relativamente a observações individuais da ocorrência de um determinado evento.

Seja f(x: θ) a função de probabilidade X (discreta/contínua) calculada no ponto X = x. O valor de θ está incluído aqui pois a distribuição da variável X depende do parâmetro θ.

Sejam $\{X_1, X_2, \ldots, X_n\}$ uma amostra aleatória da variável aleatória X e sejam $\{x_1, x_2, \ldots, x_n\}$ os seus valores amostrais.

Definição:

A função de verosimilhança L é função da amostra e do parâmetro θ:

$$\boldsymbol{L(X_1, X_2, \ldots, X_n; \theta) = f(X_1; \theta) \,.\, f(X_2; \theta) \ldots f(X_n; \theta)}$$

$$\boldsymbol{L(\theta) = Prob(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n \mid \theta)}$$

No caso discreto: $\boldsymbol{L(\theta) = \prod_{i=1}^{n} P(X_i = x_i \mid \theta)}$

No caso contínuo: $\boldsymbol{L(\theta) = \prod_{i=1}^{n} f(x_i \mid \theta)}$

Quanto maior for o valor da função, mais verosímil se tornará a ocorrência de uma amostra idêntica a $\{x_1, x_2, \ldots, x_n\}$.

Definição:

A estimativa de máxima verosimilhança de θ, baseada numa amostra aleatória obtida da população X, é o valor de θ que maximiza a função de verosimilhança L, para uma amostra $\{X_1, X_2, \ldots, X_n\}$:

$$\boldsymbol{Max} : \boldsymbol{L(\theta)} = \prod_{i=1}^{n} \boldsymbol{P(X_i = x_i \mid \theta)}$$

Observações:

θ é uma v.a., pois o seu valor depende da amostra $\{X_1, X_2, \ldots, X_n\}$.

Normalmente θ representa um valor isolado, mas se a distribuição depender de mais de um parâmetro (dois no caso da normal), θ representará um vector, por exemplo, $\boldsymbol{\theta} = (\boldsymbol{\alpha}, \boldsymbol{\sigma})$.

Para determinar a estimativa de máxima verosimilhança, deve-se determinar o valor máximo de uma função.

A Análise Combinatória (I.S.E.L., 2008) é uma área de extrema importância para o estudo das probabilidades e da estatística, servindo para estimar a incerteza associada a um acontecimento, quase sempre com base na contabilização do número de casos favoráveis à realização do evento. Os métodos ou técnicas de contagem permitem obter resultados fáceis, mesmo nos casos em que manualmente sejam muito lentos e de difícil contabilização, ou ainda, aqueles em que é possível obter o que se denomina de "falsos positivos", ou seja, resultados que parecem ser válidos, mas que o não são.

O computador no desenvolvimento da análise combinatória tem um papel de extrema importância, pois ajuda na sistematização e na resolução de problemas com um grande número de elementos, alargando o espectro de aplicação desta análise.

O método da Análise Combinatória está limitado a dados discretos ou que possam ser tornados discretos por agrupamento em categorias. O método MLE pode ser aplicado a dados contínuos, sem necessidade de agrupamento em categorias.

II.2. Definir "Informação" e mensurá-la

A Informação é como o espaço e o tempo, ou seja: é algo que todos julgamos saber mas, quando nos é perguntado, ficamos perplexos e não sabemos o que responder. Apenas quando somos confrontados com esta questão é que nos apercebemos o quão pouco sabemos na realidade.

Uma coisa é certa: somos capazes de medir e computar a quantidade de Informação e devemos ter o mínimo de dados e Informação possível para trabalhar, melhorando a qualidade do resultado final. Outro factor necessário para aumentar a qualidade do resultado final é a simplicidade e a riqueza de dados e da Informação, o que torna possível uma melhor avaliação.

Em 1925, Fisher deu a primeira definição de "quantidade de Informação" dizendo ser possível mensurar a quantidade de Informação fornecida por um conjunto de dados sobre um parâmetro/variável desconhecido. Perante um conjunto de dados é possível saber se têm Informação a mais ou menos acerca de uma variável desconhecida mas que queremos saber.

Para Fisher, uma estimativa é, em primeiro lugar, uma estatística que representa uma redução de dados, ou seja, uma estimativa é avaliada como um resumo das evidências e não o adivinhar ao acaso de quantidades não observáveis.

Quando a estrutura do sistema (Informação de natureza orgânica) tem uma simplicidade de dados, mesmo com um reduzido número de elementos no conjunto de dados, é-se conseguida a quantidade máxima de Informação sobre o sistema. Em palavras simples, quando existe uma simplicidade de dados, mesmo com poucos dados, consegue-se uma grande e valiosa quantidade de Informação.

Quando a estrutura do sistema tem dados confusos, é indiferente o tamanho de elementos no conjunto de dados, pois a quantidade de Informação sobre a estrutura do sistema não pode ser conseguida. Em palavras simples, quando existe uma confusão de dados, mesmo

com muitos dados, consegue-se uma quantidade de Informação perto do zero, ou seja, com pouco valor.

Em palavras simples: temos uma Informação de natureza orgânica (relativa à estrutura) e de natureza funcional (relativa ao serviço/uso) quando existe uma simplicidade de dados. Temos uma Informação com pouco valor quando estamos perante a existência de dados complicados e confusos.

Isto quer dizer que, perante um conjunto de dados, avaliamos a quantidade de Informação que é trazida sobre a estrutura do sistema sendo possível "saber" se os dados têm Informação a mais ou a menos sobre uma variável desconhecida que se quer e se procura conhecer. Para isso torna-se necessário os interrogatórios, ler o jornal e usar os outros Media para aumentar o conjunto de dados de forma a conseguir uma maior quantidade de Informação sobre a variável que se desconhece, sem usar a adivinhação.

Isto é suposto demonstrar a facilidade em descobrir distribuições de probabilidade ao tirar amostras delas. A grande importância disto é que a variância é uma estimativa não influenciada e, à medida que se avança, é possível conseguir estimativas mais precisas e exactas a partir dos dados em análise. Ou seja, vai-se conseguindo melhorar a qualidade da Informação e a respectiva quantidade de Informação resultante.

Quando se quer transformar dados em Informação, deve-se ter em conta três regras (SNODGRASS, 2007):

- **Organizar os dados:** Quando se é confrontado com um conjunto de pontuações, estas devem ser ordenadas numericamente;
- **Descrever os dados:** Quando se comparam dois ou mais conjuntos de pontuações, estas devem estar referidas a uma mesma escala;
- **Interpretar os dados:** Quando se está a ver graficamente os testes de pontuação, deve-se ter em conta que a representação visual é uma interpretação que respeita os testes numéricos.

A Informação e o conhecimento resultam da acção humana na agregação de dados (símbolos ou factos) de âmbito social e físico, fora de contexto, não directa nem

imediatamente significativos (sinais). Os dados colocados num determinado contexto, adquirirem significado e valor passando a ser designados de Informação. O conhecimento resulta da acumulação significativa de Informação relevante e estruturada, capaz de produzir uma acção, em parte baseada na experiência. A transformação dos dados em Informação e depois em conhecimento, requer um esforço cognitivo na percepção da estrutura e na atribuição de um significado e de um valor.

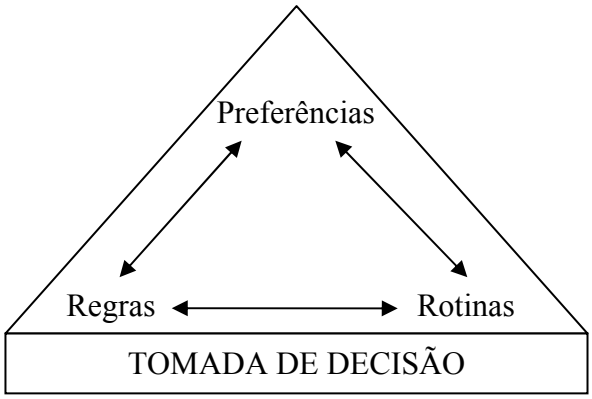
Por exemplo: se tivermos um documento com uma tabela de números que indicam as vendas de um produto/serviço num semestre, estes números são Dados. Um empregado lê esses números, reconhece o nome e a natureza do produto/serviço, observa que os números estão abaixo do normal, indicando uma tendência decrescente. Os dados transformam-se então em Informação. O empregado considera então as possíveis explicações para o sucedido (com Informação adicional e julgamento pessoal) e chega à conclusão que o produto/serviço já não é atractivo para os clientes, alcançando o Conhecimento.

Segundo Nonaka e Takeuchi (1995), a criação de Informação e de conhecimento envolve um tipo de processo que amplifica o conhecimento gerado pelos indivíduos individualmente, cristalizando-o como parte da rede do conhecimento da organização. Isto é conseguido através de duas actividades: (1) Uma conversão do conhecimento tácito em explícito; (2) A transferência do conhecimento que faz parte do nível individual para o nível grupal, organizacional e inter-organizacional.

Relativamente à partilha da Informação e do conhecimento, esta é uma das chaves na gestão do conhecimento. Contudo, existem algumas barreiras cognitivas, afectivas e organizacionais que dificultam esta partilha. Na parte cognitiva existe um esforço mental para explicar os novos conceitos, demonstrar as técnicas, dar resposta a questões, etc. não nos podendo esquecer que é possível sentir arrependimento ou relutância em perder a posse do *know-how* conseguido arduamente.

A tomada de decisão é precipitada por uma situação de escolha de um curso de acção, normalmente uma meta/objectivo e que implica efectuar uma escolha tendo agora em conta os resultados futuros possíveis. As decisões são o resultado de interacções dinâmicas entre três elementos: preferências, rotinas e regras. As **preferências** guiam na percepção e

contextualização das decisões, na avaliação e escolha das alternativas, e incorporam diversas formas de **rotinas** organizacionais que incluem as que apoiam o desempenho de uma tarefa e negociação política. O Procedimento de escolha é guiado por **regras** que especificam o comportamento apropriado e a participação desejada.



Fonte: Choo (1998)

Figura 1 – Ciclo da tomada de decisão

II.3. Níveis na "Informação"

A Informação pode ser agrupada em vários "níveis", desde a forma mais básica à mais complexa. Mostra-se a seguir uma possível estrutura dos níveis na Informação:

Os **Bits e Bytes/Sinais** são a matéria-prima, representando a Informação binária no formato compreendido pelos computadores, ou seja, zeros e uns que correspondem a ondas e impulsos eléctricos. Os zeros representam que não há corrente a passar e os uns representam corrente a passar, tal e qual um interruptor eléctrico. É o nível mais baixo existente nos computadores e, por isso, é também aquele que existe em maior quantidade. É impossível aos seres humanos discernirem o que está representado neles, só tendo utilidade quando se encontram numa forma relevante.

Os **Símbolos** são o alfabeto usado para ordenar os bits, formando *strings* finitas (palavras) e *strings* infinitas (mensagens). As palavras e mensagens tanto podem ter a forma de texto ou serem verbais, números, diagramas e até mesmo imagens estáticas ou em movimento

(vídeo). A ocorrência de certos símbolos pode influenciar a ocorrência de outros em vários períodos de tempo, influenciando a quantidade de Informação conseguida conforme cada símbolo é analisado.

Os **Dados** são medidas isoladas sobre eventos. Segundo (JONES, 2000) os dados são normalmente vistos como sendo a forma mais fundamental da Informação. Normalmente o termo "dados" significa algo bruto e não refinado, que deve ser "polido" de forma a transformar-se num produto acabado. Pode-se estar "inundado" com dados o que não significa que temos Informação. Exemplo: Os nomes de pessoas e cidades são habitualmente classificados como Informação, enquanto o número atribuído a alguém num hospital é considerado "dados".

A **Informação** é os dados num contexto possuindo um valor semântico compreendido como sememas[2]. A Informação adquirida necessita ser seleccionada, elaborada e analisada até que possa ser usada e, normalmente denota dados de uma forma combinada e com um fim específico. Os termos "dados" e "Informação" costumam na generalidade ser usados em simultâneo, pois um conjunto vasto de dados esconde Informação que é descoberta ao analisar os dados.

O **Significado** é a Informação num sistema de crenças (DORBOLO, 2003). As crenças e ideias que temos formam um sistema cujas partes estão interrelacionadas de várias formas. Esse sistema é dinâmico, ou seja, altera-se conforme nova Informação é acrescentada e, quando isso acontece, toda a Informação nova é alterada pelo sistema. Todos temos sistemas de crenças que condicionam a forma como vemos e nos relacionamos com o mundo.

O **Conhecimento** é o significado em vários contextos. É um conjunto de agregações que ultrapassam o valor semântico do elemento individual. Tem a ver com a forma como as coisas são feitas e como elas existem. O contexto (BREZILLON,1998) sendo visto como conhecimento torna necessário fazer uma distinção entre conhecimento contextualizado (o

[2] Segundo o Dicionário Editora da Língua Portuguesa da Porto Editora, a palavra "sememas" significa unidade de significação contida num lexema, e que é constituída pelo conjunto dos seus semas (componente mínima de significação de uma palavra).

conhecimento que é usado numa dada altura) e o conhecimento contextual (o conhecimento que restringe o conhecimento contextualizado). A grande dificuldade que se enfrenta é que a dada altura para uma posterior, o conhecimento contextualizado poder-se-á tornar conhecimento contextual. Temos dois tipos principais de Conhecimento (LAUDON, 2009):

- **Tácito:** Conceito introduzido por Michael Polanyi (1974) para situações em que processos cognitivos/comportamentais são conduzidos pelo inconsciente cognitivo. É o tipo de conhecimento que se caracteriza por ser conhecimento-na-prática, desenvolvido através da acção, experiência, ideias, valores, etc. e por isso partilhado através da conversação e troca de experiências. Em palavras simples, pode ser aprendido através da observação e da imitação, não podendo ser facilmente codificado, descrito ou reduzido a regras.
- **Explícito:** Representa um resumo, baseado na experiência directa e que pode ser facilmente articulado ou codificado através de um sistema de símbolos o que o torna a ser facilmente comunicado ou difundido. Este tipo de conhecimento encontra-se em produtos, patentes, código fonte de *software*, etc. O conhecimento explícito codificado é valioso pois aumenta a capacidade de conhecimento observável e negociável, facilitando a sua comunicação e codificar a aprendizagem transmitida em regras. Uma vez codificado, assim permanece, mesmo que mais tarde ou seus autores ou inventores partam.

A **Percepção** é o significado filtrado pelo sistema de crenças. É o processo mediante o qual os organismos interpretam e organizam a sensação para construir uma experiência significativa do mundo, envolvendo normalmente um processamento adicional de *inputs* sensoriais.

A **Significação** (FRASER e MACKAY, 1975) é o significado percebido em termos de objectivos. Em termos de estatística, para modelos muito simples é possível encontrar na significação uma equivalência numérica. O teste da significância tem o alcance mais amplo de aplicações e requer um modelo mas, somente quando se formulam hipóteses, o modelo pode descrever a resposta como um todo ou apenas uma redução da resposta.

II.4. Adivinhar vs. Prever vs. Certeza

Fala-se neste subcapítulo no Adivinhar pois, no passado, era considerado uma ciência possível que tinha como objectivo tentar determinar o significado ou as causas dos acontecimentos. Com os avanços da ciência, a adivinhação foi abandonada e passou só a ter-se em conta a previsão e a certeza.

Tudo aquilo que é conhecido além da dúvida (BERNOULLI, 1713), dizemos conhecer ou compreender. Em relação a tudo o resto, apenas conjecturamos ou opinamos. Fazer conjecturas sobre algo é o mesmo que mensurar a probabilidade de algo o melhor possível de forma a ser possível escolher a melhor opção para os nossos julgamentos e acções.

O acaso não é parte do conhecimento, mas é sim uma propriedade do objecto, não sendo possível fazer previsões. A probabilidade é uma medida de quanto certos estamos e é conseguida com uma combinação de argumentos. Quando um argumento pode ser matematizado, podem-se fazer previsões. Quando um argumento é uma imagem, pode-se predizer (*forecast*) pois "uma imagem vale mil palavras" sendo objectiva. Quando se tem ambos os argumentos (a imagem mais a matemática) pode-se conseguir a certeza. Cada argumento tem de ter um peso e o conjunto de argumentos com os respectivos pesos é um sistema de crenças.

As probabilidades são estimadas pelo número e peso dos argumentos que provam ou indicam o que uma certa coisa é, foi ou será. Os argumentos, só por si, são intrínsecos, ou artificiais no discurso diário, eliciados de acordo com as considerações da causa, os efeitos, da pessoa, da ligação, indicação ou quaisquer outras circunstâncias que possam ter alguma relação com a coisa sob prova. Também pode ser externo e não artificial, derivado da autoridade das pessoas e dos seus testemunhos.

A forma de aplicar os argumentos para conjecturar e mensurar as probabilidades pode seguir as seguintes nove regras ou axiomas:

1) Nas coisas onde é possível ter a certeza total, não existe lugar para conjecturas;
2) Não é suficiente apenas pesar um ou outro argumento, sendo necessário investigar todos aqueles que possam chegar ao nosso conhecimento e que sejam apropriados para provar as coisas;

3) Não devemos apenas considerar os argumentos que provam algo, mas também aqueles que possam levar a uma conclusão oposta, para ser mais claro qual deles tem um peso maior;
4) Para julgar universalidades, os argumentos remotos e universais são suficientes. Contudo, para formar conjecturas sobre coisas específicas, devemos acrescentar argumentos mais próximos e especiais se estes se encontrarem disponíveis;
5) Na incerteza deve-se cessar as nossas acções até se ter mais clareza e, se tivermos de escolher entre duas possibilidades, escolher a que pareça mais apropriada, segura, sensata ou pelo menos mais provável, mesmo que nenhuma o seja;
6) Ao que é útil e não prejudicial, deve-se ter em preferência ao que nunca é útil ou sempre prejudicial;
7) As acções humanas não devem ser avaliadas de acordo com o desfecho pois, às vezes, as acções mais imprudentes têm o melhor resultado, enquanto as acções mais razoáveis podem levar a piores resultados;
8) Nos nossos julgamentos, devemos ter cuidado antes de atribuir às coisas mais peso do que elas merecem, nem considerar algo apenas mais provável que algo com certeza absoluta, nem impor a mesma opinião a outros;
9) Uma vez que a exactidão total só pode ser conseguida raramente, considera-se como certeza absoluta apenas aquilo que é moralmente certo através da necessidade e do desejo personalizado.

O sistema de crenças é então definido como sendo o conjunto de argumentos e os respectivos pesos. Logo, a quantidade de Informação fornecida por um conjunto de dados acerca de uma variável desconhecida depende do sistema de crenças existente. Ou seja, perante o mesmo conjunto de dados obtêm-se resultados diferentes, influenciados pelos diferentes sistemas de crenças que todos temos e que condicionam a forma como vemos e como nos relacionamos com o mundo.

Para investigar o sistema de crenças, devemos colocar as seguintes questões (DORBOLO, 2003):

- Quais as crenças que temos?
- Como é que as crenças se interrelacionam?
- Como é que as crenças estão relacionadas com os nossos sentimentos e acções?

- Quais das nossas crenças são mais importantes e básicas?
- Até quando no passado conseguimos localizar o nosso sistema de crenças?
- Onde conseguimos as nossas crenças? Criámo-las ou herdámo-las?
- Experienciámos grandes alterações no nosso sistema de crenças? Como é que isso aconteceu?
- Será possível desenharmos um diagrama de um *cluster* específico de Informação, ideias, sentimentos e acções?

O Padre António Vieira (Século XVIII) disse: "Na perda de uma batalha arrisca-se o exército. Na perda de opinião, arrisca-se o reino". Perder a batalha refere-se ao que nos dias actuais chamamos *hardware* e a perda da opinião refere-se às crenças e à quantidade de Informação (Equação Relativista), ou seja, os argumentos e os respectivos pesos.

Em 1948 Shannon[3] trouxe-nos uma definição mais recente de quantidade de Informação onde diz que esta é a medida da liberdade de escolha de cada um quando se selecciona uma mensagem (dado) de entre todas as do conjunto. Logo, o outro método para perante um conjunto de dados obter mais quantidade de Informação é trabalhar e focar no sistema de crenças… os interrogatórios são uma maçada por darem demasiado trabalho e poucos resultados.

Para Shannon, o conteúdo da Informação de cada mensagem consiste apenas na quantidade de números (bits), uns e zeros, levados para transmitir a mensagem. Daí, chega-se à conclusão que os números binários (bits) são a unidade elementar da Informação e podem ser apenas: zeros ou uns, verdadeiro ou falso, sim ou não, branco ou preto, e por aí em diante. A Informação pode assim ser tratada como uma quantidade física mensurável.

Em suma: por mais completo que seja o conjunto de dados, haverá sempre um sistema de crenças onde a quantidade de Informação sobre a variável desconhecida será zero, devido às limitações do sistema de crenças dos indivíduos em causa. Muitas vezes é-nos dito a forma como as coisas são mas nós não ouvimos. Daí dizer-se: "Quem não sabe é como quem não vê". Outra coisa que se costuma dizer é: "Quem conta um conto acrescenta um

[3] Claude Elwood Shannon (1916-2001) é considerado por muitos o pai da Teoria da Informação.

ponto" o que significa que conforme a palavra sobre algo vai passando, vai sendo afectada por quem passa o conhecimento. Isto é o denominado Conhecimento Popular (não Científico).

Tipo Conhecimento	Popular	Religioso	Filosófico	Científico
Características	- Valorativo - Reflexivo - Assistemático - Verificável - Falível - Inexacto	- Valorativo - Inspiracional - Sistemático - Não verificável - Infalível - Exacto	- Valorativo - Racional - Sistemático - Não verificável - Infalível - Exacto	- Real (factual) - Contingente - Sistemático - Verificável - Falível - Aproximado

Fonte: Trujillo (1974)

Tabela 1 – Características dos 4 tipos de Conhecimento

A tabela acima mostra-nos as características dos quatro tipos de conhecimento existentes no mundo. Isto é importante saber pois influenciam o sistema de crenças de formas diferentes, ou seja, conforme o tipo de conhecimento de cada individuo, diferente será o sistema de crenças de cada um.

Também haverá um sistema de crenças em que, perante um conjunto de dados incompletíssimo, obterá o máximo de quantidade de Informação sobre a variável desconhecida. A ciberguerra é a manipulação da ambiguidade.

II.5. Dinâmicas Humanas e Sociais (HSD)

As Dinâmicas Humanas e Sociais têm em vista prever e impedir as catástrofes naturais e as criadas pelo homem. Elas trazem uma gama de experiências em políticas sociais, sociologia das catástrofes, relações internacionais, economia e previsão. Isto tem grandes aplicações em duas grandes prioridades actuais: A defesa e o ambiente.

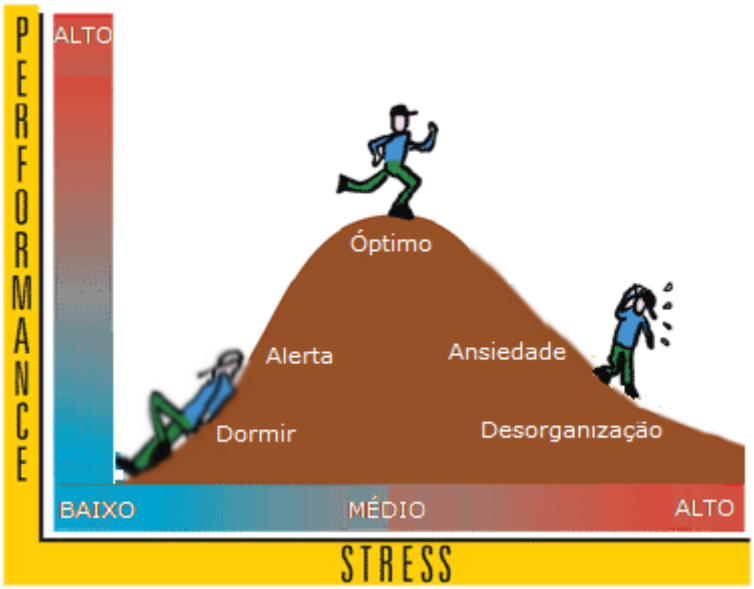
As Dinâmicas Humanas e Sociais (MAI, OWL e KERSTING, 2005) têm a ver com as actividades com vista ao manter da estrutura social e representam os grupos sociais e a forma como estes estão organizados, e que incluem a dimensão, faixa etária e o número de

indivíduos de cada sexo. Tem-se então de estudar os seres humanos a partir das suas adaptações biológicas. Os indivíduos de uma determinada população interagem entre si e também com os indivíduos de outras populações que habitem na mesma área em simultâneo, pertencendo à mesma comunidade.

Claude Bernard (1870), no seu estudo sobre a Biologia do Stress, afirmou que a constância do ambiente interno é a condição para que a vida possa ser livre e independente. Tão distante dos animais de graus mais elevados estarem indiferentes para o mundo externo, estão pelo contrário num relacionamento preciso e informado com ele, de tal forma que um equilíbrio o mais sensitivo possível resulta de uma compensação contínua e delicada.

Em palavras simples, isto significa que os animais possuem sistemas de controlo que ajustam as suas interacções e intercâmbio com o meio-ambiente, de tal forma que o estado físico e composição química do ambiente interno permanecem essencialmente constantes e inalterados pois cada célula num dado organismo concentra-se em actividades metabólicas básicas que levam à sobrevivência delas e do organismo em questão, mantendo um ambiente interno estável.

De acordo com (MOORE, 2008), Professor do Departamento de Ciências Biológicas da University of Southern Mississippi, os termos *stress* e tensão foram criados em 1822 pelo matemático Augustin Cauchy que descreveu o *stress* mecânico como sendo a força exercida por unidade de área num corpo sólido podendo resultar na deformação do mesmo. A tensão é elástica quando é baixa e nesse caso é reversível. Quando o limite da elasticidade é atingido, a deformação torna-se irreversível. Se se continuar a exercer pressão sobre o corpo sólido, chega-se ao limite e ele quebra sendo impossível reverter os danos. Mais tarde apareceram outros tipos de *stress*: fisiológico, psicológico, social e ecológico para lidar com os seres vivos (humanos e animais).



Fonte: The University of Southern Mississippi (Biology of Stress)

Figura 2 – Relação entre o Stress e a Performance

A figura acima mostra-nos a relação existente entre o *stress* e a performance, sendo o ponto mais alto da performance conseguido quando se tem um nível de *stress* médio. Quando o *stress* alcança um nível alto, os indivíduos começam a sentir uma enorme ansiedade, seguida de uma desorganização e perdem a estabilidade emocional.

O *stress* é importante pois afecta o comportamento racional e cognitivo dos seres vivos (humanos e animais), o que irá influenciar a forma como eles irão responder a estímulos externos e lidar com os mais variados problemas. Pode-se então dizer que o *stress* afecta o sistema de crenças.

A reacção ao *stress* por parte dos seres vivos poderá nem sempre ser negativa, dependendo das circunstâncias em que ocorre. Existe aquilo a que denominamos de *stress* positivo sempre que este nos proteja em alturas de perigo ou quando nos ajuda a adaptar em alturas de mudança. Isto torna o *stress* inevitável e necessário para a sobrevivência de todos os seres vivos.

A quantidade de Informação (**H**) gerada por um evento com uma probabilidade **p** de acontecer:

A multiplicação das probabilidades:

$$\mathbf{p = p_1 \times p_2}$$

A Informação adiciona:

$$\mathbf{H\ (p = p_1 \times p_2) = H\ (p_1) + H\ (p_2)}$$

$$\mathbf{H = \ln 1/p = \ln 1 - \ln p = 0 - \ln p = - \ln p}$$ pois o **ln 1** é igual a zero.

A quantidade de Informação (**H**) após **m** eventos com uma probabilidade **p**:

$$\mathbf{H = - m \ln p}$$

Se o número máximo de tais eventos for **n**:

$$\mathbf{p = m / n}$$

$\mathbf{H_{norm} = - p \ln p}$;Representa a Informação Normalizada.

$\mathbf{H_{max} \Rightarrow p = 1 / e}$;Representa o Máximo obtido pela Informação Normalizada.

O Logaritmo Natural (ln) é uma função oposta à exponencial que, neste caso, permite somar à quantidade de Informação a multiplicação das probabilidades.

II.5.1. O Comportamento Emergente

O comportamento emergente ocorre como uma forma de adaptação às alterações ao meio-ambiente e é difícil de prever devido ao elevado número de trocas e diferenças existentes. Isto porque os sistemas complexos comportam-se de formas inesperadas e difíceis de prever através do comportamento dos elementos envolvidos.

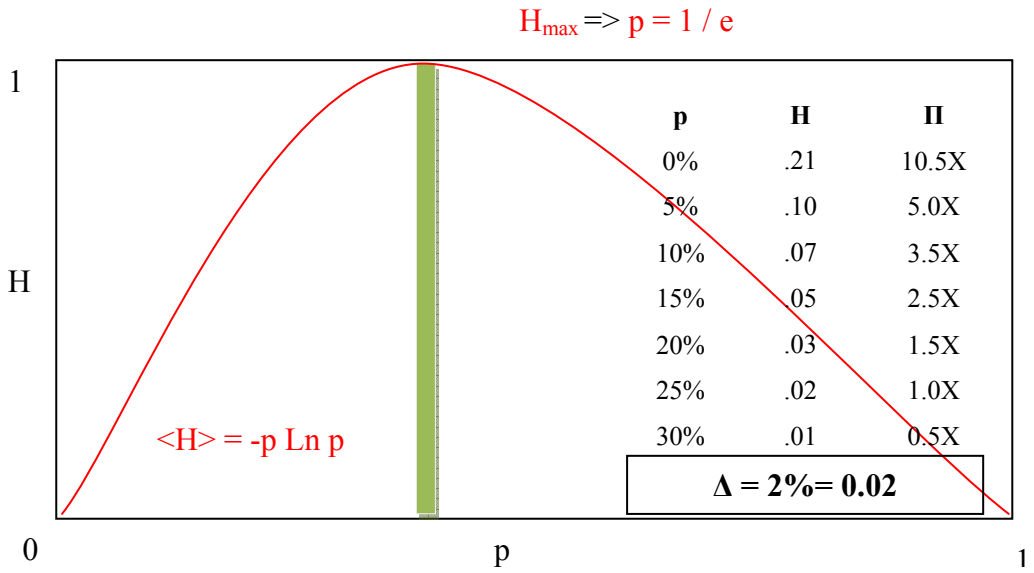
A emergência (QUADE, 2007) é o processo de formação complexa de padrões e surge através do trabalho trazido por Hartmann (1967). Decorre ao longo do tempo e é dinâmico e escalável, dependendo de ciclos de *feedback* e de relacionamentos impossíveis de controlar e prever.

O comportamento emergente tem então também influência no sistema de crenças de cada um, uma vez mais influenciando a forma como cada individuo vê e dá resposta às mais variadas situações com que se depara. Pode-se então dizer que o comportamento emergente também afecta o sistema de crenças.

De acordo com (FOGG, 2010), investigador na Stanford University, o *Fogg Behaviour Model* considera que o que causa a alteração no comportamento humano são três elementos que devem convergir ao mesmo tempo:

- **Motivação:** Aqui temos três motivadores base que se aplicam a toda a gente por serem centrais para a experiência humana: o Sentimento, a Antecipação e a Coesão Social. Cada um desses motivadores tem dois opostos: prazer/dor, esperança/medo, aceitação social/rejeição.
- **Capacidade:** Para ser possível realizar um comportamento-alvo[4] é necessário ser-se capaz disso. Tal pode ser conseguido ao treinar os indivíduos, dando-lhes mais habilidades/competências sendo a forma mais difícil de o conseguir pois as pessoas resistem a aprender coisas novas. Então, a forma mais fácil de o conseguir é tornar o comportamento-alvo mais fácil de alcançar chamando-lhe simplicidade. A capacidade envolve: tempo, dinheiro, esforço físico, ciclos cerebrais, desvio social e a não rotina.
- ***Trigger* (despoletador):** O terceiro elemento é o *trigger* pois, sem ele, o comportamento-alvo não ocorre. Por vezes o *trigger* pode ser externo tal como o som de um alarme, outras vezes poderá vir das rotinas diárias tal como o caminhar através da cozinha poderá fazer-nos abrir o frigorífico. Existem três tipos de *trigger*: Facilitador (motivação alta e fraca capacidade), Sinal (capacidade alta e motivação alta) e Faísca (capacidade alta e motivação baixa). O *trigger* para um comportamento simples pode levar os indivíduos a comportamentos mais complexos, veja-se por exemplo: se usarmos um *trigger* para fazer uma pessoa caminhar dez minutos por dia, essa pessoa pode comprar uns ténis sem nenhum *trigger* externo nem intervenção. Essa pessoa compra os ténis sem se dar conta que está a ser persuadida, pois surge de uma cadeia natural de eventos.

[4] O comportamento-alvo é o tipo de comportamento que se procura fazer acontecer (induzir) nos indivíduos.



Fonte: Prof. Carvalho Rodrigues (2011)

Figura 3 – Comportamento Emergente

A curva que se observa na figura pode ser explicada, por exemplo, como o ciclo de vida de uma pessoa. Desde que a pessoa nasce, a quantidade de Informação da mesma vai aumentando até alcançar o ponto máximo (H_{max}) que representa a morte da pessoa. Depois a curva começa a descer pois os dados começam a dispersar-se e a ficar cada vez mais confusos o que faz com que a quantidade de Informação diminua até desaparecer por completo.

Em relação aos números na Figura no lado direito, estes demonstram as diferenças entre a quantidade de Informação nossa e do adversário caso exista uma variação de 2% (0,02) a mais por parte do adversário. Por exemplo: Se tivermos uma probabilidade de algo acontecer de 10% (0,10) e o adversário tiver mais 2% (0,02), a probabilidade dele será 12% (0,12) e a quantidade de Informação dele será superior em apenas 7% (0,07) o que corresponde a uma diferença de 3.5X. Conforme a a nossa probabilidade vai aumentando, para variações do adversário de 2% (0,02), as diferenças vão diminuindo cada vez mais.

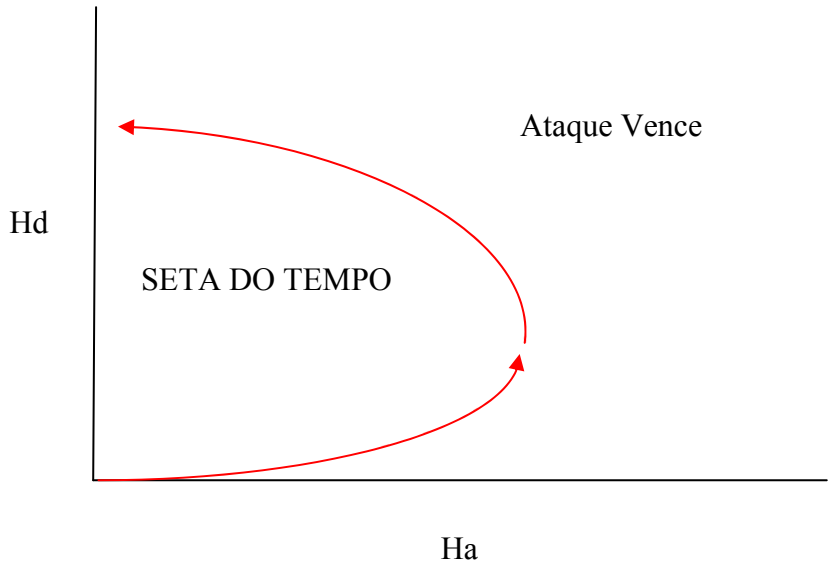
A resiliência (CASAGRANDE, 2004) é a capacidade para nos reorganizarmos após perturbações. Por quê alguns sistemas humanos falham ao tentar dar resposta a alterações no meio-ambiente? Por quê alguns ecossistemas humanos não são resilientes? Isto é devido ao facto de ser racional para a estrutura e irracional para o indivíduo, ou seja, o indivíduo

tem maior dificuldade em lidar com coisas complexas enquanto o mesmo não acontece com a estrutura. O *feedback* de Informação crítica não é a motivação primária pois existe uma proliferação de inconsistências lógicas. Como podem tais sistemas humanos complexos lidar com as alterações no meio-ambiente?

Contradições lógicas em modelos individuais podem causar dissonâncias cognitivas extremas e facilmente manipuláveis, como é o caso de se empregar os conceitos do "Bem" e do "Mal", e que podem levar a uma:

- Alteração no comportamento;
- Direccionar a atenção para assuntos socialmente relevantes;
- Abstrair-se de tudo afirmando que foi assim que Deus fez as coisas;
- A manipulação simbólica reduz a dissonância cognitiva e social.

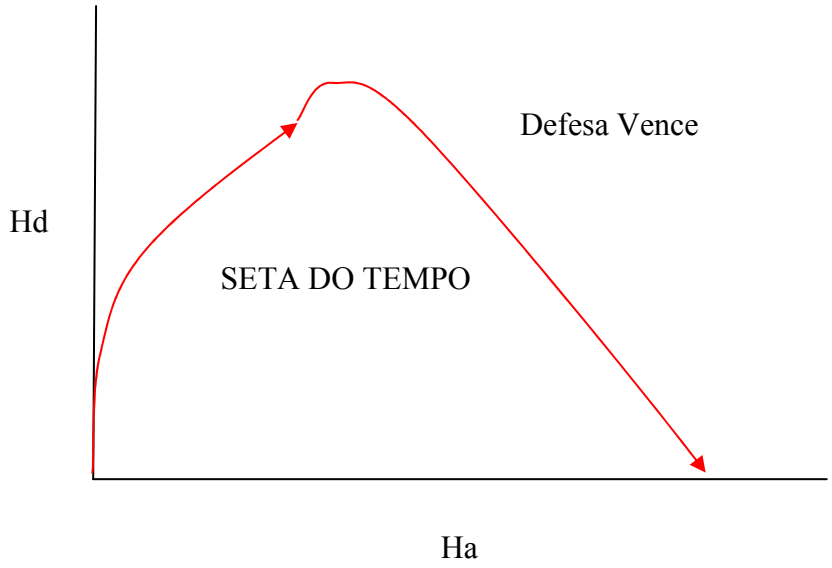
O factor chave para a resiliência está na simplicidade dos dados e, a coesão de uma estrutura (Informação orgânica), reside nas interacções entre os seus elementos com o maior grau possível de simplicidade de dados que origina uma enorme quantidade de Informação útil.



Fonte: Prof. Carvalho Rodrigues (2011)

Figura 4 – Ataque Vence

Nesta figura podemos observar que quando a Informação do Ataque é muito elevada, a Informação da Defesa é muito baixa estando a Defesa em vantagem. Mas, depois assiste-se ao longo do tempo a conseguir o efeito contrário, em que a Defesa fica com uma Informação muito elevada e caótica, perdendo a ofensiva. Neste caso vence o Ataque pois passa a ter uma Informação próxima do zero o que representa uma simplicidade de dados e, por isso, uma vantagem pois consegue uma maior quantidade de Informação útil.



Fonte: Prof. Carvalho Rodrigues (2011)

Figura 5 – Defesa Vence

Nesta figura podemos observar que quando a Informação da Defesa é muito elevada, a Informação do Ataque é muito baixa estando o ataque em vantagem. Mas, depois assiste-se ao longo do tempo a conseguir o efeito contrário, em que o Ataque fica com uma Informação muito elevada e caótica, perdendo a ofensiva. Neste caso vence a Defesa pois passa a ter uma Informação próxima do zero o que representa uma simplicidade de dados e, por isso, uma vantagem pois consegue uma maior quantidade de Informação útil.

II.5.2. Métrica da Relatividade da Informação

O interior dos seres vivos é uma Ilha de Resiliência desde que haja uma simplicidade de dados e esta Ilha mantém-se ao ter uma H_i (Informação Interna) o mais baixa, o mais simples e o mais rica possível.

Componentes da Métrica da Informação:

- **c –** Medida pelo Sistema de Crenças
- **H_0 –** Informação Externa
- **H_i –** Informação Interna
- **V –** Objectivos
- **W –** Capacidade Interna para a mudança (adaptação)

Métrica da Soma dos Quadrados:

Esta métrica (MORRIS, 1997) representa a relação matemática existente entre os três lados de qualquer triângulo-rectângulo, onde é-nos dito que a soma dos quadrados dos catetos é igual ao quadrado da hipotenusa.

$dG^2 = dx^2 + dy^2 + dz^2$ **(Pitágoras)**

Métrica do Espaço-Tempo:

Na relatividade geral (CRAWFORD, 1999) o espaço-tempo é geralmente curvo, adquirindo um carácter dinâmico que permite descrever o comportamento das partículas físicas e da luz na presença de uma dada distribuição de matéria. Daí resulta que a estrutura de cones de luz varia de ponto para ponto e a curvatura do espaço-tempo desempenha um carácter dinâmico de interacção com a matéria.

$dG^2 = cdt^2 - dx^2 - dy^2 - dz^2$ **(Einstein)**

Métrica da Informação:

Nesta métrica (CRUTCHFIELD, 1990) a quantidade de Informação pode ser interpretada como a Informação total independente e as respectivas computações numéricas das distâncias da Informação. É indicado que as origens do espaço da Informação têm uma

certa estrutura topológica, conseguindo-se desenvolver as origens da Informação: "próxima", da continuidade das funções e dos limites, e da convergência de sequências.

$dG^2 = cdH_0^2 - dV^2 - dW^2 - dH_i^2$ **(Jumarie)**

Ilha da Resiliência	C dH_0 (Exterior)	dV (Objectivos)	dW (Adaptação)	dH_i (Interior)
Destruída	> 0	= 0	= 0	> 0
Mantém-se	> 0	> 0	= 0	= 0
Mantém-se	> 0	= 0	> 0	= 0
Melhora	> 0	> 0	> 0	< 0

Fonte: Prof. Carvalho Rodrigues

Tabela 2 – Estado da Ilha de Resiliência

$dG^2 = c\ dH_0^2 - dV^2 - dW^2 - dH_i^2$

O parâmetro **c** pode ser igual a um, representando tecnologia, ou ser maior do que um, representando os seres de carbono. Segundo o General Von Moltke e com algum desenvolvimento do assunto baseado no sítio electrónico do Millennium Project (2007):

C = 1 representa Tecnologia (seres de silicone)

Os seres de silicone são aqueles que sobreviverão durante muitas gerações por serem artificiais, poderão até ter a vida eterna ao transferir os dados e Informação que possuem para outros seres de silicone. Eles evoluíram tanto quanto os seres de carbono e cada e qualquer acréscimo às comunicações é considerado uma vantagem. Quer isto dizer que os seres de silicone conseguem processar dados e Informação de uma forma cada vez mais rápida e precisa.

Os seres de silicone estão em constante evolução e, embora actualmente muitos considerem que estes são nossos escravos, a verdade é que com um cada vez maior desenvolvimento da inteligência artificial e dos computadores, é bem possível e provável que chegue o dia em que estes seres de silicone serão os nossos mestres, pois será cada vez mais difícil distinguir entre computadores e seres humanos relativamente à racionalidade.

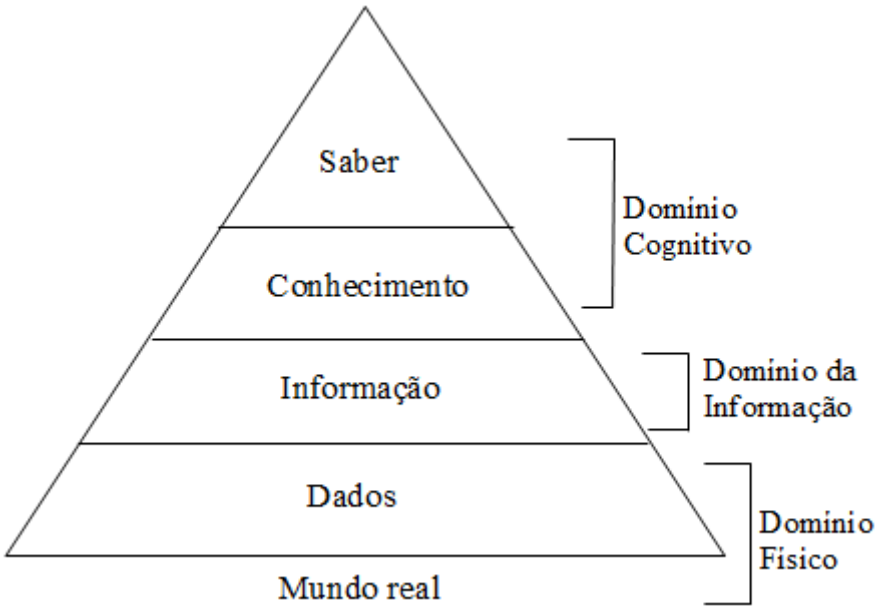
C > 1 representa Inteligência (seres de carbono)

Os seres de carbono são todos nós, os seres de carne e osso. Devido a essa limitação, temos os dias contados pois o período de vida dos seres vivos não é muito extenso actualmente.

Neste caso as oportunidades são ocultadas e são divulgadas desgraças. Um bom exemplo deste tipo de comportamento ocorre em relação a efectuar chamadas telefónicas para os amigos. Normalmente tem-se amigos aos quais nunca se telefona mas, se um dia nos encontrarmos doentes, se calhar já agarramos o telefone e ligamos para conversar com os nossos amigos e dizer-lhes que estamos doentes. Em suma, por vezes temos coisas boas para contar mas não as contamos, enquanto em relação a coisas más actuamos de forma diferente.

Em relação aos seres de silicone e aos de carbono, vence quem se conseguir adaptar melhor, quem cooperar mais e também se existir um aumento da complexidade e ao mesmo tempo conseguir manter uma simplicidade da Informação interna.

II.6. A Pirâmide Cognitiva



Fonte: Choo (1998)

Figura 6 – A Pirâmide Cognitiva

A Pirâmide Cognitiva mostra-nos a relação existente entre os três domínios/dimensões existentes (ARMISTEAD, 2007; AMARAL, 2008; LAUDON, 2009):

- **Domínio físico:**

  Representa a interconectividade das tecnologias de Informação e representa tudo aquilo que vemos todos os dias à nossa volta, ou seja: fios, redes, telefones, computadores, etc.

  - **Mundo real:** É o mundo físico (palpável e observável) onde todos nós nos encontramos.
  - **Dados:** São um fluxo fragmentado de eventos ou transacções na dimensão física e que são capturados e que só por si têm pouca utilidade. Só após serem organizados e arranjados é que podem ser usados e compreendidos, tornando-se assim em Informação.

- **Domínio da Informação:**

  Representa os conteúdos transportados pelos sistemas interconectados tais como as emissões de TV, programas da Rádio, bases de dados e chamadas telefónicas.

  - **Informação:** Para transformar os dados em Informação útil, torna-se necessário expandir recursos de forma a organizar os dados em categorias compreensíveis. Basicamente é constituída por dados transformados numa forma que os torna compreensíveis e úteis para quem deles vá fazer uso. Segundo a JP 13-3 (U.S. Department of Defense, 2006) a Informação é um recurso estratégico e vital para a segurança nacional de Estados soberanos e o domínio da Informação é aquele onde humanos e sistemas automatizados observam, orientam, decidem e agem de acordo com a Informação adquirida. O objectivo é conseguir uma superioridade da Informação, explorando ou negando a capacidade de resposta dos criminosos e evitar que estes façam o mesmo.

- **Domínio cognitivo:**

  Este é o domínio mais importante pois é neste que o conteúdo produzido pela conectividade causa impacto nos seres humanos e na forma como pensamos, decidimos e agimos.

  - **Conhecimento:** Para transformar Informação em Conhecimento, torna-se necessário recorrer a recursos adicionais para encontrar padrões, regras e contextos onde o Conhecimento resida. É um evento cognitivo e psicológico

que toma lugar na mente dos indivíduos e que é também armazenado em bibliotecas e registos. Temos o **conhecimento tácito** que é mais difícil de conseguir visto ser adquirido pela experiência e partilhado entre os indivíduos, e o **conhecimento explícito** que é aquele adquirido recorrendo a livros e afins, ou seja, adquirido teoricamente e que por isso está mais ao alcance de todos.

- **Saber:** Tem a ver com a capacidade colectiva e individual em empregar o conhecimento onde, quando e como para a resolução de problemas. Está no topo da Pirâmide Cognitiva.

Capítulo III

Terrorismo e Ciberterrorismo

No terceiro capítulo define-se terrorismo e Ciberterrorismo, citando-se algumas pessoas e entidades importantes. Fala-se dos motivos estratégicos e psicológicos por parte dos criminosos. Fala-se das tipologias do Ciberterrorismo e as respectivas dimensões. Depois fala-se dos suportes e ataques explicando a diferença existente entre ambos os termos e apresentando uma figura e explicação. Fala-se dos níveis do Ciberterrorismo descrevendo os quatro níveis de ameaça: baixa, moderada, significativa e elevada e uma análise de seis elementos e na sua análise discernir as capacidades variantes de adversários potenciais. Depois temos a figura do Espectro das ameaças e a respectiva explicação. No final apresentam-se alguns actos cometidos de Ciberterrorismo.

De seguida vão-se explanar alguns conceitos básicos sobre o tema em análise.

III.1. Terrorismo Tradicional

Segundo a Enciclopédia Verbo Fundamental (1982, p. 1505): "Terrorismo é um dos recursos da guerra subversiva ou guerrilha. Visa criar um ambiente generalizado de medo e insegurança, destruindo a capacidade de resistência moral das populações que acabam por sucumbir perante o desalento e a impotência. Pode ser selectivo ou sistemático, e regra geral o 1º antecede o 2º: este, persistindo, acaba por isolar o povo das forças armadas, e posteriormente são os terroristas que passam a proteger a população, recebendo dela em troca o apoio que necessitam".

É possível constatar que existem várias definições de terrorismo consoante as entidades e as organizações. Temos pois diferentes definições académicas, do Departamento de Estado dos EUA, do DoD, do FBI, da NATO, entre outras. De seguida apresentam-se três definições de diferentes entidades:

Departamento de Estado dos EUA:

Segundo eles, o termo "Terrorismo" é a violência premeditada e politicamente motivada, perpetuada contra alvos civis ou militares não armados, perpetuada por grupos sub-nacionais ou agentes clandestinos, normalmente com o objectivo de influenciar o público. O terrorismo internacional ameaça os EUA, os seus aliados e a comunidade mundial.

Esta definição na teoria não inclui os actos contra propriedades, mas, na prática, tais actos estão incluídos pois os terroristas causaram muitos danos em propriedades importantes (interesses) para os EUA, como foi o caso (U.S. Department of State, 1998) dos *pipelines* multinacionais na Colômbia em 1998. A ameaça de ataques terroristas ao pessoal, instalações e interesses dos EUA além-mar torna-se cada vez maior com o passar do tempo.

O Departamento de Estado detém uma autoridade estatutária global para treinar e equipar as forças no estrangeiro.

Departamento de Defesa (DoD):

O Departamento de Defesa dos EUA define o terrorismo como o uso calculado da violência ou a ameaça da violência para inculcar o medo, destinado a coagir ou tentar intimidar os governos ou as sociedades na busca de objectivos que são de forma geral políticos, religiosos ou ideológicos. Esta definição abrange a definição usada pelo Departamento de Estado e tem o objectivo de diferenciar o terrorismo de outros tipos de violência.

O DoD usa o termo "antiterrorismo" como sendo as medidas defensivas, incluindo a protecção pela força com vista a reduzir a vulnerabilidade dos indivíduos e propriedades a actos terroristas. Usa também o termo "contra terrorismo" para definir as medidas ofensivas para impedir, dissuadir e dar resposta ao terrorismo.

O DoD é a entidade líder dos EUA para operações militares contra organizações terroristas e contra os Estados que as apoiam. Se o Presidente dos EUA assim o quiser, é possível ao DoD fazer uso de forças militares para disruptir e destruir organizações terroristas e os seus protectores. Cabe também ao DoD proteger as suas forças dos terroristas em todo o mundo.

O DoD treina e equipa os governos estrangeiros de forma a melhorar as capacidades deles no combate ao terrorismo. Há que ter em conta que os EUA são muito importantes mas não são os donos da verdade.

NATO:

A concepção estratégica da Aliança (NATO, 2011) identificou em 1999 o terrorismo como sendo um dos riscos que afectariam a segurança da NATO. Visto o flagelo do terrorismo provir de várias zonas do globo, sem conhecer fronteiras, nacionalidades ou religiões, é um desafio que deve ser enfrentado pela comunidade internacional em conjunto, e a NATO é uma organização que muito pode fazer.

A luta contra o terrorismo é uma prioridade na agenda da NATO pois na Cimeira de Riga em 2006 foi declarado que o terrorismo e o Ciberterrorismo serão as principais ameaças para a aliança nos próximos 10 a 15 anos. A NATO quer ajudar no combate ao terrorismo para que os cidadãos possam prosseguir com as suas vidas diárias de forma segura e livres de quaisquer actos de terror. Embora actualmente os ataques sejam normalmente feitos com armas convencionais e explosivos, existe cada vez mais o perigo do uso de armas de destruição maciça.

A NATO encarregou-se de tomar uma diversidade de iniciativas contra o terrorismo: políticas, operacionais, conceptuais, militares, tecnológicas, científicas e económicas. Segundo a NATO, o extremismo religioso é quem cria mais ameaças terroristas à Aliança, embora não se deva esquecer os factores económicos, sociais, demográficos e políticos derivados de conflitos por resolver ou de ideologias emergentes. Apesar do patrocínio do terrorismo por parte dos Estados estar em declínio, é possível que circunstâncias políticas possam inverter isso, dando aos criminosos guarida e recursos consideráveis.

A definição genérica aceite por todos é que o terrorismo é normalmente descrito como sendo uma violência política motivada para causar coerção num governo ou numa população civil. Para fazer face ao terrorismo torna-se necessário actividades de segurança interna e um combate além-mar.

Temos por isso dois tipos de terrorismo, o "doméstico" e o internacional que dependem da origem dos grupos terroristas, de onde eles lançam os seus ataques, e quem são as vitimas. O terrorismo doméstico é o uso ilegal ou ameaçador da força por um grupo de indivíduos residentes ou a operar dentro de um estado sem direcção estrangeira. Um bom exemplo de terrorismo doméstico nos EUA foi a explosão do Edifício Federal Alfred P. Murrah em Oklahoma em 1995. O terrorismo internacional envolve cidadãos ou territórios de um ou mais países e podem transcender as fronteiras nacionais dos Estados soberanos como foi o caso dos ataques 9/11.

III.2. Ciberterrorismo

O Ciberterrorismo (NELSON et al., 1999) é a destruição ou disrupção ilícita de propriedade digital para intimidar ou coagir governos ou sociedades na busca de objectivos que sejam políticos, religiosos ou ideológicos. O Ciberterrorismo é um subnível de terrorismo e utiliza a Informação como arma, método ou alvo. Ele existe dentro e fora do ciberespaço e inclui a destruição física, disrupção, negação de serviço de equipamentos ou sistemas que usem código binário. A sua grande particularidade é a capacidade de usar meios baratos que são desproporcionais aos danos causados. O Ciberterrorismo pode aumentar ou dar apoio em muito ao terrorismo tradicional, podendo também ser empregue de forma distinta.

Segundo Mark M. Pollitt (Computer Crime Research Center, 2002), do Laboratório do FBI: Ciberterrorismo é "O ataque premeditado, politicamente motivado contra a Informação, sistemas informáticos, programas de computador e dados, que resulta numa violência contra alvos não combatentes por grupos sub-nacionais ou agentes clandestinos."

Segundo Serge Krasavin (Computer Crime Research Center, 2004), investigador da Universidade de Illinois: Ciberterrorismo é "O uso de tecnologia e meios de Informação por grupos terroristas e agentes."

Segundo Larisa Paul (Indiana University of Pennsylvania, 2001), do SANS Institute, a maior fonte para o treino em segurança da Informação no mundo: Ciberterrorismo são "Técnicas de *hacking* politicamente motivadas e usadas num esforço para causar danos

graves, incluídos mas não limitados à perda de vidas humanas ou prejuízos económicos sérios."

Segundo o FBI (Computer Crime Research Center, 2004): o Ciberterrorismo é "Um ataque premeditado e politicamente motivado contra a Informação, sistemas informáticos e dados que resultam em violência por parte de grupos domésticos ou agentes clandestinos contra alvos civis e não só". Temos pois terroristas domésticos e internacionais. Esta definição é bastante semelhante à do Departamento de Estado dos EUA mas inclui Informação, sistemas informáticos e dados. Os terroristas domésticos são aqueles que actuam dentro do país dos alvos e os terroristas internacionais são aqueles além-fronteiras.

Desde que o mundo se uniu através de uma superauto-estrada da Informação, existem grupos que procuram tirar vantagem da falta de segurança neste meio para conseguir dinheiro, quebrar (*crash*) os sistemas, brincar ou tentar a sorte em coisas que julguem ser possível fazer. No passado essas pessoas eram conhecidas como os *hackers* tradicionais, mas com o decorrer dos anos tornou-se um *hobby*, havendo até filmes sobre o assunto. Não se pode contudo esquecer que os crimes informáticos são crimes. De salientar que nos EUA o *Computer Fraud and Abuse Act*[5] de 1986 foi melhorado várias vezes para fazer face à nova tecnologia e ameaças e, em 2001, foi alterado pela *US Patriotic Act Legislation* e em 2008 pelo *Identity Theft Enforcement and Restitution Act*.

Não existe uma definição normalizada (*standard*) de Ciberterrorismo e de ciberterroristas que agrade a todos, pois a diferença entre *hacking* normal e Ciberterrorismo depende apenas da motivação do ataque (político ou pessoal). Ou seja, quando é pessoal ocorre apenas um ataque de *hacking*, mas se houver outras motivações poderá passar a ser considerado um acto ciberterrorista. Independentemente da motivação, ambos podem ser punidos pelo *Computer Fraud and Abuse Act* dos EUA. Na Europa existe uma tentativa de harmonização entre as leis da União Europeia e dos EUA, o que significa que existem muitas semelhanças nas leis aprovadas e em vigor.

[5] O *Computer Fraud and Abuse Act* é uma lei Americana aprovada pelo Congresso dos Estados Unidos em 1986 com o objectivo de diminuir o *hacking* e *cracking* de sistemas informáticos e para lidar com crimes relacionados com sistemas informáticos do governo. Esta lei sofreu várias alterações ao longo dos anos para se adequar à realidade do momento.

III.2.1. Os motivos estratégicos e psicológicos

Segundo (WILSON, 2005) é bem provável o cada vez maior aumento do Terrorismo e Ciberterrorismo terem a ver com as agendas políticas e as visões estratégicas dos seus líderes[6] e os motivos psicológicos dos respectivos seguidores. Normalmente os bombistas suicidas são indivíduos psicologicamente perturbados (SKEFFINGTON, 2009) e quem está no topo a liderar são indivíduos dementes, pois no seu juízo perfeito ninguém faria ou dirigiria tais actos. Isto pode parecer lógico, mas todos eles são fanáticos extremistas e existe uma lógica e um método neles.

Os Ciberterroristas são normalmente jovens do sexo masculino, alguns com habilitações académicas elevadas (Mestrados ou Doutoramentos), que têm a consciência de estar a violar a lei desrespeitando as normas sociais, a ordem e os sistemas de controlo social. Eles diferem dos criminosos comuns em pelo menos quatro características fundamentais: (1) Efectuam crimes de forma mais violenta; (2) Têm como meta infligir medo numa população alvo enorme; (3) Servem uma agenda social enorme tentando recrutar mais elementos para a causa deles; (4) Tentam conseguir uma exposição máxima aos media.

A natureza do Ciberterrorismo pode ter em vista: (1) Destabilizar Estados soberanos para alcançar uma maior força de influência numa certa região; (2) Causar uma visibilidade internacional para problemas persistentes como é o caso da Palestina, de forma a conseguir maior afecto; (3) Retaliar contra Estados soberanos em certas regiões que são encarados como sendo inimigos; (4) Minar a influência de forças mais poderosas que estejam a operar na região.

Segundo (IGNATIEFF, 2004), a guerra ao terror requer uma nova ética urgente que passa pela cessação de muitos direitos humanos aceites universalmente, passando a defender a existência de medidas radicais contra o terrorismo. Embora isto não seja a situação ideal, as medidas radicais contra o terrorismo são menos más tendo a ver com a própria sobrevivência das nações com democracias liberais. Ignatieff defende que os direitos

[6] Osama Bin Laden em 1998 declarou guerra contra os EUA pedindo o apoio de todos os Islâmicos no mundo.

humanos eram mais importantes nos anos 1990s do que após o 9/11 e que devem agora dar lugar a outros para assegurar os sistemas políticos democráticos liberais.

O Ciberterrorismo manifesta-se de várias formas, existindo vários tipos: (1) Politicamente motivado ou não; (2) Sancionado estatalmente ou não; (3) Afiliado a grandes organizações; (4) Praticado individualmente ou em grupo. Não esquecer que a participação de uma pessoa em actos terroristas pode não se aplicar a outra pessoa, ou seja, existem pessoas mais propícias a serem terroristas do que outras, dependendo de diversos factores, tais como a educação dos indivíduos desde a infância.

As explicações para o terrorismo não dão legitimidade aos terroristas para matar inocentes, nem justifica o comportamento deles face às vítimas, nem as culpa. O terrorismo é racional e tem a ver com as fraquezas dos criminosos e as nossas limitações, tornando-se por isso necessário compreender o flagelo do terrorismo e as vítimas, para saber qual a resposta mais adequada a dar. Tal compreensão poderá ajudar a prevenir acções que são o produto da nossa ignorância e prevenir melhor actos continuados de terrorismo.

A Declaração Universal dos direitos do homem (United Nations, 1998) é o alicerce da justiça no mundo o que levanta a questão das obrigações das sociedades para com os estrangeiros. Há mesmo quem defenda (RANDOLPH, 2010), como foi o caso de Osama Bin Laden, que o 9/11 foi um acto de protesto contra a injustiça global com o fundamento que os terroristas são agentes da justiça, desculpabilizando os seus crimes e culpabilizando as suas vítimas. A teoria que a pobreza e a opressão geram o terrorismo não é de todo verdade pois os terroristas do 9/11 não eram nem pobres, nem oprimidos, nem trazedores da justiça, embora exista pobreza e uma política autoritária nos países muçulmanos.

Os EUA têm uma grande responsabilidade em ajudar todas as nações em sofrimento e possíveis alterações na política externa poderiam reduzir em parte a atracção do Islamismo radical, mas não conseguiria pôr-lhe termo por completo. É defendido pelo mundo desenvolvido que o Ocidente nada tem a ver com tal situação, ainda mais porque têm ajudado os países a desenvolverem-se.

Estes argumentos lançam a confusão entre a explicação e a justificação dos actos terroristas pois é uma questão empírica se a política externa dos EUA é uma causa do terrorismo. A verdade é que se se quiser combater o terrorismo de forma eficaz, torna-se necessário investigar e compreender as suas causas, existindo duas razões independentes para considerar as relações entre a injustiça global e o terrorismo (Fukuyama, 2002):

1. Existe uma obrigação moral das nações desenvolvidas para rectificar a injustiça sempre que possível com um custo razoável, pois as nações Ocidentais, nomeadamente os EUA, têm muitos recursos financeiros e podem usar parte do seu capital em orçamentos apenas com o fim de ajudar os países em desenvolvimento. Deve-se lembrar que a ONU representa um papel muito importante neste sentido;
2. A injustiça normalmente está relacionada com o Ciberterrorismo. Veja-se que é defendido que a política Ocidental em relação ao Médio Oriente tem sido injusta e daí ter contribuído para o terrorismo. O facto de os EUA terem como aliado Israel gera muita perturbação no mundo Árabe visto estes odiarem os Judeus e a Terra Santa é um dos motivos de querelas entre Muçulmanos e Judeus.

Embora não exista consenso sobre as obrigações da justiça global, todos partilhamos uma humanidade em comum e existe uma interdependência complexa na estrutura social global, onde os ricos e os mais poderosos têm maior benefícios nesta estrutura do que os pobres, os fracos e os oprimidos. Todos têm o dever moral de não causar danos uns aos outros e isto é defendido pelos princípios da ONU e pela lei internacional dos direitos humanos.

Se houver falhas no cumprimento das obrigações da justiça global, ter-se-á uma responsabilidade moral pelas consequências injustas que daí possam advir, não esquecendo que o imperialismo Ocidental tem sido injusto e criando injustiças que até hoje prevalecem no mundo, como é o caso de governos maus para os povos e injustiças económicas, políticas e militares. O mundo Ocidental foi cúmplice na exploração dos pobres a nível global e também ajudou a financiar os governos tiranos corruptos que exploram e abusam dos habitantes dos seus países que nada podem fazer para alterar a situação em que vivem.

Os terroristas têm vários objectivos em mente como é o facto de punir os seus inimigos causando-lhes medo, publicitar a sua causa para dar a conhecer ao mundo a sua existência e as razões por detrás dos actos, causar danos económicos de forma a causar pressão nos

Estados, afirmar a sua dignidade para que os Estados e populações compreendam o porquê dos motivos dos terroristas, mobilizar os seus apoiantes fazendo com que consigam mais membros activos e minar a credibilidade de Estados perante outros Estados.

O grande mal no terrorismo reside no facto de pessoas inocentes serem lesadas sem terem qualquer culpa, tornando o terrorismo errado por definição e não por argumentos. Alguns terroristas chegam mesmo a distinguir (ESPOSITO, 2007) entre alvos "legítimos" e "ilegítimos" mas a maioria atacam ambos para causar maior impacto sobre a opinião pública internacional e conseguir um maior reconhecimento das causas pelas quais actuam. Tentam assim conseguir simpatia pela sua causa por parte de outros grupos de indivíduos em diferentes partes do mundo.

O líder Iraniano Ruhollah Khomeini (1979) afirmou que a América era o grande Satanás. Existem várias individualidades públicas americanas que defendem que o extremismo Islâmico tem bases sólidas e que deve ser combatido impiedosamente afirmando orgulhosamente: "Eles ainda não viram nada". Isto é apenas um exemplo das muitas pessoas do Ocidente que estão contra os Islâmicos e que manifestam o desprezo que sentem das mais diversas formas, recorrendo até à anti religião como tipo de luta. Veja-se o caso de Reverendos Americanos serem filmados a queimar (Diário de Notícias, 2010) em público o Alcorão e a incentivar a população Cristã a fazer o mesmo. Isto vai fazer com que os Islâmicos extremistas fiquem furiosos e sintam uma necessidade em fazer represálias contra os inimigos do seu Deus, pois o livro sagrado diz que se pode e se deve matar os infiéis.

Este tipo de atitudes tem a ver com o tipo de conhecimento mítico ou religioso em que se atribui a divindades ou seres superiores tudo aquilo que seja "mágico" ou inexplicável de forma a conseguir uma maior segurança para os seres humanos. Estes actuam de acordo com a vontade "superior" justificando assim a rectidão das suas acções.

III.2.2 Tipologias do Ciberterrorismo

Segundo (FORST, 2009), dada uma quase infinita variedade de circunstâncias em torno dos eventos terroristas, cada acto relacionado com as definições convencionais de terrorismo é único em vários aspectos, embora existam dimensões que distingam alguns terroristas, grupos terroristas e actos terroristas da maioria dos outros. Então, certos grupos de terroristas e actos individuais encaixam-se nas seguintes dimensões em que a variação de comportamentos nas várias dimensões pode ser maior que numa em particular:

a. Politicamente motivadas:

Os actos de terrorismo costumam ter uma certa agenda política, fazendo com que os Estados ou os cidadãos fiquem num estado de pânico e insegurança que, de outra forma, não seria possível através de meios legítimos. Normalmente, os terroristas alcançam os seus objectivos ao criar medo num alvo chave e assim causar pressão para que os Estados ajam de acordo com o que é desejado pelos criminosos, destabilizando a ordem política, económica ou social.

b. A operar sob a autoridade de um Estado:

O termo "terrorismo" foi rotulado no século XIX para relatar actos cometidos pela República Francesa. Actualmente os Estados soberanos continuam a perpetuar e a patrocinar o terrorismo de forma devastadora, como por exemplo: (1) A chacina de quase dois milhões de cambojanos sob a ditadura de Pol Pot em finais de 1970; (2) O gaseamento de milhares de curdos no Norte do Iraque por Sadam Hussein em 1988; (3) A chacina de milhares de muçulmanos na Bósnia sob a governação de Slobodan Milosevic nos anos 1990.

c. Grau de associação com redes ou outras organizações terroristas superiores:

São os indivíduos e os grupos terroristas que trabalham sob a tutela de redes terroristas maiores, normalmente livremente afiliados, como é o caso da Al Qaeda. No outro extremo os terroristas tendem a agir como membros independentes, como foi o caso do

"Unabomber"[7] de acordo com o sítio electrónico do FBI (2008). O grau de eficácia do grupo é melhorado através da preparação, prática e secretismo como foi o caso do 9/11 e o ataque ao metro em Londres em 2005. Cada grupo é tão forte quanto a competência dos membros mais fracos.

d. Extensão da organização e planeamento:

Os grupos terroristas e indivíduos são operacionais de redes terroristas maiores, tal como os *franchisings* de negócios. Num extremo temos criminosos que actuam sozinhos como lobos solitários e no outro extremo temos grupos mais ligados que têm a vantagem do trabalho em equipa, uma divisão do trabalho e um maior poder em números, mas estão sujeitos a um maior risco de exposição e detecção que é tanto maior quanto maior o número de elementos envolvidos. Quanto mais sofisticado for o ataque planeado, também será necessário um maior número de elementos envolvidos, de forma a alcançar os resultados planeados. O sucesso do ataque dependerá da prática, da preparação e do secretismo.

e. Justificações religiosas ou étnicas:

Este tipo de motivação está normalmente associado a factores genéticos, como a cultura, a religião e a uma herança comum. Isto envolve grupos étnicos ou tribais com rivalidades desde há um longo tempo, normalmente acompanhado de *slogans* contra os outros grupos. Quando um governo mostra o seu apoio a um grupo étnico os outros praticam terrorismo contra o governo, desde o nível local de clãs ou tribos até ao nível de Estado e mais além. Normalmente é defendido que o terrorismo étnico é o resultado de intervenções governamentais contra minorias étnicas.

f. Destino dos alvos são civis ou simbólicos:

Os terroristas podem atacar alvos simbólicos tais como edifícios governamentais, estátuas sagradas como a de Buda no Afeganistão em 2001, ou locais sagrados de oração como é o caso de templos, mesquitas ou igrejas. Isto causará uma ira tremenda por parte das pessoas com afinidade aos alvos destruídos.

[7] Theodore Kaczynski era um génio com uma mente perturbada que aspirava ser o assassino perfeito e anónimo que andou pelos EUA a enviar e a colocar pessoalmente cartas armadilhadas. Foram necessárias quase duas décadas de investigação pelo FBI para capturar este perigoso criminoso.

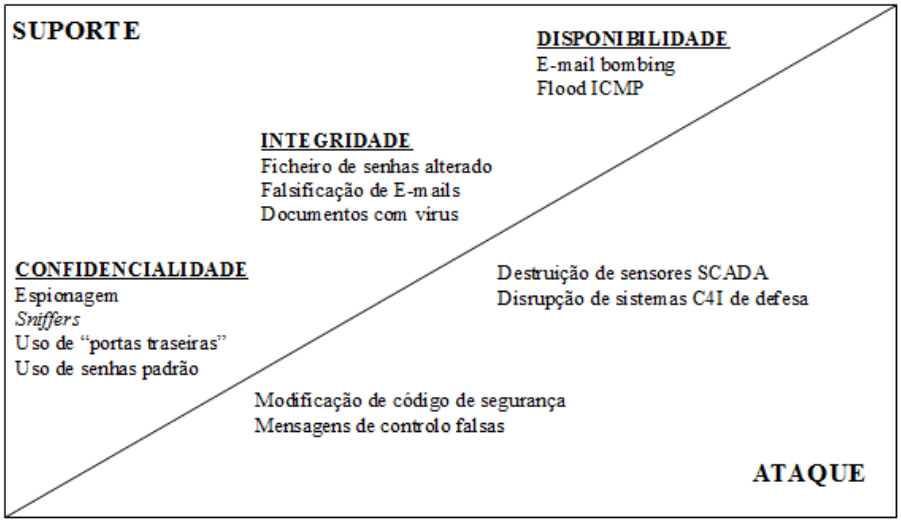
Acção	Definição	Fonte	Exemplo
Uso	Usar a Internet para facilitar a expressão de ideias e comunicação	Utilizadores da Internet	E-mail, mailing lists, newsgroups, Websites
Mau uso	Usar a Internet para disruptir ou comprometer Websites ou infra-estruturas	Hackers, Hacktivistas	Ataques DoS
Uso ofensivo	Usar a Internet para causar danos ou roubo	Crackers	Roubo de dados (ex: detalhes de cartões de crédito)
Ciberterrorismo	Ataques feitos por terroristas via a Internet resultando em violência contra pessoas ou danos económicos severos	Terroristas	Um grupo terrorista a usar a Internet para um grande ataque tal como ao New York Stock Exchange

Fonte: Information Warfare: Separating hype from reality

Tabela 3 – Tipologia dos ciberataques

III.2.3. Ciberterrorismo – Suporte e Ataques

É necessário diferenciar entre o suporte e aos ataques. O suporte/actividade é o uso ilícito de SI por terroristas, sem o objectivo claro de causar efeitos coercivos numa audiência alvo, servindo mais para ampliar o impacto de outros actos terroristas. O Ciberterrorismo pode então ser classificado em actos/ataques ou actividades/suporte visto que para realizar um acto de Ciberterrorismo são necessárias várias actividades que incluem e não estão limitadas à recolha de Informações, comunicações, logística e abastecimento. O resultado final do uso de tecnologias de Informação é o que determina se os incidentes são ataques ou suporte, sendo os ataques uma forma de intimidar ou coagir directamente de acordo com as metas do grupo atacante. Por sua vez, o suporte destina-se a aumentar algum outro acto ou ameaça podendo ser terrorismo tradicional ou Ciberterrorismo.



Fonte: Adaptado de Cyberterror: Prospects and Implications

Figura 7 – Diferenças entre Ataque e Suporte ciberterroristas

Assim, na figura acima (NELSON et al., 1999; BIDGOLI, 2006), podemos distinguir três áreas importantes:

Confidencialidade:

Assegurar a confidencialidade evitando a intercepção da Informação para impedir que a Informação sensível possa cair em mãos erradas e ser utilizada para fins perversos. Deve-se ter protecções contra o acesso não autorizado quando a Informação se encontra em trânsito para haver uma privacidade da Informação, evitando a sua divulgação não intencional que poderia comprometer o sistema. Uma quebra de confidencialidade ocorre sempre que alguém consiga acesso à Informação, sendo um exemplo simples quando se consegue a senha de alguém. Este tipo de violação é normalmente passiva tornando-se somente um acto de Ciberterrorismo quando o resultado da quebra de confidencialidade e acesso à Informação têm como uso os ataques. Deve-se ter mecanismos de detecção de intrusão, cifra de dados e monitorização.

Integridade:

Assegurar a integridade da Informação para que esta chegue ao receptor absolutamente igual à original enviada pelo emissor. Torna-se necessário definir políticas e procedimentos para que a Informação não seja adulterada por pessoal não autorizado. Uma violação da integridade de um SI ocorre sempre que a Informação lá contida é modificada ou destruída.

A modificação da Informação pode ocorrer quando esta reside no SI ou quando está a ser transferida entre sistemas. Este tipo de incidente pode ser mantido secreto permitindo o atacante conseguir acesso a um sistema chave ou pode ser publicitado publicamente de forma a intimidar uma audiência enorme. Este tipo de violação à integridade pode tanto ser caracterizado como ataque ou suporte.

Disponibilidade:

Assegurar a disponibilidade entre o emissor e o receptor para que a comunicação não possa ser afectada por interrupções casuais ou intencionais. A disponibilidade é o mais próximo que temos da recuperação de dados e envolve procedimentos de *backup*, redundância e tudo aquilo que impeça a perda de acesso a dados quando é necessário. As violações de disponibilidade normalmente devem-se a ataques DoS/DDoS podendo também ser caracterizado como ataque ou suporte. Perdas de serviço podem acontecer como consequência como é o caso de servidores de páginas Web ou de correio electrónico irem abaixo e demorar algum tempo até se conseguir que funcionem novamente. Isto fará com que não se consiga acesso à Informação atempadamente o que acarreta riscos tremendos. Como exemplo temos: Um ataque DoS a servidores que impeçam a detecção de acessos físicos a uma embaixada é considerado uma melhoria a um ataque, podendo ser considerado um suporte ciberterrorista. Por sua vez, um ataque DoS a um sistema de controlo de tráfico aéreo, devido às consequências horríveis que poderá trazer como é o caso de perda de vidas humanas, é considerado um ataque.

Todos os actos de Ciberterrorismo envolvem uma violação de confidencialidade, integridade ou disponibilidade. Em palavras simples, actos de criminosos contra Sistemas de Informação (SI) que não tenham fins terroristas não são Ciberterrorismo sendo normalmente feitos por criminosos que tentam conseguir ganhos financeiros ou animosidade pessoal através das suas actividades. Para organizações terroristas e instituições estatais, os actos de Ciberterrorismo têm motivações políticas.

Um exemplo de ataque ciberterrorista (JOYNER e LOTRIONTE, 2001) é fazer despenhar um avião cheio de passageiros usando um dispositivo de pulso electromagnético transportado a bordo por um criminoso, usado para disruptir e corromper os componentes de SI no avião. Se isto afectar o trem de aterragem, o avião não conseguirá aterrar em

segurança, batendo no solo. Neste caso, em vez do uso de uma bomba, usou-se um dispositivo electrónico e observam-se outras condições para ser um acto terrorista, como é o caso da intenção.

Os grupos terroristas usam sistemas informáticos para prosseguirem com os seus objectivos usando *Websites* para o financiamento, o recrutamento e o treino dos seus elementos. Alguns criminosos extremistas chegaram mesmo a roubar dados de cartões de crédito para depois serem usados para financiar as actividades terroristas. Ou seja, os criminosos extremistas e grupos terroristas estão a trabalhar em conjunto criando um novo tipo de ameaça onde poderão conseguir acesso a ferramentas de rede de forma a roubar Informação pessoal, ou causar a disrupção de sistemas informáticos usados no suporte a serviços na Internet.

Existem vários métodos de disrupção (WILSON, 2005) que podem ser efectuados através de ciberataques ou CNA onde código malicioso é usado para afectar o processamento dos computador, roubar dados, ou afectar a confidencialidade das transmissões. Apresenta-se de seguida três métodos de como o fazer:

1. Armas convencionais cinéticas[8] (Universidade do Minho, 2010) podem ser usadas contra equipamento informático, instalações informáticas, ou linhas de transmissão de forma a criar um tipo de ataque físico que cause a disrupção à fiabilidade do equipamento. Este tipo de ataque pode afectar a capacidade de reacção das forças amigas, podendo mesmo chegar a destruí-la na totalidade;
2. O uso de energia electromagnética, como é o caso do pulso electromagnético, pode ser usado como um EA contra equipamento informático ou transmissão de dados. Ao sobreaquecer os circuitos ou causar obstrução está-se a desruptir a fiabilidade do equipamento e a respectiva integridade dos dados ou Informação;
3. Código malicioso ou *exploits*[9] podem ser usados num ciberataque ou CNA, tendo como alvo o processamento de código de computadores, a lógica de instruções, ou

[8] As armas cinéticas são armas não letais, usadas para arremesso de projécteis contra alvos humanos ou veículos, com o objectivo de os incapacitar.

[9] Os *exploits* são vulnerabilidades no *software* ou sistema operativo que podem ser usados pelos criminosos para comprometer o sistema informático. Por exemplo, é possível através dos *exploits* executar código malicioso e danificar os sistemas informáticos ou abrir portas traseiras para os criminosos.

dados. Os *exploits* actuam como fraquezas e são um alvo muito apetecível pelos criminosos. Este tipo de ataque pode causar uma disrupção na fiabilidade do equipamento, na integridade dos dados e na confidencialidade das comunicações.

III.2.4. Níveis de Ciberterrorismo

Segundo a JP 3-07.2 (U.S. Department of Defense, 2006) a avaliação do nível de ameaça terrorista enfrentada pode ter quatro níveis:

- **BAIXA:** Não há indicações da presença de grupos terroristas;
- **MODERADA:** Existe a presença de ameaças, mas não existe uma actividade em curso;
- **SIGNIFICATIVA:** Existe uma presença de ameaça com uma actividade operacional limitada e capaz de realizar ataques;
- **ELEVADA:** Os terroristas estão activos e existe um potencial para ataques com elevado número de baixas.

Estes níveis de ameaça são baseados numa análise contínua de "inteligência" de pelo menos seis elementos:

- **Existência de grupo terrorista:** Se o grupo terrorista está presente, se tem valor suficiente para estar presente, ou a capacidade em conseguir acesso a um dado local;
- **Capacidade:** A capacidade do grupo terrorista em realizar ataques, sendo uma capacidade adquirida, avaliada ou demonstrada;
- **Tendências:** A intenção por parte dos grupos terroristas em prosseguir com as suas actividades, como é o exemplo de actividades recentes demonstradas;
- **História:** As actividades terroristas feitas ao longo dos tempos. Por exemplo: escolhe-se uma organização terrorista e faz-se uma listagem de todos os actos cometidos ao longo da sua existência;
- **Alvos:** A Informação credível conseguida com o objectivo de saber preparações para actos terroristas específicos e que sejam eminentes. Isto torna possível reduzir o grau de severidade por parte dos ataques terroristas;
- **Ambiente de segurança:** Os factores políticos internos e de segurança que têm influência nos terroristas para que estes consigam prosseguir com as suas operações.

São três os níveis/tipos distintos de capacidade de ameaça de adversários potenciais, que ajudam a quantificar as diferentes habilidades e recursos necessários para uma capacidade proposta. Os níveis/tipos definidos em termos de alcance do alvo, análise do alvo, grau de controlo sobre os efeitos desejados e metodologia de selecção dos alvos são:

Simples-Não estruturado:

A capacidade para efectuar ataques de *hacking* básicos contra sistemas individuais através do uso de ferramentas criadas por outros. A organização detém pouca análise de alvos, C2 ou capacidade de aprendizagem. Este é o modo de ataque mais utilizado na Internet pois os criminosos vão a sítios electrónicos onde existem ferramentas já construídas, transferem-nas para os seus computadores, instalam-nas e são depois usadas para fazer os ataques, sem ser necessário grandes conhecimentos do funcionamento interno de tais ferramentas. Em palavras simples, são os indivíduos ou grupos que trabalham com reduzida estrutura, premeditação ou preparação.

Avançado-Estruturado:

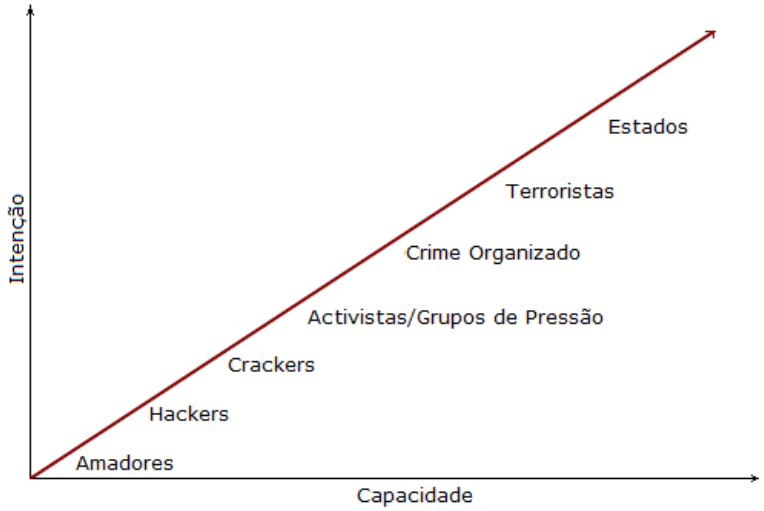
A capacidade para efectuar ataques de forma mais sofisticada tendo como alvo sistemas ou redes múltiplos e a capacidade em criar ferramentas de *hacking* básicas. Estas ferramentas básicas são normalmente criadas com base em código fonte já existente, fazendo apenas algumas alterações de acordo com as necessidades dos criminosos. Neste caso a organização detém uma capacidade de análise de alvo elementar e uma estrutura de controlo para ataques a partir de uma localização comum. Detém também capacidades de aprendizagem básicas podendo assimilar conhecimentos simples e treinar os membros. Em palavras simples, representa grupos que operam com alguma estrutura, mas escassa premeditação ou preparação.

Complexo-Coordenado:

A capacidade para fazer ataques coordenados com a ameaça de causarem disrupção em grande escala, tal como fazer uma análise de vulnerabilidades, penetrar em sistemas complexamente defendidos, incluindo aqueles que usam criptografia, e criar ferramentas de ataque. Neste caso os criminosos dominam completamente o assunto e eles próprios sabem como programar as ferramentas de ataque sem recorrer a *software* já existente. Caracteriza-se também por uma forte capacidade de análise dos alvos e certezas nos

resultados, uma forte estrutura de C2 fornecendo a capacidade de ataques simultâneos a partir de diferentes localizações. Existe também uma capacidade de aprendizagem enorme que está sempre actualizada em relação à tecnologia, treino de membros, difusão do conhecimento e fazer a mudança na organização para melhorar as capacidades de ataque e destruição. Em palavras simples, são grupos que detêm uma preparação avançada com alvos e objectivos específicos.

O Espectro das Ameaças (ALBERTS e PAPP, 2000) mostra a relação existente entre as intenções e as capacidades dos diferentes actores:



Fonte: Martin C. Libicki (1996);
Morris (1995).

Figura 8 – Espectro das ameaças

Nesta figura podemos observar os diversos tipos de actores face às intenções e às capacidades, assim temos:

Amadores:

Estão no nível mais baixo pois são aqueles que não oferecem grande perigo quando tentam fazer actividades ilícitas. Normalmente são cidadãos comuns que tentam ganhar algum dinheiro fácil ou obter qualquer proveito de terceiros, mas que não compreendem bem os pormenores técnicos de como as coisas funcionam nem têm o respectivo treino para coisas mais complexas. Estes adquirem o seu conhecimento, por exemplo, lendo livros.

Hackers*:*

Estes normalmente tentam entrar nos sistemas informáticos mais pelo desafio que isso representa, embora alguns estejam mais no nível seguinte de ameaça. Normalmente costumam usar ferramentas já existentes para efectuar os ataques e detêm conhecimentos técnicos de como as coisas funcionam. Existem diversos filmes sobre os *hackers* baseados em factos verídicos fazendo estes parecerem heróis para o público. Exemplo de filmes[10] sobre *hackers*: (1) WarGames (Jogos de Guerra) (1983) de Lawrence Lasker e Walter Parkes; (2) Sneakers (Heróis por Acaso) (1992) de Phil Alden Robinson; (3) The Net (A Rede) (1995) de Irwin Winkler; (4) Hackers (1995) de Lain Softley.

Crackers*:*

São criminosos mais perigosos que entram nos sistemas informáticos para conseguir algo tal como obter informações confidenciais ou danificar Informação. Também lesam as grandes empresas ao produzirem aplicações de *cracks* ou *key generators* para que o *software* comercial das empresas possa ser usado ilicitamente por outros indivíduos que assim conseguem, através da pirataria, ter acesso a *software* caríssimo e usá-lo como se fosse genuinamente adquirido. Os *crackers* dominam o funcionamento técnico das coisas.

Activistas / Grupos de pressão:

São organizações não-governamentais sem fins lucrativos e que podem lesar economias de países através da paralisação de serviços ao mobilizar a opinião pública e conseguir o apoio das populações para alterar certos aspectos da sociedade. Ex: Greenpeace.

Crime organizado:

Tem um enorme poder de lesar Estados soberanos. São organizações que pretendem obter poder e lucro violando as leis como é o caso de traficar droga, os jogos de azar, a corrupção, a imigração clandestina, o tráfico de pessoas para a prostituição. Estas organizações chegam mesmo a assassinar pessoas para atingir os seus fins. Ex: A Máfia Italiana e a Tríade Chinesa.

[10] Ver Anexo A.2.

Terroristas:

Fazem uso de técnicas violentas de terror para intimidar os diversos actores de forma a tentar impor a sua ideologia, religião, política atacando alvos civis e militares. Os terroristas não olham a meios para levarem a sua adiante e possuem armamento militar.

Estados:

Os Estados são territórios grandes com comunidades organizadas politicamente sob a tutela de um governo com recursos financeiros enormes para usar em combate e protecção. É importante constatar que os Terroristas estão logo abaixo dos Estados soberanos sendo extremamente perigosos podendo causar grandes danos em tudo o que se encontra na figura, desde os amadores aos Estados.

III.2.5. Alguns actos de Ciberterrorismo

De seguida descrevem-se alguns actos marcantes cometidos por ciberterroristas ao longo dos tempos. Apenas estão aqui como exemplos ilustrativos para dar a conhecer como foram cometidos e os alvos dos ataques:

Torre de controlo de tráfego aéreo desactivada (1997):

Em 1997 um jovem *hacker* desactivou (VATIS, 2001) a torre de controlo de tráfego aéreo no aeroporto em Worcester, Massachusetts. Este ataque foi efectuado no antigo sistema de comunicações NYNEX[11] que foi mais tarde substituído pelo sistema Bell Atlantic.

Não houve acidentes mas o serviço foi afectado. Basicamente, os aviões que iam aterrar faziam ligar automaticamente as luzes da pista de aterragem. Mas, quando o *hacker* desactivou as telecomunicações, conseguiu impedir que os aviões que chegassem pudessem ligar as luzes da pista. Isto poderia ter causado a perda de vidas humanas, coisa que felizmente não aconteceu.

[11] NYNEX foi uma companhia de telecomunicações que mais tarde foi comprada pela Bell Atlantic. NYNEX é um acrónimo que significa: "**N**ew **Y**ork/**N**ew England" com o "**X**" representando o futuro desconhecido.

Departamento de Defesa atacado (1998):

Solar Sunrise (GILANI, 2009) que foi o nome de código da investigação, constituiu uma vaga de ataques de redes informáticas do DoD ocorridas entre 1 a 26 de Fevereiro de 1998. Para o ataque, os criminosos fizeram uso de uma vulnerabilidade bem conhecida no sistema operativo usado pelo DoD.

Os atacantes conseguiram acesso a Informação pessoal e à das folhas de pagamento e fizeram o ataque usando o seguinte esquema: (1) Sondar para determinar se a vulnerabilidade existia; (2) Explorar a vulnerabilidade; (3) Introduzir um *sniffer* para conseguir obter dados; (4) Voltar mais tarde para recuperar os dados recolhidos.

Estes ataques ocorreram quando os EUA estavam a preparar a ofensiva militar contra o Iraque aquando da inspecção de armamento da ONU e poderia ter como alvo disruptir as implantações e operações. Contrariamente ao que se esperava, por detrás desses ataques não estiveram o Iraque, terroristas, Estados nem *hackers* de aluguer, mas sim dois adolescentes da Califórnia e um adolescente de Israel.

NASA, Marinha e sistemas universitários atacados (1998):

A NASA, Marinha e sistemas universitários foram atacados (FESTA, 1998) por todo os EUA por ataques DoS tendo como alvo o sistema operativo Windows NT e Windows 95.

Estes ataques lançados via Internet fizeram com que os sistemas de ligação de redes fossem danificados e muitos computadores crasharam com o ecrã azul ("*blue screen of death*"). Quando isto ocorre é necessário reiniciar os computadores e todos os dados que não foram gravados são perdidos.

Os administradores de sistemas relataram que os ataques apenas causaram uma perda de tempo ao tentar resolver o problema e que não houve perda de dados nem danos permanentes. Disseram também que alguns computadores tinham sistemas operativos com actualizações de segurança e neste caso safaram-se do ataque.

Segundo o técnico de segurança da Microsoft, Jason Garms, os ataques foram do tipo "New Tear", "Bonk" ou "Boink" e actualizações de segurança foram tornadas disponíveis para fazer face a este tipo de ataques.

Departamento do banco do tesouro (2001):

Em 2001 dois estudantes de pós-graduação (RADNOFSKY, 2006) conseguiram aceder ao sistema bancário usado para transacções na Internet e também usado para assegurar a confidencialidade dos dados pessoais das contas dos clientes, tendo informado o mundo como o fizeram.

Os sistemas foram *crackados* e os números pessoais de identificação foram acedidos, entre outras Informações confidenciais. Isto tornou evidente que os ciberterroristas com um treino adequado, poderão ser capazes de fazer estragos e causar danos tremendos a governos, organizações, empresas e civis.

Instalações nucleares do Irão (2010):

O stuxnet (MACLEAN e Symantec, 2010) é um *worm* com vista a atingir sistemas de controlo industriais usados para monitorizar e gerir infra-estruturas industriais como é o caso de centrais eléctricas, centrais nucleares, barragens, linhas de montagem, entre outras. A forma de actuação deste *worm* é procurar sistemas de controlo industriais e modificar o código neles para permitir aos atacantes tomarem controlo sem que os operadores dêem conta, permitindo manipular equipamento sensível com impacto elevado a nível de perigosidade.

Este tipo de *worm* é diferente de todos aqueles vistos até agora pois pode causar danos tremendos no mundo físico e é constituído por código extremamente complexo que requer programadores com enormes conhecimentos de sistemas de controlo industrial e recursos significativos, estimando-se que nele trabalharam entre cinco a dez pessoas durante um período de seis meses.

Segundo consta, este *worm* é tão poderoso que só poderá ter sido criado por um Estado, havendo especulações que os EUA e Israel seriam os protagonistas, de forma a atrasar os avanços nucleares do Irão, ao atacar a sua primeira central nuclear. O Irão é visto como um

grande factor de risco para o planeta caso consigam ir em frente com o projecto nuclear que tinham em mente. E, embora o Irão defenda que o seu projecto nuclear tem apenas em vista produzir energia eléctrica, o Ocidente defende que na realidade o objectivo é produzir armas nucleares.

Ataque a servidor da NATO (2011):

Um grupo de *hackers* conhecidos por "Inj3ct0r Team" afirmam ter comprometido (KIRK, 2011) um servidor da NATO, do qual tiraram Informação secreta importante que vieram a disponibilizar no sítio electrónico do grupo.

Os ficheiros, que eram uma cópia de segurança com dados confidenciais, foram colocados no servidor de armazenamento de ficheiros MediaFire com o nome "NATO Tomcat 5.5 Servlet Backup".

Este grupo de *hackers* fundado em 2003 tem um sítio electrónico, http://1337day.com/team, com um arquivo de *exploits* usados para entrar nos sistemas informáticos. Estes *hackers* autodefinem-se como "*hacktivistas*" que normalmente designa o comprometimento de sistemas informáticos por razões de índole política e semelhantes.

Capítulo IV

Formas de Ciberterrorismo

No quarto capítulo fala-se das principais formas de Ciberterrorismo existentes para efectuar os ataques e lesar Estados, infra-estruturas, organizações, empresas e indivíduos: vírus, *worms*, *trojans*, *spyware*, *SPAM*, *phishing*, domínios expirados, jogos de computador, música, *firmware* e a engenharia social que representa a exploração das fraquezas humanas como sendo o elo mais fraco na tecnologia.

IV.1. Vírus

Os vírus informáticos (BIDGOLI, 2006) são muito semelhantes aos vírus biológicos, ou seja, reproduzem-se automaticamente infectando outras aplicações e causam danos nos computadores infectados. Contudo, nem todos são destrutivos, muitos têm um *payload*[12] atrasado e, em casos muito raros, alguns chegam a melhorar o *software* dos computadores infectados.

Os vírus são programas que, após serem executados, duplicam-se e infectam outros ficheiros dos computadores propagando-se. Existe inúmero *software* antivírus no mercado hoje em dia mas os criminosos estão sempre activos a melhorar o *software* malicioso tentando tornar mais difícil a sua detecção. Em palavras simples, os criminosos andam sempre um passo à frente de quem lhes tenta fazer frente.

No passado houve vírus mal concebidos que reproduziam-se na memória dos computadores tantas vezes que os computadores começavam a ficar lentos e os utilizadores começavam a desconfiar que algo estranho estaria a acontecer. Os vírus mais recentes não apresentam este defeito passando muito mais despercebidos aos utilizadores. Os criminosos estão cada vez mais evoluídos.

[12] *Payload* refere-se ao efeito resultante da execução ou carregamento de código num computador ou dispositivo alvo. É normalmente associado a vírus informáticos.

Há quem defenda que os vírus informáticos surgiram prior aos anos 1980s mas não existem provas disso. O primeiro vírus propagado através de *e-mail* ocorreu em 1987 e o primeiro *virus hoax*[13] surgiu em 1988. Existe evidência que os primeiros vírus foram criados nos anos 1980 mas apenas no final dessa década é que o mundo ficou a conhecer o fenómeno que aos poucos se foi disseminando por todo o lado, sendo o método mais comum de disseminação as disquetes, o que de alguma forma tornava mais lenta a disseminação.

No início dos anos 1990s os programadores de vírus começaram a usar novas funções para tornar a detecção mais difícil como é o caso do polimorfismo[14]. Em meados dos anos 1990 surgiram os vírus que faziam uso de *macros* e *scripts* e que vieram a afectar nomeadamente documentos do Office e *software* que aceitasse *scripts*.

Por volta do ano 2000 os vírus começaram-se a propagar de forma frenética usando a Internet para acelerar esse processo. O mundo entrou numa nova era de perigo pois actualmente são produzidos mais vírus do que aqueles que são detectados pelos principais *softwares* antivírus. Normalmente os computadores infectados com vírus enviam vírus por *e-mail* para todos os contactos existentes na lista de contactos do cliente de *e-mail*.

Actualmente os próprios vírus já possuem ferramentas criptográficas embutidas no código que lhes permite alterar partes deles e partes de outros ficheiros, tornando mais difícil detectar a sua *fingerprint* pois são vírus *stealth*. Assim, pode-se aplicar o termo "Criptovirologia" (RAYNAL, 2010). Um exemplo de um vírus deste tipo: O programador do vírus cria uma chave RSA cuja chave pública aparece no corpo do vírus. A chave privada é guardada pelo autor. O vírus difunde-se e usa a chave pública para cifrar dados (ficheiros, *e-mails*, discos rígidos, etc). O autor do vírus pede um resgate antes de enviar a chave privada que permite decifrar os dados e normalmente recebe-se um aviso que, se alguém tentar desactivar o vírus, este destruirá o sistema infectado de forma irreparável.

[13] *Virus Hoax* são normalmente mensagens de correio electrónico a informar sobre ameaças de falsos vírus. São normalmente *chain letters* que pedem aos destinatários para reencaminhar a mensagem para todos os contactos.

[14] O polimorfismo é a capacidade dos vírus alterarem automaticamente o seu código de forma a serem mais difíceis de detectar. Em palavras simples, tornam-se programas mutantes.

IV.2. Worms

Os *worms* (OUDOT, 2010) propagam-se através das redes informáticas atacando *hosts* vulneráveis, infectando-os e fazendo uso disso para se propagarem para outros alvos vulneráveis. Uma grande diferença entre vírus e *worms* é que o segundo faz uso de vulnerabilidades nos sistemas informáticos e os vírus chegam a usar técnicas de engenharia social para funcionarem. No caso dos *worms* temos o facto de chegar mesmo a ser apenas necessário a um computador estar ligado à Internet para ser infectado, como aconteceu em Agosto de 2003 em que o *worm* MSBlast infectou milhões de sistemas informáticos que faziam uso do Microsoft Windows e que tinham uma vulnerabilidade anunciada em Julho de 2003.

São semelhantes aos vírus também se reproduzindo automaticamente mas, neste caso, não infectam outras aplicações pois o ficheiro do *worm* é usado ele próprio nas infecções. Os *worms* apagam ficheiros do computador anfitrião e enviam para os criminosos Informação sensível e confidencial dos computadores infectados. Um efeito muito indesejado é o facto de os *worms* poderem conduzir a uma lentidão terrível das redes informáticas.

Enquanto os vírus se anexam e tornam-se parte de outros ficheiros, os *worms* são ficheiros individuais e não necessitam ser parte de outros ficheiros para se propagarem. Além de se reproduzirem, têm como objectivo eliminar ficheiros ou enviar documentos via correio electrónico nos sistemas que infectam.

Também existem *worms* criados com boas intenções como foi o caso do "Nachia worm" que entrava em computadores com vulnerabilidades e tentava fazer *download* de actualizações de segurança a partir do site da Microsoft de forma a corrigir as vulnerabilidades e depois reiniciava o computador. No entanto estes *worms* benignos também consumiam uma grande largura de banda quer na sua propagação, quer no *download* de actualizações. A maioria dos especialistas em segurança informática considera no entanto que todos os *worms* são *malware*, quer sejam benignos ou malignos.

IV.3. Trojans (Cavalos de Tróia)

Os *trojans* são diferentes dos vírus e *worms* pois não se reproduzem usando outros ficheiros e não se propagam eles próprios, tendo de ser transferidos e executados deliberadamente pelos utilizadores dos sistemas informáticos pois tendem a parecer ficheiros inofensivos, mas na realidade apagam ficheiros, alteram as configurações do sistema operativo e abrem *backdoors* para que os criminosos entrem nos computadores infectados de forma a obter controlo sobre eles, podendo roubar/destruir/adulterar Informação confidencial.

Os *trojans* são programas que dão a entender supostamente serem inofensivos mas têm resultados maliciosos por parte de quem os programou mas que os utilizadores não estão à espera. O termo é derivado da velha história dos Gregos e Troianos em que os Gregos conseguiram entrar em Tróia fazendo uso de um suposto presente de amizade que era um cavalo gigante dentro do qual estavam escondidos soldados, que durante a noite saíram e abriram os portões e os Gregos conseguiram invadir Tróia.

Alguns exemplos de *trojans* são por exemplo: jogos na Internet que ao os utilizadores executarem para jogar, passam a ter os seus computadores comprometidos. Outro são programas que afirmam que quem os executar ganhará um prémio grande mas, na realidade, vêem os seus computadores comprometidos.

IV.4. Spyware

São uma espécie de *trojans* pois não se reproduzem através de outros ficheiros, mas violam a privacidade das organizações, empresas e indivíduos ao enviar Informação para fora, para os criminosos. Também normalmente alteram a configuração dos sistemas e se estes possuírem *modems* é bem possível que façam ligações para números de valor acrescentado, havendo números em que se paga €500 por ligação.

De forma geral, o *spyware* consiste em programas que reúnem Informação sobre os utilizadores de sistemas informáticos sem o conhecimento nem consentimentos destes e depois enviam a Informação para criminosos que de alguma forma vão obter proveito com o que recebem.

Temos por exemplo: entrega de publicidade por correio electrónico e pop-ups (no *browser*), colher informação pessoal, alterar o endereço da página a visitar no *browser* (*browser hijacking*), ligam a linhas telefónicas de valor acrescentado caso esteja-se a usar um modem analógico e fazem registo de todas as teclas premidas para que os criminosos consigam recolher a Informação de *login* e senha de diversos sítios electrónicos dos utilizadores dos sistemas informáticos.

De forma geral, o *spyware* não costuma danificar os sistemas de forma irreparável e quem opera os sistemas raramente se dá conta que está infectado e o *spyware* mais sofisticado é executado sempre que o computador é iniciado

O *spyware*, ao contrário dos vírus, geralmente não se reproduz, infectando os sistemas de utilizadores ignorantes ou com pouca experiência e que fazem *download* e o instalam quando são incentivados através de um "isco". Por vezes a tentação é grande e os utilizadores que são o elo mais fraco caem no risco de instalar programas maliciosos.

IV.5. SPAM

O *SPAM* é o envio de mensagens publicitárias não solicitadas em grande escala, normalmente via correio electrónico, contendo às vezes hiperligações para sítios electrónicos que contêm vírus ou outro *software* indesejado. O *SPAM* enche as caixas de correio electrónicas com lixo fazendo os utilizadores dos sistemas perder imenso tempo a tentar ver quais as mensagens boas, também consumindo enormes recursos informáticos e de rede.

O *SPAM* também é gerado normalmente por computadores infectados com *spyware* ou vírus o que faz o cliente de correio electrónico auto-enviar mensagens a todos os contactos nele existentes. Temos então o marketing virulento em que computadores comprometidos estão constantemente a enviar mensagens a outros sobre a compra de bens e serviços e o ganho de prémios monetários, mas que na realidade não passa de "banha da cobra".

Ao contrário de correio comercial legítimo, o *SPAM* é enviado sem o consentimento do receptor e habitualmente contém "truques" para tentar contornar os "*junk filters*" usados

para detectar mensagens indesejadas. Também, muitos *spammers* fazem o seu melhor para tentar que a origem dos *e-mails* seja muito difícil de detectar como é o caso de fazer *spoof* [15] de endereços de *e-mail*, ou seja: tentar simular que o endereço de correio electrónico de quem enviou o *SPAM* pertence a outra pessoa.

Uma característica do *SPAM* é que os criminosos normalmente colocam no sítio electrónico publicitado uma caixa de texto para os utilizadores serem removidos da lista, mas, na realidade, isso não passa de uma forma de confirmar que os endereços de correio electrónico são válidos e isto vai ainda mais aumentar o tráfego de *SPAM* ao contrário de o eliminar. Há *SPAM* que também indica um endereço de correio electrónico para qual os utilizadores podem enviar uma mensagem para serem removidos da lista, mas que tem o mesmo efeito que a caixa de texto.

Os *spammers* colectam os endereços de correio electrónico a partir de salas de conversação (IRC por exemplo), *Websites*, listas de clientes, *newsgroups*, e vírus. Esses endereços de correio electrónico são vendidos a outros *spammers* por preços que variam consoante a dimensão da lista, tipo de lista e valor/importância que esta aparenta ter. O grande "boom" do *SPAM* teve origem na década de 1990 onde quase todos os endereços de correio electrónico eram disponibilizados na Internet, incluindo mesmo endereços de militares do Pentágono e da Força Aérea dos EUA. Actualmente é muito difícil ou mesmo impossível encontrar tais endereços.

Crê-se que cerca de 90% das mensagens electrónicas a circular na Internet são *SPAM* e parte destas são enviadas para endereços de correio electrónico inválidos, que ou eram falsos ou deixaram de existir. Actualmente até se conseguiu banir a maioria dos *Web Crawlers* que são *software* que vasculham toda a Internet em busca de endereços de correio electrónico nos sítios electrónicos e que depois enviam os resultados aos criminosos.

Geralmente os *e-mails* de *SPAM* publicitam medicamentos, como é o caso do viagra, esquemas financeiros e outros produtos que apresentam alguma ilegalidade.

[15] *Spoof* em segurança informática consiste em falsificar ou esconder elementos de identificação de forma a não ser possível saber quem é o verdadeiro responsável por certas acções.

IV.6. Phishing

O *phishing* (APWG, 2011) é a tentativa de conseguir dados pessoais para depois serem usados para lesar os afectados. Inclui o furto de identidade, roubo de cartão de crédito, senhas de acesso a contas na Internet, etc. Para isso os criminosos podem alterar o *design* de sítios electrónicos fazendo-os parecer de organizações legítimas onde os indivíduos inserem os seus dados pessoais que são depois roubados pelos criminosos e usados para proveito próprio ou para financiar actividades ilícitas como o Ciberterrorismo.

O modo de operação dos *phishers* é simples: enviam *e-mails* em grande escala que podem ser milhões de mensagens. Essas mensagens contêm um texto, logótipo e *design* que aparentam ser de uma empresa bem conhecida e de confiança. Normalmente essas mensagens falam de uma urgência em aceder ao sítio electrónico para regularizar alguma situação. Nesses sítios electrónicos falsos é pedido aos utilizadores que insiram Informação confidencial tal como o número da segurança social, números de contas bancárias, senhas e afins. Essa Informação é depois colectada pelos criminosos.

Após o ano 2005 os criminosos tornaram-se mais sofisticados e começaram a usar *crimeware* em conjunto com os seus *Websites* falsos e hostis tendo em vista explorar vulnerabilidades nos *browsers* para infectar os sistemas informáticos. Usando esta técnica, é feito um furto de identidade dos utilizadores não sendo sequer necessário a inserção de dados pessoais pois estes são roubados quando se acede a sítios legítimos de bancos e de outros serviços *online*.

O número de horas médias em que os sítios electrónicos de *phishing* estão activos está a aumentar o que é muito preocupante visto que quanto mais tempo estão activos, maior é o sucesso dos ataques por parte dos criminosos. Os criminosos conseguem assim mais dinheiros das vítimas e instituições alvo. Em média, os dois primeiros dias de um ataque de *phishing* são os mais lucrativos e às vezes pode demorar semanas ou meses até que os sítios electrónicos sejam desactivados.

Actualmente observa-se uma tendência dos criminosos registarem domínios com poucos caracteres que publicitam em redes sociais e outros locais e que quando clicados redireccionam os visitantes a domínios escondidos muito maiores. Isto dos poucos caracteres visa fazer face a estarem limitados a espaço em algumas redes sociais e também para ser mais fácil enganar os lesados pois nomes pequenos enganam mais.

	2H2010	1H2010	2H2009	1H2009
Domínios alvo de Phishing	42624	28646	28775	30131
Ataques	67677	48244	126697	55698
TLD usados	183	177	173	171
IPs únicos	2318	2018	2,031	3563
Domínios Maliciosamente registados	11769	4755	6372	4382
Domínios IDNS	10	10	12	13

Fonte: Global Phising Survey: Trends and Domain Name Use in 2H2010

Tabela 4 – Tendências e uso de Domínios

IV.7. Domínios expirados

Os criminosos estão sempre à procura de domínios importantes para tentarem apropriar-se deles, quer através da tentativa em descobrir as senhas ou à espera que eles expirem (STEINER, 2003) para rapidamente os adquirir. Depois podem alterá-los para actos criminosos como colocarem *software* malicioso nos sítios electrónicos que irá danificar ou comprometer os sistemas de quem visita os domínios agora pertencentes a criminosos.

Existem criminosos que mal sítios da Internet famosos expiram, registam-nos logo e activam a opção de "*catch all*" [16] para que se qualquer pessoa ou organização que estava em contacto tente contactar o domínio, os criminosos tenham conhecimento disso. Muitos deles mantêm a aparência do sítio electrónico original de forma a enganar os antigos utilizadores que, ao fazerem *login*, estão a dar a conhecer aos criminosos dados pessoais.

O registo de domínios expirados é um risco enorme pois assim consegue-se saber mais facilmente quem estava em contacto com os detentores originais do domínio e, caso

[16] A opção "catch all" (apanhar tudo) significa que, num dado domínio, todos os *e-mails* para ele enviados, independentemente de existir alguém com essa conta no domínio, são enviadas às pessoas que detêm o domínio. Assim, mesmo que o emissor da mensagem se engane no destinatário, o *e-mail* é recebido.

existissem contas associadas a serviços comerciais, como é o caso da eBay, os criminosos podem usar a opção de enviar a senha para eles e assim fazerem furto de identidade e conseguir dinheiro através de fraudes financeiras. Assim conseguem financiar as suas actividades ilícitas.

Normalmente os domínios expirados são registados fraudulentamente usando cartões de crédito roubados, ou por roubo físico, ou através de meios electrónicos como é o caso dos computadores dos lesados estarem comprometidos. Alguns registos são até feitos por *bots*, embora actualmente a maioria dos *Websites* de registo de domínios usem um "*challenge*"[17] para evitar registos em grande escala, assegurando que quem de facto está a registar o domínio é um ser humano. Os criminosos normalmente recorrem a empresas que mantêm a Informação do registo de sítios electrónicos (DOMAIN WHOIS) anónima apontando para moradas em países distantes que nada têm a ver com os criminosos.

IV.8. Jogos de computador

Os jogos racistas (LOADER, 1997) alcançaram uma grande audiência tendo sido conhecidos na Áustria em 1988 embora se acredite terem como ano de início de criação 1986. Crê-se que eram um passatempo popular para a juventude Austríaca.

Contudo, tem-se uma opinião sólida que quem está por detrás dos jogos são grupos Nazis na Alemanha. Estes programam os videojogos de forma clandestina e depois são vendidos ou trocados no mercado negro e nos dias actuais na Internet e, devido às leis internacionais antinazis, os governos da Áustria e Alemanha negam que estes possam ser comercializados e levaram até mesmo vários anos a admitir a existência deste tipo de jogos.

Estes jogos não são todos contra os Judeus pois há também contra os Árabes, Turcos, minorias étnicas e imigrantes sendo a última geração destes jogos interactivos e muito

[17] O "challenge" é um pequeno artefacto para evitar que *bots* registem ou façam *login* automaticamente. Consiste em mostrar um conjunto de caracteres numa imagem e uma caixa de texto onde os utilizadores têm de inserir manualmente esses caracteres. Normalmente alguns criminosos têm *software* para contornar isto que interpreta os caracteres na imagem.

sofisticados. Em 1992 a popular revista Britânica *Amiga Format* fez publicidade a um jogo chamado "Operation Thunderbolt" cujo objectivo do jogo era matar soldados Árabes. Esteve em curso um processo contra esta revista que mais tarde foi abandonado.

Actualmente os jogos têm uma qualidade técnica excelente e são gratuitos visto os distribuidores não terem quaisquer interesses comerciais, mas apenas ideológicos que pretendem alcançar as mentes das camadas mais jovens de forma a moldá-las. Fazendo uso da Internet é possível alcançar uma audiência enorme de jogadores em todo o mundo. Temos como exemplo de jogos feitos para os jovens: "Concentration Camp Manager", "Aryan Test", "Hitler Diktator 1", "Anti-Turk Test" e "Escape from Colditz".

A Agência Federal do Governo Bundesprüfstelle na Alemanha que é responsável por monitorizar livros de banda desenhada, revistas, vídeos, jogos de computador entre outros, relativamente ao acesso às camadas mais jovens, colocou numa lista negra e baniu centenas de videojogos que incitavam ao ódio racial e à glorificação da violência.

IV.9. Música

A música (Australian Human Rights Commission, 2002) é uma linguagem universal pois afecta de alguma forma todos os que a ouvem. Os ciberterroristas usam a música para promover o racismo sendo normalmente semelhante aos ritmos da música normal mas a letra é que difere. O tema dominante destas músicas costuma ser a supremacia branca, falar mal dos Judeus e outras religiões, guerra racista e violência. Não esquecer que as outras religiões, como é o caso do Islão, também fazem uso da música para promover os seus valores e ódio contra o mundo Ocidental e contra as outras religiões existentes no planeta.

Temos como exemplos de géneros musicais o Nazi Punk, o Hatecore, o Oi!, o black metal Nacional-socialista, as músicas fascistas e a música popular. A música é actualmente difundida via Internet em sítios electrónicos, YouTube e partilha de ficheiros. Um bom exemplo de um cantor que poder-se-á considerar um ciberterrorista é o Valete cuja letra de uma das suas músicas no YouTube encontra-se em anexo[18] nesta dissertação.

[18] Ver Anexo A.1.

A música racista normalmente deriva do movimento de extrema-direita Neonazi e é difundida através da Internet e serve para promover o ódio racial, obter receitas para apoio ao movimento (como é o caso de financiar as operações e publicações) e até mesmo para recrutar novos elementos para o movimento, pois o potencial da música para propagação ideológica e de recrutamento é enorme. Uma empresa de música Neonazi existente nos EUA consegue lucros anuais de mais de $1 000 000 e vende mais de 250 títulos de CD. Exemplos de títulos de músicas racistas são: "Still Just a Nigger", "Mud Man" e "Islam (Religion of Whores)" e estas podem ser encontradas facilmente na Internet.

O David Goldman que tem um sítio electrónico para monitorizar o nível de ódio na Internet, "HateWatch", explica o potencial dizendo que mal os indivíduos comecem a ouvir, a comprar CDs, normalmente o próximo passo será ir a um concerto e, quando isso acontece, o mais certo será esses indivíduos tornarem-se recrutas destes movimentos extremistas e eles próprios contribuírem para o recrutamento de mais membros.

Em palavras simples, o uso da Internet para a disseminação deste tipo de música levanta inúmeras questões éticas e de ordem legal, como é o caso da distribuição de materiais ilegais, financiamento de grupos, recrutamento de novos membros e até já existem estações de rádio virtuais especializadas neste tipo de música que se estão a tornar um problema emergente sério da mesma forma que os *downloads* de ideologia racista.

IV.10. Firmware

Existem *hackers* que alteram o *Firmware*[19] de forma a alcançar um determinado fim. Um bom exemplo disto acontece com as *drives* de DVD em que existe uma limitação na velocidade de leitura de filmes DVD-Video conhecida por RIPLOCK (SlySoft, Inc, 2011) para evitar a cópia em grande escala de filmes. Os *hackers* fizeram um *patch* em que removeram esse limite e os utilizadores podem copiar os filmes à máxima velocidade suportada pelas *drives*.

[19] *Firmware* é o *software* que vem embutido no *hardware* e que internamente controla os dispositivos electrónicos. Ex: Motherboards, impressoras, discos rígidos, monitores, drives.

Também é necessário ter cuidado com as zonas onde se compra o *hardware* pois nos países emergentes é bem possível que o *Firmware* tenha sido adulterado e usado para fins criminosos, como é o caso de servirem como *trojans* ou lançarem ataques DDoS pré-definidos e até mesmo dar controlo do sistema informático aos criminosos. O mesmo acontece com o *hardware* comprado em leilões na Internet como é o caso da eBay.

Por sua vez existem ciberterroristas que lançam ataques ao *hardware* apagando o *Firmware* nele existente fazendo com que sistemas informáticos deixem de funcionar. Neste caso provavelmente não será fácil reparar o estrago, ou será até mesmo impossível, pois o *Firmware* é colocado na fábrica. Por exemplo, se o *Firmware* de uma *motherboard* for apagado, o computador deixará de funcionar e a única forma de remediar a situação será comprar uma nova *motherboard*.

Compete aos grandes produtores de *hardware* produzir as devidas actualizações de segurança de *Firmware* de forma a reduzir ou até mesmo eliminar todas as possíveis vulnerabilidades existentes no *Firmware* armazenado em memória *flash*.

Até os EUA lançaram um ciberataque ao Iraque (SMITH, 2003) em 1991 ao enviarem uma impressora através da Jordânia para ser usado pelo Iraque nas instalações de defesa aérea e cujo *Firmware* estava infectado com um vírus chamado AF/91. Este vírus afectou o sistema de defesa aérea Iraquiano ao fechar as janelas dos computadores. Sempre que um técnico abria uma janela com Informação, a janela fechava-se automaticamente e a Informação nela contida desaparecia causando o caos na detecção da aviação Norte-americana. Isto proporcionou aos EUA uma supremacia aérea pois é actualmente defendido que quem controla os céus consegue traçar o destino das guerras.

IV.11. Engenharia Social

A engenharia social (WOZNIAK, MITNICK e SIMON, 2003) usa a influência e persuasão com o intuito de enganar as pessoas fazendo-as pensar que a pessoa ou organização com a qual estão a lidar é algo que não é, ou através do uso de manipulação. O resultado disto é o engenheiro social ser capaz de obter Informação com ou sem recurso a tecnologia.

O Engenheiro Social ganha a vida fazendo uso da sua capacidade de manipular as pessoas para que estas o ajudem a alcançar a meta pretendida, requerendo normalmente que os criminosos tenham enormes conhecimentos e habilidade com sistemas informáticos e telefónicos. Os criminosos estão dispostos a tudo para alcançar os fins pretendidos.

As pessoas são o elo mais fraco da tecnologia e da segurança e é bastante fácil serem usadas. Vejamos pois quando a Informação que parece inofensiva na realidade não o é, bastando apenas os criminosos pedir a Informação alegando que querem ajudar, que procuram ajuda, usando simpatia, culpa, intimidação e uma falsa sensação de confiança.

Algumas formas de engenharia social:

Basta perguntar:

Qualquer engenheiro social pode atacar de forma intricada, com alguns passos e planeamento elaborado, usando manipulação e *know-how* tecnológico. Ele consegue habitualmente alcançar os objectivos com um ataque directo bastando perguntar o que deseja saber. O exemplo de um truque usado: através de uma chamada telefónica só precisa conhecer o dialecto de uma empresa/organização e as suas estruturas corporativas (os vários escritórios e departamentos, o que cada faz e a Informação que cada detém).

Faz parte da natureza humana confiar nos nossos semelhantes, especialmente quando o que é pedido parece razoável e os engenheiros sociais exploram isto.

Construir confiança:

Quanto mais o engenheiro social fizer o seu contacto parecer como negócios regulares, mais se livra de suspeição e é mais fácil ao criminoso conseguir confiança que, uma vez adquirida, ele consegue qualquer Informação sem dificuldades. Por exemplo, o engenheiro social pode fazer uma chamada para uma empresa e dizer estar supersatisfeito com o serviço prestado e que queria enviar uma carta ao gestor a agradecer. A pessoa que atente o telefone fica tão contente que diz o nome e endereço do gestor.

A técnica de construir confiança é uma das mais eficazes e, para tentar escapar a ela, é necessário reflectir se de facto conhecemos a pessoa com que estamos a falar.

“Deixe-me ajudar”:

Sempre que uma pessoa é atormentada por um problema e alguém com conhecimentos, habilidades e força de vontade aparece para ajudar, as pessoas ficam agradecidas. O engenheiro social sabe isso e como conseguir vantagens.

O engenheiro social sabe como criar e depois solucionar problemas para que os lesados fiquem agradecidos e abusar da gratidão das pessoas para conseguir Informação ou favores que lesarão a pessoa envolvida ou a sua empresa/organização.

Se um completo estranho nos fizer um favor de depois nos pedir um favor, não devemos retribuir sem reflectir seriamente sobre o que o estranho está a pedir.

“Pode-me ajudar?”:

O engenheiro social manipula a vítima ao fingir necessitar de ajuda e todas as pessoas simpatizam com as pessoas em dificuldades procurando ajudá-las. Por exemplo: o engenheiro social telefona a uma empresa e diz querer falar com o Sr Pinto. A telefonista pergunta-lhe o primeiro nome do Sr. Pinto e o engenheiro social responde que não se lembra mas tem isso escrito algures. Então pergunta à telefonista quantos Pintos há na empresa, pelo que ela responde “três” e o engenheiro social pergunta o primeiro nome de cada e departamento e a telefonista é bem capaz de dar essa Informação. Depois o engenheiro social já pode ligar novamente para a empresa e conseguir acesso à pessoa que pretendia e tentar lesar a vítima de alguma forma, tal como dizer que houve problemas com o cartão de crédito da vítima e tentar conseguir Informação sobre o cartão.

Capítulo V

As *Botnets* e o Ciberterrorismo

No quinto capítulo fala-se das *botnets* (SCHILLER et al., 2007) que são centenas ou milhares de computadores comprometidos usados (vendidos ou alugados) para ataques em grande escala, que são uma arma cada vez mais utilizada pelos criminosos devido à facilidade e baixo custo que apresentam para o seu uso. É assim possível aos ciberterroristas fazerem ataques em grande escala quase ou até mesmo sem serem reconhecidos e usando poucos recursos financeiros. Neste capítulo sobre as *Botnets*, explica-se o que são, como se propagam, como operam, formas de as detectar e como fazer face a esta ameaça.

As *Botnets* estão a tornar-se a principal ferramenta para os ataques de cibercrime pois conseguem disruptir os sistemas informáticos alvo de várias formas e também devido ao facto de os utilizadores mal-intencionados e sem grandes conhecimentos podem fazer uso de *Botnets* ao simplesmente pagar o aluguer das mesmas a criminosos que cobram mais ou menos dinheiro consoante o número de máquinas comprometidas por estes alugadas. Os preços normalmente rondam os $200 ou $300 à hora.

V.1. O que é uma *Botnet*

Uma *botnet* é a fusão de várias ameaças, normalmente consistindo num servidor *bot* e centenas ou milhares de clientes *bot*, também chamados zombies ou *drones*. Isto é um exemplo de uma pequena *botnet* pois podem existir dezenas de milhares de clientes *bot*. Normalmente o servidor *bot* é um servidor de IRC onde o *bot herder*[20] comunica com os clientes *bot* usando um servidor remoto de comando e controlo (C&C).

[20] *Bot herders/Bot Master* são *crackers* que usam técnicas automatizadas para procurar vulnerabilidades nos sistemas, tal como a falta de *firewalls* ou de actualizações de segurança, ou portas abertas, para instalarem programas *bot* que dar-lhes-ão acesso aos sistemas para poderem conduzir ataques em grande escala. Os

Torna-se necessário saber distinguir entre um cliente de *Botnet* e um *cracker* a tentar entrar no sistema. É muito fácil, pois num cliente de *Botnet* os criminosos não têm de fazer *login* no sistema operativo e há também o facto de os clientes funcionarem coordenadamente para atingir os objectivos dos criminosos sem praticamente qualquer intervenção dos criminosos. Os grupos de computadores que atendam a estes critérios são *Botnets*.

As *Botnets* são um encanto para os *crackers* devido ao facto que os computadores que perpetuam os ataques nem o servidor de IRC não é o computador deles, o que lhes dá uma maior cobertura e impugnação dos seus actos criminosos.

As *botnets* modernas estão organizadas como exércitos zombie com divisões semelhantes às militares e que são controladas por diferentes servidores, para que quando um canal de comunicações é destruído, só é perdido o controlo sobre uma divisão. Assim, as restantes divisões podem ser usadas para retaliar ou continuar com o objectivo em curso dos criminosos.

As *Botnets* são formadas por um vasto número de computadores comprometidos que estão infectados por código malicioso, e podem ser remotamente controlados através de comandos transmitidos pela Internet. Daí, centenas ou milhares de computadores comprometidos podem operar de forma a disruptir ou a impedir o tráfego das vítimas, colher Informação, distribuir *SPAM* e vírus em grande escala, etc.

V.2. Como se propagam

No início os computadores eram comprometidos através de anexos de *e-mail*, mas os utilizadores começaram a ficar mais cuidadoso o que fez os atacantes optar por outros métodos. Temos como exemplo os sítios da Internet infectados com vírus que instalam secretamente código malicioso no computador do visitante. O simples clique em *banners* pode instalar código de *Botnet* fazendo uso de *exploits* quando os utilizadores visitam sítios electrónicos e comprometer o sistema dos utilizadores.

---

criminosos para ocultarem o endereço IP de forma a permanecerem anónimos podem usar *proxy servers*, *shell accounts* e *bouncers*.

Algum *software* malicioso pode mesmo desactivar o antivírus do computador antes de o infectar. Este *software*, além de permitir ao *Bot herder* controlar o computador, também pode ser usado para adquirir dados pessoais ou fazer o registo das teclas premidas e enviar esta informação aos criminosos. O registo das teclas premidas pode conter Informação importante como é o caso de senhas de acesso a sítios electrónicos que poderão fazer com que os criminosos façam furto de identidade e lesem os utilizadores. Pior ainda é quando estas senhas de acesso pertencem a empresas ou organizações tornando os resultados do furto de identidade mais desastrosos.

Um exemplo simples de como uma *botnet* é criada para ataques em grande escala:

- Um *bot herder* ou *botnets* enviam vírus ou *worms* com o objectivo de infectar computadores de forma a instalar uma aplicação maliciosa que neste caso é o *bot*.
- O *bot* que está activo no computador comprometido faz *login* num certo servidor IRC de C&C ou até mesmo num servidor Web.
- Um outro criminoso compra ou aluga os serviços ao *bot herder*.
- O *bot herder* comanda aos computadores infectados que procedam aos ataques comprados pelos criminosos.

As *botnets* tentam conseguir infectar o maior número de computadores possível, incluindo computadores de universidades, organizações e até mesmo governamentais de forma a conseguir uma largura de banda tão ampla quanto for possível.

Um cliente *botnet* surge sempre que um sistema informático é explorado ficando comprometido, o que pode acontecer ao executar-se código malicioso, ataques contra vulnerabilidades, portas traseiras, descobrir senhas, etc:

Código malicioso:

Temos por exemplo *e-mails* que fazem uso de *phishing* que dirigem os utilizadores a sítios electrónicos que depois infectam os sistemas informáticos das vítimas e até podem mesmo fazer-se passar por sítios electrónicos bancários oficiais, e por vezes as vítimas têm conta naquele banco, enganando as pessoas que introduzem lá os seus dados pessoais e bancários. Também temos *e-mails* com anexos que quando são abertos executam código malicioso e comprometem os computadores. Não se pode esquecer o *SPAM* em *software* de *chat* em que por vezes as pessoas com os seus computadores comprometidos enviam

mensagens automáticas a todos os seus contactos a dizer para clicar numa hiperligação para ver algo engraçado e que, na realidade, irá comprometer o computador das vítimas. É muito comum no *software* e sistemas operativos da Microsoft existirem muitas vulnerabilidades e estão sempre a sair actualizações de segurança. Por exemplo: O Internet Explorer que é o *browser* da Microsoft sempre foi conhecido por ter muitas vulnerabilidades e daí, parte da população estar a deslocar-se para outros *browsers* mais seguros como é o caso do Firefox da Mozilla que, além de mais seguro e rápido, sempre que é descoberta uma vulnerabilidade, é lançada uma nova versão para a corrigir. Ainda referente ao Firefox, a correcção de vulnerabilidades é mais rápida e fácil devido ao facto de existir uma enorme comunidade *online* que está sempre a participar na melhoria do produto, quer através de sugestões ou de relatos de erros no *software*.

Vulnerabilidades:

Os criminosos procuram vulnerabilidades nos sistemas operativos e noutro *software* como o Office não corrigidas pela Microsoft, de forma a comprometer os computadores e depois usam esses computadores para tentar comprometer outros, normalmente usando aplicações que permitem fazer *scan* a portas abertas associadas a vulnerabilidades e tomar partido disso. Em anos recentes a Microsoft lançava actualizações na primeira ou segunda terça-feira de cada mês, mas os *hackers* são inúmeros e revertem a engenharia das actualizações em busca de novas fraquezas e alguns dias mais tarde já estão novamente a comprometer os sistemas informáticos, ainda mais que milhões de utilizadores não actualizam o Windows. Convém sempre instalar as actualizações e ter um antivírus e uma *firewall* em dia pois, o sistema uma vez comprometido, poderá fazer com que o *malware* desactive as protecções (antivírus e *firewall*). Os programas que fazem *scan* a portas são actualmente proibidos em quase todo o mundo, pelo menos os com maior grau de perigosidade (que fazem *scan* a mais portas), mas os criminosos têm acesso a eles mesmo assim e usam-nos nos seus ataques. No IRC há criminosos a fazer uso de *bots* para fazer *scan* a IPs para descobrir portas abertas e apoderarem-se dos computadores. Por exemplo, ao escrever: !scanip 213.24.244.3 num canal de IRC, um *bot* dava a resposta no canal e todos os utilizadores do canal tinham acesso ao resultado dado pelo *bot*.

Uso de portas traseiras (back doors):

Algumas *botnets* procuram entradas deixadas por *trojans* que estiveram activos nos computadores. Alguns *trojans* ainda poderão estar activos e permitir aos criminosos controlar remotamente os computadores. Temos por exemplo o SDBot que é um *worm* que abre portas traseiras nos sistemas informáticos e dá acesso remoto aos criminosos, permitindo: (1) Realizar ataques DoS contra outros computadores; (2) Ligar a sítios electrónicos; (3) Fazer *upload* e *download* de ficheiros; (4) Executar programas; (5) Realizar o *scan* de portas, como por exemplo:

- Optix (porta 3140)
- Bagle (porta 2745)
- Kuang (porta 17300)
- Mydoom (porta 3127)
- NetDevil (porta 903)
- SubSeven (porta 27347)

Descobrir as senhas de acesso:

Hoje em dia os criminosos tentam descobrir as senhas dos computadores de forma a conseguir aceder de preferência à conta do administrador e à de outros para conseguirem acesso remoto ao sistema informático. Após terem sucesso é possível partilhar pastas do computador para que os criminosos tenham acesso a elas. Normalmente este tipo de ataque continua a ser lançado às portas 139, 445 e 1433. A força de uma senha tem a ver com o seu tamanho, complexidade e imprevisibilidade. Existem quatro formas principais de conseguir as senhas:

- ***Uso de força bruta:*** Consiste em tentar todos os caracteres possíveis até conseguir acertar. É a forma mais comum de conseguir *crackar* senhas, e funciona principalmente nas protecções criptográficas mais fracas e nas senhas com poucos caracteres.
- ***Palavras comuns:*** Esta é a forma mais rápida de conseguir descobrir senhas. A maioria dos utilizadores colocam palavras fáceis de adivinhar como é o caso do nome do cão, dos filhos, da mulher e outros como: “caneta”, “bola”, etc. e os criminosos têm a lista de palavras no *software* que usam e o sucesso é eminente.
- ***Uso de dicionários:*** Uma forma de ataque muito usado é ter todas as palavras de um dicionário no *software* usado para o ataque e este vai tentando palavra a palavra

até conseguir alcançar o sucesso. Mais uma vez, o uso de palavras que existem num certo idioma é uma vulnerabilidade que poderá ser explorada pelos criminosos.

- ***Uso de senhas padrão:*** São as senhas pré-definidas que costumam vir já configuradas de origem e que por isso são as primeiras a serem tentadas pelos criminosos. Temos como exemplos mais frequentes:
    - Administrator
    - Administrador
    - admins
    - admin
    - staff
    - root
    - computer
    - owner
    - student
    - teacher
    - wwwadmin
    - guest
    - default
    - database
    - dba
    - oracle
    - db2
    - user
    - home
    - work

As senhas são basicamente estas, mas o *bot herder* pode substituí-las por outras que tenham funcionado nos outros computadores do alvo. O mais certo é que vários computadores pertencentes à mesma organização usem algumas senhas idênticas tornando mais fácil comprometer os sistemas informáticos.

V.3. Como operam

O modo de operação das *botnets* consiste em cinco passos simples:

1. As *botnets* entram automaticamente em canais específicos de IRC e ficam à escuta de comandos;
2. O *bot herder* envia mensagens ao servidor de IRC para os clientes;
3. Os clientes recebem os comandos através do canal de IRC e actuam de acordo com o que lhes é comandado;
4. Os clientes realizam ataques DDoS contra alvos específicos;
5. Os clientes retornam os resultados dos ataques para que o *bot herder* tenha conhecimento.

As *botnets* estão organizadas como exércitos reais, possuindo diferentes servidores de IRC para que, quando um canal de IRC estiver comprometido, o *bot herder* continue na posse de outros clientes, tendo sempre vantagem sobre quem tenta por termo aos ataques e retaliar ou continuar a fazer negócio. Fala-se aqui de negócio pois o *bot herder* também aluga computadores infectados para que quem paga também possa fazer ataques em grande escala a alvos específicos de acordo com as necessidades.

Não querendo entrar em grande detalhes sobre os protocolos de IRC, vai-se falar de conceitos que são importantes relacionados com as *botnets*:

- **JOINS**: São usados pelos clientes de IRC para entrar num certo canal num servidor de IRC. Aqui temos em uso o nome do canal e a senha;
- **PINGS**: São enviados a partir de um servidor para um cliente para confirmar se este continua ligado ao servidor de IRC pois o cliente pode ter desligado a ligação, *crashado* ou pode ter ocorrido algum erro. Normalmente os PINGS são enviados em períodos múltiplos de 30 segundos;
- **PONGS**: Se o Ping é enviado pelo servidor de IRC, este é o oposto, sendo enviado pelo cliente de IRC em resposta ao Ping a dizer que ainda está activo;
- **PRIVMSG**: Contém o nome do canal e os dados enviados ao canal, de forma a serem enviados a todos os *hosts* no canal lógico de IRC.

Os JOINS e PRIVMSG contêm os nomes dos canais e existe *software* específico de monitorização e de detecção de anomalias que usa ambos os JOINS e PRIVMSG em conjunto com uma lista de endereços IP de forma a criar uma lista de canais associados aos *hosts* de IP, mantendo também registo de PINGS e PONGS pois quando estes ocorrem em grande número é possível que exista algum canal de IRC muito grande cheio de computadores comprometidos e usados com a finalidade das *botnets*.

Por vezes os *crackers* são maus a escolher os nomes dos canais de IRC onde irão manter os clientes da *botnet*. Esse mau gosto em escolher os nomes de canais, por exemplo: "#xploit" torna mais fácil a um analista investigar e descobrir *botnets*. Este é um ponto fraco por parte dos criminosos e que pode ser usado como uma vantagem para os investigadores.

A arquitectura das *botnets* evoluiu ao longo dos tempos e nem todas apresentam a mesma topologia para C&C o que limita o potencial de aluguer e de venda das *botnets*. As topologias típicas (OLLMANN, 2009) são:

- **Estrela:** Nesta topologia existe um ponto de C&C centralizado, a partir do qual se comunica directamente novas instruções para todos os *bots*. Quando os criminosos conseguem comprometer o sistema informático de uma vítima, este normalmente é pré configurado para ligar-se a este ponto central de C&C, onde é registado como membro da *botnet* e fica a aguardar instruções. A grande vantagem para os criminosos é uma mais rápida transferência de instruções e de dados roubados. A desvantagem é que se o ponto de C&C central é atingido, a *botnet* fica desactivada.
- **Multiservidor:** Esta é uma topologia de extensão lógica à anterior, em que existem múltiplos servidores para enviar instruções aos *bots*. Esses sistemas múltiplos de comando comunicam entre si conforme gerem a *botnet*. Caso um dos servidores falhe, os restantes continuam a controlar a *botnet*. Este tipo de topologia é mais complexa e requer planeamento e esforços acrescidos da parte do *bot herder* que tentará colocar os servidores em locais geograficamente afastados para ser mais difícil acabar com a *botnet*. As grandes vantagens para os criminosos são o facto de se algum ponto de C&C for desactivado, continuam com controlo da *botnet* a partir dos outros pontos e os locais geográficos distintos podem optimizar a comunicação entre os *bots*. A grande desvantagem é que requer um planeamento avançado que nem todos os criminosos têm.
- **Hierárquica:** Este tipo de topologia reflecte a dinâmica dos métodos usados para a propagação e comprometimento dos *bots* pois facilita a mistura de tácticas de propagação. Contudo, as instruções de comando mais recentes sofrem de alguma latência dificultando os criminosos a utilizarem a *botnet* para actividades em tempo real. Este tipo de topologia significa que nenhum *bot* está ciente da ligação de toda a *botnet* e também facilita a divisão de grandes *botnets* em mais pequenas para venda ou aluguer. As vantagens são que a intercepção de *bots* não denuncia todos os membros da *botnet* nem revela o servidor de C&C. Outra vantagem é que pode subdividir a *botnet* e depois vender ou alugar a outros criminosos. A grande desvantagem é a latência nos comandos devido ao facto destes terem de percorrer mais canais dentro da *botnet* o que dificulta alguns tipos de ataques e operações.

- **Aleatória:** Neste tipo de topologia existe uma relação dinâmica entre *master-slave* e *peer-to-peer*, não existindo um servidor C&C centralizado. Os comandos são assinados como tendo autoridade e enviados à *botnet* a partir de quaisquer *bots*. Este tipo de *botnets* é mais difícil serem encerradas devido ao facto de não possuírem um ponto de C&C centralizado e devido ao facto de existir várias vias de comunicação entre os *bots*. Contudo, é fácil identificar membros da *botnet* ao monitorizar a comunicação de um certo *bot* com os outros. Neste tipo de topologia também existe um problema de latência de comandos. A grande vantagem nesta topologia para os criminosos é que, devido ao facto dos *bots* enviarem os comandos entre eles, torna-se mais difícil encerrar a *botnet*. As grandes desvantagens são a grande latência na distribuição de comandos por parte dos criminosos e o facto de ser fácil a partir de um *bot*, descobrir as suas ligações aos outros.

V.4. Como as detectar

A seguir vai-se explicar algumas formas principais para tentar detectar *botnets*:

Recepção de correio electrónico a dizer que a organização está a enviar *SPAM*:

Se alguém enviar *e-mails* a dizer que a nossa organização está a enviar *SPAM,* é necessário ser cuidadosos e verificar se é de facto verdade, pois poderá na realidade ser a prova de que existe actividade de *botnet* e que os nossos sistemas informáticos poderão estar comprometidos. Vejamos pois:

- Se uma organização tiver um computador a enviar *SPAM*, é possível que todo o seu domínio ou subdomínio possa ser colocado numa lista negra, o que poderá afectar seriamente todas as actividades;
- É preciso ter cuidado com *proxies* abertos no sítio electrónico da organização, pois estes aceitam ligações de endereços IP e redireccionam a ligação para outro endereço IP. Um *proxy* aberto pode indicar um *host* comprometido que é fácil de descobrir caso exista um volume de tráfego fora do normal.

Este tipo de correio electrónico enviado é vulgarmente conhecido por *abuse e-mail* e ocorre quando alguém na Internet decide queixar-se sobre algo que julgue estar errado no sítio electrónico/sistemas informáticos das organizações. Isto pode incluir *SPAM*, *scan* de

portas, ataques DoS, *phishing*, etc. . Normalmente os *e-mails* com queixas são enviados para o domínio da organização com o destinatário "abuse", por exemplo: **abuse@cia.gov** .

Registo nas *firewalls*:

Outra forma de detectar *botnets* é através do registo de actividade nas *firewalls*. O tráfego de saída dos computadores comprometidos que tentam recrutar outros computadores é bloqueado e registado pelas *firewalls*, mesmo que os antivírus nada detectem.

Logo, os registos das *firewalls* são muito importantes e úteis na detecção de sistemas comprometidos, de forma a impedir entradas e saídas de coisas más e de pacotes de dados. Em caso de suspeita de estarmos perante uma *botnet*, deve-se analisar com cuidado o tráfego do dia anterior. Se prestar-se a devida atenção, ver-se-á que a Internet está a atacar as organizações 24/7 e daí ser importante ver se a nossa organização também está a atacar.

Convém aos administradores de sistemas bloquear algumas portas específicas e usadas pelos criminosos, nas *firewalls* e ver os registos dos resultados, podendo saber através de avisos quando alguns computadores internos ficam infectados. É também possível configurar as *firewalls* para que dêem um alerta quando algo de errado acontece, de forma a melhorar o tempo de resposta para os problemas que possam surgir.

Detecção de Intrusões:

A detecção de intrusões é muito importante para a detecção de *botnets*. Segundo (SLADE, 2006) é "um sistema automatizado para alertar um operador sobre uma penetração ou outra contravenção de uma política de segurança". Normalmente, na detecção de intrusões, é verificado o tráfego de pacotes de dados, ficheiros do sistema e ficheiros de registos. Também não esquecer que os sistemas de detecção de intrusões podem ser usados para armadilhar ou monitorizar actividade intrusiva.

Os sistemas de detecção de intrusões podem ser baseados em *hosts* ou em rede, dependendo do tipo de algoritmo de monitorização usado bem como a detecção de assinaturas e de anomalias, cabendo aos administradores definir o que é considerado actividade normal e anormal e indo alterando os parâmetros:

- **Em *hosts*:** Monitoriza a actividade suspeita de sistemas individuais num sistema protegido, tais como actividade inapropriada de aplicações, acessos suspeitos a ficheiros ou serviços. Também monitorizando o estado do sistema como é o caso da respectiva configuração e o estado do sistema de ficheiros. Permite detectar os seguintes tipos de ataques:
    - Ataques de computadores *peer* na rede interna;
    - Adulteramento directo de utilizadores internos;
    - Verificar ficheiros que possam conter código malicioso;
    - Verificar definições, normalmente o *Windows Registry,* em busca de sinais de código malicioso;
    - Verificar sistemas de ficheiros, caixas de correio em busca de sinais de uso indevido, tal como pastas ocultas que contenham material ilícito que poderá ser: imagens pornográficas, *software* pirata, dados roubados, etc.;
    - A introdução de código malicioso a partir de media removível.
- **Em rede:** Monitoriza uma rede, vendo *hosts* protegidos em termos de interfaces externas em relação ao resto da rede, em vez de apenas um único sistema, e grande parte dos resultados obtidos baseiam-se na análise de pacotes de dados. Isto torna possível detectar os seguintes tipos de ataques:
    - Ataques DoS detectados por assinaturas específicas ou por uma análise de tráfego;
    - *Scan* de Portas, ou seja, a sondagem de portas abertas ou que estão à escuta. Também a sondagem de apenas portas à escuta numa variedade de *hosts*;
    - Verificar sinais de possíveis *bots* a fazer uso indevido dos serviços da rede;
    - Assinaturas específicas de sondagem/ataque.

Detecção de *malware*:

Este é um ponto importante de segurança para lidar com possíveis *botnets*, onde a detecção é apenas parte do processo de gestão da segurança. Em organizações bem protegidas, tem-se antivírus em PCs, portáteis, servidores LAN, servidores de aplicações, etc. de forma a detectar em tempo real qualquer ameaça que surja. Pode-se até ter alguma medida de filtragem automática, por exemplo: no envio e recepção de correio electrónico e tráfego Web e ambos os tipos de análise heurística e específica.

Actualmente os antivírus trazem algumas facilidades de utilização que permitem uma gestão central, reportar e registo de tudo o que acontece nos sistemas informáticos. Tudo o que é necessário é ter sempre as definições de vírus actualizadas, o que permite detectar precocemente problemas e anomalias tais como ficheiros colocados em quarentena devido a serem suspeitos. Existe também antivírus que vão enviando amostras de código aos respectivos programadores para análise, tendo como exemplo o antivírus da Microsoft, Microsoft Security Essentials, que tem uma definição chamada Spy Net em que é possível escolher se todos os ficheiros novos são enviados para análise, bem como outras opções, tal como perguntar antes de enviar ou não enviar.

Uma coisa boa nos antivírus mais recentes é que não apenas detectam o *malware* existente na base de dados, mas também utilizam um sistema/motor heurístico (GORETSKY, 2010) em que tentam detectar *malware* não existente na base de dados. Isto tem como objectivo tentar detectar *malware* no espaço de tempo existente entre cada actualização do antivírus.

Esta coisa de detecção heurística consiste em utilizar um sistema de pontuação aplicado a código que não corresponda na totalidade a *malware* conhecido, permitindo detectar ameaças que apresentem características semelhantes a ameaças já conhecidas. É ainda possível escolher o nível de detecção que, quanto mais elevado, aumenta o risco de detectar falsos positivos. Mas, é sempre melhor ter falsos positivos do que o contrário.

O motor heurístico usado pelos antivírus contém regras para o seguinte:

- Programas que tentem copiar-se para outros programas;
- Programas que tentem escrever directamente para o disco;
- Programas que tentem permanecer residentes na RAM após terminarem de executar;
- Programas que se decifrem quando executados;
- Programas que se "agarrem" a portas TCP/IP e que fiquem à escuta nas ligações;
- Programas que tentem manipular (copiar, apagar, modificar, substituir) ficheiros pertencentes ao Sistema Operativo;
- Programas que sejam semelhantes àqueles já conhecidos como maliciosos.

V.5. Como enfrentar esta ameaça

Para enfrentar esta ameaça os investigadores tem que analisar desde os computadores infectados até ao servidor de IRC e daí até os *crackers*. Os criminosos podem acrescentar outra camada de complexidade ao enviarem todos os comandos ao canal de IRC usando *proxies*, *shell accounts*, *bouncers*, até usando por exemplo uma ferramenta como o Tor[21] (Tor, 2011). Aliado a isso, o facto dos criminosos se encontrarem noutros países também prejudica a investigação pois as leis internacionais costumam ser diferentes das leis locais de cada Estado e torna-se necessário usar investigadores estrangeiros.

Até se os criminosos se encontrarem no mesmo país que as vítimas, o processo para obter Informação dos ISPs é muito burocrático. No passado os ISPs davam a Informação voluntariamente ao dizerem que os termos de serviço foram violados ou quando havia suspeita de crime, mas agora, neste mundo litigioso isto raramente acontece.

Algumas bases de código de *botnets* incluem comandos para eliminar as provas, técnicas de cifra de tráfego e *stealth*. Torna-se necessário: (1) Mais educação sobre segurança e *botnets*; (2) Mais comunicação entre os profissionais de segurança; (3) Ter boas práticas de segurança. Ao conseguir estas três coisas é mais fácil enfrentar esta ameaça da qual ninguém está completamente seguro.

A educação sobre como manter os computadores seguros já é muito antiga, mas continua a haver pessoas que não sabem as regras mais elementares de segurança. Com a proliferação da banda larga e os computadores estarem ligados à Internet 24 horas por dia, o grau de ameaça aumentou em muito. A verdade é que os criminosos estão 365/24/7 a tentar invadir os sistemas informáticos e, sem boas políticas e práticas de segurança, os computadores

[21] O Tor é *software* livre *open source* que ajuda a proteger contra a vigilância na Internet defendendo que esta vai contra a liberdade pessoal, a privacidade, actividades de negócio confidenciais, relacionamentos e a segurança estatal (também conhecida por análise de tráfego). O Tor impede saber a localização ou hábitos de navegação das pessoas, sendo utilizado em *Web Browsers*, clientes de *chat*, *login* remotos, etc. e existe para várias plataformas como é o caso do: Windows, Mac, Linux/Unix e Android.

tornam-se alvos fáceis até mesmo para os criminosos "amadores" que usam ferramentas que se encontram na Internet, para tentar comprometer os sistemas informáticos.

A comunicação e debate entre as organizações e os profissionais de segurança são cruciais pois não existe Informação sobre como combater *botnets* em muitas esferas, pois é necessário saber o que fazer para manter as redes mais seguras. As *botnets* podem desenvolver-se ainda mais, mas o mesmo também é verdadeiro para as medidas defensivas, desde que sejam postas em prática.

O que pode ser feito para combater esta ameaça:

- A resposta das organizações face às *botnets* deve tomar lugar muito antes de descobrir que a organização já está comprometida. Ou seja, devem-se tomar acções preventivas e proactivas. Uma forma de resposta é ver se os endereços IP das organizações constam em listas negras e tomar medidas para reparar isso caso seja esta a situação. Mas, em palavras simples: é sempre melhor prevenir que remediar;
- Melhorar a política de segurança local com boas práticas que impeçam que os criminosos consigam as senhas de acesso dos sistemas. Devem-se usar senhas que sejam difíceis de adivinhar e todas as contas devem estar protegidas com senhas;
- Usar *firewalls* para limitar o alcance dos ataques e obter relatos e registos de tentativas de intrusão nos sistemas informáticos das organizações. Nas organizações é aconselhado ter-se uma *firewall* de *hardware* e uma *firewall* de *software* de forma a ter-se mais camadas de protecção. A *firewall* de *hardware* impedirá que os trabalhadores das organizações fiquem vulneráveis a certas ameaças mais sofisticadas que podem danificar a *firewall* de *software*;
- Fazer todas as actualizações de segurança do Sistema Operativo pois os criminosos estão sempre informados sobre as mais recentes vulnerabilidades dos sistemas e usam isso para os comprometer;
- É preciso ter cuidado com o *download* de ficheiros da Internet, tornando-se necessário assegurar que os sítios electrónicos são legítimos. Se houver dúvidas, nunca se deve transferir ficheiros e deve-se sempre olhar com cuidado e atenção para o *software* grátis que poderá conter *malware*. Observar ainda com precaução *software* caro a baixos preços, como é o caso do Microsoft Office, pois é bom demais para ser verdade.

- Deve-se ter sempre um antivírus para tentar proteger de ficheiros maliciosos. Também se deve fazer análises periódicas ao disco rígido com o antivírus para tentar descobrir possíveis ameaças pois estas nem sempre são detectadas no momento em que ocorrem. Não esquecer também de actualizar sempre o antivírus de forma a ter as "assinaturas" mais recentes das possíveis ameaças;
- Enviar mensagens de correio electrónico de abuso sobre ataques remotos para que as organizações tomem conhecimento que os sistemas informáticos delas estão comprometidos. Em palavras simples, isto significa reportar quaisquer *botnets* que sejam detectadas, de forma a tentar que sejam encerradas.
- Pode-se contactar as entidades judiciais caso os incidentes sejam considerados muito danosos financeiramente ou legalmente. É sabido que a motivação primária para a criação e uso de *botnets* é o dinheiro e, enquanto houver oportunidades lucrativas, sempre existirão *botnets*. Embora muitas vezes os criminosos não são presos, mas deve-se sempre tentar pois é uma forma de reduzir o número de *botnets* existentes e futuras;
- As ferramentas *darknets*, *honeynets* e *honeypots* são muito úteis para saber o que se está a passar. As *darknets* são usadas no contexto de redes de partilha privada de ficheiros. As *honeynets* consistem num número de *honeypots* com grande interacção. Estas oferecem aos criminosos sistemas reais, aplicações e serviços de forma a fazê-los pensar que estão a atacar as organizações mas, na verdade, as organizações estão a observar os atacantes. Assim é possível estudar as tácticas dos criminosos e aprender com isso.

Conclusões

Na conclusão registamos as principais ideias e ilações retiradas de todo o processo de investigação e redacção.

A nossa pergunta central é: **"***Como minimizar ataques ciberterroristas que usam meios electrónicos, acessíveis a toda a população, através da mensuração do seu grau de severidade e da transformação de dados em Informação?"*. Esta pergunta tem a ver com a problemática do facto da tecnologia e a Internet estarem acessíveis a toda a população mundial e, por isso, devemos tentar minimizar o ataque de ciberterroristas, através da mensuração do respectivo grau de severidade dos ataques e da transformação de dados em Informação. A tecnologia e a Internet são de acesso barato a qualquer pessoa nos dias actuais e, por isso, uma enorme ameaça nas mãos dos criminosos.

Ir-se-á verificar ou não as hipóteses, as questões derivadas e, por fim, responder concretamente à pergunta de partida.

Temos a seguir as hipóteses que são explicações possíveis tidas para o tema abordado, sendo afirmações e não questões, podendo-se apenas confirmá-las ou negá-las.

Hipóteses:

Passando de seguida à verificação ou não da primeira hipótese:

H1 – Se utilizarmos técnicas combinatórias que transformam dados em Informação, então poderemos detectar os ataques ciberterroristas e assim proceder à sua monitorização.

(VERIFICA-SE)

A Teoria da Informação é muito importante para transformar dados em Informação ao quantificar a quantidade de Informação gerada na ocorrência de um evento, conseguindo uma redução de incertezas e eliminação de possibilidades.

Temos uma técnica criada por Ronald Fisher em 1922 denominada "Estimação de Máxima Verosimilhança" (MLE) e uma outra técnica chamada "Análise Combinatória" (AC):

A MLE é um método que permite "testar" hipóteses estatísticas e necessita basicamente de dois elementos: (1) Uma amostra da população em estudo que seja suficientemente grande e significativa; (2) Um modelo estatístico da população, o qual se quer validar.

A AC é outro método frequentemente utilizado em estatística mas que só se aplica a dados discretos, ou dados que podem ser tornados discretos por via de agrupamento em categorias. O método permite calcular a probabilidade de se obter um resultado que cumpre um certo critério e consiste em calcular o número de eventos que cumprem o critério e o número de eventos possíveis.

O método da AC parece estar limitado a dados discretos ou que possam ser tornados discretos por agrupamento em categorias. O método MLE pode ser aplicado a dados contínuos, sem necessidade de agrupamento em categorias. Ambos os métodos obrigam a que se assuma um modelo estatístico (uma distribuição) que se considera aplicável à população em questão. O modelo da AC é normalmente aplicado a casos onde os diferentes eventos individuais têm igual probabilidade e é depois usado para calcular a probabilidade de se obter combinações que podem ser muito complexas, contudo o modelo pode também ser aplicado a casos em que as probabilidades individuais não são iguais.

Passando de seguida à verificação ou não da segunda hipótese:

H2 – Se o Ciberterrorismo permanecer, então causará danos cada vez maiores.

(VERIFICA-SE)

O Ciberterrorismo tem motivações políticas, ideológicas, sociais com o objectivo de causar prejuízos severos para os governos, que podem chegar mesmo à perda de vidas humanas.

O Ciberterrorismo conduz à destruição ou disrupção ilícita de propriedade digital para intimidar ou coagir governos ou sociedades na busca de objectivos que sejam políticos, religiosos ou ideológicos, usando a Informação como arma, método ou alvo. Existe dentro e fora do ciberespaço e inclui a destruição física, disrupção, negação de serviço de equipamentos ou sistemas que usem código binário. A sua grande particularidade é a capacidade de usar meios baratos que são desproporcionais aos danos causados. O Ciberterrorismo pode aumentar ou dar apoio ao terrorismo tradicional, podendo também ser empregue de forma distinta.

Um bom exemplo de Ciberterrorismo actual será conseguir penetrar no sistema informático de um hospital e alterar a medicação de pacientes com o objectivo de causar a morte deles. Este é um exemplo muito compreensível e muito provável de ocorrer. Outro bom exemplo de Ciberterrorismo será mexer com o sistema de crenças dos médicos, ao ensiná-los mal, o que poderá causar a perda de vidas humanas.

Passando de seguida à verificação ou não da terceira hipótese:

H3 – Se o Ciberterrorismo prevalecer, então será o principal conflito do século XXI.

(VERIFICA-SE)

A grande particularidade do Ciberterrorismo é a capacidade de usar meios baratos que são desproporcionais aos danos causados sendo necessário fazer face a este tipo de ameaça por parte dos Estados. Deram-se exemplos de alguns actos de Ciberterrorismo mais marcantes ao longo dos tempos. Foram apenas escolhidos alguns pois na realidade eles estão sempre a ocorrer e cada vez mais frequentemente e com maiores consequências.

O Ciberterrorismo veio para ficar e irá piorar pois cada vez mais pessoas têm acesso à Internet e cada vez mais novos e sai muito barato atacar usando meios electrónicos, ou seja, já existem crianças que sabem mais sobre ataques cibernéticos do que muitos adultos. Desde cedo que os criminosos começam o seu percurso.

O Sistema de Crenças é de extrema importância na temática da Teoria Relativista da Informação e corresponde aos argumentos e ao peso atribuído a cada um deles. Logo, diferentes pessoas ou computadores interpretarão ou agirão de forma diferente perante os problemas e cenários, de acordo com os sistemas de crenças que têm. Tem-se então que focar em trabalhar e melhorar os sistemas de crenças de forma a obter melhores resultados.

Tem-se então de trabalhar o Sistema de Crenças para que seja possível a Defesa vencer e o Ataque perder, conforme se demonstrou nas figuras 4 e 5.

Passando de seguida à verificação ou não da quarta hipótese:

H4 – Se os ciberterroristas não têm rosto nem um país certo de origem dos ataques, então a utilização de técnicas de detecção e de monitorização são essenciais para a manutenção da Segurança.

(VERIFICA-SE)

Deve-se ter a maior simplicidade possível dos dados/Informação de forma a conseguir mensurar a quantidade de Informação sobre um conjunto de dados tendo uma variável desconhecida, mas que queremos saber. Evitar sempre o uso de dados complicados e confusos (caóticos) pois irá impossibilitar conseguir quantidade de Informação fiável sobre a estrutura de um sistema. Se tivermos dados simples, mesmo com poucos dados, é possível conseguir uma quantidade de Informação enorme e muito rica e útil, sabendo se temos Informação a mais ou a menos durante esse processo.

A probabilidade permite determinar o grau de certeza sobre algo e a quantidade de Informação fornecida por um conjunto de dados sobre uma variável desconhecida depende em muito do sistema de crenças existente, ou seja, perante o mesmo conjunto de dados é possível obter resultados diferentes dependendo de quem está a interpretar os dados. Por mais completo que seja o conjunto de dados, haverá sempre um sistema de crenças onde a quantidade de Informação sobre a variável desconhecida será zero.

De seguida vai-se passar da verificação das hipóteses para as questões derivadas que, como o nome indica, derivam da questão central e são usadas para dar respostas:

Questões Derivadas:

Em resposta à primeira questão derivada:

Q1 – Qual a ligação entre o terrorismo tradicional e o Ciberterrorismo?

O terrorismo tradicional é a forma clássica e em algumas ocasiões assemelha-se mais à guerra do que ao crime, face aos grandes recursos financeiros que consegue para comprar armamento militar e até mesmo armas de destruição maciça. O terrorismo tradicional implica que os membros da organização estejam fisicamente presentes no local do ataque para levar a cabo os seus actos, tal como é o exemplo de ataques bombistas ou o desvio de aviões.

O Ciberterrorismo pode ser operações de *hacking* com o objectivo de causar prejuízos severos (perda de vidas humanas, prejuízos económicos, ataques ou ameaças contra sistemas informáticos, redes e a respectiva Informação neles armazenada). Pode chegar a

ser um ataque físico com o objectivo de destruir nós computorizados de infra-estruturas críticas (Internet, telecomunicações) ou a grelha eléctrica de um país ou de uma cidade. No Ciberterrorismo os membros da organização podem fazer os ataques à distância.

Os níveis de ameaça do Ciberterrorismo podem ser: Baixa, Moderada, Significativa ou Elevada, baseando-se em seis elementos: (1) Presença do grupo terrorista; (2) Capacidade em realizar ataques; (3) Intenção por parte dos grupo; (4) Actividades feitas ao longo dos tempos; (5) Informação credível sobre possíveis alvos; (6) Factores políticos internos e de segurança que têm influência no prosseguir das operações.

Em resposta à segunda questão derivada:

Q2 – Quais as motivações e como actuam os ciberterroristas (métodos e perfis-psicológicos)?

Os Ciberterroristas são normalmente jovens do sexo masculino, com habilitações académicas elevadas (mestrados e doutoramentos) e que têm a consciência de estar a violar a lei e a desrespeitar as normas sociais, a ordem e os sistemas de controlo social. Temos até crianças por detrás de alguns dos ataques. Estes indivíduos diferem dos criminosos comuns em pelo menos quatro características: (1) Usam maior violência; (2) A meta é infligir medo numa população alvo enorme; (3) Têm uma agenda social enorme e tentam recrutar novos elementos; (4) Procuram uma exposição máxima aos media.

As explicações para o terrorismo não lhe dá legitimidade para matar inocentes, nem justificam o comportamento face às vítimas. O terrorismo é usado para o mundo saber que aqueles que usam métodos extremistas têm reclamações e são alvo de injustiças e que o mundo Ocidental tem de fazer algo para pôr cobro a isto, ou terão de sofrer represálias.

Em resposta à terceira questão derivada:

Q3 – Até que ponto será possível anular as repercussões dos ataques, detectando-os atempadamente através de técnicas combinatórias, designadamente, da Teoria da Informação de Fisher?

Tudo aquilo que é conhecido além da dúvida (BERNOULLI, 1713) dizemos conhecer ou compreender. Em relação ao restante, apenas se conjectura ou opina e as probabilidades são estimadas pelo número e peso dos argumentos que provam uma coisa ser, foi ou será. Ao fazer conjecturas está-se a mensurar a probabilidade de algo o melhor possível de forma a ser possível escolher a melhor opção para os nossos julgamentos e acções.

O acaso não é parte do conhecimento, mas é sim uma propriedade do objecto, não sendo possível fazer previsões. A probabilidade é uma medida de quão certos estamos e é conseguida com uma combinação de argumentos. Quando um argumento pode ser matematizado, podem-se fazer previsões. Quando um argumento é uma imagem, pode-se predizer (*forecast*) pois "uma imagem vale mil palavras" sendo objectiva. Quando se tem ambos os argumentos (a imagem mais a matemática) pode-se conseguir a certeza. Cada argumento tem de ter um peso e o conjunto de argumentos com os respectivos pesos é um sistema de crenças.

Ao se ter maior quantidade de Informação do que o adversário é possível ganharmos a ofensiva. Tem tudo a ver com a complexidade ou simplicidade dos dados e a respectiva quantidade de Informação útil que conseguimos adquirir face ao tipo de dados.

A resiliência é a capacidade de reorganização após perturbações, tentando perceber porquê alguns sistemas humanos falham ao tentar dar resposta a alterações no meio-ambiente, sendo racional para a estrutura e irracional para o indivíduo. É racional para a estrutura pois esta não fica afectada pela Informação com que tem de lidar, contudo, para o indivíduo é bem possível que ele seja afectado pela subjectividade. O interior é uma Ilha de Resiliência desde que haja simplicidade na Informação e o factor chave para a resiliência está na simplicidade da Informação e a coesão de uma estrutura reside nas interacções existentes entre os seus elementos nesse âmbito.

Em resposta à quarta questão derivada:

Q4 – Onde actuam os ciberterroristas, dentro dos Estados ou além-fronteiras?

Os ciberterroristas actuam dentro dos Estados e além-fronteiras pois não existem fronteiras na Internet, nem uma legislação comum e aceite por todos os Estados e, por isso, não

existe uma cooperação entre todos. Devido a isto torna-se difícil aos Estados planearem o melhor possível as suas acções contra o Ciberterrorismo como o fazem contra o terrorismo tradicional. Aos poucos os Estados vão procurando trabalhar em conjunto de forma a harmonizar a legislação, mas ainda há um longo percurso pela frente pois os governos são diferentes havendo ainda regimes ditatoriais e extremistas no mundo.

Alguns países têm recentemente criado legislação mais severa para os crimes informáticos, como é o caso da criação e propagação de vírus informáticos e outros actos criminosos como o acesso não autorizado a sistemas informáticos. Temos o exemplo do Japão (The Mainichi Daily News, 2011) que em Junho de 2011 criou legislação severa que pune com até três anos de prisão e 500 000 *yens* de caução os criadores de vírus e até dois anos de prisão e 300 000 *yens* de caução para quem compre vírus ou os armazene para fins impróprios. Tornou também possível aos ISPs guardarem os registos das comunicações dos utilizadores até 60 dias.

A figura intitulada "Espectro das Ameaças" mostra a relação existente entre as intenções e as capacidades dos diferentes actores: amadores, *hackers*, *crackers*, ONG, crime organizado, terroristas e Estados. Os terroristas estão logo debaixo dos Estados.

Em resposta à quinta questão derivada:

Q5 – Como irão os ciberterroristas incrementar o grau de severidade dos seus ataques produzindo danos cada vez maiores?

Uma vez que o mundo está unido por super auto-estradas da Informação, existem grupos que procuram tirar vantagem da falta de segurança neste meio para conseguir dinheiro fácil, danificar sistemas informáticos, fazer brincadeiras e até mesmo tentar a sua sorte em coisas que julguem possível fazer.

Temos três níveis de capacidade de ameaças consoante a sofisticação dos ciberterroristas que permitem produzir danos cada vez maiores: (1) **Simples-Não estruturado**: Uso de ferramentas de ataque já existentes; (2) **Avançado-Estruturado**: Criar ferramentas a partir de código fonte existente fazendo alterações no código e treinam os membros da

organização; (3) **Complexo-Coordenado**: Criar ferramentas de ataque e têm bons conhecimentos de criptografia;

As ferramentas comuns usadas pelos ciberterroristas para lesar Estados, infra-estruturas, organizações, empresas e indivíduos são: (1) **Vírus**: Reproduzem-se infectando outras aplicações e causam danos nos computadores infectados. Dificultam a sua detecção usando o polimorfismo, *macros* e *scripts*, e até criptografia; (2) ***Worms***: Propagam-se através de redes atacando *hosts* vulneráveis, infectando-os e propagam-se para outros alvos vulneráveis, mas não infectam as aplicações; (3) ***Trojans***: Não se reproduzem nem se propagam. Ao serem executados, abrem portas traseiras nos sistemas informáticos dando acesso aos criminosos; (4) ***Spyware***: Não se reproduzem mas violam a privacidade das organizações, empresas e indivíduos ao secretamente enviar Informação para os criminosos; (5) ***SPAM*:** As mensagens publicitárias não solicitadas enviadas em grande escala, normalmente por correio electrónico contendo às vezes hiperligações para sítios electrónicos comprometidos; (6) ***Phishing:*** Técnicas para conseguir dados pessoais das vítimas e inclui o furto de identidade, roubo de cartão de crédito, senhas de acesso, etc. Pode passar pela alteração do *design* de sítios electrónicos fazendo-os parecer legítimos; (7) **Domínios expirados:** Quando certos domínios expiram, os criminosos procuram registá-los e usam a opção "*catch all*" para conseguir as senhas de acesso daqueles que pensam que os domínios ainda pertencem aos donos antigos. Podem ainda ficar comprometidos; (8) **Jogos de computador:** Os jogos racistas servem para modelar a mente dos jovens fazendo-os sentir ódio e repulsa por outras raças ou religiões, tornando fácil recrutá-los para as organizações extremistas; (9) **Música:** Promove o racismo, disponíveis na Internet. Nos anexos temos uma música do cantor Valete que incentiva ao ódio contra os EUA; (10) ***Firmware:*** Adulterar o *software* que vem embutido em equipamentos electrónicos para efectuar ataques a quem os usa ou ataques DDoS a outros sistemas; (11) **Engenharia Social:** A manipulação dos seres humanos por serem o elo mais fraco na tecnologia, de forma a conseguir acesso a Informação sensível.

As *botnets* são milhares ou até mesmo dezenas de milhares de computadores comprometidos usados para fazer ataques DDoS em grande escala. São verdadeiros exércitos Zombie e actualmente cada vez mais usadas pelos ciberterroristas podendo-se vender ou alugar *botnets*.

As *botnets* são ataques direccionados, ou seja, os criminosos procuram comprometer certos sistemas informáticos numa rede procurando *bugs* nos Sistemas Operativos ou *software* usados e depois fazer com que os PCs se conectem a um servidor específico na Internet onde os criminosos emitem comandos que são obedecidos pelos computadores comprometidos. Este tipo de ameaça continuará a prevalecer e a ser cada vez mais comum.

Posição	País	Rácio Infecção
1	Tailândia	66.97%
2	China	62.82%
3	Taiwan	59.90%
4	Letónia	55.75%
5	Arábia Saudita	55.42%
6	Federação Russa	54.32%
7	Israel	53.30%
8	Lituânia	53.22%
9	Turquia	51.55%
10	Polónia	50.35%

Fonte: Global Phising Survey: Crimeware Development and Contagion Surging Worldwide in 2H2010

Tabela 5 – Crimeware - Desenvolvimento e contágio

Para responder à pergunta central de investigação, estabelecida em **"***Como minimizar ataques ciberterroristas que usam meios electrónicos, acessíveis a toda a população, através da mensuração do seu grau de severidade e da transformação de dados em Informação?"* devemos considerar então que:

A técnica para conseguir descobrir fraquezas nos sistemas informáticos é pôr-se na pele dos criminosos, ou seja, conseguir pensar como eles para descobrir as suas tácticas e técnicas de ataque. Assim será possível precaver contra a maioria dos ataques embora não todos, pois a mente dos criminosos é fértil e estão sempre a surgir novos tipos de ataques. Está técnica é sugerida pelos grandes "crânios" peritos em segurança interna e externa.

Os criminosos podem usar técnicas como o uso de *port scanners* para descobrir entradas nos sistemas informáticos e depois comprometem-nos enviando e instalando *malware* que pode ser *key loggers* por exemplo. Com os *key loggers* conseguem registar todas as teclas

premidas nos sistemas comprometidos que conterão senhas de acesso, nomes de utilizador, números de cartões de crédito, etc. enviado aos criminosos e depois usados para fins ilícitos como é o caso de roubo de dinheiro e usurpação de identidade.

Normalmente são descobertas portas abertas em sistemas informáticos que não dispõem das mais recentes actualizações de segurança ou que têm as *firewalls* mal configuradas. Também é possível fazer uso de *phishing* como é o envio de *e-mails* no qual os criminosos fazem-se passar por entidades oficiais e pedem directamente os dados das pessoas dizendo que se as pessoas não responderem, a conta delas será cancelada dentro de um certo período de tempo. Assim conseguem uma vez mais lesar as pessoas tendo acesso a Informação sensível. Os criminosos têm sempre uma mente fértil para o crime informático.

Os criminosos, para tornar mais difícil a identificação deles, podem usar técnicas de *IP spoofing* tal como o uso de redes *wireless* de outros através de *software* que pode ser usado para descobrir as senhas de redes com criptografia mais fraca e depois o endereço IP que aparece nos ataques é o das redes *wireless* que estão a ser usadas ilicitamente. É possível tentar saber geograficamente a localização dos computadores ligados às redes, mas se os criminosos estiverem a usar um computador portátil e mudarem frequentemente de localização, torna-se quase impossível apanhá-los.

Deve ter-se em conta que quando os sistemas informáticos ficam comprometidos, perde-se a confiança neles pois existem vírus mutantes e uma vez uma porta traseira aberta, é possível aos criminosos entrar nos computadores e danificar o antivírus e/ou *firewall* o que põe em causa a fiabilidade do sistema. O mais seguro em alguns casos é reinstalar o sistema operativo e todas as aplicações de raiz, após serem feitos *backups*.

Torna-se imperativo fazer *backups* periódicos dos dados/Informação importantes para que se estes sofrerem danos seja possível recuperar do estrago. Pode-se fazer *backups* locais e *backups* remotos que são armazenados em servidores remotos usando criptografia de forma a aumentar a segurança. Os servidores remotos têm ainda a vantagem de, se algo acontecer localmente, teremos os dados importantes seguros noutras partes do planeta.

Torna-se necessário a existência de planos para recuperação de desastres de forma a tornar conhecido o que é necessário fazer para recuperar os dados o mais rapidamente possível e restaurar os serviços. Para isto é necessário ter em conta: (1) Identificar os sistemas críticos que armazenam dados e Informação sensível, as localizações e as respectivas funções; (2) Avaliação dos riscos e impactos de forma a determinar se houver perdas, qual será o impacto negativo destas; (3) Os *Hot sites* são importantes caso a localização original se tornar inoperável e servem como *backups* ou sistemas redundantes podendo ser accionados caso um servidor principal seja destruído, danificado ou comprometido; (4) Testar os procedimentos de recuperação para que se tenha a prática e o conhecimento suficiente para agir caso aconteça algo na localização principal e deve ser testado pelo menos uma ou duas vezes por ano de forma a serem eficazes no caso de um desastre.

Torna-se necessário o uso de *Honeypots* e *Web Mining* para tentar contornar a questão e tentar atempadamente detectar os ataques ciberterroristas, uma vez que o cibercrime tem aumentado consideravelmente nos anos recentes, desde *software* malicioso (*malware*) e até mesmo as *botnets*. Existem mesmo Estados soberanos a encenar ataques contra outros Estados soberanos, ou contra organizações/empresas noutros Estados.

Em suma:
Conclui-se que tudo é relativo dependendo de cada indivíduo e de cada computador, tendo-se de trabalhar com enorme prioridade nos sistemas de crenças para fazer face às ameaças e aos desafios, pois o ataque ou a defesa vence dependendo da complicação ou simplicidade dos dados que afectam a quantidade de Informação útil.

Temos então como chave para vencer ou perder face aos atacantes, a **Métrica da Informação**, que nos mostra o estado da Ilha de Resiliência, dizendo se temos simplicidade ou complexidade de dados na tomada de decisões. De acordo com isso, podem-se tomar boas ou más decisões. Quanto maior for a complexidade de dados pior será a nossa tomada de decisão pois a quantidade de Informação útil será perto do zero. Em palavras simples, podemos ter muita Informação mas a quantidade de Informação útil que esta representa poderá ser nula.

Temos a **Métrica da Informação**:

$$dG^2 = cdH_0^2 - dV^2 - dW^2 - dH_i^2$$ **(Jumarie)**

Componentes da Métrica da Informação:

- **c –** Medida pelo Sistema de Crenças
- **H_0 –** Informação Externa
- **H_i –** Informação Interna
- **V –** Objectivos
- **W –** Capacidade Interna para a mudança (adaptação)

Esta é a métrica mais importante relativamente à Teoria Relativista da Informação pois o interior dos seres vivos é uma Ilha de Resiliência quando há uma simplicidade de dados, e esta Ilha mantém-se ao ter uma H_i (Informação Interna) o mais baixa, o mais simples e o mais rica possível.

Esta métrica corresponde à Informação Externa **MENOS** os objectivos **MENOS** a Capacidade Interna para a Mudança **MENOS** a Informação Interna e que, de acordo com a Tabela 2 descrita no Capítulo 2, é possível determinar o estado da Ilha da Resiliência (pode apresentar-se: destruída, mantém-se, melhora). O **c** é a medida pelo Sistema de Crenças: **C=1** Representa Tecnologia (seres de silicone, conseguem processar dados e Informação de uma forma cada vez mais rápida e precisa) e **C>1** Representa Inteligência (seres de carbono, são todos nós, os seres de carne e osso).

Para finalizar as conclusões, não se pode esquecer as limitações e pressupostos deste trabalho, e as perspectivas de investigação futura.

As limitações e pressupostos do trabalho são o que geralmente se denomina de subsecção de humildade, não existindo trabalhos perfeitos existindo sempre algo que pode ser melhorado. A principal limitação e dificuldade encontrada ao longo do tratamento do tema e da própria investigação foi derivada do tema escolhido, sensível e novo, onde as pesquisas já efectuadas estão pouco divulgadas e os livros são de difícil acesso e muito caros. Tentou-se contudo conseguir o máximo possível de Informação e com qualidade,

procurando também Informação em sítios electrónicos de universidades Americanas e em de organizações credíveis como sendo o caso de militares ou do governo dos EUA.

As perspectivas de investigação futura representam uma abordagem de carácter positivo e construtivo. Por exemplo: disponibilizar de forma gratuita ou com preços reduzidos, *software* que permita detectar possíveis tentativas de intrusão em sistemas informáticos mostrando num mapa do mundo a localização de onde os ataques provêm. Este *software* poderia enviar dados estatísticos para uma base de dados internacional de uma organização credível e permitir a todos os indivíduos e organizações terem acesso a eles de forma a perceber as zonas do globo mais perigosas e mais afectadas. Isto permitiria realizar estudos mais aprofundados sobre o assunto e a respectiva mobilização e sensibilização da opinião pública face à ameaça do Ciberterrorismo. Não esquecer que os computadores são cada vez mais uma tecnologia persuasiva que moldam a forma como as pessoas vêem e interagem entre si e com o mundo. Devia ser feito um estudo mais aprofundado sobre essas implicações pois o futuro da população do planeta depende de todos nós.

Referências Bibliográficas

ALBERTS, David S., PAPP, Daniel S. – *Information Age Anthology: National Security Implications of the Information Age*. CCRP, 2000.

AMARAL, Paulo Cardoso – *TOP SECRET: Como proteger os segredos da sua empresa e vigiar os seus concorrentes*. Academia do Livro, 2008.

APWG (2011). *Global Phishing Survey: Trends and Domain Name Use in 2H2010*. Internet: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf, consultado em [19/08/2011]

ARMISTEAD, E. Leigh - *Information Warfare: Separating hype from reality*. Potomac Books, Inc., 2007.

Australian Human Rights Commission (2002). *Examples of Racist Material on the Internet*. Internet: http://www.hreoc.gov.au/racial_discrimination/cyberracism/examples.html#1.3, consultado em [19/08/2011]

BERNOULLI, Jakob - *Ars Conjectandi (The Art of Conjecturing)*. [s.n.], 2010.

BIDGOLI, Hossein - *Handbook of Information Security*. California State University, 2006.

BOWERS, Stephen R., KEYS, Kimberly R. - *Technology and Terrorism: The New Threat for the Millennium*. Liberty University, 1998.

BREZILLON, Patrick (1998). *Introduction to the Special Issue "Using context in applications"*. University of Nevada, Reno. Internet: http://www.cse.unr.edu/~syco/papers/hci/Intl_Journal_of_Human_Studies/ContextInApps_Brezillon.pdf, consultado em [19/08/2011]

STOICA, P., VIKALO, H., HASSIBI, B. (2003). *Joint Maximum-Likelihood Estimation and Signal Detection for Simo Channels*, California Institute of Technology. Internet: http://www.ee2.caltech.edu/Faculty/babak/pubs/conferences/01202529.pdf, consultado em [19/08/2011]

CARMO, Hermano; FERREIRA, Manuela Malheiro - *Metodologia da Investigação: Guia para a auto-aprendizagem*. Universidade Aberta, 2008.

CASAGRANDE, David (2004). *Resilience and Information Discontinuity across Organizational Scales of Human Ecosystems*, Western Illinois University. Internet: http://faculty.wiu.edu/DG-Casagrande/pdfs/esa04.pdf, consultado em [19/08/2011]

Computer Crime Research Center (2002). *What is Cyber-terrorism?*. Internet: http://www.crime-research.org/library/Cyber-terrorism.htm, consultado em [19/08/2011]

Computer Crime Research Center (2004). *Cyber Terrorism: The new kind of Terrorism*. Internet: http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism, consultado em [19/08/2011]

Computer Crime Research Center (2004). *What is Cyber-terrorism?*. Internet: http://www.crime-research.org/analytics/Krasavin, consultado em [19/08/2011]

CRAWFORD, Paulo (1999). *O Espaço-tempo Curvo da Relatividade Geral*, Faculdade de Ciências da Universidade de Lisboa. Internet: http://cosmo.fis.fc.ul.pt/~crawford/artigos/cc_sr/node2.html, consultado em [19/08/2011]

CRUTCHFIELD, J. P. (1990). *Information and its Metric*, The Pennsylvania State University. Internet: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.57.5786&rep=rep1&type=pdf, consultado em [19/08/2011]

D'OLIVEIRA, Teresa - *Teses e dissertações: Recomendações para a elaboração e estruturação de trabalhos científicos*. 2ª ed. Editora RH. 2007.

Department of Defense (2011). *Dictionary of Military and Associated Terms*. Internet: http://www.dtic.mil/doctrine/dod_dictionary, consultado em [19/08/2011]

Diário de Notícias (2010). *Pastor quer queimar Alcorão no dia 11 de Setembro*. Internet: http://www.dn.pt/inicio/globo/interior.aspx?content_id=1657359&seccao=EUA%20e%20Am%E9ricas, consultado em [19/08/2011]

DORBOLO, Jon (2003). *Systems of Belief*, Oregon State University. Internet: http://oregonstate.edu/instruct/phl201/modules/frameworks/belief_systems.html, consultado em [19/08/2011]

DREKSTE, Fred I. - *Knowledge & the Flow of Information*. Cambridge University Press, 1999.

ECO, Umberto - *Como se faz uma tese em Ciências Humanas*, 15ª ed. Editorial Presença, 2007.

Editorial Verbo - *Enciclopédia Fundamental Verbo*, Editorial Verbo, 1982.

ESPOSITO, John (2007). *Legitimate, illegitimate acts of violence*, Georgetown University. Internet: http://acmcu.georgetown.edu/135371.html, consultado em [19/08/2011]

EurekAlert! (2011). *How do we fight the war against cyber terrorism?*. *Internet*: http://www.eurekalert.org/pub_releases/2011-04/ip-hdw041111.php, consultado em [19/08/2011]

Faculdade de Ciências da Universidade de Lisboa (1998). *Teoria da Combinatória*. Internet: http://www.educ.fc.ul.pt/icm/icm98/icm13/3c.htm, consultado em [19/08/2011]

FBI (2008). *FBI 100 The Unabomber*. Internet: http://www.fbi.gov/news/stories/2008/april/ unabomber_042408, consultado em [19/08/2011]

FESTA, Paul (1998). *Hackers attack NASA, Navy*, CNET News. Internet: http://news.cnet.com/2100-1001-208692.html, consultado em [19/08/2011]

FOGG, B. J. - *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, 2003.

FOGG, B. J. (2010). *BJ Fogg's Behavior Model*, Stanford University. Internet: http://www.behaviormodel.org, consultado em [19/08/2011]

FORST, Brian - *Terrorism, Crime and Public Policy*, Cambridge University Press, 2009.

FRASER, D. A. S., MACKAY, Jock (1975). *Parameter factorization and inference based on significance, likelihood, and objective posterior*, University of Toronto. Internet: http://www.utstat.toronto.edu/dfraser/documents/57.pdf, consultado em [19/08/2011]

FRIEDEN, B. Roy (1998). *Physics from Fisher Information*, Cambridge University Press. Internet: http://cscs.umich.edu/~crshalizi/reviews/physics-from-fisher-info, consultado em [19/08/2011]

FRIEDEN, B. Roy - *Science from Fisher Information: A Unification*. 2ª ed. Cambridge University Press, 2004.

FRIEDEN, B. Roy (2009). *Fisher Information, a New Paradigm of Science*, University of Arizona. Internet: http://www.optics.arizona.edu/frieden/fisher_information.htm, consultado em [19/08/2011]

FRIEDEN, B. Roy, GATENBY, Robert A. - *Exploratory Data Analysis Using Fisher Information*, Springer, 2011.

GILANI, Syed H. (2009). Solar Sunrise, the most organized and systematic attack on US Defence Department by Mossad, SYED HAROON HAIDER GILANI. Internet: http://haroonhaider.com/2009/09/21/solar-sunrise-the-most-organized-and-systematic-attack-on-us-defence-department-by-mossad, consultado em [19/08/2011]

GILLIES, Duncan, THORNLEY, David, BISDIKIAN, Chatschik - *Probabilistic Approaches to Estimating the Quality of Information in Military Sensor Networks*. Oxford University Press, 2008.

GORETSKY, Aryeh (2010). *What are Heuristics?*, ESET. Internet: http://www.eset.com/about/blog/blog/article/what-are-heuristics, consultado em [19/08/2011]

IGNATIEFF, Michael - *The Lesser Evil: Political Ethics in an Age of Terror*. Princeton University Press, 2004.

IMDb (2011). *The Internet Movie Database*. Internet: http://www.imdb.pt, consultado em [19/08/2011]

Indiana University of Pennsylvania (2001). *When Cyber Hacktivism Meets Cyberterrorism*. Internet: http://www.lib.iup.edu/comscisec/SANSpapers/paul.htm, consultado em [19/08/2011]

I.S.E.L. (2008). *Revisões de Análise Combinatória*. Internet: http://www.deetc.isel.ipl.pt/matematica/EP_IEP/Revis%C3%B5es%20de%20An%C3%A1lise%20Combinat%C3%B3ria.pdf, consultado em [19/08/2011]

JONES, P. (2000). *Hodges' Health Career - Care Domains - Model, Defining Information*. Internet: http://www.p-jones.demon.co.uk/infdefs.html, consultado em [19/08/2011]

JOYNER, Christopher C., LOTRIONTE, Catherine – *Information Warfare as International Coercion: Elements of a Legal Framework*. EJIL, 2001.

KIRK, Jeremy (2011). *Hacking Team Claims NATO Server Compromised*, PCWorld Business Center. Internet: http://www.pcworld.com/businesscenter/article/235106/hacking_team_claims_nato_server_compromised.html, consultado em [19/08/2011]

LAUDON, Ken, LAUDON, Jane - *Management Information Systems: Global Edition*, 11ª ed. Pearson Education, 2009.

LEBOW, Richard Ned, RISSE-KAPPEN, Thomas (1996). International Relations Theory and the end of the Cold War. Columbia University Press. Internet: http://library.northsouth.edu/Upload/IR%20Theory.pdf, consultado em [19/08/2011]

LOADER, Brian D. - *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, Routledge, 1997.

MACLEAN, William (2010). *Cyber-attack appears to target Iran -US tech firm*, REUTERS. Internet: http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE68N0WG20100924, consultado em [19/08/2011]

MAI, Larri L., OWL, Marcus Young, KERSTING, M. Patricia - *The Cambridge Dictionary of Human Biology and Evolution*. Cambridge University Press, 2005.

Millennium Project (2007). *Annotated Scenarios Bibliography*. Internet: http://millennium-project.org/millennium/annotated-scen.html, consultado em [19/08/2011]

MOORE, Frank R - *Introduction to Biological Sciences*. The University of Southern Mississippi, 2008.

MOORE, Terrence, SADLER, Brian - *Maximum-Likelihood Estimation and Scoring Under Parametric Constraints*, Army Research Laboratory, 2006.

MORRIS, Stephanie J. (1997). *The Pythagorean Theorem*, The University of Georgia. Internet: http://jwilson.coe.uga.edu/emt669/student.folders/morris.stephanie/emt.669/essay.1/pythagorean.html, consultado em [19/08/2011]

MYUNG, Jae - *Tutorial on maximum likelihood estimation*. Ohio State University, 2002.

NAGRE, Dhanashree, WARADE, Priyanka - *Cyber Terrorism: Vulnerabilities and Policy Issues "Facts Behind the Myth"*. Carnegie Mellon University, 2008.

National Institute of Standards and Technology (2010). Maximum Likelihood Estimation. Internet: http://www.itl.nist.gov/div898/handbook/apr/section4/apr412.htm, consultado em [19/08/2011]

NATO (2003). *Cyberterrorism*. Internet: http://www.nato.int/structur/library/bibref/cyberterrorism.pdf, consultado em [19/08/2011]

NATO (2011). *NATO and the fight against terrorism*. Internet: http://www.nato.int/cps/en/natolive/topics_48801.htm, consultado em [19/08/2011]

NATO (2011). *NATO's military concept for defence against terrorism*. Internet: http://www.nato.int/cps/en/natolive/topics_69482.htm, consultado em [19/08/2011]

NELSON, Bill [et. al.] - *Cyberterror: Prospects and Implications*. U.S. Navy, 1999.

NSA (2010). *UKUSA Agreement Release 1940-1956*. Internet: http://www.nsa.gov/public_info/declass/ukusa.shtml, consultado em [19/08/2011]

NUNES, Paulo Viegas – *Slides das aulas de Guerra de Informação*, Academia Militar, 2010.

OLLMANN, Gunter (2009). *Botnet Communication Topologies: Understanding the intricacies of botnet Command-and-Control*, DAMBALLA. Internet: http://www.damballa.com/downloads/r_pubs/WP%20Botnet%20Communications%20Primer%20%282009-06-04%29.pdf, consultado em [19/08/2011]

OUDOT, Laurent (2010). *Fighting Internet Worms With Honeypots*, Symantec. Internet: http://www.symantec.com/connect/articles/fighting-internet-worms-honeypots, consultado em [19/08/2011]

Porto Editora - *Dicionário Editora da Língua Portuguesa*. Porto Editora, 2011.

QUADE, Kristine (2007). *The Traditional Meets The Emergent: The Modernization of T-Groups*, Human Systems Dynamics Institute. Internet: http://www.hsdinstitute.org/learn-more/library/articles/Traditional-Meets-Emergent.pdf, consultado em [19/08/2011]

RADNOFSKY, Mary L. (2006). *Corporate and Government Computers Hacked by Juveniles*, The Socrates Institute. Internet: http://www.socratesinstitute.org/research/ Hackers.html, consultado em [19/08/2011]

RANDOLPH, Eric (2010). *Why Al-Qaeda Doesn't Care If It Kills Muslims*, Current Intelligence MAGAZINE. Internet: http//www.currentintelligence.net/agenda/tag/ideas?currentPage=2, consultado em [19/08/2011]

RAYNAL, Frederic (2010). *Malicious cryptography, part one*, Symantec. Internet: http://www.symantec.com/connect/articles/malicious-cryptography-part-one, consultado em [19/08/2011]

RODRIGUES, Carvalho – *Slides sobre a Teoria da Informação*. NATO, 2011.

SCHILLER, Craig [et. al.] - *Botnets: The Killer Web Applications*. Syngress Publishing, Inc., 2007.

SKEFFINGTON, Jennifer Sheehy (2009). *Social psychological motivations of suicide terrorism: A community level perspective*, Defence Science and Technology Laboratory. Internet: http://harvard.academia.edu/JenniferSheehySkeffington/Papers/113323/Social_psychological_motivations_of_suicide_terrorism_A_community_level_perspective, consultado em [19/08/2011]

SLADE, Robert - *Dictionary of Information Security*. Syngress, 2006.

SlySoft, Inc. (2011). *DVD Protections*. Internet: http://www.slysoft.com, consultado em [19/08/2011]

SMITH, George (2003). *One printer, one virus, one disabled Iraqi air defence*, The Register. Internet: http://www.theregister.co.uk/2003/03/10/one_printer_one_virus_one, consultado em [19/08/2011]

SNODGRASS, John (2007). *Turning data into Information*, U.S. Department of Education. Internet: http://www2.ed.gov/teachers/how/tools/initiative/summerworkshop/snodgrass/index.html, consultado em [19/08/2011]

SOUSA, Gonçalo de Vasconcelos - *Metodologia da Investigação, redacção e apresentação de trabalhos científicos*. Livraria Civilização Editora, 2005.

STEINER, David (2003). *Expired Domains Expose eBay Security Glitch*, EcommerceBytes.com. Internet: http://www.auctionbytes.com/cab/abn/y03/m05/i15/s01, consultado em [19/08/2011]

SYMANTEC (2010). *The Stuxnet Worm*. Internet: http://www.symantec.com/business/outbreak/index.jsp?id=stuxnet, consultado em [19/08/2011]

The Mainichi Daily News (2011). *Legislation criminalizing creation of computer viruses*. Internet: http://mdn.mainichi.jp/mdnnews/news/20110617p2g00m0dm013000c.html, consultado em [19/08/2011]

THOMAZ, João Pedro da Cruz Fernandes – *O Apoio à Tomada de Decisão na Avaliação do Desempenho de Pessoas: Contributos para o Processo de Decisão Militar em Tempo de Paz*, Instituto Superior Técnico, 2005.

Tor (2011). *Tor Project*. Internet: https://www.torproject.org, consultado em [19/08/2011]

United Nations (1998). *Universal Declaration of Human Rights*. Internet: http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=eng, consultado em [19/08/2011]

Universidade de Aveiro (2003). *Método da máxima verosimilhança*. Internet: http://www2.mat.ua.pt/disciplinas/mne/aula18.pdf, consultado em [19/08/2011]

Universidade do Minho (2010). *Armas Não Letais*. Internet: http://www3.dsi.uminho.pt/academiamilitar/2002/Capitulo6/futuro.htm#Cin%C3%A9ticas , consultado em [19/08/2011]

U.S. Army - *US Army Cyber Terrorism Instruction Lesson Plan: Cyber-Terrorism: ISO6C47L/Version 1*. U.S. Army, 2004.

U.S. Army (2004). *U.S. Army Cyber Terrorism Instruction Lesson Plan*. Internet: http://www.docstoc.com/docs/67527149/US-Army-Cyber-Terrorism-Instruction-Lesson-Plan, consultado em [19/08/2011]

U.S. Department of Defense (2006). *Information Operations Related Documents: JP 13-3*. Internet: http://information-retrieval.info/docs/DoD-IO.html, consultado em [19/08/2011]

U.S. Department of Defense (2006). *JP 3-07.2*. Internet: http://file.wikileaks.info/leak/us-antiterrorism-jp3-07-2-2006.pdf, consultado em [19/08/2011]

U.S. Department of State (1998). *1998 Global Terrorism: Year in Review.* Internet: http://www.state.gov/www/global/terrorism/1998Report/review.html, consultado em [19/08/2011]

U.S. General Accounting Office (2003). *Combating Terrorism*. Internet: http://www.acq.osd.mil/cp/gao/gao_03-165.pdf, consultado em [19/08/2011]

Valete (2009). *Música do Valete*, YouTube. Internet: http://www.youtube.com/watch?v=bonP6Z1cwR4, consultado em [19/08/2011]

VATIS, Michael (2001). *Cyber Terrorism and Information Warfare: Government Perspectives*, Transnational Publishers, Inc.. Internet: http://www.terrorismcentral.com/Library/Teasers/vatis.html, consultado em [19/08/2011]

WACKS, Raymond - *Privacy: A Very Short Introduction*. OUP Oxford, 2010.

WILSON, Clay - *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service, 2005.

WILSON, Richard Ashby - *Human Rights in the "War on Terror"*. Cambridge University Press, 2005.

WordIQ.com (2010). *WordIQ.com Encyclopedia: Ronald Fisher – Definition*, WorldIQ.com. Internet: http://www.wordiq.com/definition/Ronald_Fisher, consultado em [19/08/2011]

WOZNIAK, Steve, MITNICK, Kevin D., SIMON, William L. - *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, 2003.

Anexos

A.1. Exemplo de música ciberterrorista do Valete

O cantor Valete (2009) pode ser considerado um ciberterrorista pois tem músicas partilhadas na Internet que incitam à violência e revolta contra nações democráticas Ocidentais como é o caso dos EUA, fazendo os terroristas parecerem os bons.

Apresenta-se a seguir a letra da música do Valete "Fim da Ditadura" que se pode encontrar no YouTube, e por isso acessível a qualquer pessoa:

" Yo, Valete, o people está a preparar um K.O. definitivo a América.
Vai haver uma concentração clandestina no México, em Guadalajara... e queremos saber se vais ou não?"

Valete:
Eu sou Valete, bro, e sempre quis ser regicida
Sacrificar a vida pela maioria oprimida
Sem contrapartida, pela revolução sou suicida
Reserva um bilhete de ida para mim, tou de partida
E vou com antiamericanismo que Mao Tse Tung propagandeara
Com a filantropia com que Platão revolucionara, outrora
Com aquele Marxismo que Trotsky impulsionara
Estou farto da senzala, chao, só me galas em Guadalajara
A minha aversão ao imperialismo não sara
Não quero fama, nem glória, dá-me só uma t-shirt de Che Guevara
Põe-me num 747, México aqui vou
Viajo lembrando de como a segunda torre se desmoronou
Depois de 15 horas de voo, meu Boeing aterrou
Já fora do aeroporto, houve um bro que me identificou

"irmão Valete, eu vim-te buscar para a concentração
Entra no carro só faltas tu para começar a acção"

Chegámos ao ponto rapidamente, assim clandestinamente
Provavelmente eu nunca vira pela frente tanta gente
Era uma cidade subterrânea cheia de dissidentes
Só resistentes e combatentes naquele contingente
Eu vi Sardar, Saramago, Mia Couto e Chomsky
Também vi os mentores do atentado de Nairobi
Nipónicos pa' vingar Hiroxima e Nagasaki
Fidel Castro, Arafat, Chavez e Khadafi
Activistas do Hamas, Jihad e Hezbollah
Zapatistas, Talibãs e bombistas da Fatah
Todos diferentes mas com um objectivo em comum:
Acabar com esta ditadura que a América implantou
A sede de vingança deixava todo o exército operante
Deram o sinal pa' nos reunirmos numa sala gigante
Em cima do palanque tava um fulano que elaborava o plano
Com style de saudita ou iraquiano, só queria saber quem é esse mano
Deixava toda a gente focada enquanto ele liderava

(Outro Revolucionário) "Yo Valete é o Bin Laden"

(Valete) "Bin Laden?!?"

Bin Laden
Voz alterada sem barba e com cara totalmente modificada
Eu não o curtia mas ele era o que a América merecia
Radical sem diplomacia, assim como se exigia
Formulou o plano perfeito pá' revolução que se pretendia
Tínhamos túneis subterrâneos até à cidade de Alexandria
Hackers bloqueavam a informação da NSA e da CIA
Tínhamos M1's, F 16's e muita artilharia, eu ria.

Informador

"Informação, informação.

As bases militares americanas em todo o mundo, já estão controladas pelas FARC, Al Qaeda e milhões de civis revoltosos.

O ataque aéreo ao pentágono está previsto para as 3h e 36 m.

Os ataques bombistas serão às 3h e 42 m

A invasão à Casa Branca ficará para 4h e 28m

Já sabem o que têm a fazer!"

Era um batalhão de insubmissos pa' acabar com aquela arrogância
Tava incluído na missão Invasão à Casa Branca
Que seria reforçada pelo movimento black panther
Garanto qu'América nunca vira tanta encrenca
Fomos pelo túnel a dentro e chegámos em meio-dia
Alexandria tinha como Washington, cidade vizinha
E quando lá cheguei era inenarrável o que eu vira
América já ardia, rendida à nossa investida
Ficaram na defensiva, deixámos tropas sem vida
Éramos só homicidas com ira, topa a chacina
Numa outra ofensiva, edifício da ONU caíra
Largámos bué da mísseis em New York, Carolina
Califórnia, Louisiana, Detroit e Virgínia
Geórgia, Indiana, Illinois, Pensilvânia e Kansas
Ás quatro e um quarto já tava tudo controlado
Nossos soldados já tinham a Rádio a TV e o Pentágono
Passado mais um bocado, Fidel leu o comunicado
"Acabou a Ditadura" podes crer é o golpe de estado.
E à porta da Casa Branca fiquei com Bin Laden a sós
Disse-lhe sem hesitar um coche: Deixa-me liquidar o George
Ele esboçou um sorriso e olhou-me fundo nos olhos
Sentiu segurança na minha voz e passou-me uma Kalashnikov
Era só ódio destrutivo na minha cabeça
Kalash fui exibindo assim a dar paleta

Eu fui o homem escolhido pa' ditar a sentença
Olha o meu peito erguido pa' vingar o planeta
Entrei na Casa Branca assim cheio de moral
Nossos snipers iam abatendo a escolta presidencial, eu andava
No piso inferior de corredor em corredor.
Abria porta a porta à procura daquele estupor...
Vi a porta dos fundos, senti um feeling interior.
Abri... até que enfim seu Ditador!..
Agora sente o pavor!
Vais pagar pela tua m*rda e pela dos teus antecessores!
Isto é pelas vítimas das guerras que vocês fabricaram!!
Pelas bocas que morreram pela falta de pão que vocês negaram!!
Pelo terror que semearam, alastraram, perpetuaram!!
Pelos homens e mulheres que as vossas bombas mutilaram!!
Pelo suor dos trabalhadores que vocês escravizaram!!
Pela alma deste planeta que vocês danificaram!!
Morre Filho da P*ta!!

A.2. Filmes sobre *hackers*

A seguir descrevem-se (IMDb, 2011) alguns filmes mais marcantes sobre *hackers* com algumas bases em factos verídicos:

– **WarGames (Jogos de Guerra):**

Ano: 1983

Director: John Badham

Escritores: Lawrence Lasker e Walter Parkes

História do filme:

Um jovem rapaz génio informático acidentalmente consegue ligar-se a um supercomputador ultra secreto que tem controlo total sobre o arsenal nuclear dos EUA.

É-lhe colocado então um desafio para um jogo entre a América e a Rússia, e o rapaz inocentemente inicia a contagem decrescente para a Terceira Guerra Mundial e ele tenta convencer o computador que só queria jogar e não a coisa real.

- **Sneakers (Heróis por acaso):**

Ano: 1992

Director: Phil Alden Robinson

Escritores: Phil Alden Robinson e Lawrence Lasker.

História do filme:

Martin Bishop é o líder de um grupo de peritos na avaliação de sistemas de segurança. Quando é chantageado por agentes do governo para roubar uma caixa negra ultra secreta, a sua equipa vê-se enrolada num jogo de perigo e intriga.

Após recuperarem a caixa, fazem a descoberta surpreendente que esta permite descodificar todos os sistemas de cifra existentes no mundo e que os agentes que os contrataram afinal não trabalham para o governo.

- **The Net (A Rede):**

Ano: 1995

Director: Irwin Winkler

Escritores: John D. Brancato e Michael Ferris

História do filme:

Angela Bennett é analista de *software* e trabalha a partir da sua casa, onde passa grande parte do seu tempo, e tem poucos amigos fora do ciberespaço.

Ao gozar as suas primeiras férias em anos, vê-se envolvida numa rede de espionagem informática e vê os seus registos de identidade alterados.

- **Hackers:**

Ano: 1995

Director: Lain Softley

Escritores: Rafael Moreu

História do filme:

Um rapaz jovem é preso pela CIA por programar um vírus informático e é impedido de usar computadores até fazer 18 anos. Anos mais tarde, ele e os seus novos amigos descobrem uma trama para lançar um perigoso vírus informático, e têm de usar os seus

dotes informáticos para descobrir as provas enquanto são perseguidos pela CIA e pelo maligno génio informático por detrás do vírus.

A.3. *Botnet* usada para ataques de *SPAM*

Fonte: Tom-b, ilustrador de São Paulo, Brasil.

Figura 9 – Botnet a fazer ataque de SPAM

Um exemplo simples de como um criminoso compromete computadores pessoais e faz ataques de *SPAM* em grande escala:

1. O operador da *botnet* envia *malware* que infecta vários computadores;
2. O *bot* nos sistemas infectados acede a um servidor C&C;
3. Um *Spammer* paga o aluguer da *botnet* ao *bot herder*;
4. O *bot herder* dá instruções à *botnet* para enviar mensagens de *SPAM* em grande escala através de servidores de correio electrónico, causando perturbações nos serviços de correio electrónico e enchendo as caixas de correio dos destinatários com lixo ou com *malware*.