À Marizé, à Ana e à memória do meu sogro, Sr. António Rios

# Agradecimentos

O trabalho de doutoramento é eminentemente solitário, mas não seria possível sem a preciosa colaboração de muitos que, de uma forma generosa, deram a sua contribuição para o sucesso deste projecto. Não posso, assim, deixar de expressar o meu profundo agradecimento:

- Em primeiro lugar aos meus orientadores, Prof. Doutor Henrique Santos e Prof. Doutor Leonel Santos, pela sua dedicação, empenho, sapiência e rigor. Agradeço também a amizade que me dedicaram e o apoio nas alturas mais difíceis.

- Aos muitos alunos de licenciatura e de mestrado que participaram nas avaliações das tecnologias, pela sua contribuição voluntária e postura sempre prestável. Seria fastidioso enumerar todos, mas não me esqueço de nenhum... muito obrigado.

- À Prof. Doutora Maria da Graça Alves, da Universidade Católica Portuguesa, e ao Prof. Doutor Luís Amaral, ao Prof. Doutor João Álvaro de Carvalho e ao Prof. Doutor Henrique Santos, da Universidade do Minho, por me darem a oportunidade, durante os últimos anos, de leccionar e investigar em instituições com prestígio e rigor.

- Aos meus colegas e amigos do Departamento de Sistemas de Informação da Universidade do Minho e da Faculdade de Ciências Sociais da Universidade Católica Portuguesa, por todo o apoio e incentivo que me deram, mesmo nas alturas mais difíceis.

- Ao Eng.º António Graça, da Universidade Católica Portuguesa, pela paciência para me ouvir e pelas palavras de incentivo, sempre que as forças me faltaram.

- Aos autores e editores que me autorizaram a reprodução das suas imagens.

- Ao meu grande amigo Dr. Nuno Casalta, pela constante preocupação e pela amizade incondicional que sempre me dedicou.

- À minha mãe, D. Delmina Tenreiro, por uma vida de esforço dedicada à minha formação.

- À minha filha Ana, pelos seus sorrisos e pelas traquinices que dão sentido ao meu trabalho.

- À minha querida mulher... tanto à Prof. Doutora Maria José, pela partilha da sua experiência na investigação e pelos seus conselhos sempre sábios, como à Marizé, que esteve sempre lá, para tudo, de tal forma que as palavras não chegam para agradecer.

**Resumo:** Os processos de autenticação representam, em qualquer sistema, um ponto crítico que exige processos confiáveis, dado que são a base para o estabelecimento das relações de confiança que estão subjacentes aos privilégios atribuidos a cada utilizador. Tradicionalmente, estes processos baseiam-se na partilha de um segredo entre o utilizador e o sistema: a palavra chave. No entanto, diversos estudos mostram que os sistemas de código secreto apresentam diversas vulnerabilidades como a sua transmissibilidade que pode acontecer voluntariamente ou involuntariamente. Além disso, as palavras passe são, em si mesmo, uma contradição, já que têm que ser longas, complexas e mudadas com frequência para serem seguras, mas não o podem ser porque a capacidade humana de memorização é limitada, especialmente porque não deve haver reutilização de palavras chave e, cada vez mais, o utilizador é chamado a registar-se e a escolher uma palavra passe num número crescente de sistemas. A solução poderia passar pela exigência de apresentação de um determinado objecto que acrescenta um nível de segurança aos processos de autenticação, mas ainda assim não fica ultrapassada a questão da transmissibilidade. A solução parece ser a utilização de biometrias que, avaliando o que o utilizador é, ao invés daquilo que sabe ou possui, se apresentam como um recurso valioso para o incremento da segurança da autenticação.

Os serviços prestados pelo Estado aos cidadãos apresentam-se cada vez mais como estratégicos para o desenvolvimento do país, aumentando a produtividade dos serviços e dos utentes, ao permitir a diminuição do número de funcionários públicos e do tempo gasto pelos utentes em filas nas repartições públicas. No entanto, por representarem simultaneamente uma forma de relação crítica entre o cidadão e o Estado e uma porta de entrada nos sistemas estatais, estes sistemas requerem processos de autenticação ainda mais confiáveis. No entanto, a necessária universalidade dos serviços prestados impõe ainda mais exigências aos processos adoptados, que não podem exigir *hardware*, *software* ou competências específicas.

Este doutoramento tem como objectivos demonstrar a existência da necessidade de utilização de tecnologias biométricas comportamentais nos serviços electrónicos do Estado, demonstrar a existência de algoritmos compatíveis entre si e com e com as diversas plataformas de acesso lógico aos serviços, demonstrar a possibilidade de integração com os sistemas existentes e, após avaliação, concluir a existência de níveis satisfatórios de qualidade dos algoritmos criados, nomeadamente no que respeita ao nível de segurança (precisão e dificuldade de transmissão do segredo), nível de aceitação da tecnologia e nível de conforto (facilidade de utilização, de memorização do segredo e da sua troca regular). Estes objectivos resultam, na sua globalidade, na demonstração da viabilidade da utilização de biometrias comportamentais para a autenticação do cidadão perante os serviços electrónicos do Estado e foram alcançados através de diversas metodologias de investigação, de acordo com a sua adequação para cada objectivo: estudo-de-caso, prova de conceito, amostragem aleatória e sondagem.

Os resultados apresentados demonstram, por um lado, a necessidade de proceder a melhorias substanciais nos processos de autenticação existentes e, por outro, a existência de algoritmos biométricos comportamentais que satisfazem os requisitos impostos, em particular uma combinação de *keystroke dynamics*, uma biometria que avalia a forma como um texto é digitado, com *pointer dynamics*, uma nova biometria proposta que recorre à avaliação comportamental da forma como é efectuada uma autenticação gráfica.

O sistema proposto apresenta níveis de fiabilidade satisfatórios (embora exista margem para melhorias nos algoritmos), dispõe de processos automáticos que reduzem significativamente as vulnerabilidades dos sistemas actuais, é facilmente integrável com os sistemas existentes, tem uma boa aceitação pelos utentes, respeita a actual legislação nacional e não está abrangido por nenhuma patente conhecida na Europa ou nos Estados Unidos da América.

**Abstract:** The authentication processes are, in every system, a critical aspect that requires processes that can provide an adequate level of trust, once they are the base for the privilegies that will be granted to each user. Traditionally, those processes involve sharing a secret between the system and the user: the password. But several studies show that the password's systems present several vulnerabilities such as their transmissibility, that can happen both voluntarily or not. Besides that, passwords are them selfs a contradiction, once they must be long, complex and frequently changed in order to be secure, but they cannot satisfy all of those requirements once the human memory has limitations, specially when there is a requirement not to reuse passwords and one faces an increasing number of systems, all of them requiring a password. The solution could be in the use of a token, providing an extra security level to the authentication processes but the token can also be transmitted to an illegitimate user. The solution seems to be in the use of biometric technologies that, by evaluating what the user is, instead of what he knows or has, are an valuable resource in the increase of the authentication security.

The services provided by the Estate to citizens are of an increasing strategic value for the development of the country, increasing the productivity of both the services and the users, by allowing a reduction on the number of public servants and on the time spent by the citizens of queues. But, once they simultaneously represent a critical form of relation to the Estate and a door to the Estate's systems, they must ensure even safer authentication processes. Furthermore, the universality, that must be granted in the services provided, is another requirement to be fulfilled, once the system cannot demand specific hardware, software or skills.

This thesis has as objectives to demonstrate the existence of a need to use behavioural biometric technologies in the electronic services of the Estate, demonstrate the existence of algorithms compatible between them and with the several existing platforms, demonstrate the possibility of integration with the existing authentication systems and, after evaluation, conclude of the existence of

satisfactory quality levels of the created algorithms, namely to what concerns to the security level (precision and possibility of transmission), technology acceptance and confort level (easiness of use, secret memorization and frequent exchange). These objectives were achieved through several research methodologies, according to their adequacy to each objective: case study, proof of concept, random sampling and probing.

The presented results show thar their is a need to significantly improve the existing authentication processes and the existence of behavioural biometric algorithms that meet the demanded requirements, namely a combination of keystroke dynamics, a technology that evaluates the way that the user inserts a text, with pointer dynamics, a new biometric technology that evaluates the behaviour of the user when inserting a graphical authentication secret.

The proposed system presents satisfying precision levels (although there is space for improvements), presents automatic processes that reduce the existing systems' vulnerabilities, it is easily integrated with the existing systems, it has a good user's acceptance level, it respects the national legislation and it is not covered by any patent published in Europe or in the United States of America.

# Índice de conteúdos

# Índice de ilustrações

# Índice de tabelas

# Introdução

A segurança dos Sistemas de Informação é uma disciplina que atravessa horizontalmente diversas actividades das organizações, podendo afectar significativamente (sobretudo a falta de segurança) o seu desempenho. Desde questões tecnológicas até questões culturais e comportamentais, é possível encontrar diversos trabalhos que procuram responder a velhos e novos desafios que se levantam, provenientes de novos modelos de organização e, sobretudo, de uma evolução tecnológica notável. A autenticação fraudulenta pode acarretar custos elevados para uma organização e a procura de um método de autenticação que respeite os requisitos impostos tem sido objecto de investigação intensa. No entanto, tradicionalmente, envolve sistemas que têm a ver com a partilha de um segredo entre utilizador e objecto de segurança. Um dos problemas deste método é a transmissibilidade do segredo que, como qualquer outro, pode ser cedido (voluntariamente ou não) por quem o conheça a terceiros. Outro problema deste método é a necessidade de armazenamento ou memorização do segredo. Quando o segredo é armazenado, naturalmente herdamos o conjunto de vulnerabilidades que o(s) sistema(s) de armazenamento evidencia(m). Quando o segredo é memorizado pode ser esquecido, o que normalmente leva à escolha de segredos simples que facilitem a respectiva memorização, com consequências graves para as vulnerabilidades associadas.

A resposta a estas questões pode passar por soluções que permitam complementar os métodos existentes de autenticação com algum factor de identificação inerente ao sujeito autenticado, que dispense a criação arbitrária de segredos. É assim que surge, no contexto da autenticação, a autenticação biométrica, isto é, a utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um Sistema de Informação de uma organização.

No final do século passado, com a proliferação das tecnologias informáticas (nomeadamente o computador pessoal) e o avanço dos estudos sobre biometrias, tornou-se viável a implementação de autenticação por recurso a características físicas dos indivíduos. No entanto, estas soluções, além das dificuldades técnicas, acarretavam algumas dificuldades de carácter social, já que a novidade da tecnologia incutia alguns receios na população, agravados pela desconfiança criada pelos frequentes erros, normais numa fase embrionária de qualquer tecnologia.

Com a generalização de equipamentos de captura de características biométricas físicas e com a sua divulgação em filmes de grande sucesso, o cidadão comum encara hoje a autenticação biométrica como algo que lhe é familiar, embora alguns ainda não se sintam confortáveis com a sua utilização. Os resultados de um inquérito realizado pela epaynews (www.epaynews.com) em Dezembro de 2004 indicavam que 36% dos inquiridos afirmam preferir um sistema biométrico para a sua autenticação ao realizar pagamentos com cartões, enquanto que apenas 9% prefere a verificação da assinatura. Este nível de confiança só era igualado pelos códigos numéricos designados por PIN – *Personal Identification Number*. Por outro lado, o medo provocado pelo terrorismo, nomeadamente o atentado de 11 de Setembro de 2001 ao World Trade Center, levou os governos a aumentar os gastos em aquisição de tecnologias biométricas para autenticação de indivíduos na sua qualidade de cidadãos ou de funcionários (IBG, 2003) tornando-os, através da generalização do seu uso, mais habituais, com a consequente evolução na curva de adopção destas tecnologias.

Ao longo dos anos a investigação científica tem-se dedicado também ao estudo de biometrias que não avaliam características físicas, mas sim comportamentais, como a forma como um utilizador digita os caracteres num teclado, a forma como um cidadão caminha num corredor ou a força com que aperta o manípulo de uma porta ao abri-la. No entanto, estes estudos foram sempre realizados de uma forma isolada do contexto, normalmente limitando-

-se à aplicação a um pequeno conjunto de dados de uma determinada técnica com vista à obtenção de uma ou mais regras de decisão. Estes trabalhos isolados do contexto apresentam aspectos negativos determinantes, como a não generalização. Por exemplo, a forma de digitação de texto num teclado não é aplicável a sistemas de informação que incluam componentes móveis como PDAs e telemóveis de terceira geração; a forma de caminhar ou a pressão exercida sobre um manípulo de uma porta poderão ser um dia elementos de autenticação, mas ainda se encontram numa fase inicial do seu desenvolvimento e só poderão ser utilizados para controlo de acesso físico, nunca para acesso lógico.

Nesta tese pretende-se demonstrar que é viável utilizar as biometrias comportamentais para a autenticação electrónica do cidadão perante os serviços da administração pública, fazendo-o com vantagem significativa e sem um esforço considerável de alteração dos sistemas existentes. É claro que esta demonstração implica a possibilidade de utilização destas tecnologias também noutros contextos, mas a autenticação perante a administração pública é um desafio único, já que não pode ser limitativa. Enquanto uma empresa pode escolher um público-alvo para os seus produtos e/ou serviços e desenvolver uma tecnologia que lhe seja adequada, o governo central, regional ou local não pode excluir ninguém. Os serviços electrónicos devem estar acessíveis a todos, mesmo que em computadores colocados nas juntas de freguesia e com o apoio dos seus funcionários e, portanto, a autenticação não deve exigir ao cidadão que saiba, por exemplo, escrever. Neste contexto, a autenticação por palavra passe não pode, ou pelo menos não deve, ser utilizada. Também as tecnologias biométricas físicas devem ser evitadas por exigirem hardware específico, que poderá não estar disponível, para a captura das características do cidadão. Por exemplo, não é razoável assumir que todos os utilizadores têm um leitor de impressão digital para procederem à autenticação num sítio Web do Estado, mesmo que muitos computadores já incluam leitores destes dados biométricos.

A avaliação dos sistemas biométricos foi cuidadosamente estudada, essencialmente nos finais da década de 1980 e no início da década de 1990, tendo resultado na criação de alguns documentos orientadores desse processo. Destes, destaca-se o BEM – Biometric Evaluation Methodology Supplement (Common Criteria Biometric Evaluation Methodology Working Group, 2002), um suplemento do Common Criteria – Common Methodology for Information Technology Security Evaluation (Common Criteria for Information Technology Security Evaluation, 2006). No entanto, as abordagens propostas não são, no seu todo, adequadas ao contexto deste trabalho já que, por um lado, destinam-se à avaliação de um sistema completo e operacional que inclua um dispositivo dedicado à captura dos dados biométricos; por outro lado, propõem testes que se destinam à avaliação da qualidade, robustez e estabilidade do dispositivo de captura, o que é fundamental para a avaliação de biometrias físicas, mas completamente desadequado na avaliação das biometrias comportamentais em estudo, por não existirem perdas na recolha dos dados (não faria sentido repetir um processo de captura de tempos de digitação apenas para verificar quantas vezes seria possível recolher esses tempos, já que sabemos que essa recolha é sempre possível). Ainda assim, o contexto ambiental terá de ser levado em conta, embora de formas muito diferentes. Para a demonstração da tese optou-se por decompor este estudo de viabilidade em problemas de menor dimensão, simplificando a demonstração e permitindo recorrer em cada problema à metodologia que é mais adequada para encontrar a resposta que lhe está associada. Os objectivos desta tese serão, seguindo sempre que possível as recomendações do BEM:

- Demonstrar a existência da necessidade de utilização de tecnologias biométricas comportamentais nos serviços electrónicos do Estado.
- Demonstrar a existência de algoritmos compatíveis entre si e com e com as diversas plataformas de acesso lógico aos serviços.
- Demonstrar a possibilidade de integração com os sistemas existentes.

- Após avaliação, concluir a existência de níveis satisfatórios de qualidade dos algoritmos criados, nomeadamente no que respeita ao nível de segurança (precisão e dificuldade de transmissão do segredo), nível de aceitação da tecnologia e nível de conforto (facilidade de utilização, de memorização do segredo e da sua troca regular).

O conjunto dos objectivos desta tese confluem para o objectivo mais global: demonstrar a viabilidade dos processos biométricos comportamentais no contexto dos serviços estatais.

As metodologias de investigação adoptadas serão distintas de acordo com o objectivo a alcançar. A demonstração da necessidade será feita por inferência a partir do estudo de casos suficientemente documentados. A existência dos algoritmos de autenticação, de integração com os sistemas existentes e de troca regular da palavra secreta nos sistemas de autenticação gráfica (implícita, mas desconhecida do utilizador) será feita por apresentação dos algoritmos que respondem a cada uma dessas necessidades, isto é, por prova de conceito. A avaliação da precisão será feita através do estudo do estado-da-arte e, como é tradicional nesta área de estudo, por amostragem aleatória simples nos novos algoritmos propostos. Por último, os parâmetros de carácter subjectivo serão avaliados por sondagem, recorrendo ao Technology Adoption Model.

Os capítulos que se seguem tentam reflectir na sua organização as fases correspondentes à demonstração da tese. Assim, o primeiro capítulo descreve o contexto actual da utilização das tecnologias biométricas pelas organizações governamentais, enquanto o segundo aborda a problemática da autenticação nos serviços electrónicos do Estado demonstrando, através dos estudos de caso, a necessidade de introduzir um factor acrescido de segurança nos correspondentes factores de segurança. Estes estudos de caso demonstram que existem diversos grupos, com interesses distintos, que têm em comum o interesse no ataque aos sistemas electrónicos operados pelo Estado e em especial naqueles que fornecem serviços ao cidadão ou que permitem a divulgação de informação ao público e à comunidade internacional. Mais do que

o interesse, eles têm ou terão a breve prazo a capacidade para o fazer. O capítulo 3 é dedicado às tecnologias biométricas em geral, apresentando a sua descrição e o contexto legal da sua utilização em Portugal, de acordo com as recomendações efectuadas pelo BEM, embora este seja facilmente alterável para se adequar às necessidades do sistema adoptado, uma vez que a entidade adoptante das tecnologias em estudo é o Estado, que é também a entidade legisladora. O capítulo 4 apresenta as contribuições deste doutoramento no âmbito da tecnologia biométrica comportamental denominada dinâmica de digitação ou *Keystroke Dynamics*, recorrendo à teoria dos *Rough Sets*, a contribuição com uma nova tecnologia, desenvolvida para responder a alguns dos requisitos encontrados: o *Pointer Dynamics*, que reúne a avaliação de parâmetros comportamentais biométricos com a tecnologia de autenticação gráfica e a apresentação dos algoritmos para integração das tecnologias apresentadas com os sistemas existentes. Este capítulo inclui também o estudo das componentes subjectivas da avaliação de qualidade do sistema proposto. Este trabalho termina com a apresentação das conclusões da tese e das propostas de trabalho futuro.

# 1 A autenticação biométrica nas organizações governamentais

A tecnologia de autenticação biométrica tem sido utilizada pelos governos ocidentais para reforçar os métodos de combate ao banditismo, embora ainda só tenham sido utilizadas as características físicas dos indivíduos, nunca as comportamentais.

Recentemente, os Estados Unidos da América (EUA) decidiram fotografar (com o objectivo de utilizar as imagens em sistemas de reconhecimento facial) e recolher as impressões digitais (electronicamente) dos visitantes estrangeiros que entrem no país com um visto no seu passaporte. Por outro lado, exigiram aos países com acordos que dispensam os seus cidadãos de vistos em estadias curtas a criação de um sistema tendo em vista a introdução de dados biométricos nos seus passaportes, até 26 de Outubro de 2004. Os passageiros dos países que não conseguiram cumprir este prazo sujeitaram-se então, à chegada ao aeroporto, à introdução de dados biométricos (duas imagens digitais do dedo indicador e uma fotografia digital) no sistema norte-americano (U. S. Department of Homeland Security: Machine-Readable Passport Requirement, 2004; U. S. Department of State, 2004). Também o Reino Unido passou a recolher dados biométricos (impressão digital) dos cidadãos da Etiópia, do Djibuti, da Eritréia, da Tanzânia e do Uganda que solicitem um visto de permanência, bem como a todos os indivíduos africanos que viagem com o estatuto de refugiados. Além disso, o Reino Unido iniciou testes com o objectivo de introduzir dados biométricos nos novos bilhetes de identidade dos seus cidadãos (cartões únicos de identidade nacional), nomeadamente relativos à impressão digital e ao padrão da íris. Após as mais recentes negociações com os EUA, os países da União Europeia tiveram que introduzir nos seus passaportes informação relativa à face dos seus cidadãos até 28 de Agosto de

2006 e terão que introduzir a informação relativa à impressão digital até 28 de Junho de 2009. No entanto, vários grupos de defesa dos direitos civis têm-se manifestado contra a introdução da biometria no controlo de fronteiras. Numa carta enviada ao *International Civil Aviation Organization* (ICAO), a *Privacy International*, a *Statewatch*, a *European Digital Rights*, a *American Civil Liberties Union* entre outras associações, alegam que a introdução da tecnologia biométrica tem um efeito na perda de privacidade e de direitos civis que é desproporcional às vantagens de segurança que proporciona. Estes grupos criticam ainda a adopção por este organismo do reconhecimento facial como norma, invocando as altas taxas de erro desta tecnologia (Privacy International, Statewatch, & European Digital Rights, 2004). Os seus argumentos foram apresentados por estas instituições, em carta aberta, ao Parlamento Europeu (Privacy International et al., 2004).

Nas secções seguintes serão abordados com maior detalhe os casos que, por um motivo ou por outro, se destacam como paradigmas na utilização de autenticação biométrica por organizações governamentais.

## *1.1 Holanda*

Em Agosto de 2006, Lukas Grunwald, na altura consultor da Hacking Lab (uma empresa alemã que efectua testes de segurança a soluções informáticas), anunciou na DefCon 2006 ter quebrado o sistema de cifra utilizado pelos passaportes holandeses (Grunwald, 2006). Apesar da vulnerabilidade ser do processo de comunicação e não da componente biométrica do sistema, esta questão levantou alguma polémica entre a opinião pública. Por exemplo, o *The Guardian* (Johnson, 2006) questionou os processos implementados e afirmou que o método utilizado por Grunwald pode ser generalizado aos restantes passaportes, como os do Reino Unido e dos Estados Unidos da América, uma vez que os algoritmos de cifra só diferem no comprimento da sequência aleatória utilizada como semente. Na realidade esta alegação não é correcta, uma vez que o aumento do comprimento da sequência pode ser (actualmente é) sinónimo

de uma tal exigência computacional que impeça o sucesso do ataque. Além disso as autoridades defenderam-se com o facto de ser possível copiar os dados dos passaportes mas não ser possível alterá-los. No entanto, essas alegações não surtiram efeito, mantendo-se a oposição ao sistema até que a normal acção do tempo permitiu a recuperação da sua credibilidade. De facto, embora expressem algum receio relacionado com possíveis falhas na protecção da privacidade, uma parte significativa dos utilizadores reconhecem e valorizam a vantagem desta tecnologia no aumento do conforto e da segurança (Perakslis & Wolk, 2006). No pico da polémica levantada por Grunwald houve mesmo quem, partindo do facto de ser possível detectar a existência de um passaporte num bolso a dez metros de distância e de ser possível ler os dados biométricos nele inseridos, imaginasse atentados terroristas com bombas activadas pela presença de um determinado número de passaportes de uma determinada nacionalidade. Entraríamos então na era do terrorismo cirúrgico, um fenómeno que, em boa verdade, não é de excluir completamente!

## *1.2 Estados Unidos da América*

Os Estados Unidos da América (EUA) têm assumido um papel de liderança no desenvolvimento de tecnologias relacionadas com a segurança, mas os atentados terroristas de 11 de Setembro de 2001, em que aviões comerciais desviados por terroristas foram lançados contra o pentágono e contra as torres gémeas do World Trade Center, foram um factor impulsionador que levou os governos, não só o dos EUA, a aumentar o investimento em tecnologias biométricas de autenticação. Além da reacção natural aos atentados, causador de receios que justificam os investimentos, os estados parceiros dos EUA viram-se forçados a abordar a questão da tecnologia biométrica de autenticação por força das medidas de protecção de fronteiras impostas pelos EUA que, entre outras medidas, forçam os estados membros do acordo *Visa Waiver Program* a substituir os seus passaportes tradicionais por passaportes dotados de tecnologia biométrica e em conformidade com a norma ISO14443. Esses

passaportes são identificáveis por exibirem um símbolo (Figura 1) indicador da conformidade com esta norma.

*Figura 1 – Símbolo de compatibilidade com a norma ISO14443*

A utilização de tecnologia biométrica pelo governo norte-americano tem o seu expoente máximo, de acordo com um relatório interno do Parlamento do Canadá entretanto tornado público (Acharya, 2006), em três grandes sistemas:

Integrated Automated Fingerprint Identification System (IAFIS): é a maior base de dados biométricos do mundo e contava em 2006 com os dados da impressão digital dos dez dedos de 47 milhões de indivíduos.

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program: trata-se de um sistema criado pelo departamento de segurança interna (Department of Homeland Security) e colocado em prática em 2004 que compara as impressões digitais e a fotografia de visitantes seleccionados com os dados biométricos armazenados de indivíduos criminosos ou que tenham violado as regras de imigração. Os dados recolhidos são armazenados no IDENT (*Automated Biometric Identification System*), uma base de dados que inclui os dados constantes no IAFIS (o recíproco não é ainda verdadeiro). Este sistema tem sido instalado por fases, começando pelas entradas e saídas por via aérea e marítima, estendendo-se às passagens pelas fronteiras terrestres e terminando com a possibilidade de fazer as verificações de identidade remotamente sem intervenção do indivíduo avaliado (U. S. General Accountability Office, 2005). Este sistema tem sido alvo de críticas pelo *U.S. Government Accountability Office* (GAO) por alegadamente não estar a apresentar resultados que justifiquem o investimento (U. S. General Accountability Office, 2005).

Registered Traveler (RT) Program: trata-se de um programa essencialmente comercial, desenvolvido por entidades privadas sob a supervisão do Estado norte-americano. O objectivo é permitir a cidadãos idóneos que viajem com frequência, dispensar parte dos processos fronteiriços, mediante o pagamento de uma quota e o fornecimento de informações que facilitem a definição do seu nível de segurança. Os primeiros ensaios desta tecnologia foram realizados no final de 2006 no aeroporto de *Schiphol* na Holanda, apesar dos vários protestos de organizações como a *Air Transport Association of America*, que considera que este programa irá esvaziar a capacidade da *Transport Security Administration* para preparar programas que beneficiem a totalidade dos passageiros, ou a *American Civil Liberties Union* que considera que sugere que este programa força os cidadãos americanos a escolher entre preservar a sua privacidade e passar de uma forma mais célere no aeroporto além de representar uma vulnerabilidade no sistema de fronteiras norte-americano por poder permitir que um terrorista se registe com uma identidade falsa.

## *1.3 Espanha*

De acordo com a *Biometric Watch* (Biometric Watch, 2006) a *Siemens Communications Group* anunciou, no final de 2006, estar a participar no projecto de criação de um novo cartão de identificação biométrico que será disponibilizado em 2012 a 30 milhões de cidadãos espanhóis. A *Siemens* tem sido uma das empresas mais activas no desenvolvimento de produtos suportados pelas tecnologias biométrica e RFID – *Radio-Frequency Identification*, tendo conseguido diversos contratos para autenticação dos cidadãos através das suas características físicas como, por exemplo, a criação dos novos passaportes da Suíça.

O projecto espanhol, entretanto divulgado pelo *Ministério de Administraciones Publicas* de Espanha, denomina-se DNI Electrónico (DNIe – *Documento Nacional de Identidad Electrónico*) e pretende juntar num só documento as funcionalidades de identificação presencial, de autenticação

electrónica e de assinatura digital (com a mesma validade jurídica da assinatura manuscrita).

A introdução do DNIe representa a face visível da criação de uma *Public Key Infrastructure* (PKI) nacional, permitindo, por exemplo, a comunicação segura entre dois interlocutores equipados com este dispositivo. O DNIe, do tamanho de um cartão de crédito comum, dispõe de informação impressa, similar à apresentada nos cartões de identificação tradicionais (nome, apelido, sexo, data de nascimento, local de nascimento, filiação, morada, etc.) para leitura normal, informação de identificação para leitura mecanizada de acordo com as normas do ICAO para documentos de viagem (a informação é impressa em OCR-B, um tipo de fonte normalizada desenvolvida no final da década de 1960 para permitir o reconhecimento óptico de caracteres por equipamentos que respeitassem as normas da *European Computer Manufacturer's Association*) e informação cifrada contida num chip com capacidade de armazenamento e processamento interno (Figura 2).

As autoridades de certificação, que fazem a associação de um par de chaves a um cidadão em concreto, são quatro (uma de raiz e três subordinadas), todas do *Ministerio del Interior – Dirección General de la Policia*. A validade dos certificados armazenados no chip do DNIe, pode ser atestada a qualquer momento por uma das "autoridades de verificação", a *Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda* (para cidadãos, empresas e administração pública) e o *Ministerio de Administraciones Públicas* (apenas para a administração pública). Estas instituições, através do protocolo OCSP – *Online Certificate Status Protocol* – verificam, a pedido, o estado dos certificados, sem efectuar um relacionamento entre eles e as identidades dos cidadãos. Assim, não ficam numa só instituição registos que permitam relacionar os cidadãos com as suas actividades.

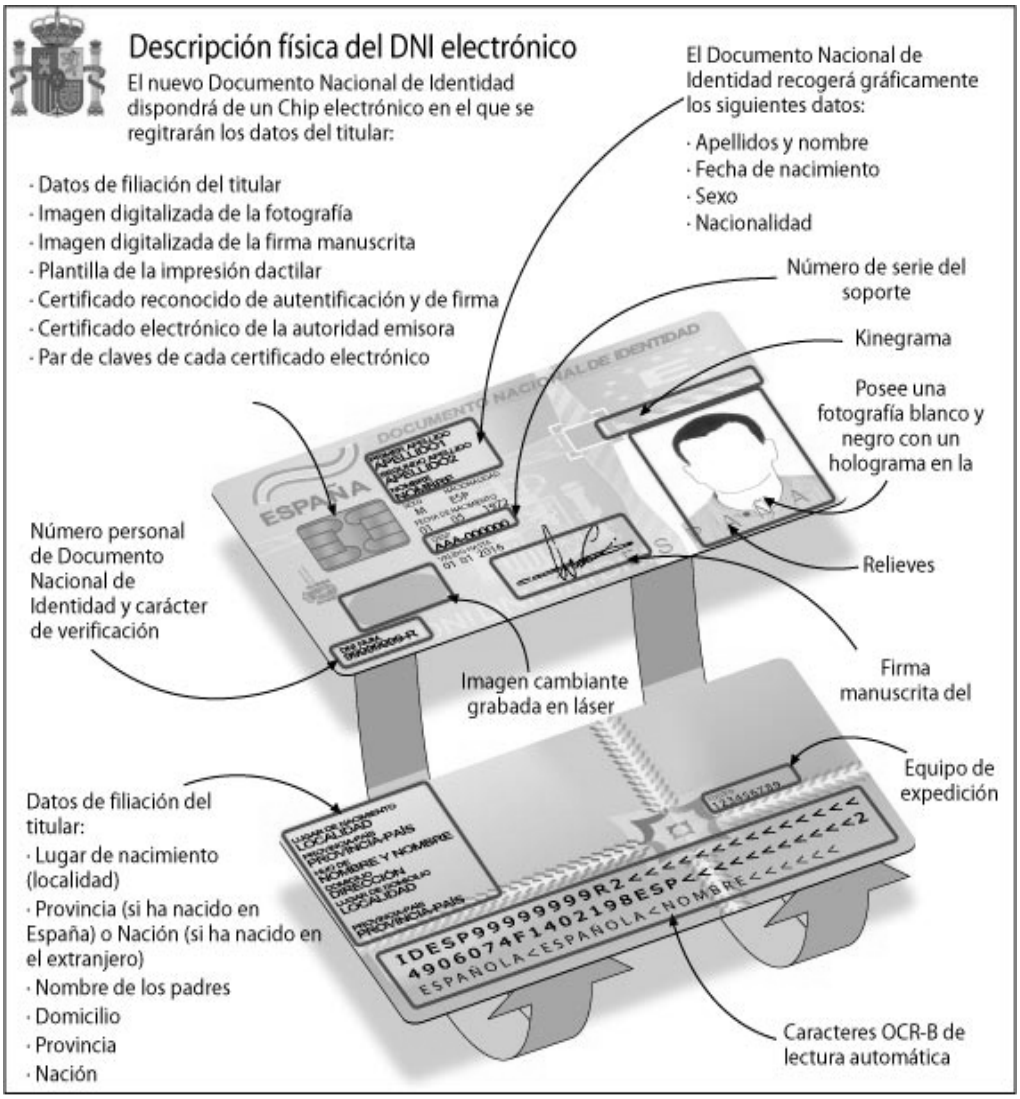



*Figura 2 – Descrição dos elementos contidos no documento de identificação espanhol (fonte: http://www.dnielectronico.es)*

## *1.4 Japão*

Em 2005 o Estado japonês anunciou estar a construir um estabelecimento prisional, de exploração privada, equipado com tecnologia de leitura dos padrões das veias dos dedos para autenticação dos reclusos (Kyodo News, 2005). Esta tecnologia foi combinada com câmaras de vídeo e sensores de movimentos para permitir a movimentação de reclusos no estabelecimento sem acompanhamento de guardas prisionais. A autenticação é realizada sempre que um recluso muda

de divisão para impedir que haja troca das etiquetas identificadoras entre os reclusos. Também neste caso se ouviram vozes discordantes, nomeadamente a Federação Japonesa de Associações de Advogados que considerou que a matéria não tinha sido suficientemente discutida, nomeadamente no parlamento.

A cadeia de Yamaguchi, denominada *Mine Social Reintegration Promotion Center*, recebeu os seus primeiros reclusos em Maio de 2007 (The Associated Press, 2007) e não há notícia de incidentes relacionados com o uso desta tecnologia. Esta cadeia é mista, tem capacidade para receber cerca de 1000 reclusos (500 homens e 500 mulheres, todos encarcerados pela primeira vez) e é pioneira no uso de diversas estratégias que visam a adaptação dos reclusos ao ambiente prisional como, por exemplo, a alteração da cor dos uniformes para laranja ou verde em substituição do tradicional e soturno cinzento, um passo de gigante se considerarmos a cultura japonesa, herdeira do código de conduta dos antigos guerreiros samurais – o *bushido* – que valoriza a humilhação em situações de desonra.

## *1.5 Angola, Haiti e Zâmbia*

Os primeiros países a anunciar a adopção de formas biométricas de autenticação nos processos eleitorais não foram as velhas nações democráticas. Nestas, os processos eleitorais foram estabilizados pela passagem dos séculos em ambiente de harmonia e o receio de alterar as metodologias que, embora lentas e mais assentes na confiança do que na certeza, nunca foram questionadas pelos eleitores, cria uma inércia conservadora que impede esses Estados de estarem na frente da revolução tecnológica. De facto, os primeiros países a anunciarem a adopção a uma escala nacional das tecnologias biométricas para suporte aos processos eleitorais foram o Haiti, Angola e a Zâmbia. Teoricamente estes países têm em comum, por um lado, a juventude das suas formas actuais de governo e a necessidade de rapidamente agilizarem os seus novos processos eleitorais de forma a obterem uma eleição realmente universal, por outro, a tradição de um Estado musculado pouco habituado a

auscultar os cidadãos, o que permite ultrapassar as resistências que estas tecnologias muitas vezes despertam.

Em Angola, um país do Sudoeste do continente africano (Figura 3), o processo de recolha digital de dados biométricos esteve a cargo de uma empresa portuguesa, a Sinfic S. A.. Este país, que esteve sob o domínio do império português até 1975, viveu 27 anos de guerra civil e teve as suas únicas eleições em 1992 mas o seu resultado não foi aceite pelos partidos derrotados, nomeadamente pela União Nacional para a Independência Total de Angola (UNITA) uma das facções beligerantes. O processo de independência e a guerra civil que se seguiu deixou a estrutura organizativa deste país com uma população estimada de um pouco mais de 12 milhões de habitantes (Embaixada da República de Angola em Portugal, 2008), num caos. A Sinfic deu início ao primeiro processo de recenseamento da Angola independente em 2004, com o objectivo imediato de restabelecer uma base de dados de pensionistas univocamente determinados, incluindo uma representação matricial da sua impressão digital. Mais tarde, a Sinfic recenseou mais de 7 milhões de cidadãos no processo de preparação das eleições que se realizarão brevemente.


*Figura 3 – Localização geográfica de Angola em África*

O caso do Haiti é paradigmático no que respeita à possibilidade de adopção de tecnologias biométricas nos processos eleitorais sem que exista uma compreensão da opinião pública sobre o tema. Este país das Caraíbas

(Figura 4) tem uma história complexa desde a descoberta da ilha *Hispaniola* por Cristóvão Colombo, passando pelo processo de independência e de sucessivas integrações e separações com a vizinha República Dominicana, até à ditadura dinástica do século XX do famoso tirano *Papa Doc* e do seu filho *Baby Doc* suportados pelo medo do vudu e pelo terror imposto pela sua tropa de elite. Em 1990 Jean-Bertrand Aristide venceu as eleições tidas como livres mas foi deposto um ano depois num golpe de Estado. Aristide recuperou o poder em 1994 após uma intervenção militar multinacional liderada pelos Estados Unidos da América. Estranhamente, as eleições de 2000 ficam manchadas pela suspeita de que Aristide e o seu partido tenham manipulado os resultados e a onda de suspeitas e de contestação só terminou em 2004 com um novo golpe de Estado que resultou no exílio de Aristide e na posterior entrada de uma força das Nações Unidas para a estabilização do Haiti. Em consequência deste golpe de Estado é agora Aristide quem, a partir da África do Sul onde está exilado, aponta o dedo ao último processo eleitoral decorrido em 2006 apelidando-o de traição contra o povo e levantando suspeitas de aniquilação dos seus apoiantes. Perante tal cenário, não é de estranhar que após ter sido anunciada que a realização de eleições em 2006 seria efectuada com recurso à tecnologia biométrica de autenticação por impressão digital fornecida pela Cogent Systems Inc. a única referência relevante sobre este assunto seja um documento do jornalista canadiano Andréa Schmidt (Schmidt, 2005) onde se questiona a universalidade deste tipo de recenseamento. Publicado pela primeira vez na revista norte-americana CounterPunch auto-intitulada como uma “Out of Bounds Magazine”, este artigo é reproduzido em inúmeros blogs e está publicado em diversas línguas em sites como o da Associação Resistir.info (http://resistir.info), do rebelión (http://www.rebelion.org) e do La Fogata Digital (http://www.lafogata.org).

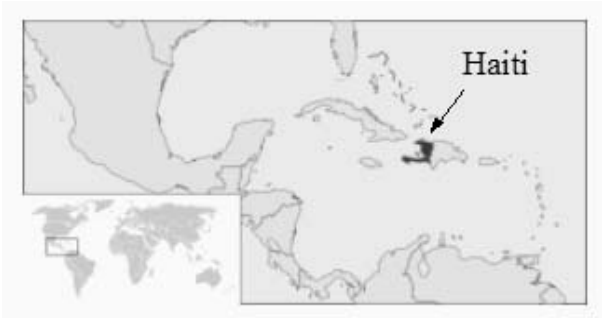



*Figura 4 – Localização geográfica do Haiti*

A Zâmbia é um exemplo paradigmático de utilização das tecnologias biométricas como forma de propaganda, permitindo uma exposição mediática que, quando comparada com a relevância do país no contexto internacional, é desproporcionada. Foi este o caso das eleições de 2006 na Zâmbia (presidenciais, parlamentares e autárquicas), um país africano (Figura 5) independente desde 1964 e que transitou para um sistema multipartidário em 1991 embora, como é habitual nestes casos, a transição para um sistema totalmente democrático tenha durado vários anos, culminando nas eleições de 2006 que foram reconhecidas por muitos, tanto nacional como internacionalmente, como livres e justas. Foram estas eleições de 2006 que foram amplamente noticiadas após a biometric watch divulgar que de acordo com a agência noticiosa Highway Africa o processo eleitoral decorreria com recurso às tecnologias biométricas de autenticação. Estiveram presentes nestas eleições mais de 500 observadores internacionais e o relatório do grupo de observadores da Commonwealth não menciona a utilização, mesmo que em zonas limitadas, de quaisquer tecnologias biométricas (Commonwealth Observer Group, 2006). Aliás, o relatório do Zimbabwe Election Support Network chega a descrever os processos de autenticação e de prevenção de repetição do voto em nome próprio ou de outro eleitor: cadernos eleitorais com fotografia distribuídos aos membros da mesa e tinta não lavável com “parafina ou outros químicos obscuros semelhantes”(The Zimbabwe Election Support Network, 2006).

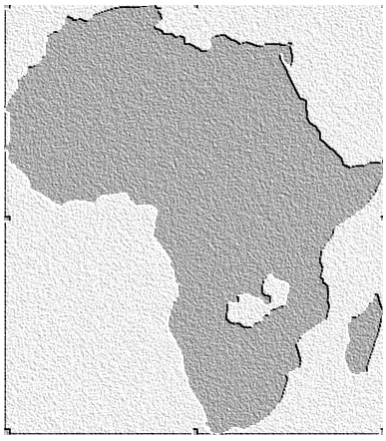


*Figura 5 – Localização geográfica da Zâmbia em África*

O exemplo da Zâmbia é bem ilustrativo da forma como o anúncio da utilização de tecnologia biométrica nas eleições tem servido o interesse daqueles que pretendem difundir uma imagem dos seus países de transição efectiva para a liberdade e democracia. Este processo é facilitado por algumas empresas fornecedoras de produtos e serviços de autenticação biométrica que, na procura de publicidade, se apressam a divulgar internacionalmente a assinatura dos acordos realizados com as nações com quem tiveram frequentemente casos anteriores de sucesso na implementação de soluções biométricas em áreas menos sensíveis, como as cartas de condução, ou na implementação de soluções que respondam às exigências de parceiros internacionais como é o caso da modernização dos passaportes.

# 2 A autenticação e o Estado electrónico

Os Estados têm aplicado os avanços processuais e tecnológicos desenvolvidos para o mercado empresarial para melhorar a qualidade do acesso e da disseminação dos serviços oferecidos aos cidadãos (Silcock, 2001). Em Portugal, alguns dos processos de interacção entre o cidadão e o Estado são já efectuados apenas de forma electrónica, por exemplo a entrega das declarações periódicas do Imposto sobre o Valor Acrescentado (IVA) e a candidatura aos concursos de colocação de professores do ensino básico e secundário, enquanto noutros serviços o processo electrónico coexiste com o processo tradicional, por exemplo a entrega das declarações do Imposto sobre o Rendimento das Pessoas Singulares (IRS). Mas em 2002 a presença do Estado na Internet era ainda essencialmente informativa, centrada na divulgação dos princípios de organização e funcionamento das instituições, da missão e no enquadramento legal de cada organismo, apesar de esta ser a data prevista pela *Iniciativa Internet* para a publicação *online* de todos os formulários oficiais e de estar prevista para 2003 a possibilidade generalizada de submissão electrónica e para 2005 a presença *online* de todos os serviços públicos (UMIC, 2003).

Por força das alianças estabelecidas (Organização do Tratado do Atlântico Norte, União Europeia, participação militar/militarizada no Iraque, no Líbano e no Afeganistão, organização da *Cimeira dos Açores*, etc.) e do Plano Tecnológico, também em Portugal o Estado electrónico está sob uma ameaça acrescida, uma vez que Portugal pertence ao grupo dos países alvo da *Jihad* electrónica, ou guerra santa electrónica (Al-Salem, 2003). Aliás, o *Plano de Acção para o Governo Electrónico* (Conselho de Ministros, 2003) apresentado pelo governo em Agosto de 2003 refere-se à necessidade de criação de um "Plano Nacional de Segurança" e coloca a segurança e a confidencialidade como condicionantes dos negócios electrónicos. A questão da autenticação assume-se, então, como fundamental e a(s) tecnologia(s) adoptada(s) deve(m) garantir elevados níveis de

fiabilidade e de conforto e baixos níveis de intrusividade, ao mesmo tempo que é necessário assegurar uma fácil integração com os meios existentes. Neste documento o governo refere-se explicitamente à necessidade da definição de uma *Public Key Infrastructure* (PKI) como uma forma de melhorar os níveis de segurança dos Sistemas de Informação. No entanto, as PKIs são vulneráveis quando não estão associadas a processos de autenticação seguros e o sucesso da sua implementação à escala governamental e inter-governamental está dependente da sua integração com as tecnologias biométricas (Tenreiro de Magalhães, Santos, & Nunes, 2006).

Com o objectivo de encontrar evidências que sustentem a necessidade de aumentar a segurança dos sistemas de autenticação nos processos electrónicos utilizados pelos Estados, foram usados diversos documentos que permitem o estudo de casos que se afiguram no actual contexto social como fundamentais para a compreensão do nível dos requisitos de segurança na autenticação perante os serviços electrónicos do Estado. As secções seguintes descrevem esses estudos e correspondentes conclusões.

## *2.1 Information Warfare*

O mundo físico está cada vez mais vulnerável a ataques no mundo digital, o ciberespaço, já que está cada vez mais dependente dos sistemas informáticos e da informação. De facto, só o sistema de informação do Departamento de Defesa dos Estados Unidos da América sofre todos os anos 250.000 ataques (DSCINT, 2005).

O recurso ao ciberespaço para condução de operações de carácter militar, enquanto mais uma frente de combate, embora se enquadre na guerra irregular, por não existirem frentes de combate ou retaguardas bem delineadas e ocorrer num espaço infinito (Oliveira, 2004), pode envolver a preparação e execução de operações militares realizadas pelas entidades de uma nação contra outra, com objectivos idênticos aos de uma guerra convencional e até tendo em vista o enfraquecimento das defesas convencionais, da comunicação e do controlo do

inimigo, de forma a enfraquecer a sua capacidade de resposta convencional (Bezerra, Nakamura, Lima, & Ribeiro, 2004). Isto pode significar a interferência, o controlo ou mesmo a destruição da informação e dos sistemas de poder civil e militar, de infra-estruturas críticas como centros de comunicação do sistema de emergência médica, transportes, energia, água e outros, podendo mesmo afectar os sistemas informáticos da população civil. Assim, as consequências de um combate no ciberespaço podem ser tão reais quanto os de uma guerra convencional, podendo mesmo causar baixas (Bezerra *et al*., 2004; Shimeall, Williams, & Dunlevy, 2002).

A expressão anglo-saxónica *Information Warfare* tem, consoante os autores, diversos significados. Na sua definição mais abrangente apresenta duas vertentes: a vertente militar, tradicionalmente da responsabilidade dos serviços de informações e executada com o objectivo de obter uma vantagem táctica sobre o inimigo, potencial ou real, e a vertente civil, normalmente de carácter comercial e executada com o objectivo de eliminar uma vantagem competitiva de um concorrente. Alguns autores preferem uma definição de *Information Warfare* mais restrita (mais próxima do conceito português de “Guerra da Informação”), limitando a aplicação deste termo a situações militares ou paramilitares. Estes autores utilizam o termo Competitive Intelligence, para classificar as actividades similares mas de carácter civil. Optou-se por adoptar a definição mais geral, considerando que a Guerra de Informação se aplica tanto no caso civil como no caso militar uma vez que, como se mostrará mais adiante, tanto as entidades civis como as entidades militares ou paramilitares estão, actualmente, envolvidas tanto em actividades civis como militares.

Quando perguntaram a Willie Sutton, um famoso assaltante de bancos, porque é que assaltava bancos, ele respondeu “*because that’s where the Money is*” (porque é onde está o dinheiro). Uma vez que, actualmente, a maior fonte de informação disponível é a Internet, é natural que ela se tenha transformado no palco principal das várias formas de Guerra de Informação.

Os Estados estão no centro de toda a movimentação relativa à guerra de informação, seja por se tratar de informação relativa às actividades tradicionalmente atribuídas aos organismos na dependência do Estado, nomeadamente organismos ligados à segurança e à defesa, seja por se tratar de informação com importância comercial que, pela sua natureza, possa interessar às indústrias estratégicas do país. Como a entrada no ciberespaço implica uma ligação das redes internas às redes externas, os organismos governamentais transformaram-se em alvos apetecíveis para todo o tipo de entidades, desde as organizações terroristas até aos outros estados, como se demonstra nos casos de estudo apresentados nas secções seguintes. Os dois primeiros referem-se a um ataque concertado às infra-estruturas tecnológicas de Estados independentes, a Estónia e a Geórgia, realizado de forma organizada ou por um governo estrangeiro, ou por um grupo de cidadãos de um Estado estrangeiro, consoante as fontes consideradas. O terceiro caso de estudo pretende aferir a capacidade tecnológica actual e potencial das entidades terroristas, aferindo-se também a forma como esses grupos podem beneficiar da Guerra da Informação. O quarto e último caso de estudo, refere-se ao envolvimento dos Estados na luta pela vantagem competitiva das empresas, com recurso à Guerra da Informação.

### 2.1.1 Ciberataques à Estónia (Abril/Maio de 2007)

#### A Sociedade da Informação na Estónia

A Estónia dispõe de uma estrutura governamental tecnologicamente avançada e faz da tecnologia um dos pilares do seu desenvolvimento, fruto de uma estratégia definida em 1998, que permitiu o desenvolvimento de uma boa rede de dados, de portais institucionais, de um programa para o uso das novas tecnologias no ensino e de uma infra-estrutura nacional de chaves públicas (PKI – *Public Key Infrastructure*) armazenadas nos cartões de identificação. Como consequência indirecta da estratégia adoptada, deu-se a generalização dos serviços prestados pelas empresas aos cidadãos, fruto da apetência da

população pela tecnologia, do ambiente motivador gerado e das estruturas disponíveis.

Em Novembro de 2006, o governo aprovou um plano de desenvolvimento sectorial, denominado Estratégia para a Sociedade da Informação 2013 (E*stonian Information Society Strategy 2013*, 2006), que define o contexto, os objectivos e as acções a realizar para a utilização das tecnologias de informação e comunicação no desenvolvimento de uma economia e sociedade baseadas no conhecimento. O plano apresentado inclui, à semelhança de outros planos tecnológicos entretanto desenvolvidos, como o Plano Tecnológico Português, a possibilidade de criar uma empresa em apenas duas horas, a disseminação do acesso *wireless* e a digitalização dos processos burocráticos. O plano apresentado define as tecnologias da informação e da comunicação como o pilar do desenvolvimento do país e assenta em três princípios:

- Cada indivíduo vive uma vida completa, recorrendo de todas as formas à tecnologia e participando activamente na vida pública (no documento apresentado pode ler-se "*nobody will stay or will be left behind*" – ninguém ficará ou será deixado para trás).
- O crescimento da economia da Estónia é baseado no uso generalizado das tecnologias de informação e comunicação.
- O sector público é centrado no utilizador, é transparente e é eficiente.

Esta evolução tecnológica permite à Estónia uma vantagem competitiva mas criou uma nova vulnerabilidade: a sua infra-estrutura de comunicações tornou-se um elemento crítico para a sua forma de vida.

## A ciberguerra

Em Maio de 2007 a Estónia entrou para a História como o primeiro país a ser alvo de um ataque sistemático à totalidade dos seus sistemas informáticos públicos, dirigidos apenas a esse país e tendo como objectivo a interrupção da totalidade dos seus serviços fundamentais: um ciberataque que, de acordo com o Ministério dos Negócios Estrangeiros da Estónia, foi proveniente em grande

parte de computadores de agências governamentais russas (Paet, 2007). O anexo I apresenta uma descrição da relação histórica (sempre conflituosa) entre a Rússia e a Estónia, o que pode ajudar a compreender algumas das razões deste conflito e das alegações apresentadas. Andres Tarand, deputado do Partido Social-democrata da Estónia no Parlamento Europeu, na sessão plenária em que se debatia a cimeira EU-Rússia afirmou mesmo que alguns dos rastos deixados pelos atacantes provinham do próprio Kremlin (Parlamento Europeu, 2007), apesar das autoridades terem também detido um jovem de 19 anos por, de acordo com a Procuradoria-geral da República citada pelo Sidney Morning Herald (“Estonian hold suspect over 'cyber-attacks'”, 2007), incitar, em diversos *fora*, à organização de ataques por *Denial of Service* contra vários servidores da Estónia, além de listar servidores passíveis de ser atacados e de descrever os meios para o fazer.

Em declarações à imprensa ("Cyberwarfare worries", 2007) Jose Nazario, um perito em segurança da *Arbor Networks*, declarou que a sua empresa encontrou sinais de nacionalismo russo, mas não encontrou sinais de um envolvimento governamental russo. Uma afirmação que pode corresponder à realidade ou pode ser apenas a resposta possível, dada a ausência de provas que definam o(s) culpado(s) por estas acções. A *Arbor Networks* assumiu algum protagonismo durante esta acção por ter divulgado publicamente estatísticas referentes aos ataques por *Distributed Denial of Service* realizados. As estatísticas divulgadas referem-se ao número de ataques por endereço IP (Tabela 1), ao número de ataques por data (Figura 6), ao número de ataques por duração (Figura 7), ao número de ataques por largura de banda utilizada (Figura 8) e ao número de ataques por protocolo (Figura 9).

| *Número de ataques* | *Endereço Web* | *Entidade* |
|---|---|---|
| *35* | pol.ee | Polícia |
| *7* | www.riigikogu.ee | Parlamento |
| *36* | www.riik.ee<br>www.peaminister.ee<br>www.valitsus.ee | sítio Web nacional<br>Primeiro-ministro<br>Governo |
| *2* | m53.envir.ee | Ministério do ambiente |
| *2* | www.sm.ee | Ministério dos Assuntos Sociais |
| *6* | www.agri.ee | Ministério da agricultura |
| *35* | www.fin.ee | Ministério das finanças |
| *5* | 213.184.50.6<br>62.65.192.24 | Outras não identificadas pela *Arbor* |

*Tabela 1 – Número de ataques por IP e correspondentes proprietários [1] ("Cyberwarfare worries", 2007)*

1 Os 2 IPs não identificados pela Arbor são, segundo a RIPE – Network Coordination Centre, propriedade da Starman (um fornecedor de televisão por cabo e de Internet) e do "Department of Data Communications, Estonian Informatics Center".

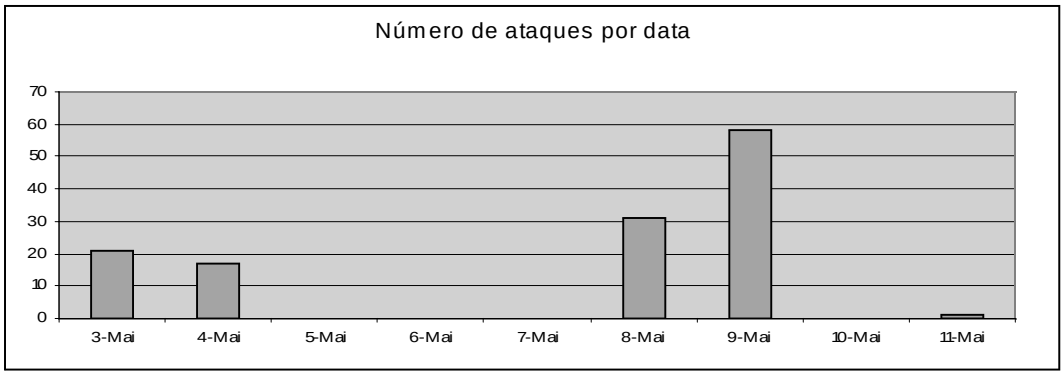



*Figura 6 – Número de ataques do tipo DDoS (Distributed Denial of Service) por data, ("Cyberwarfare worries", 2007)*

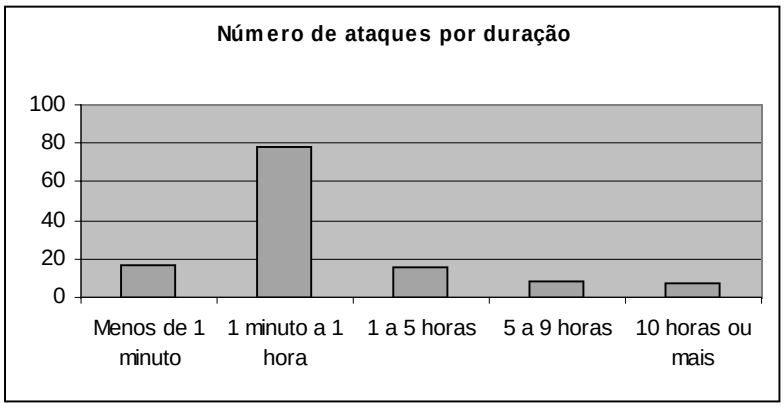



*Figura 7 – Número de ataques por duração, ("Cyberwarfare worries", 2007)*

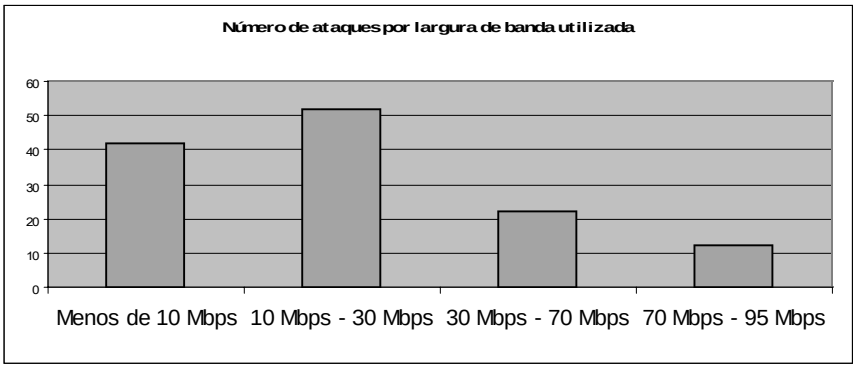



*Figura 8 – Número de ataques por largura de banda utilizada ("Cyberwarfare worries", 2007)*

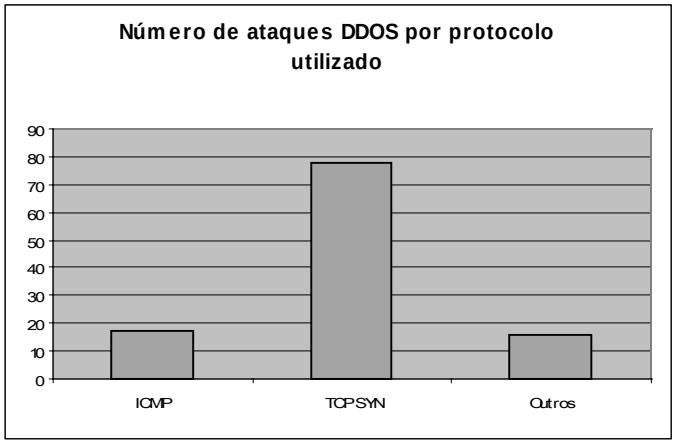



*Figura 9 – Número de ataques por protocolo utilizado ("Cyberwarfare worries", 2007)*

Outra possível justificação para a divergência entre os factos apresentados pela *Arbor Networks* e o Governo da Estónia, no que respeita à origem dos ataques, pode ser o âmbito dos dados. Se as duas entidades dispõem de indicadores aparentemente contraditórios, poderá ser apenas por não se referirem aos mesmos dados. Neste caso, considerando que a *Arbor Networks* só monitoriza ataques do tipo DDoS, isso poderá ser um indicador de que este ataque não se limitou a técnicas de DDoS, ao contrário do que foi inicialmente divulgado e ainda é amplamente difundido. Sabe-se que alguns sítios *Web* oficiais foram alterados para conter propaganda nacionalista russa, como é o caso dos sítios *Web* do governo da Estónia e do seu partido, o Partido Reformador da Estónia, de outros partidos da Estónia, de sítios *Web* noticiosos e comerciais. A Figura 10 apresenta uma imagem colocada num sítio *Web* alterado, onde se vê um soldado russo com a mensagem “Feliz Dia da Vitória! A vitória do meu avô é a minha”, enquanto que a Figura 11 apresenta o aspecto do sítio *Web* do partido do governo da Estónia alterado para apresentar, em russo, uma mensagem que indicava que a estátua seria reposta no antigo local e onde são pedidas desculpas ao povo russo. Estas situações foram amplamente divulgadas pela BBC News ("Estonia fines man for 'cyber war'", 2008; "Estonia hit by 'Moscow cyber war'", 2007; Jackson, 2007). Sabe-se também que foram

utilizadas técnicas de SQL *injection* (Ottis, 2008), embora não se conheça a dimensão deste tipo de ataques.


*Figura 10 – Sítio Web estónio com mensagens pró-Federação Russa*


*Figura 11 – Sítio Web do partido do governo da Estónia alterado*

Apesar dos imensos meios utilizados neste ataque concertado e das declarações oficiais do Governo da Estónia, a Rússia negou sempre qualquer envolvimento nestas acções e são muitos os que alegam que os IPs podem ser forjados e que, portanto, não se podem tirar conclusões sobre a origem dos ataques. Outros vão ao ponto de assegurarem que o ataque não é proveniente de uma estrutura governamental por ser bastante simples, o que não é um argumento que ponha um fim à discussão e, por último, existem aqueles que utilizam o facto de alguns sítios *Web* russos também terem sido atacados por Estónios (Figura 12) para, alegadamente, demonstrarem que estas acções foram

perpetradas por privados. Também estes ataques são negados pela Estónia, que apresenta como alegada prova da sua inocência o facto de existirem erros ortográficos nalguns desses sítios *Web*, incluindo no nome da sua capital, Tallin, que terá sido escrito incorrectamente (Ottis, 2008).

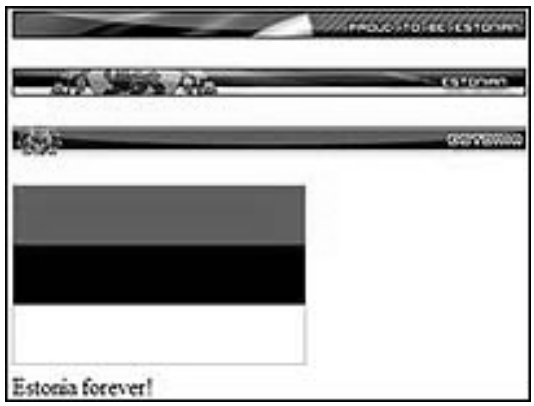



*Figura 12 – Também os sites russos foram atacados, ou contra-atacados*

Das várias possibilidades colocadas para enquadrar o ataque à Estónia, destacam-se a possibilidade de se tratar de uma reacção espontânea às decisões do parlamento da Estónia, a possibilidade de se tratar de uma *false flag operation* (uma operação realizada por terceiros sob a bandeira Russa, sem a sua autorização e com o objectivo de a fazer passar por responsável pelos eventos) e a possibilidade de se tratar, de facto, de um ataque da Federação Russa à Estónia.

A possibilidade de se tratar de uma reacção popular independente é contrariada pelo apoio indirecto das entidades governamentais russas que se recusaram a prestar apoio aos investigadores da Estónia e da NATO na localização dos responsáveis pelos eventos e que não forneceram os recursos necessários para assegurar a segurança física do embaixador e da embaixada da Estónia na Federação Russa, o que elimina, pelo menos, a possibilidade do ataque popular ser independente de organizações estatais (Ottis, 2008). Aliás, esta situação parece remeter para a estratégia oriental denominada “guerra do povo”, onde o papel do Estado é criar um ambiente favorável ao patriotismo e garantir protecção estatal aos cidadão que, em caso de conflito, decidam

envolver-se no combate (Wu, 2006; Jincheng, 1997). Assim, também esta possibilidade acabaria por significar que o que aconteceu, de facto, foi um ciberataque da Federação Russa à Estónia.

A possibilidade de se tratar de uma operação realizada sob uma falsa bandeira tem argumentos a seu favor: o ataque teve um início e um fim abruptos, com fases distintas direccionadas para níveis cada vez mais fulcrais da infra-estrutura da Estónia, podendo significar que não se tratou de um ataque com a utilização de todos os recursos disponíveis mas de um teste que serviu para obter lições para um ataque futuro, à semelhança das experiências realizadas por terroristas antes dos ataques físicos (McAfee, 2007). Também esta possibilidade parece menos provável pelo facto de a Federação Russa não ter prestado qualquer apoio no esclarecimento dos acontecimentos, o que neste caso levaria à declaração da sua inocência (Ottis, 2008). Mas este argumento não é definitivo uma vez que a situação gerou uma onda nacionalista que não era inconveniente para a Federação Russa e, num momento em que parece querer demonstrar a recuperação da sua operacionalidade, ficar com a fama deste acontecimento, sem ficar com as retaliações, pode ser até uma escolha agradável para os dirigentes russos que podem, assim, ter aproveitado esta situação para transmitir uma capacidade tecnológica que não têm. Por outro lado, o ataque pode ter sido realizado por um país que, por um motivo ou por outro (compra ou venda de petróleo, gás ou armamento, alinhamentos geopolíticos, etc.), pode contar com a discrição da Federação Russa.

Da globalidade dos elementos disponíveis é possível deduzir que o ataque teve alguma ligação à Federação Russa, mas se houve ou não uma primeira ciberguerra entre a Federação Russa e a Estónia não é possível, neste momento, afirmar. Depende do conceito de guerra assumido e da forma como os factos são interpretados. Houve, pelo menos, um conjunto de acções efectuadas de forma concertada por um grupo de indivíduos, poucos ou muitos, que poderão estar ligados a entidades governamentais ou não. Se a acção foi desencadeada por acção directa ou indirecta de um governo, então existiu uma ciberguerra pela

primeira vez na história. Se a acção é de um conjunto de indivíduos independentes que atacaram as estruturas de um Estado, de forma organizada, mesmo que *ad hoc*, com vista a fortalecerem/imporem a sua posição ideológica, então estamos perante o primeiro caso de ciberterrorismo (diferente de terrorismo tecnologicamente assistido). O que é certo é que este caso fez correr muita tinta nos jornais e, o que é mais importante, fez disparar os alertas de organizações internacionais de cooperação militar, já que as provocações de carácter militar efectuadas pela Federação Russa, como os voos de longo curso para treino de bombardeiros que alegadamente entraram em espaço aéreo da Grã-Bretanha ou as ameaças de retaliação contra o escudo anti-míssil que os Estados Unidos da América pretendem instalar na Europa, fazem daquela super-potência uma forte suspeita e, agora que os efeitos de uma ataque deste tipo são conhecidos, pelo menos parcialmente, os estados aliados compreenderam que o conceito de guerra pode estar a sofrer alterações que levarão a modificações nos seus conceitos estratégicos de defesa nacional e nos mecanismos de activação dos tratados internacionais de protecção mútua como, por exemplo, o Tratado do Atlântico Norte que é a base da NATO (*North Atlantic Treaty Organization*). Os anexos II e III apresentam, respectivamente, a evolução na forma e nos campos de batalha até chegarmos ao ciberconflito e os efeitos, deste conflito, que já se podem verificar nas alianças internacionais.

### A reacção aos ataques

A compreensão da reacção aos ciberataques, tanto políticas como tecnológicas, só pode ser completa se for enquadrada no contexto geopolítico e temporal. No que respeita ao contexto geopolítico, o enquadramento das relações entre as partes beligerantes está sintetizado no Anexo I, quanto ao contexto internacional é de salientar que a Federação Russa faz parte do Conselho de Segurança das Nações Unidas e pode, portanto, vetar qualquer resolução que lhe seja desfavorável. Acresce a este facto a evidente diferença de capacidade militar instalada dos dois países directamente envolvidos no

conflito, factor ainda mais relevante num momento em que a Rússia tenta recuperar a sua dominância nas regiões que lhe são fronteiras e, por último, a dependência energética da União Europeia que conta com o gás natural e o petróleo provenientes da Federação Russa para satisfazer 25% das suas necessidades destas matérias-primas, num momento em que esta controla 6% das reservas mundiais de petróleo e 34% das de gás natural e em que o petróleo bate recordes consecutivos. Já no que respeita ao contexto temporal dos ciberconflitos, muito há para dizer, já que as pequenas escaramuças têm já algumas dezenas de anos de história digna de ser relatada, conforme se pode constatar no Anexo II.

A Estónia, perante um ataque paralisante da sua estrutura económica e política fortemente dependente dos recursos tecnológicos, por sua vez dependente da Internet, não teve capacidade de resposta. As acções do governo da Estónia limitaram-se aos protestos perante as autoridades diplomáticas internacionais e a imprensa e à solicitação da intervenção dos seus aliados. A solução encontrada por várias organizações acabou por ser o corte de comunicações entre a Estónia e o resto do mundo, permitindo a continuação da prestação aos cidadãos dos serviços sedeados no país. Esta solução provisória criou dificuldades aos cidadãos da Estónia que se encontravam fora do seu país, uma vez que ficaram sem acesso aos serviços do seu Estado e das suas empresas, nomeadamente no que se refere ao uso de cartões bancários estónios para levantar dinheiro ou efectuar pagamentos fora da Estónia. Com o decorrer do ataque a lista de países com acesso aos sistemas sediados na Estónia foi sendo alargada de forma a incluir os países com muitos clientes mas poucos atacantes (Ottis, 2008).

A solução veio naturalmente com um simples regresso à normalidade, já que os ataques perderam a sua intensidade após o dia 9 de Maio, dia da *Vitória na Europa* na Federação Russa, um feriado nacional em que o país comemora a vitória na Europa na Segunda Grande Guerra. No entanto, este regresso à normalidade só é possível porque os ataques efectuados mantiveram sempre

uma posição exterior ao alvo, uma espécie de cerco ao "castelo" que acabou por ser "levantado". No entanto, se o ataque tivesse incluído a substituição de utilizadores legítimos por utilizadores ilegítimos, por exemplo por entrada forçada nas contas e posterior alteração das credenciais de acesso, toda a estrutura de autenticação nos serviços electrónicos da Estónia poderia estar afectada. Além dos efeitos imediatos que poderiam ocorrer em alguns casos (transferências bancárias para contas dos usurpadores, introdução de dados falsos nos sistemas de finanças, etc.), seria necessário registar novamente muitos utilizadores, alterar todas as credenciais (já que não se saberia quais as comprometidas), regredir alguns sistemas para o estado anterior ao ataque e solicitar a verificação daqueles em que isso não fosse possível. Seria o caos. Assim, para que este cenário não se venha a verificar, já que a sofisticação dos ataques tende a aumentar, é necessário garantir a fiabilidade dos processos de autenticação e, uma vez que existem formas de obter um conjunto vasto de credenciais (nomeadamente através do suborno dos administradores de sistemas), as formas biométricas de autenticação apresentam-se como processos privilegiados.

### 2.1.2 Ciberataques à Geórgia (Agosto de 2008)

Pouco mais de um ano após ser acusada de atacar a Estónia, a Rússia é novamente acusada de realizar um ataque cibernáutico a um país da extinta União Soviética. Desta feita o ataque ocorreu em simultâneo com o ataque militar convencional realizado pelas forças armadas russas à Georgia, por questões relacionadas com a Ossétia do Sul, uma região pró-Federação Russa da Geórgia com pretensões separatistas (Figura 13).

Embora não existam ainda muitos dados sobre os tipos de tecnologias utilizados no ataque ou sobre a sua intensidade, foi já possível detectar na Internet alguns dos apelos ao cibercombate e, a partir daí, perceber as intenções e alguns dos recursos utilizados. Os apelos foram feitos em diversos *fora* de

língua russa e nos sítios *Web* www.stopgeorgia.ru e www.stopgeorgia.info numa acção com uma componente popular muito forte, senão mesmo exclusiva.


*Figura 13 – Localização geográfica da Geórgia*

## A guerra do "povo"

O ataque informático à Georgia parece ter sido coordenado a partir dos domínios www.stopgeorgia.info (sediado na Alemanha e rapidamente encerrado pelo fornecedor do alojamento) e www.stopgeorgia.ru (Figura 14) sediado no Reino Unido, criado a 9 de Agosto de 2008 e que se manteve em funcionamento até ao dia 13 de Agosto, altura em que esteve suspenso, para voltar a operar pouco mais de 24 horas depois, já sem a secção de *software* e com um forum inoperacional.

No manifesto apresentado no sítio *Web* pode ler-se:

> *Nós, os representantes do submundo do hacking russo, não iremos tolerar as provocações dos georgianos, em todas as suas manifestações. Nós queremos viver num mundo livre e livre da agressão e das mentiras no espaço da rede. Não precisamos de orientação das autoridades ou outras pessoas, mas de agir de acordo com as suas convicções baseadas em patriotismo, de consciência e de crença na força da justiça. Pode chamar-nos de ciber-criminosos e terroristas,*

*desencadeando a guerra e matando pessoas. Mas nós vamos lutar e é inaceitável a agressão contra a Federação Russa na Internet.*

Exigimos o fim dos atentados em matéria de informação e recursos, bem como apelamos a todos os meios de comunicação social e jornalistas com um pedido para cobrir os eventos objectivamente. Até que a situação mude, vamos impedir a divulgação de informações falsas dos governos ocidentais e do governo georgiano e meios de informação. Não fomos nós quem lançou a guerra de informação, não somos nós os responsáveis por suas conseqüências. Apelamos para a contribuição de todos os que não são indiferentes às mentiras dos sítios Web políticos georgianos, todos, os que são capazes de inibir a disseminação de informações negras. (traduzido de www.stopgeorgia.ru)

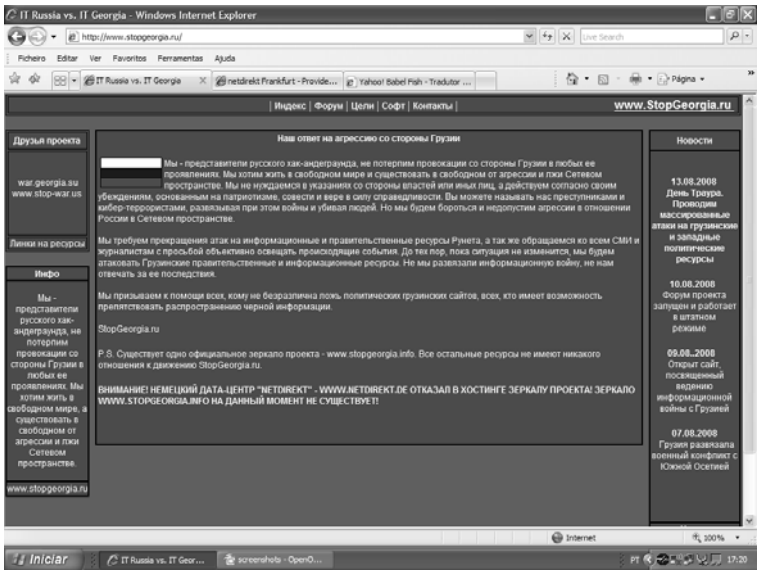



*Figura 14 – Sítio Web www.stopgeorgia.ru com apelos ao cibercombate*

Na secção de *software* (Figura 15) era possível fazer o download de uma ferramenta para efectuar ataques por saturação (*flood*) com vista a realizar um ataque por DDoS (*Distributed Denial of Service* – Inviabilização distribuida do serviço), uma ferrameta de anonimização, uma ferramenta de saturação de linhas telefónicas com recurso ao *software* de voz sobre IP Skype e uma ferramenta para saturação de telemóveis com recurso ao envio de SMS (*Short Message Service*).

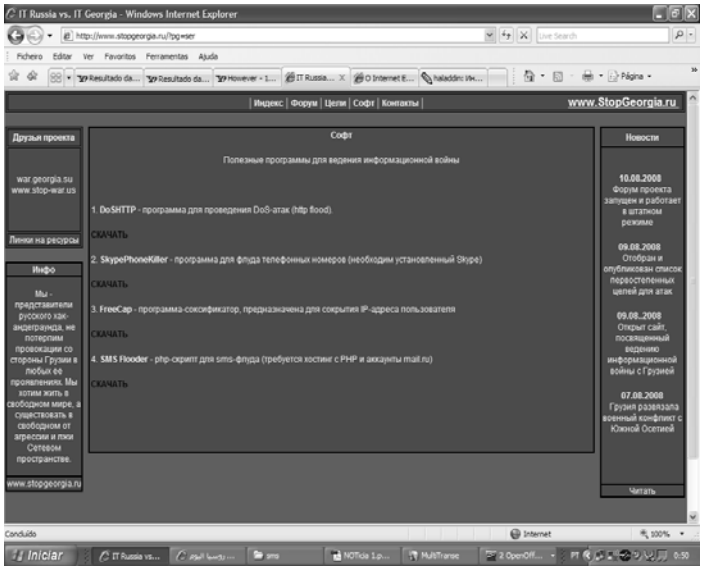



*Figura 15 – Secção de software do sítio Web www.stopgeorgia.ru*

Este sítio *Web* apelou ao ataque a uma lista de alvos e convocou os internautas para um esforço especial no dia 13 de Agosto, declarado dia de luto pelas vítimas da invasão da Ossétia do Sul. A lista de alvos disponibilizada no sítio Web e o seu estado nos dias 13/08/2008 a 25/08/2008 estão apresentados na Tabela 2. É de salientar que alguns dos sítios *Web* mudaram a sua localização para tentar evitar os ataques, seja por questões de inoperacionalidade, como é o caso do canal de televisão Rustavi2 (habitualmente com emissões em directo na Internet), seja por questões de alterações de conteúdo, como é o caso do sítio Web www.civil.ge que foi, no início dos confrontos, alterado para incluir imagens que comparavam o

presidente georgiano a Adolf Hitler. É importante referir também que alguns dos sítios *Web* conseguiram estar, durante o pico dos ataques, temporariamente disponíveis, pelo que a tabela pretende apenas verificar o estado comparativo dos efeitos do combate ao longo dos dias monitorizados. O gráfico da Figura 16 mostra a evolução da intensidade dos efeitos sendo que alguns demorarão a ser resolvidos já que a Geórgia é um país pouco dependente da Internet e, uma vez que o país têm outras prioridades, muitos dos sítios *Web* continuam por refazer, apesar de terem recuperado o controlo sobre eles.

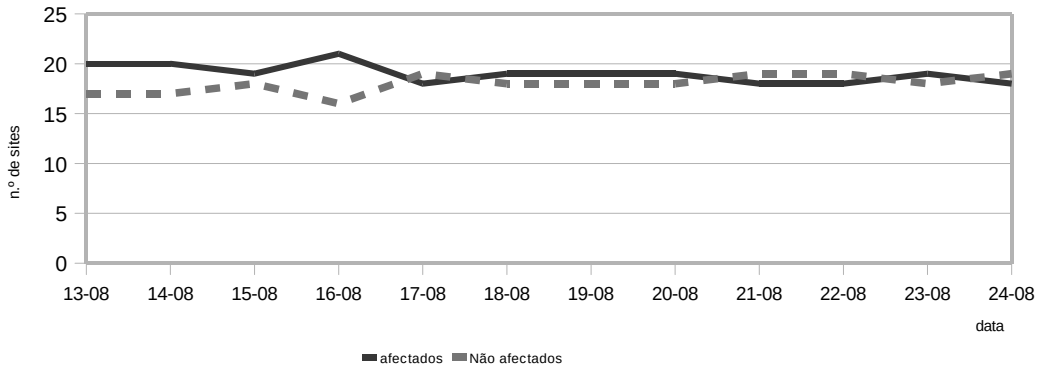



*Figura 16 – Evolução dos efeitos do ciberataque de 13/08 a 24/08*

Alguns rumores afirmam que a *Russian Business Network* (RBN), uma organização criminosa detectada há alguns anos, estaria envolvida também nestes ataques e que teriam desviado o tráfego dirigido à Geórgia através da Rússia. Uma vez que os acessos à Geórgia a partir de Portugal são, normalmente, efectuados através da Turquia, os dados apresentados na Tabela 2 não reflectem eventuais penalizações de desempenho que resultem desse tipo de ataques. Ainda assim, foi possível verificar em determinadas situações que o acesso a sítios *Web* na Geórgia era efectuado através do Azerbaijão, via Rússia, sem qualquer dificuldade. Foi também utilizado por diversas vezes um sítio Web de *traceroute* russo e não houve diferenças significativas, no que respeita às respostas dos servidores, nos resultados obtidos nos acessos a partir da Federação Russa, quando comparados com os obtidos nos acessos a partir de Portugal.

| | | *Estado do sítio Web (verificado entre as 17h30 e as 18h30, hora portuguesa)* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Domínio | Local | 13/08 | 14/08 | 15/08 | 16/08 | 17/08 | 18/08 a 20/08 | 21/08 e 22/08 | 23/08 | 24/08 |
| parliament.ge | Geórgia | Inactivo | | | | | | Não afectado | | |
| assistancegeorgia.org.ge | Geórgia | Muito lento | Inactivo | Muito lento | | | | | | |
| cec.gov.ge | Geórgia | Não afectad | X | | | | | | | |
| | Holanda | X | Não afectado | | | | | | | |
| mdf.org.ge | Holanda | X | Não afectado | | X | | | | | |
| | Geórgia | Não afectad | X | | Inactivo | Não afectado | | | | |
| mfa.gov.ge | Estónia | Muito lento | Não afectado | | | | | | | |
| corruption.ge | n/d | Inactivo | | | | | | | | |
| constcourt.gov.ge | Geórgia | Não afectado | | | Inactivo | Não afectado | | | | |
| insurance.caucasus.net | Geórgia | Não afectado | | | Inactivo | Não afectado | | | | |
| mc.gov.ge | n/d | Inactivo | | | | | | | | |
| nsc.gov.ge | Geórgia | "under construction" | | | | | | | | |
| supremecourt.ge | Geórgia | Não afectado | | | | | | | | |
| iberiapac.ge | Geórgia | Não afectado | | | | | | | | |

| | | *Estado do sítio Web (verificado entre as 17h30 e as 18h30, hora portuguesa)* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Domínio | Local | 13/08 | 14/08 | 15/08 | 16/08 | 17/08 | 18/08 a 20/08 | 21/08 e 22/08 | 23/08 | 24/08 |
| court.gov.ge | Geórgia | "under reconstruction" | | | | | | | | |
| civil.ge | Estónia | Não afectado | | | | | | | | |
| georgia.usembassy.gov | USA | Não afectado | | | | | | | | |
| ukingeorgia.fco.gov.uk | Reino Unido | Não afectado | | | | | | | | |
| all.ge | Geórgia | "under construction" | | | | | | | Inactivo | |
| geres.ge | Geórgia | Não afectado | | | | | | | | |
| rustavi2.com.ge | USA | Inactivo | | | Não afectado | | | | | Lento |
| opentext.org.ge | Alemanha | Não afectado | | | | | | | | |
| svobodnaya-gruzia.com | Geórgia | Não afectad | Inactivo | Não afectad | Inactivo | Não afectado | | | | |
| sanet.ge/gtze | Geórgia | Inactivo | | | | | | | | |
| messenger.com.ge | Geórgia | Não afectado | | | | | | | | |
| primenewsonline.com | USA | Inactivo | | | | | | | | Não afectad |
| presidpress.gov.ge | Geórgia | Em branco | | | | | | | | |
| sakinform.ge | n/d | Inactivo | | | | | | | | |

| | | *Estado do sítio Web (verificado entre as 17h30 e as 18h30, hora portuguesa)* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Domínio | Local | 13/08 | 14/08 | 15/08 | 16/08 | 17/08 | 18/08 a 20/08 | 21/08 e 22/08 | 23/08 | 24/08 |
| sakartvelo.ru | n/d | Inactivo | | | | | | | | |
| internews.ge | Geórgia | Inactivo | | | | | | | | |
| internews.org.ge | Geórgia | Inactivo | | | | | | | | |
| interpressnews.ge | Geórgia | Lento | Muito lento | | Não afectad | Lento | | | | |
| internet.ge | Geórgia | Não afectado | | | | | | | | |
| stream.ge | Geórgia | Não afectado | | | X | | | | | |
| | Holanda | X | | | Não afectado | | | | Inactivo | |
| presa.ge | Geórgia | Não afectado | | | | | | | | |
| medianews.ge | Geórgia | Não afectado | | | | | Lento | | | Não afectad |

*Tabela 2 – Situação, ao longo do conflito, dos sites listados como alvos preferenciais*

Um dos sítios *Web* com maior responsabilidade na defesa da ideia de que a RBN é a responsável por estes e outros ataques cibernáuticos é o http://rbnexploit.blogspot.com/. Mas, a fazer fé neste *blog* todos os males da informática, desde os vírus, ao SPAM, passando pela pornografia e pela pedofília, são da responsabilidade da RBN e, indirectamente, do governo da Federação Russa, sem que seja apresentado qualquer facto que prove estas alegações.

Também nalguns *fora* de lingua russa se apelou ao combate. A maioria limitou-se a divulgar o endereço www.stopgeorgia.ru, mas alguns disponibilizaram outros meios para realizar os mesmos ataques. É esse o caso do http://clubs.ya.ru que propõe a criação de uma *batch* para o envio automático de pedidos *ping* à lista de alvos a afectar e do http://aeterna.ru que disponibiliza um *link* para um ficheiro HTML (Figura 17) que acede aos alvos e, através da actualização automática da página, possível em alguns *browsers*, vai saturando os servidores atacados.

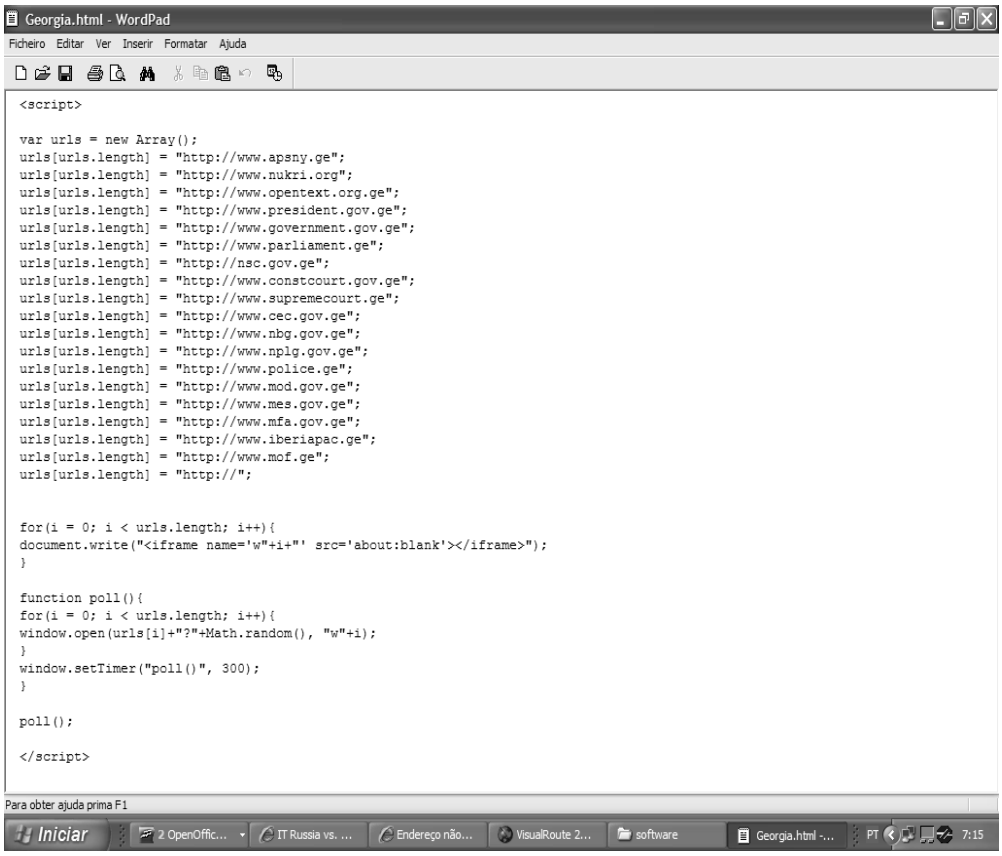



*Figura 17 – Código fonte da página HTML distribuida para realização de ataques*

O sítio *Web* disponibilizava também uma lista de servidores *proxy* (incluindo alguns disponíveis apenas para máquinas localizadas na Federação Russa) e uma lista de sítios *Web* georgianos vulneráveis a ataques por injecção de *SQL*, explicando para cada caso a forma de proceder para alcançar os

resultados pretendidos. Verifica-se, portanto, que uma parte dos ataque foi organizada com poucos recursos. Ainda assim, como se verifica pela observação da Tabela 2, os efeitos foram consideráveis.

Uma vez que o governo Georgiano acusou a Federação Rússia de ser responsável por estas acções ("Georgia accuses Russia of waging cyberwar", 2008), importa tentar perceber quem é responsável por esses sítios *Web*. É uma tarefa difícil mas que, neste caso, é facilitada pela existência de um sítio *Web* dedicado a esta ciberguerra. Um *traceroute* e uma consulta a um servidor *whois* dão a indicação de que se trata de um domínio alojado no Reino Unido sob a alegada responsabilidade de alguém com o endereço de correio electrónico anac109@mail.ru e com um número de telefone de contacto de Irkutsk, na Sibéria (Figura 18). Algumas pesquisas em motores de busca levaram à informação de que este endereço de correio electrónico foi usado também para registar outros domínios: dokim.ru (Figura 19) e rakar.ru (Figura 20), ambos sediados nos Estados Unidos da América, permitindo obter mais alguns dados sobre o alegado dono dos domínios, nomeadamente o seu alegado nome: Andrej V. Uglovatyj que, claro, é provavelmente falso, principalmente se atendermos ao objectivo do sítio *Web* alojado no domínio dokim.ru: a venda de passaportes falsos! De facto, este sítio *Web* dedica-se à venda de passaportes da Federação Russa supostamente emitidos legalmente (Figura 21) e de alguns países da União Europeia, nomeadamente a Lituânia, a Letónia, o Reino Unido e a Alemanha (Figura 22). Alegadamente todos estes passaportes são verdadeiros e do último modelo em vigor. O preço de um passaporte da União Europeia varia entre os 3000€ e os 3500€ conforme seja dado um sinal de 50%, ou não. O outro domínio associado ao mesmo endereço de correio electrónico tem também um objectivo ilícito: a venda de cartões de plástico com bandas magnéticas com os dados de cartões legítimos e respectivos códigos PIN (Figura 23) obtidos, claro, de forma ilegal e vendidos por um preço unitário que, de acordo com a quantidade adquirida, varia entre os US$70 e os US$450 (Figura 24). As figuras

apresentadas correspondem a traduções automáticas dos sites e o anexo IV apresenta as imagens na versão original, em Russo.

É, portanto, muito provável que o sítio Web que coordenou o ciberataque não tenha ligações a qualquer entidade oficial de Moscovo, o que demonstra a existência de outras entidades capazes de mobilizar os recursos necessários para atacar com êxito sítios *Web* de entidades governamentais, seja através de ataques por DDoS, seja por exploração de vulnerabilidade a injecções de SQL ou por exploração de quaisquer outras vulnerabilidades. Aliás, numa mensagem colocada no *forum* do sítio *Web* www.stopgeorgia.ru podia ler-se: "os ataques por DDoS têm efeitos limitados. Devemos encontrar vulnerabilidades e utilizá-las. DDoS só como último recurso". A segurança da autenticação assume, assim, uma importância acrescida no contexto dos ciberconflitos.

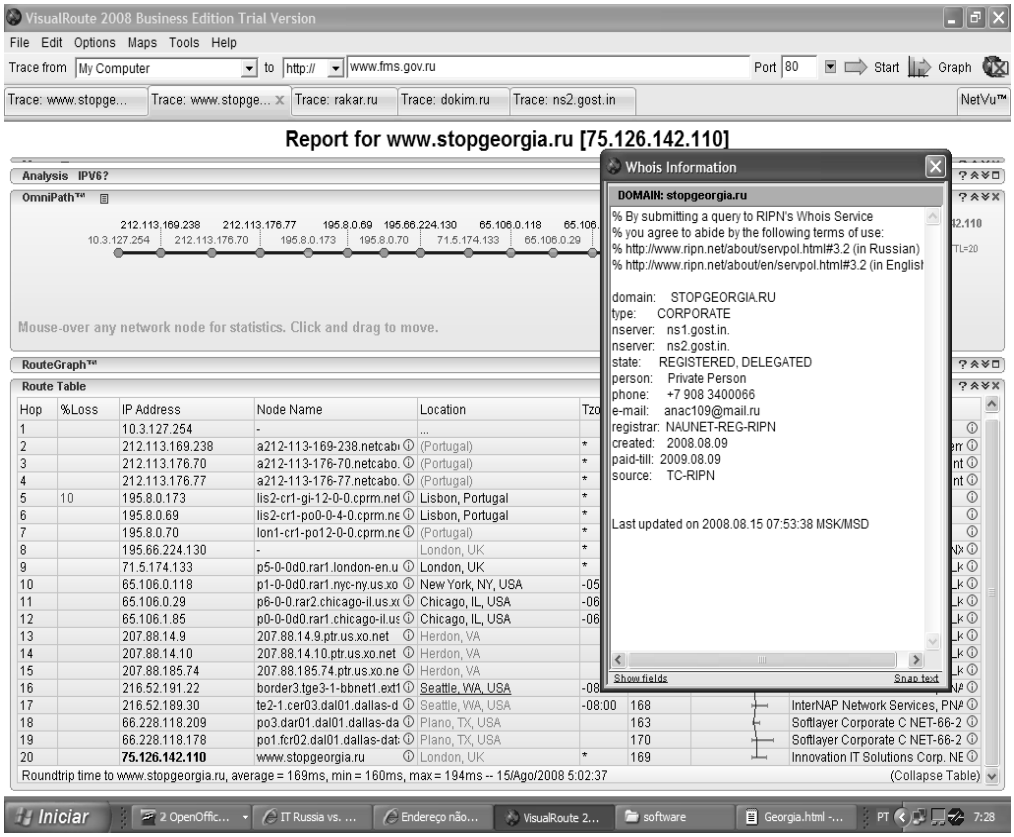



*Figura 18 – Localização e dados do proprietário do domínio stopgeorgia.ru*

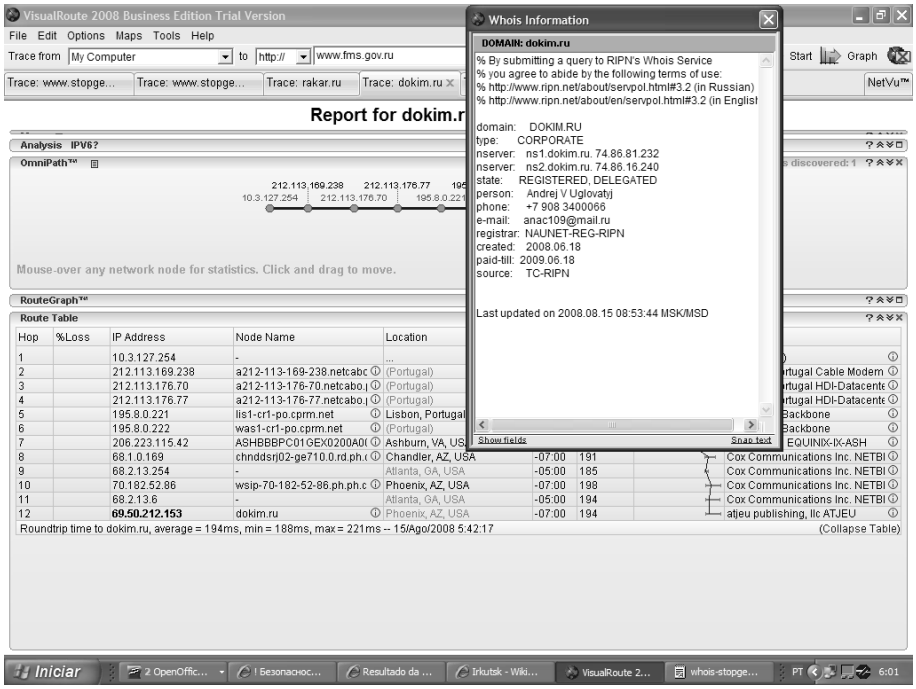



*Figura 19 – Dados do proprietário do domínio dokim.ru*

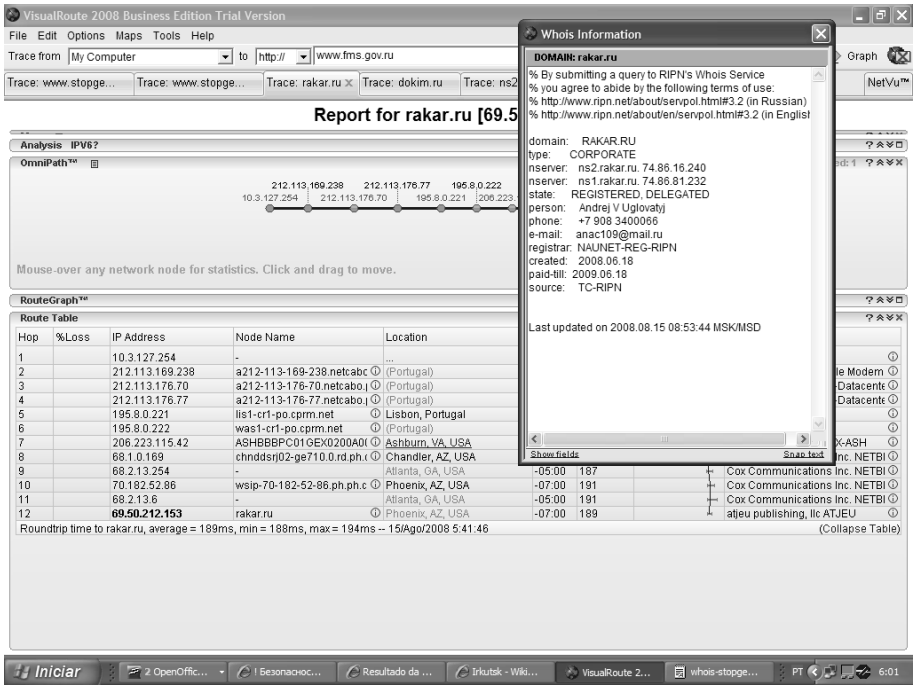



*Figura 20 – Dados do proprietário do domínio rakar.ru*

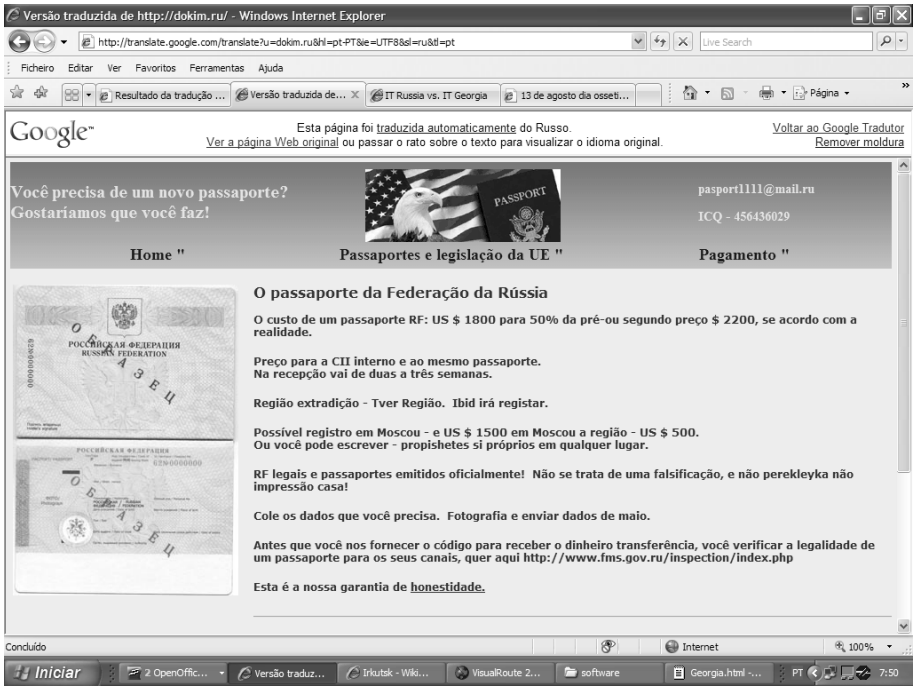



*Figura 21 – Tráfico de passaportes russos (tradução)*


*Figura 22 – Tráfico de passaportes da União Europeia (tradução)*

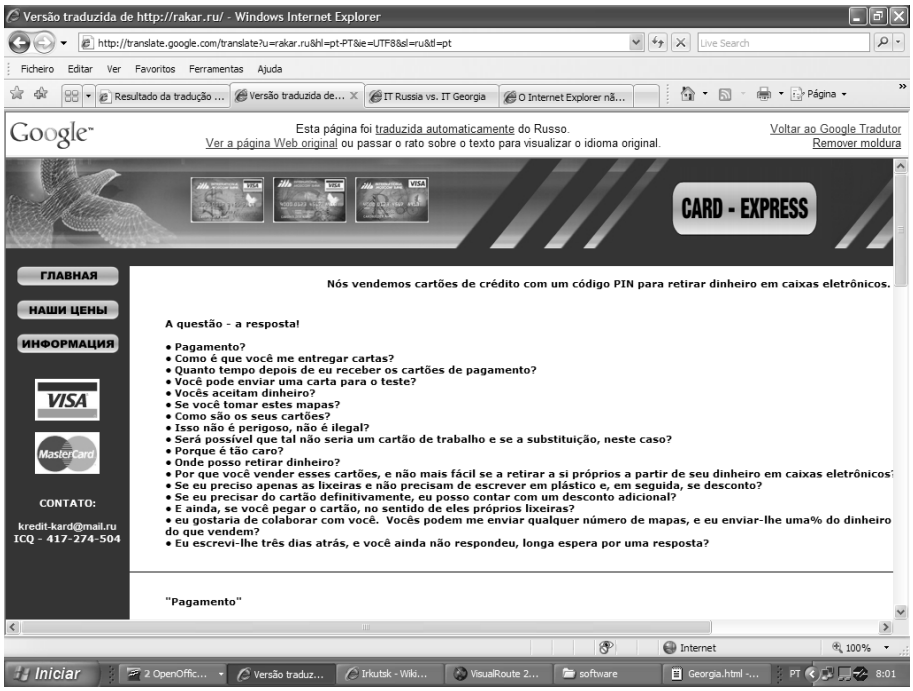



*Figura 23 – Tráfico de cartões de crédito (tradução)*

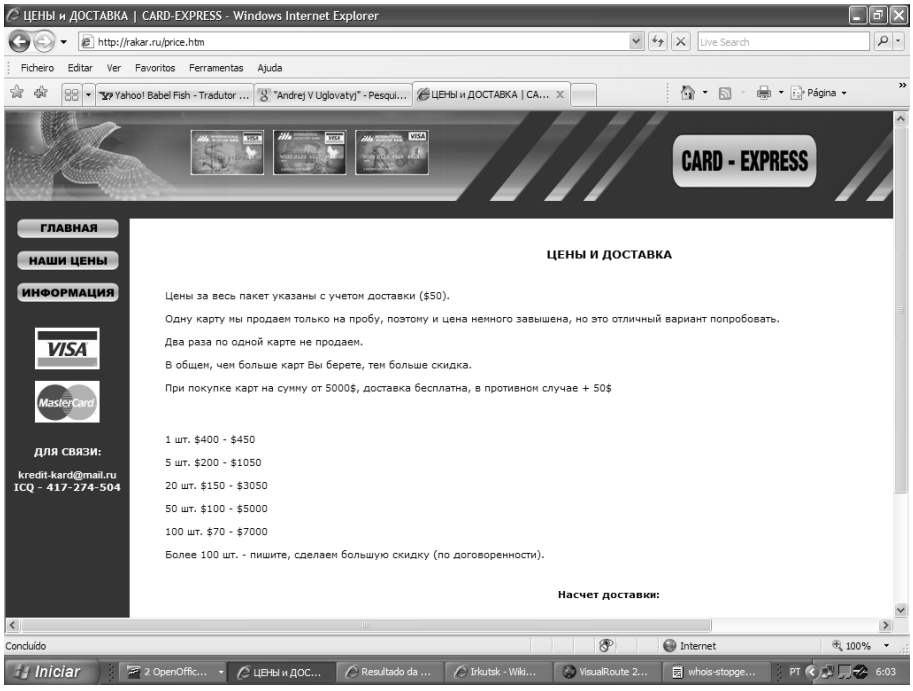



*Figura 24 – Preço das cópias de cartões e PINs*

Mais uma vez, como já tinha acontecido no caso de estudo anterior, os efeitos deste ataque seriam bem mais graves e ainda mais duradouros se o ataque tivesse tirado proveito de vulnerabilidades nos processos de autenticação.

## *2.2 O ciberterrorismo*

As organizações terroristas têm recrutado para as suas fileiras indivíduos tecnologicamente habilitados nas mais diversas áreas, desde a medicina à engenharia. Em consequência disso, o seu *modus operandis* pode facilmente ser alterado e gerar espanto, com todas as vantagens que advêm do efeito surpresa. Assim aconteceu a 11 de Setembro de 2001 quando um grupo de fundamentalistas islâmicos afectos ao grupo *Al-Qaeda* se apoderou de vários aviões civis de transporte de passageiros e os fez despenhar contra as torres do *World Trade Center* e contra as instalações do Pentágono. A preparação deste atentado implicou o estudo, recorrendo a simuladores, da forma de pilotagem dos aviões das linhas aéreas e foi realizado por indivíduos com formação na área da engenharia. Mas esta não foi a primeira vez que organizações terroristas se mostraram tecnologicamente capazes já que, no passado, demonstraram com frequência um conhecimento profundo das tecnologias de carácter militar que lhes permitiu utilizar e até construir armamento portátil, tecnologia de minas e armadilhas, equipamento de comunicações em ambiente operacional, etc. Além disso, a rede de formação dos grupos terroristas islâmicos conseguiu manter-se activa, graças ao apoio explícito ou implícito de alguns países e apesar de funcionar num regime presencial, concentrado em autênticas “escolas práticas” com formação teórico-prática e campos de treino, que facilita a sua localização e posterior destruição pelas forças de segurança, pelo menos em teoria. Neste confronto assimétrico uma das partes recorre a um suporte tecnológico imenso, incluindo as redes de satélites espiões e armamento com ligação à rede de dados das forças armadas, procurando contrariar as técnicas de dissimulação utilizadas pelos terroristas. Exemplo paradigmático desta assimetria foi a

aniquilação do terrorista palestiniano conhecido como “o engenheiro”, Iehia Aiash, que durante anos formou outros terroristas nas áreas relacionadas com a preparação de explosivos e estratégia militar/terrorista, com recurso a um míssil teleguiado que seguiu o sinal do seu telemóvel.

A História mostra que as organizações paramilitares não governamentais procuraram sempre aceder a tecnologia que lhes permitissem, mantendo a protecção da clandestinidade, reequilibrar as forças. Foi esse o caso, por exemplo, dos mísseis *Stinger* utilizados pela primeira vez pelos *Moujahideen* afegãos para o combate ao poderio aéreo soviético (equipamento desenvolvido e fornecido pelas forças armadas norte-americanas), das *kalashnikov* (originalmente de fabrico soviético) utilizadas por tantos grupos rebeldes e terroristas, incluindo a Al-Qaeda e a OLP (Organização de Libertação da Palestina) e, se quisermos recuar mais no tempo, foi também esse o caso da aquisição pelas tribos nativas de armas de fogo, nomeadamente a espingarda de repetição, para fazer frente aos colonos ingleses e, mais tarde, ao exército norte-americano que avançava para Oeste. Poucos foram os casos em que a tecnologia foi desdenhada e, mesmo nesses casos, o tempo acabou com a oposição. Foi esse o caso na Europa medieval do recurso a armas que não envolvessem o combate corpo-a-corpo, como o arco-e-flecha, a besta e mais tarde o mosquete. Assim, seria de esperar que o movimento realizado pelas forças armadas e de segurança no sentido tecnológico fosse rapidamente secundado pelos terroristas já que se tratam de recursos muitas vezes acessíveis a um preço razoável, acessíveis em quase qualquer parte do globo, discretas e furtivas já que são também de uso civil e que, graças à quantidade de tráfego, é muito difícil monitorizar as actividades do ciberespaço. E, de facto, as organizações terroristas viraram-se para a Internet, primeiro como forma privilegiada de comunicação, depois como forma de divulgação de informação e de preparação de atentados.

De acordo com o *Washington Post*, o principal canal de comunicação da *Al-Qaeda* foi, até ser fechado, o sítio *Web* localizado em www.alneda.com

(Figura 25) onde, entre outros materiais, se podiam encontrar declarações de Osama Bin Laden. O domínio, criado por um monitor da *Al Qaeda* no Afeganistão morto em combates com militares sauditas em 2003, apontava continuamente para servidores localizados em locais sempre diferentes e imprevisíveis e encontra-se agora alterado, como se pode verificar na Figura 26, após John Messner, um vigilante da Internet ter, alegadamente, utilizado técnicas de *hacking* para assumir o controlo/propriedade sobre esse domínio (Coll & Glasser, 2005).


*Figura 25 – Sítio Web de divulgação da Al Qaeda*

Desde que as autoridades de segurança passaram a estar atentos a estas formas de comunicação, a Internet transformou-se num jogo de gato e de rato, com os sites a serem construídos, detectados e desligados para, imediatamente a seguir, surgirem noutro domínio. Este processo de detecção é mais complexo no caso do terrorismo islâmico porque a comunicação é efectuada em árabe, o que impede a colaboração da generalidade da população. A Figura 27 mostra uma revista *online* denominada *Muaskar al-battar* (Campo da Espada) criada em 2004 pelo ramo saudita da *Al-Qaeda* (Coll & Glasser, 2005) e que, apesar do sítio *Web* da revista estar fechado, está disponível através do *Internet Archive* (www.archive.org).


*Figura 26 – Sítio Web da Al Qaeda alterado por hackers*

A Figura 28 mostra o sítio *Web* da *Global Islamic Media Front*, no endereço utilizado em 8 de Novembro de 2007, www.gimf.22web.net, e que durou pouco como todos os outros que vai tendo, uma organização fundada com o objectivo de promover a *jihad* electrónica.


*Figura 27 – Capa do número 22 da revista Mu' askar al battar*


*Figura 28 – Sítio Web (em servidor provisório) da Global Islamic Media Front*

Os *fora* islâmicos são, frequentemente, apontadores para os locais onde foram deixados os ficheiros com o material a transmitir. Há medida que o tempo vai passando, os *links* vão sendo desactivados pelos fornecedores dos serviços de alojamento, pelo que cada documento é colocado em dezenas de locais. Estes *fora* são também um bom indicador do estado tecnológico dos simpatizantes da *Al-Qaeda*, quer pela informação que está disponível nos sites, quer pela forma como é disponibilizada.

Em Setembro de 2006 foi lançada a primeira parte do video sobre a guerra santa na Arábia Saudita. Este video de 48 minutos, legendado em Inglês, estava disponível no formato MPEG-1 (extensão mpg), um ficheiro com 404MB, e no formato MP4 (uma versão de 73MB e outra de 31MB). Em Fevereiro de 2007 foi disponibilizada uma nova versão no formato WMV com 130MB. Assim, mudaram os locais, os nomes dos ficheiros e até as suas extensões. Não é fácil, de facto, localizar estes documentos.

Em Julho de 2007 o *forum minbar-sos* (http://www.minbar-sos.com) apontava para um video do Sheikh al-Fadhil / Abu Yahya al-Libi subordinado ao

tema *Convergence des Religions – Une nouvelle étape de la guerre des Croisés* (convergência das religiões – uma nova etapa na Guerra das Cruzadas), relacionado com os esforços ecuménicos da Igreja Católica (Figura 29)[2]. Este ficheiro estava depositado em 18 locais na versão de 513MB (ficheiro no formato DIVX), 123 locais na versão de 77MB (ficheiro no formato RMVB), 121 locais na versão de 31MB (ficheiro no formato RM), 92 locais na versão de 12MB (ficheiro no formato 3GP), 74 locais na versão de 9,48MB (ficheiro no formato mp3) e 51 locais na versão em ficheiro de texto com a transcrição do conteúdo do video (em caracteres árabes, facilmente traduzíveis com um *software* como o *Multitrans*, disponível gratuitamente na Internet). É necessário conhecer bem a Internet e os programas de edição/conversão de video para alcançar estes resultados e, com ficheiros desta dimensão, os computadores utilizados não podem ser máquinas obsoletas. Para aceder a qualquer um dos ficheiros onde são transmitidas mensagem ideológicas é necessário introduzir uma palavra passe, disponível no *forum*. As palavras passe escolhidas não têm semântica e recorrem a letras, símbolos e números. Além disso, são enormes e de tamanho variável, desde 23 caracteres até 37 caracteres. A escolha dessas palavras passe demonstra um cuidado na utilização da tecnologia que não é próprio de quem não a domina.

Além da forma como o material é criado, armazenado, protegido e distribuido, também o seu conteúdo pode ser revelador da capacidade tecnológica adquirida. A maior parte do material disponível está relacionado com a actividade dos *Moujahideen* na Península Arábica ou no Afeganistão, logo trata-se principalmente de material de carácter militar tradicional, propaganda dos feitos alcançados, informação de carácter religioso com vista ao recrutamento de combatentes e apelo ao combate e ao martírio (Figura 30 e Figura 31). Ainda assim, é possível reconhecer o uso das tecnologias de informação e de comunicação na sua actuação.

2 Durante toda a intervenção pode ver-se na imagem de fundo o Santo Padre, alvo principal do seu discurso.


*Figura 29 – Intervenção do Sheikh al-Fadhil sobre as negociações ecuménicas.*

O segundo video da série dedicada à *Jihad* na Arábia Saudita mostra como dois mártires bombardearam em 2003 as instalações de Al-Muhayya em Riade, onde estavam alojados centenas de ocidentais, desde a preparação do atentado até à sua concretização. O video refere que na preparação do atentado foram tiradas fotos do local, foram efectuadas vigilâncias para identificar os moradores e os hábitos de segurança, foram estudados mapas e foram efectuadas simulações no computador (Figura 32). O video não refere de que tipo de simulações se trata, se tempos de percurso, se de capacidade dos explosivos, se ambas ou outras. No video foi incluído um outro vídeo: o do atentado. Os mártires transmitiram o seu percurso até às instalações onde iriam efectuar o atentado e transmitiram imagem e som, mesmo durante os combates, até serem atingidos (Figura 33). Pela qualidade da gravação e pelo facto de se ter sido transmitido em directo, é provável que o aparelho utilizado para a gravação tenha sido um telemóvel. Os resultados do atentado seriam rapidamente divulgados pela comunicação social, portanto essa transmissão só pode ter sido efectuada com o propósito de fornecer dados para futuras operações ou com o objectivo de servir de material de propaganda com vista ao recrutamento. Em qualquer dos casos estamos perante o uso de tecnologias de comunicação e informação em actividades marcadamente terroristas.


*Figura 30 – Elevação dos atentados de 11 de Setembro de 2001 e apelo ao envolvimento no combate*


*Figura 31 – Demonstração de treino e apelo ao combate*

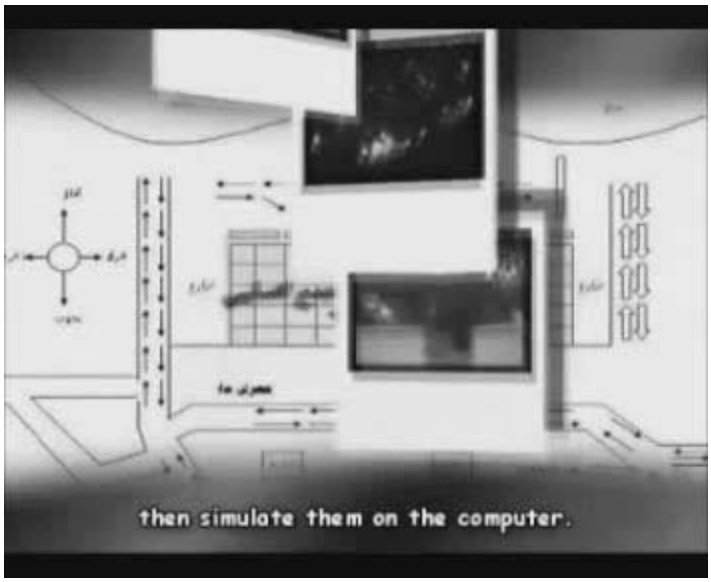



*Figura 32 – Referência ao uso do computador como simulador*


*Figura 33 – Video da transmissão em directo de um atentado suícida emitido pelos mártires*

A Internet é também um espaço de formação, permitindo a rápida divulgação de materiais pedagógicos destinados à formação de terroristas. Um

dos documentos mais emblemáticos da formação de terroristas é o *The Moujahideen Explosives Handbook* (Abdel-Aziz, 1996), difundido pela *Organization for the Preparation of the Moujahideen* (OPM) como parte da *Encyclopedia Jihad*. Este documento é fundamental para a compreensão da acção terrorista islâmica uma vez que nos dá informações sobre a forma de comunicação digital utilizada por estes grupos. O documento prevê como pagamento pela sua leitura a digitalização de um livro militar qualquer (à escolha do leitor) que deverá ser entregue à OPM por via electrónica. Para que isso seja possível, são descritos os passos necessários para conhecer o endereço de correio electrónico em utilização pela organização num determinado momento, o que é feito recorrendo a um servidor de chaves públicas (keys.pgp.net). Aliás é fortemente recomendado que a comunicação seja cifrada e, para tal, é fornecida a chave pública PGP (*software* para cifrar comunicações e documentos) da OPM, pedindo-se que o leitor recorra a um colega com conhecimentos de computadores se não souber o que fazer com a chave pública disponibilizada. O facto de esta organização utilizar PGP em 1996 é um indicador claro de que as organizações terroristas estão na vanguarda do uso das tecnologias de informação e de comunicação.

Na secção de Ciências Islâmicas e Jurisprudência do *forum minbar-sos*, está disponível um texto sobre o papel das mulheres na Jihad. Embora nos papeis possíveis da mulher o autor inclua a participação activa em combate, ele afirma que "*Élever des enfants Moujahideen c'est peut être le rôle le plus important que les femmes puissent jouer dans le Jihad"* (criar crianças *Moujahideen* pode ser o papel mais importante que as mulheres podem desempenhar na *Jihad*) e para o alcançar são propostas diversas acções. Entre elas, estão actividades como ler histórias sobre os *Moujahideen* ao deitar, eliminar a televisão, preparar os jovens para a actividade militar, por exemplo ensinando a apontar uma arma de brincar, incentivar os jovens a diversões mais apropriadas para a preparação para a *jihad*, como as artes marciais, a natação, a corrida, a orientação e a condução de diversos veículos. No entanto, é também

recomendado que sejam visitados com a criança sítios *Web* como o http://stcom.net/ (um sítio *Web* anti-ocidental) e que sejam utilizados outros recursos da Internet (Alrafidha, 2006). Neste documento está claramente definido o papel da Internet na formação de mentalidades e na preparação dos combatentes. Mas a actividade informática enquanto uma actividade de Guerra Santa propriamente dita é também reconhecida, já que o autor conclui que:

> *Une mère connaît très bien les capacités de ses enfants. En fonction de cela, elle peut encourager ses enfants aux aspects du Jihad correspondant. Notez que la participation au Jihad peut se faire de différentes façons. Par exemple, un physicien nucléaire peut aider à renforcer le système de défense nationale des musulmans, un expert en communication peut l'assister, un expert en ordinateur peut mettre ses connaissances au service des Moujahideen, un journaliste peut aider à la cause du Jihad en apportant des informations authentiques au monde, et un docteur ou une infirmière peut aider les Moujahideen au point de vue médical. Il est nécessaire à l'enfant que ses buts soient clairs, ainsi que soit clair ce qui ne fait partie de ses projets, en prenant une profession donnée – que son but est de servir Allah de la façon la plus haute (à travers le Jihad) et non pas d'accumuler les biens et le confort physiques en soient. On doit souligner ici que, quelle que soit la profession qu'il choisit, même si c'est en vue du Jihad, l'entraînement militaire est une obligation. En fait, l'entraînement militaire est le droit de l'enfant sur ses parents* (Alrafidha, 2006).

Ou seja:

> *Uma mãe conhece muito bem as capacidades das suas crianças. Em função disso, pode incentivar as suas crianças aos aspectos Jihad correspondentes. Notem que a participação na Jihad pode fazer-se de diferentes maneiras. Por exemplo, um físico nuclear pode ajudar a reforçar o sistema de defesa nacional dos muçulmanos, um perito em comunicação pode assisti-lo, um perito em computadores pode pôr os seus conhecimentos ao serviço dos Moujahideen, um jornalista pode ajudar à causa Jihad trazendo informações autênticas ao mundo, e um doutor ou uma enfermeira pode ajudar os Moujahideen do ponto de vista médico. É necessário à criança que os seus objectivos sejam claros, bem como o seja claramente o que não faz parte dos seus projectos, tomando uma profissão dada - o seu único objectivo é servir Allah da maneira mais elevada (através da Jihad) e não acumular os bens e o conforto físico. Deve-se sublinhar aqui que, qualquer que seja a profissão que escolhe, ainda que com o propósito da Jihad, o treino militar é uma obrigação. Com efeito, o treino militar é o direito da criança sobre os seus pais.*

Este texto pode ser a explicação para o facto de, apesar de existir capacidade tecnológica, não existirem ainda ciberataques terroristas. É que todas as actividades que não conduzem à morte física dos “infiéis” são consideradas como actividades de suporte. Na realidade, se é certo que os terroristas islâmicos dispõem de uma capacidade tecnológica considerável, é questionável que disponham, actualmente, de recursos humanos capazes de garantir um ataque cibernáutico do tipo letal. Ainda assim, com o passar do tempo, esses recursos humanos podem ser formados e/ou recrutados, além de

que existem outros grupos radicais, de extrema esquerda e de extrema direita, capazes de realizar actos terroristas sem os constrangimentos da fé. Sinal dessas mudanças são os sítios *Web* em Russo, como o http://volnyj-strelok.narod.ru/ que juntam no mesmo sítio *Web* propaganda revolucionária, documentos sobre tácticas de combate corpo a corpo, indicações precisas para a construção de armas de fogo em casa, manuais para o uso de explosivos e manuais de segurança informática (Figura 34). Nele pode ler-se "Aqui é possível ler os livros interessantes na teoria e na prática do terror. Para aprender! Para aprender e destruir outra vez o burguês!".

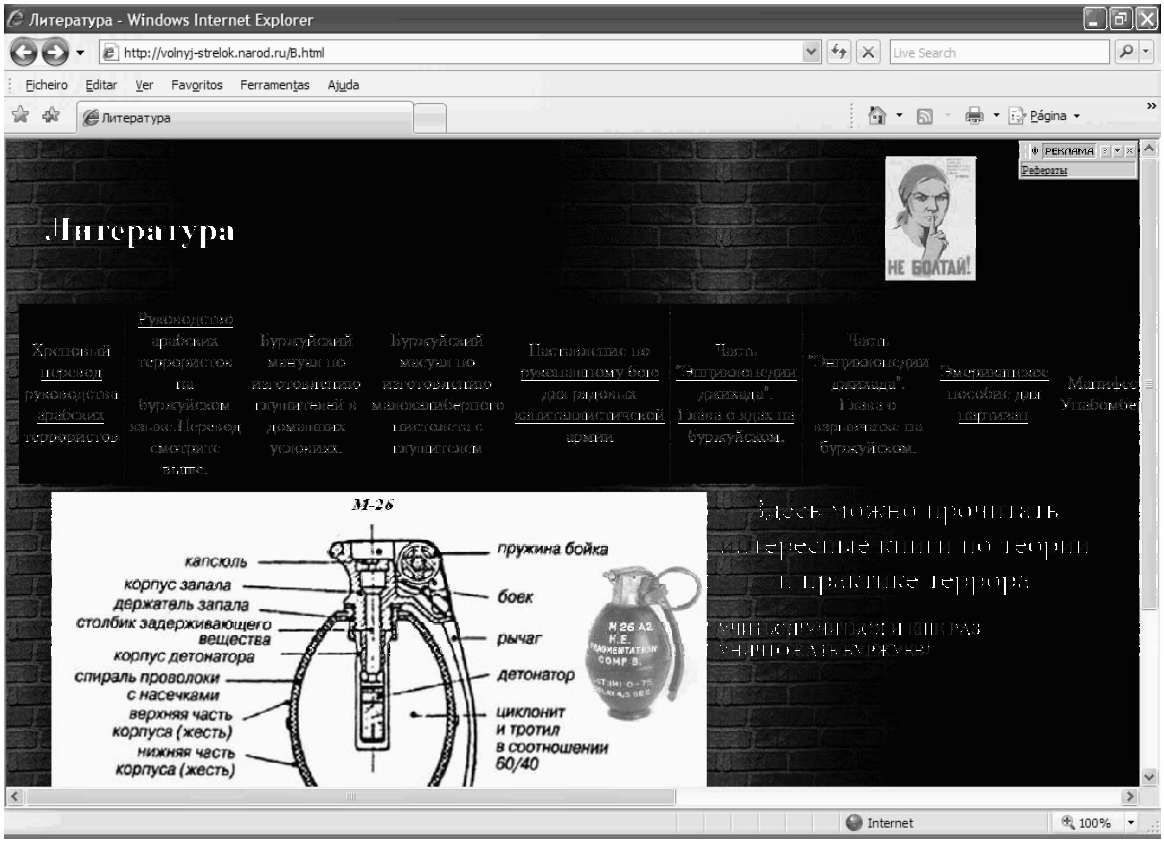



*Figura 34 – Secção de "Literatura" do sítio Web http://volnyj-strelok.narod.ru/*

O livro electrónico *39 wasila Li-Kidmat Al-Jihad Wa-Al-Musharaka Fihi* (39 caminhos para o bem do combate santo) escrito por Mohammad Bin Ahmad Al-

Salem (Al-Salem, 2003) e traduzido e analisado por Jonathan Halevi (Halevi, 2003) refere-se à Internet em dois dos 39 caminhos:

Caminho 21 – Publicar as actividades dos guerreiros santos (Moujahideens) de forma a incentivar a noção de solidariedade e fortalecer o orgulho e a esperança entre os crentes; (…) Há várias formas recomendadas de distribuir informação enaltecendo o combate santo (jihad), incluindo sítios *Web* e *fora*, listas de distribuição, (…).(Halevi, 2003)

Caminho 34 – Realizar o combate santo electrónico (jihad electrónica). De acordo com Halevi, Al-Salem apela à participação dos crentes nos *fora* da Internet para defender o Islão e os Moujahideen, para pregar o combate electrónico e encorajar os muçulmanos a aprender mais sobre este dever sagrado. A Internet representa uma oportunidade para chegar a um público-alvo muito vasto e responder de forma ágil a falsas alegações. De acordo com o autor, os especialistas informáticos são solicitados para utilizarem as suas competências e experiência para destruir sítios *Web* de americanos, judeus e outros "moralmente corrompidos" (Halevi, 2003).

Ainda assim, não são frequentes os relatos de actividades ilegais do tipo das descritas no "caminho 34". Sabe-se, quando muito, que a Internet tem sido utilizada para recolher informações ou para discutir posições em *fora* ou *chats*, mas isso não pode ser considerado como terrorismo, assemelhando-se à pesquisa em bibliotecas ou ao normal e democrático debate de ideias (Nelson, Choi, Lacobucci, Mitchell, & Gagnon, 1999). É também provável que o *Google Earth* tenha sido utilizado para o reconhecimento de áreas onde vieram a ser perpetrados ataques terroristas, mas essa actividade é semelhante à consulta de mapas e, portanto, não será, em si mesma, uma actividade de carácter terrorista.

Nos tempos mais recentes surgiram dúvidas sobre a presença de terroristas no mundo virtual tridimensional *online* denominado *Second Life*. As

autoridades de segurança suspeitam que esta plataforma esteja a ser usada para dar formação a terroristas numa versão e-learning dos tradicionais campos de treino (“Virtual jihad hits Second Life website”, 2007). É fácil verificar que o *Second Life* pode ser utilizado como local de formação, basta verificar as comunidades académicas que desenvolvem actividades nesse ambiente. No caso terrorista é possível, pelo menos, encontrar sem dificuldade modelos tridimensionais de armas de fogo (Figura 35) que podem ser adquiridos por um preço que vai desde um ou dois dólares até algumas dezenas e que incluem manual de instruções. Assim, com algum dinheiro e vontade é possível, portanto, adquirir um conhecimento relativamente grande sobre armamento, sem qualquer comportamento ilegal. Essa informação está também disponível na Internet mas aí não está disponível em simultâneo um formador técnico para transmitir a informação que não é descrita nas descrições técnicas. É este, provavelmente, o primeiro caso em que a Internet é utilizada em actividades de carácter eminentemente terrorista, ainda que no campo da formação e planeamento, e será, portanto, o primeiro caso de ciberterrorismo.

Apesar de, no que respeita à Europa, não haver informação pública sobre a actividade digital de carácter terrorista, ou de suporte à actividade terrorista, as instituições ligadas à segurança terão conhecimento de factos concretos, já que o comissário europeu para a justiça e assuntos internos em funções em 2007 divulgou à imprensa que a União Europeia se prepara para divulgar propostas legislativas relativas ao uso da Internet. O comissário baseia essa pretensão na alegação de que os terroristas têm utilizado a Internet para actividades de recrutamento, divulgação e organização de atentados. Em declarações à *Reuters* Franco Frattini afirma mesmo que procurá junto de empresas informações “*on how it is possible to use technology to prevent people from using or searching dangerous words like bomb, kill, genocide or terrorism*" (sobre como é possível recorrer à tecnologia para impedir as pessoas de utilizarem ou pesquisarem palavras perigosas como bomba, matar, genocídio ou terrorismo) (“Web search for bomb recipes should be blocked: EU”, 2007)! Será, no entanto,

muito difícil aprovar medidas tão radicais, por constituírem violações de alguns direitos fundamentais previstos na legislação de vários países da União Europeia, como o direito à informação e o direito à liberdade de expressão.

Quaisquer dúvidas sobre a capacidade tecnológica dos grupos ligados ao terrorismo ficaram desfeitas na guerra entre Israel e o Hezbollah, após o sequestro de alguns militares das forças de defesa israelitas. Nesse conflito Israel deparou-se com um grupo terrorista que num cenário de conflito directo e frontal assume um comportamento de força de guerrilha apoiada por meios normalmente associados a exércitos convencionais. Provavelmente graças à transferência de tecnologia e *know-how* de países como a Síria e o Irão, o Hezbollaw foi capaz de interceptar e descodificar as comunicações entre as unidades de cavalaria israelitas antecipando, assim, todos os seus movimentos, o que permitiu a colocação antecipada de equipamento anti-tanque em localizações privilegiadas.


*Figura 35 – Secção de uma loja de "armas" no Second Life*

Mais uma vez, os processo de autenticação revelam-se críticos e, felizmente, ainda não foram afectados. A obtenção por parte de terroristas de credenciais válidas com um nível de confiança alto dentro de um sistema estatal pode revelar-se desastroso e, considerando a típica partilha pelos utilizadores de credenciais entre os vários sistemas, por exemplo recorrendo à mesma palavra

passe para vários sistemas de e-mail, mesmo a autenticação perante sistemas menos críticos deve revestir-se de cuidados imensos, especialmente se considerarmos que o processo de recuperação de palavras passe é frequentemente 100% dependente da confiança que se deposita no processo de autenticação do sistema de correio electrónico.

## *2.3 Ciberespionagem industrial com envolvimento estatal*

A espionagem industrial tem muitas faces, a maioria relacionada com abordagens sociais, nomeadamente o suborno de funcionários das empresas atacadas. No entanto, as empresas mantém, cada vez mais, um conjunto grande de dados em suporte digital, frequentemente em máquinas ligadas à rede, e as comunicações entre os funcionários das empresas, mesmo as que abordam assuntos confidenciais, são frequentemente efectuadas através de recursos digitais, como o correio electrónico, sem a preocupação de cifrar a informação. Estes factos, estão a tornar a espionagem industrial com recurso a técnicas de *hacking* cada vez mais frequentes, quer através de ataques a máquinas, quer através da intercepção de comunicações. Os Estados, graças à capacidade instalada, por motivos relacionados com a segurança e com a defesa, e à importância da economia no desempenho de um país, têm uma presença muito relevante nestas actividades, muito embora essa participação seja mais forte em determinados momentos do que noutros.

A actividade de intercepção de comunicações civis realizadas pelos governos no âmbito das suas actividades de segurança e defesa tornaram-se, após os ataques da *Al-Qaeda* em 11 de Setembro de 2001, um assunto pouco discutido e, para a generalidade dos decisores, dado como um mal necessário. Mas nem sempre foi assim, principalmente na Europa, onde a tradição de defesa dos direitos do cidadão tem já alguma idade e onde existem diversos partidos com uma ideologia de esquerda que, nos tempos mais recentes, tende a manifestar-se contra o desenvolvimento militar. De facto, no dia 5 de Setembro de 2001 o Parlamento Europeu, após um debate em plenário, aprovou uma

resolução que exige o reforço das medidas de protecção da privacidade do cidadão e de monitorização das actividades normalmente designadas de inteligência (Parlamento Europeu, 2001).

O Parlamento Europeu dispõe de diversos relatórios técnicos relativos aos sistemas em utilização pelas agências de segurança das várias potências militares existentes para recolha, monitorização e tratamento das comunicações internacionais (Comissão Temporária sobre o Sistema de Intercepção ECHELON, 2001)

O primeiro relatório a provocar agitação no Parlamento Europeu data de Janeiro de 1998 e foi elaborado pelo gabinete de *Scientific and Technology Options Accessment* (Campbell, 2001) – STOA – com o objectivo de ajudar a esclarecer as capacidades do sistema ECHELON, posto a descoberto pela imprensa mas não reconhecido oficialmente, e as respectivas consequências. Uma das consequências do debate foi a encomenda, por parte do STOA, de dois estudos com o objectivo de compreender as consequências das capacidades instaladas de intercepção de comunicações na protecção da actividade económica europeia. Um desses estudos viria a ser conhecido como o relatório IC2000, Interception Capabilities 2000, ou como relatório Campbell, mas o seu título completo é bem mais esclarecedor: “O Estado da Arte na Inteligência de Comunicações (COMINT), do Processamento Automatizado, para Efeitos de Inteligência, de Intersecção de Sistemas de Transporte, Dedicados ou Comuns, Multilingues e em Banda Larga, e da sua Aplicabilidade à Selecção e Objectivos da COMINT, Incluindo o Reconhecimento da Fala”. O IC2000 foi apresentado ao Parlamento Europeu em Fevereiro de 2000 numa reunião sobre privacidade e protecção de dados, que viria a resultar na constituição de uma comissão temporária de 36 deputados, liderada por Carlos Coelho, encarregue de aprofundar o estudo sobre as implicações das questões levantadas para a privacidade dos cidadãos e para a salvaguarda das empresas europeias. A comissão viria a concluir da indubitabilidade da existência do ECHELON e a emitir um alerta para o facto de que este sistema representava uma ameaça ao

comércio e à privacidade, alertando também para a existência de violações das convenções sobre direitos do homem, no que diz respeito ao seu direito à reserva da sua intimidade e à privacidade (Campbell, 2001).

O sistema ECHELON foi, alegadamente, desenvolvido pelos Estados Unidos da América e pelo Reino Unido, aos quais se juntaram mais tarde a Austrália, o Canadá e a Nova Zelândia, para interceptar e monitorizar as comunicações comerciais via satélite, após o lançamento da constelação de satélites de comunicações denominada Intelsat. Este e/ou outros sistemas terão sido utilizados na aquisição de informação de carácter comercial para alterar as relações de força existentes no mercado. De acordo com o *Washington Post*, citado pelo IC2000, a CIA (*Central Intelligence Agency*) e a *National Security Agency* (NSA) terão estado directamente envolvidas na escolha pelo governo saudita das empresas *Boeing* e da *McDonnell Douglas*, em detrimento da *Airbus*, num contrato de seis milhões de dólares. Mas, aparentemente, este não foi caso único e, na verdade, parecem ter sido imensas (pelo menos centenas) as empresas prejudicadas durante a década de 90, em particular empresas francesas e japonesas, pela actuação das agências de segurança, numa altura em que os Estados Unidos da América eram liderados pelo presidente Bill Clinton, eleito com um programa assente na recuperação económica do país. Os dados conhecidos parecem indicar que perto de 10% do mercado internacional conquistado pelos Estados Unidos da América na década de 90 esteve intimamente ligado à actuação dos organismos de espionagem que, tendo a sua actividade militar reduzida, concentraram a sua capacidade no apoio aos interesses económicos americanos (Campbell, 2001; Comissão Temporária sobre o Sistema de Intercepção ECHELON, 2001).

O sistema ECHELON terá sofrido evoluções constantes de forma a abarcar um leque cada vez mais variado de formas de comunicação, incluindo a Internet, e a processar um número sempre crescente de dados por segundo. Os fabricantes norte-americanos de *software* estão também sujeitos às leis de protecção das técnicas criptográficas, o que levanta dúvidas sobre a segurança

dos métodos criptográficos implementados (Campbell, 2001; Comissão Temporária sobre o Sistema de Intercepção ECHELON, 2001).

Mais recentemente, um outro país tem sido repetidamente acusado de utilizar os recursos digitais para a espionagem industrial. Trata-se da República Popular da China, um país emergente que tem conseguido alcançar uma posição internacional de relevo a nível militar, político e económico.

## *2.4 A República Popular da China – a ciberpotência emergente*

A China desempenhou durante séculos um papel de liderança regional, sendo um dos países mais desenvolvidos cientificamente até ao século XVIII. As opções culturais e políticas tiveram implicações económicas que impediram a agora denominada República Popular da China de assumir uma posição dominante no mundo no final do século XX. No entanto, o século XXI tem correspondido a um período de reorganização desta nação e as suas estruturas têm recuperado a grandeza de outros tempos, nomeadamente a militar, fruto do crescente investimento da área da defesa. A figura Figura 36 apresenta o orçamento anunciado pelo governo da República Popular da China desde 1996, bem como as estimativas do Departamento de Defesa dos Estados Unidos da América para os gastos reais, já que existem indicadores de que os dados oficiais correspondem apenas a alguma das componentes do orlamento da defesa chinesa (Department of Defense, 2008. Com uma população estimada de mais de 1300 milhões de habitantes (sujeita a serviço militar obrigatório por 24 meses) e um produto interno bruto que além de já ser significativo apresenta crescimentos acima de 10% ao ano (Central Intelligence Agency, 2008), a China tem condições para criar um exército com uma capacidade operacional incontornável no equilíbrio internacional. Acrescem a este facto a tradição milenar na área dos estudos de estratégia militar e a experiência de espionagem e contraespionagem modernas do período da Guerra Fria. Assim, é sem surpresa que se constata que a China tem estado activa na sua preparação para

um eventual ciberconflito e que é frequentemente apontada como responsável por diversas acções de espionagem económica e militar no ciberespaço.

No que respeita à reflexão sobre a importância do combate digital, a China tem alguns dos primeiros documentos sérios sobre o assunto, sendo pioneira no seu estudo. O primeiro documento produzido pelo exército chinês sobre guerra da informação terá sido publicado em 1985 mas foi com a Guerra do Golfo, em 1991, que a atenção dos militares se focou sobre os recursos da era digital.

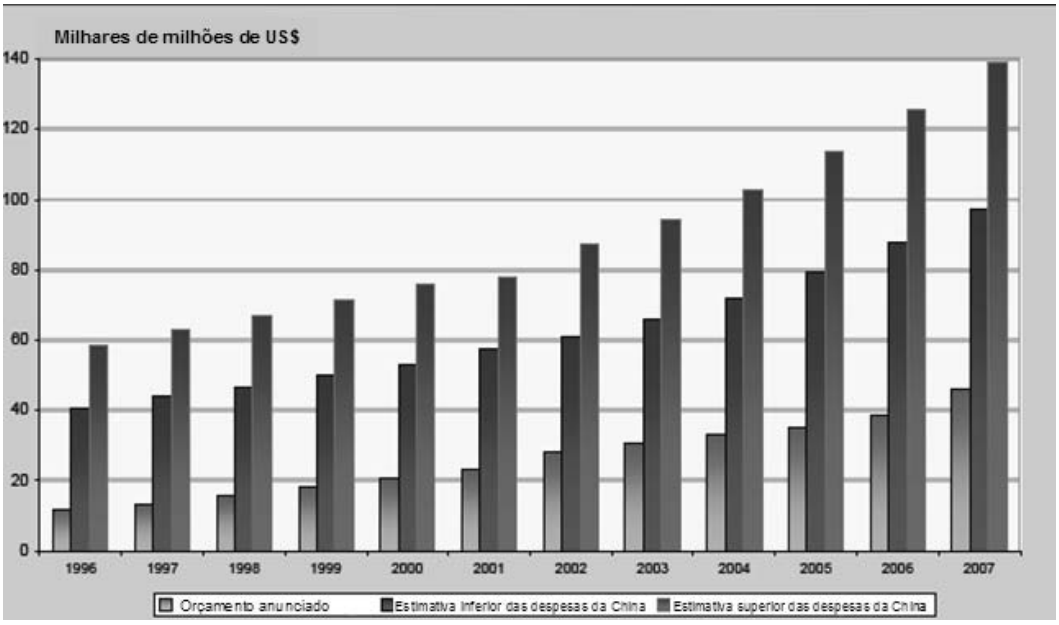



*Figura 36 – Orçamento anunciado e estimado para despesas de defesa da República Popular da China desde 1996 (Department of Defense, 2008)*

Em 1995 o Major General Wang Pufeng, da Academia de Ciências Militares de Pequim publicou um documento dedicado aos desafios da *Information Warfare.* Nesse trabalho é salientada a importância estratégica do controlo da informação dos recursos conducentes à informação, requerendo mais formação e desenvolvimento de tecnologias da era da informação do que equipamentos da era industrial. Pufeng reflecte sobre as particularidades da guerra da informação e conclui da necessidade estratégica de formar quadros tecnologicamente

capazes, desenvolvendo o estudo da tecnologia tanto nos ambientes militares como no ensino regular (Pufeng, 1995).

Em 1999, o Coronel Qiao Liang e o Coronel Wang Xiangsui, do Exército de Libertação Popular, publicaram o livro *超限战* (literalmente "Guerra para lá dos limites"), traduzido e divulgado no ocidente pelo *Foreign Broadcast Information Service* (FBIS) da CIA (Liang & Xiangsui, 1999). Neste livro, conhecido no ocidente pelo título em Inglês *Unrestricted Warfare*, os autores reflectem sobre a forma como as formas não convencionais de combate poderiam permitir à China ultrapassar as suas limitação militares existentes no final do Século XX, dados os preços de aquisição e/ou desenvolvimento de equipamento militar como o que estava disponível para uma potência económica como os Estados Unidos da América. As principais formas alternativas de combate apontadas são:

- A guerra comercial: a alteração das leis comerciais e das tarifas alfandegárias, a imposição de sanções comerciais ou de embargos à exportação de tecnologias críticas e o favorecimento do comércio com algumas nações podem ter efeitos devastadores no inimigo. Os autores apontam como exemplo as sanções económicas impostas ao Iraque após a operação "Tempestade no Deserto" (Liang & Xiangsui, 1999).

- A guerra económica: alteração das condições de mercado de forma a gerar uma crise económica e, com isso, subjugar o inimigo. Os autores referem o uso do Marco Alemão para forçar a queda do Muro de Berlim e a situação da Albânia (Liang & Xiangsui, 1999).

- A guerra ecológica: alteração do estado natural dos rios, dos oceanos, da crosta terrestre ou de outros elementos da natureza por forma a criar calamidades naturais provocadas deliberadamente pelo Homem. Os autores reflectem sobre a possibilidade de a médio prazo ser possível gerar, com o objectivo da guerra, por exemplo um *el-niño,* e referem um

> exemplo deste tipo de acção de combate: o uso na guerra do Vietname de pó de iodeto de prata para provocar chuvas torrenciais e de desfolhantes para despir a floresta subtropical. Parece ser mais provável que uma guerra ecológica seja iniciada por uma organização terrorista, já que estas não sentem que tenham uma responsabilidade perante as pessoas ou a sociedade em geral e que a sua actividade é gerar o terror sem respeitar regras (Liang & Xiangsui, 1999).

Liang e Xiangsui afirmaram que "*the advent of bin Ladin-style terrorism has deepened the impression that a national force, no matter how powerful, will find it difficult to gain the upper hand in a game that has no rules*" (o advento do terrorismo do tipo do de Bin Laden fortaleceu a impressão de que uma força nacional, por muito poderosa que seja, terá dificuldade em levar a melhor num jogo sem regras) e também que existiria uma incapacidade do exército norte americano para lidar com eventos como uma intrusão informática, uma grande explosão no *World Trade Center* ou um ataque bombista de Bin Laden (Liang & Xiangsui, 1999). Estas reflexões seria confirmadas dois anos depois com os atentados da *Al-Qaeda* ao *World Trade Center* e a guerra antiterrorismo que passados sete anos ainda não produziu os resultados desejados.

A obra de Liang e Xiangsui demonstra a existência de oficiais superiores das forças armadas chineses que já em 1999 compreendiam, por um lado que a popularização dos computadores pessoais e a criação da Internet resultava na possibilidade de actos maliciosos realizados por *hackers* alterarem a ordem social vigente e, por outro lado, que o conceito de guerra mudou, deixando de ser um exclusivo dos militares ambicionando a destruição directa do inimigo, para passar a ser um conjunto de acções em diversas áreas que não são tradicionalmente consideradas como guerra, apenas por não serem actividades militares.

Com a disseminação dos computadores, o crescimento da Internet, o crescimento económico da China e a sua influência crescente no mundo,

aumenta a importância da guerra não convencional e da vantagem competitiva proporcionada pela liderança no tabuleiro da espionagem cibernáutica. Como resultado da consciência desse facto e da implementação concreta de estratégias com vista ao seu aproveitamento temos um conjunto crescente de nações que se queixam de ataques cibernáuticos por parte da República Popular da China, o que é ainda mais relevante quando a China é o país que inventou o conceito de "Guerra do Povo" e existem documentos militares que reflectem sobre a extraordinária adequação deste conceito ao combate cibernáutico (Wei, 1996; Pufeng, 1995) num país com dezenas de milhões de utilizadores da Internet. Acresce a este número a comunidade chinesa residente no estrangeiro e que, no caso de existir um ciberconflito, pode atacar os países a partir do seu próprio território, recorrendo aos fornecedores de Internet e à largura de banda do próprio país atacado, inviabilizando desta forma o uso de filtros no tráfego internacional como forma de restauro da operacionalidade interna dos serviços afectados. De acordo com os dados disponíveis, no início da década de 1990 residiam fora da China perto de 37 milhões de chineses, em 136 países, estimando-se que em 2016 sejam cerca de 76 milhões (Postan, Mau, & Yu, 1994). Dados oficiais indicam que em 2006 residiam nos Estados Unidos da América 1,6 milhões de pessoas nascidas na China, dos quais mais de 1 milhão eram adultos em idade activa (Terrazas & Devani, 2008) e em 2003 residiam na União Europeia mais de 150.000 imigrantes nascidos na República Popular da China (Laczko, 2003).

As actividades de espionagem através da Internet, embora negadas pelo governo de Pequim, são actualmente assumidas pelos governos ocidentais como um facto. Como veremos adiante, vários jornais reputados têm divulgado situações em que as actividades chinesas foram detectadas, mas em Junho de 2008 o congressista Frank Wolf divulgou no seu discurso ao Congresso (Wolf, 2008) que um relatório de 2007, classificado, sobre o estado das relações económicas e de segurança entre os Estados Unidos e a República Popular da

China apresenta conclusões alarmantes, referindo-se a actividade chinesas nas áreas da espionagem, da ciberguerra e da proliferação de armas.

No seu discurso ao congresso, Wolf declarou que o *Congressional Research Service* acredita que o ataque realizado em 2004, com o nome de código *Titan Rain*, que permitiu o acesso a informação sensível localizada em computadores da *Lockheed Martin*, da *Sandia National Labs* e da NASA (*National Aeronautics and Space Administration*) foi proveniente da China (Wolf, 2008). A *Lockheed Martin* é um fabricante de produtos aeroespaciais e o *Sandia National Labs* é um centro de investigação e desenvolvimento operado por uma subsidiária da *Lockheed Martin* para a Administração Nacional de Segurança Nuclear do Departamento de Energia dos Estados Unidos da América. Mas existem, como veremos de seguida, outras fontes oficiais que asseguram a existência de actividade cibernáutica ilegal. No que respeita ao *Titan Rain*, a *Time Magazine* tem uma reportagem onde detalha muita da informação obtida sobre este ataque, disponibilizada por um ex-agente envolvido nas actividades de contra-informação. Aparentemente, esses ataques partiam de perto de trinta máquinas instaladas na provincia chinesa de Guangdong e durante meses permitiram a cópia de informação proveniente de diversas fontes, como aquelas referidas por Wolf mas também como a base militar de Redstone Arsenal (“The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)”, 2005).

A capacidade militar da República Popular da China tem sido reportada pelo Departamento de Defesa, através do Pentágono, ao Congresso anualmente desde 2002 e, desde então, as referências à visão estratégica da República Popular da China e à correspondente implementação táctica, no que respeita à guerra da informação têm sido uma constante.

Em 2002 e 2003 os relatórios faziam referência à evolução sistemática da capacidade chinesa de C4I (*Command, Control, Communications, Computers, and Intelligence*) e à sua vontade de continuar esse progresso, além de referirem a aptidão da China para o desenvolvimento de meios assimétricos,

nomeadamente na área das operações de informações. Os relatórios afirmam que as forças armadas chinesas têm recrutado especialistas em tecnologias de informação por forma a assegurarem uma capacidade real de acção tanto defensiva como ofensiva e ambos os relatórios afirmam categoricamente que a China dispõe da capacidade para penetrar em sistemas informáticos norte-americanos com defesas mais pobres e utilizar ataques por redes informáticas para alvejar infraestruturas civis e militares dos Estados Unidos da América. Além disso, a investigação em curso na China tem como resultado um aumento do entendimento do comportamento e disseminação dos virus informáticos, o que cria uma base de conhecimento sólida não apenas para a defesa dos sistemas informáticos, mas também para o ataque de redes de computadores, através do desenvolvimento de *software* malicioso. Os relatórios fazem ainda referência à possibilidade do espírito nacionalista dos cibernautas chineses, em número crescente, poder ser utilizado para a aplicação do princípio da guerra do povo ao espaço digital (Department of Defense, 2002; Department of Defense, 2003).

Os relatórios do Pentágono de 2004 e 2005 estiveram essencialmente focados na capacidade/vontade da República Popular da China atacar a ilha Formosa, principalmente o relatório de 2005. Ainda assim, faziam referência à alteração da visão chinesa da forma moderna de actuação em combate, resultante essencialmente da análise da Operação Iraque Livre. De acordo com os relatórios, a actuação combinada dos meios aéreos e dos meios terrestres alterou a visão chinesa da importância da força aérea na subjugação de um país e, se já existia uma preocupação com a evolução dos equipamentos de C4I, notou-se em 2004 e em 2005 uma preocupação acrescida com o investimento em C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance*). Os relatórios salientavam a estratégia governamental chinesa para, através da regulamentação do acesso ao mercado chinês, forçar as grandes empresas tecnológicas internacionais a transferir tecnologia, partilhar *know-how* e abrir centros de investigação e desenvolvimento

na China (Department of Defense, 2004, 2005). Ainda assim, os relatórios dão pouca credibilidade à capacidade tecnológica da China, afirmando que:

> *"(...) poor information technology management skills and a corporate culture that does not emphasize innovation are hindering development of advanced technology capabilities and programs*" (Department of Defense, 2004).

ou seja,

> as fracas competências de gestão da tecnologia de informação e uma cultura empresarial que não enfatiza a inovação estão a impedir o desenvolvimento de programas e capacidades tecnológicas.

O relatório de 2006 dedica alguma atenção à formação de unidades de reservistas dedicada à guerra da informação, bem como a constituição de milícias informáticas que poderiam apoiar, através de ciberataques, a actuação do exército regular chinês em caso de conflito. É ainda apontada a participação regular das unidades militares de reservistas e mesmo das milícias em treinos e exercícios militares, mesmo naqueles que abordam as tácticas militares ofensivas. No entanto, algumas afirmações de dirigente chineses relativos a uma possível alteração da sua filosofia de uso do armamento nuclear monopolizou a atenção do Pentágono e, consequentemente, o relatório é essencialmente dedicado à capacidade chinesa de actuação nuclear (Department of Defense, 2006).

O relatório de 2007 dá pouco relevo às questões relacionadas com a guerra da informação, embora refira o reforço dos conceitos relacionados com uma visão mais global da actividade de guerra (Department of Defense, 2007). No entanto, o relatório de 2008 apresenta uma secção dedicada à capacidade

chinesa de ciberguerra, indicando a República Popular da China como a origem provável de várias intrusões nas redes do Departamento de Defesa. de outros departamentos e agências governamentais e de empresas com contratos de desenvolvimento militar com os Estados Unidos da América (Department of Defense, 2008). Segundo o *Financial Times*, um desses ataques bem sucedidos conseguiu forçar o Pentágono a desligar parte da sua rede durante semanas, enquanto os ataques continuaram a decorrer ("Chinese hacked into Pentagon", 2007). Uma vez que os ataques continuaram após a rede ser desligada, logo o ataque tinha sido detectado, é provável que este ataque represente uma avaliação de situação, que permitirá o seu estudo e a reflexão sobre formas de actuação em situações de conflito. Esse pode ter sido também o caso no apagão de 2003 que deixou 40 milhões de pessoas sem energia eléctrica durante 24 horas e que, de acordo com o *National Journal Magazine*, terá sido também provocado por *hackers* sediados na China (Harris, 2008).

Pelos casos apresentados é possível depreender a capacidade e a vontade chinesa no que respeita à actuação no ciberespaço. No entanto, não são apenas as empresas e o governo dos Estados Unidos da América a protestarem contra a acção da China. De acordo com o relatório da McAfee sobre criminalidade (McAfee, 2007), em 2007 a China além de ser acusada de atacar sistemas nos Estados Unidos da América é também o principal suspeito de ataques realizados na Índia (*National Informatics Center*), na Alemanha (Chancelaria), na Nova Zelândia e na Austrália (sistemas governamentais não especificados). A imprensa, citando fontes oficiais, anunciou ainda ataques provenientes da República Popular da China a sistemas governamentais franceses (Mandraud, 2007) e a sistemas empresariais críticos britânicos. De acordo com o governo britânico, os ataques são provenientes do exército chinês e foram desenhados para ultrapassar sistemas com as melhores práticas de segurança da informação (Blakely, Richards, Rossiter, & Beeston, 2007). Também a Alemanha terá sido vítima de ataques provenientes da China mas, graças a uma rápida intervenção para criar a maior operação de defesa digital

alguma montada na Alemanha, conseguiu impedir a transmissão de 160GB de dados provenientes dos computadores da chancelaria e de três outros ministérios (assuntos estrangeiros, economia e investigação) embora não se saiba quanta informação poderá ter alcançado o seu destino em Lanzhou (Norte da China), na Província de Cantão e em Pequim. Esta operação decorreu alguns dias antes da visita da Chanceler alemã Angela Merkel a Pequim (McAfee, 2007; "Merkel's China Visit Marred by Hacking Allegations", 2007). Mais recentemente, o Ministro da Justiça da Bélgica comunicou à imprensa a sua convicção de que o governo chinês tentou penetrar em redes informáticas críticas belgas, presumivelmente em busca de informações relacionadas com o facto de a União Europeia e a NATO estarem sediadas em Bruxelas e com as relações privilegiadas da Bélgica com alguns países de África, um continente com uma importância crescente para *o Império do Meio (*"Is China attacking Belgian computers?", 2008).

A República Popular da China nega qualquer actividade de hacking. Aliás o Ministério da Indústria da Informação acusa os Estados Unidos e as outras "potências hostis" de explorarem, com o objectivo da espionagem, as vulnerabilidades dos sistemas informáticos chineses incluindo aquelas colocadas propositadamente pelas empresas tecnológicas americanas (Buckley, 2007).

A evolução da estratégia e da capacidade da República Popular da China tende a colocar este país numa posição dominante a nível mundial o que é suficiente para assumir um papel fundamental na evolução das estratégias nacionais de defesa por todo o mundo, justificando só por si um reforço das tecnologias e das políticas de segurança dos serviços informáticos disponibilizados pelo Estado, nomeadamente no que respeita à autenticação dos utilizadores, em particular através do recurso às tecnologias biométricas. A existência de uma comunidade de sino-descendentes muito grande, com ligações emocionais e culturais à pátria dos seus antepassados mas gozando da confiança dos países de nascimento, reforça a necessidade de criação de processos que impeçam a transmissão das credenciais de autenticação, mesmo

a transmissão voluntária, desaconselhando portanto tecnologias como a impressão digital que, embora seja biométrica permite a transmissão das credenciais se essa for a vontade do seu proprietário, já que é possível fazer um molde das impressões que pode então ser livremente utilizado. É, portanto, necessário encontrar tecnologias abrangentes, de baixo custo e que dificultem, tanto quanto possível, a transmissão do segredo de autenticação. Algumas tecnologias biométricas representam a solução para este problema como veremos adiante.

# 3 As tecnologias biométricas e a autenticação gráfica

O termo biometria deriva do grego bios (vida) + metron (medida) e, nos sistemas de informação (SI), refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um SI de uma organização.

O problema de estabelecer uma associação entre um indivíduo e uma identidade, denominado reconhecimento, pode ser dividido em duas categorias: autenticação e identificação. Autenticação refere-se ao problema de confirmar ou negar uma alegada identidade de um indivíduo, enquanto identificação refere-se ao problema de estabelecer a identidade, desconhecida à partida, de um indivíduo. Os processos de reconhecimento biométrico incluem sempre uma fase de registo do utilizador, denominada *enrolment*, que consiste na introdução dos dados biométricos, que permitirão o estabelecimento de um padrão, no sistema. Mais tarde, o padrão armazenado será comparado com os dados recolhidos aquando da tentativa de acesso ao sistema e permitirá aferir o grau de confiança na identidade do utilizador, aceitando-o ou rejeitando-o consoante esse valor seja maior ou menor que um limite estabelecido, denominado *threshold*. Este processo é facilitado na autenticação porque existe uma identidade proposta pelo utilizador e, portanto, a comparação é um-para-um. No caso de se tratar se um processo de identificação, o padrão recolhido é comparado com todos os padrões armazenados, em busca daquele que lhe é mais semelhante, um processo muito mais computacionalmente exigente e demorado.

Existem hoje muitas características utilizadas, isoladamente ou em conjunto, para autenticar e/ou identificar um sujeito. As tecnologias biométricas são, normalmente, classificadas como comportamentais (por exemplo, reconhecimento de voz) ou físicas (por exemplo, leitura de retina), de acordo com a classificação das características avaliadas. Mas elas podem também ser classificadas (Figura 37) como colaborativas, se exigem que o utilizador tenha

conhecimento da sua existência e participe conscientemente no processo, ou como furtivas, se podem ser utilizadas sem o conhecimento daquele que é identificado ou autenticado (Magalhães & Santos, 2003).

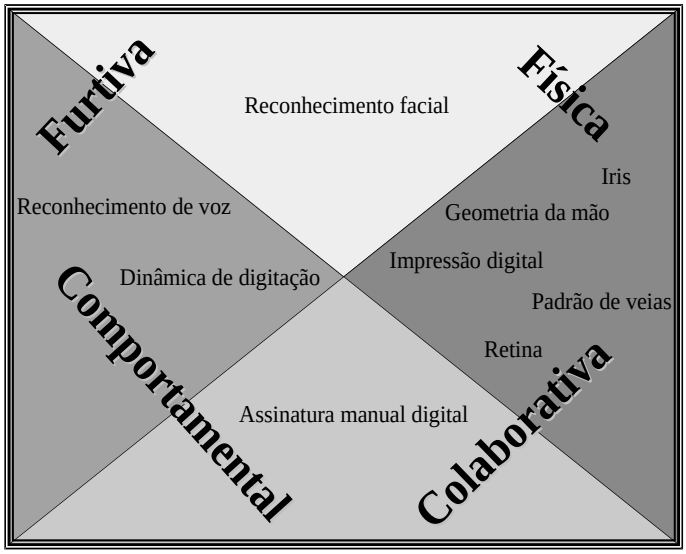



*Figura 37 – Classificação das tecnologias biométricas de autenticação*

O grau de fiabilidade de uma tecnologia biométrica pode ser aferido atendendo aos valores de FAR (*False Acceptance Rate* – Taxa de Falsas Aceitações) e de FRR (*False Rejection Rate* – Taxa de Falsas Rejeições). Infelizmente estas variáveis são mutuamente dependentes, não sendo possível minimizar ambas num mesmo algoritmo. Assim, normalmente procura-se o ponto de equilíbrio ou de igualdade (Figura 38) a que chamamos CER (*Crossover Error Rate* – Taxa de Intersecção de Erros) ou EER (*Equal Error Rate*). Quanto mais baixo for o CER mais preciso é um sistema biométrico (Poh & Korczak, 2001).

A escolha do(s) método(s) a utilizar depende da análise de risco que necessariamente deve ser feita, relativamente à informação/infra-estrutura que se pretende proteger. Por exemplo, a *Central Intelligence Agency*, o *Federal Bureau of Investigation* e a *National Aeronautics and Space Administration* utilizam leitores de retina para proteger o acesso a zonas sensíveis. No entanto, seria excessivamente dispendioso e desajustado utilizar leitores de retina para

autenticar/identificar o utilizador de cada computador pessoal de cada serviço da Administração Pública.

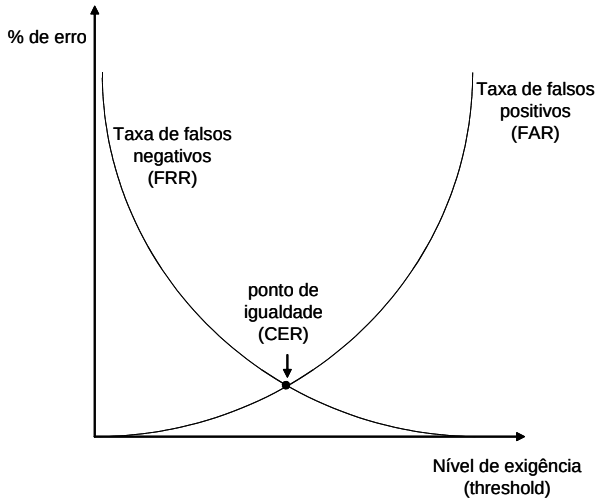



*Figura 38 – Crossover Error Rate (CER)*

Perceber os níveis de precisão das tecnologias biométricas é uma tarefa difícil, não só pela complexidade dos testes necessários para os conhecer, mas pela dificuldade de obter esses dados do universo de empresas fabricantes destes dispositivos de autenticação, pelo que as secções seguintes limitar-se-ão a descrever, de uma forma não exaustiva, cada tecnologia e só apresentarão valores de precisão quando existirem testes exaustivos realizados por entidades idóneas e considerados de referência.

Um outro processo de autenticação com uma utilização crescente e com potencial para substituir as palavras passe é a autenticação gráfica. A última secção deste capítulo dedica-se à descrição dos trabalhos existentes nessa área de investigação.

## *3.1 Reconhecimento facial*

O processo de reconhecimento facial tem início com a captura de uma imagem, seguida da detecção de um rosto que será comparado com modelos armazenados numa base de dados, comparação essa complementada com a

análise da cor da pele, detecção de linhas ou ainda de um modelo híbrido (Thian, 2001). As maiores dificuldades neste processo são essencialmente provocadas por diferentes orientações da cabeça (Poh & Korczak, 2001).

Os processos baseados neste tipo de biometria foram durante muito tempo limitados pelo facto de o utilizador ter que ser enquadrado com o modelo, dada a dificuldade (processamento necessário) em adaptar o modelo à sua cara, isto para além da necessidade de adaptar o modelo a todas as condições que podem alterar a aparência de um indivíduo, como o uso de óculos, envelhecimento, barba, etc.. Este processo baseia-se essencialmente na localização de pontos fixos como os olhos, nariz e boca (Poh & Korczak, 2001; Thian, 2001). Mais recentemente é possível verificar um aumento da capacidade dos modelos se adaptarem às posições da face, nomeadamente através do sucesso de alguns algoritmos em competições que recorrem a imagens com amplitudes de orientação das faces de 90º (Phillips et al., 2007). Um dos grandes clientes desta tecnologia é o negócio da segurança dos casinos que têm utilizado esta tecnologia com sucesso para criar uma base de dados de faces de burlões, de modo a facilmente serem identificados (Liu & Silverman, 2001).

O *Counterdrug Technology development Program Office* do Departamento de Defesa dos Estados Unidos da América promoveu o *Facial Recognition Vendor Test 2002* (FRVT2002) num esforço internacional de colaboração com diversas entidades governamentais como, por exemplo, o FBI, o *Canadian Passport Office*, o *Australian Customs* e o *United Kingdom Biometric Work Group*. Participaram dez algoritmos neste teste de grupo. Os valores exactos de FAR e FRR não se encontram disponíveis. No entanto, por observação dos gráficos, podemos obter valores aproximados. A Tabela 3 sistematiza os desempenhos do melhor algoritmo, considerando diversas combinações dos dois parâmetros, FAR e FRR.

Da informação disponibilizada pode-se concluir que a autenticação/identificação com recurso a esta classe de tecnologias é mais precisa em indivíduos do sexo masculino do que em indivíduos do sexo feminino.

Ainda assim, a maturidade actual destas tecnologias parece estar ao nível em que se encontravam em 1998 as tecnologias biométricas baseadas na impressão digital (Phillips et al., 2003), com a agravante de ser uma biometria muito dependente das condições de ambiente como se pode observar, na Figura 39, pela variação da taxa de verificações (igual a 1-FRR) em contextos diferentes.

| *FAR* | *FRR* | *Género* |
|---|---|---|
| *0,0001* | 0,275 | Masculino |
| | 0,29 | Feminino |
| *0,001* | 0,09 | Masculino |
| | 0,12 | Feminino |
| *0,01* | 0,09 | Masculino |
| | 0,11 | Feminino |
| *0,1* | 0,04 | Masculino |
| | 0,05 | Feminino |

*Tabela 3 – Fiabilidade do Reconhecimento Facial de acordo com o FRVT2002*

Outra característica interessante dos algoritmos de reconhecimento facial que se apresentaram ao FRVT2002 é a sua dependência da idade do utilizador, verificando-se que os algoritmos são, tendencialmente, mais precisos ao avaliar indivíduos mais velhos (Figura 40).

Em 2006 realizou-se o FRVT 2006 com a participação de 22 organizações de 10 países diferentes, notando-se uma evolução muito significativa da precisão dos algoritmos apresentados a concurso, conseguindo-se um algoritmo automático com precisão de FRR de 1% para uma FAR de 0,1%, o que representa uma evolução muito significativa numa tecnologia que 10 anos antes, para a mesma FRR, apresentava uma FAR superior a 50% (Figura 42) (Phillips et al., 2007). Esta evolução é resultado da evolução dos algoritmos, mas é também consequência da evolução dos recursos de digitalização de imagens, nomeadamente a foto digital, bem como da capacidade de processamento dos computadores utilizados.

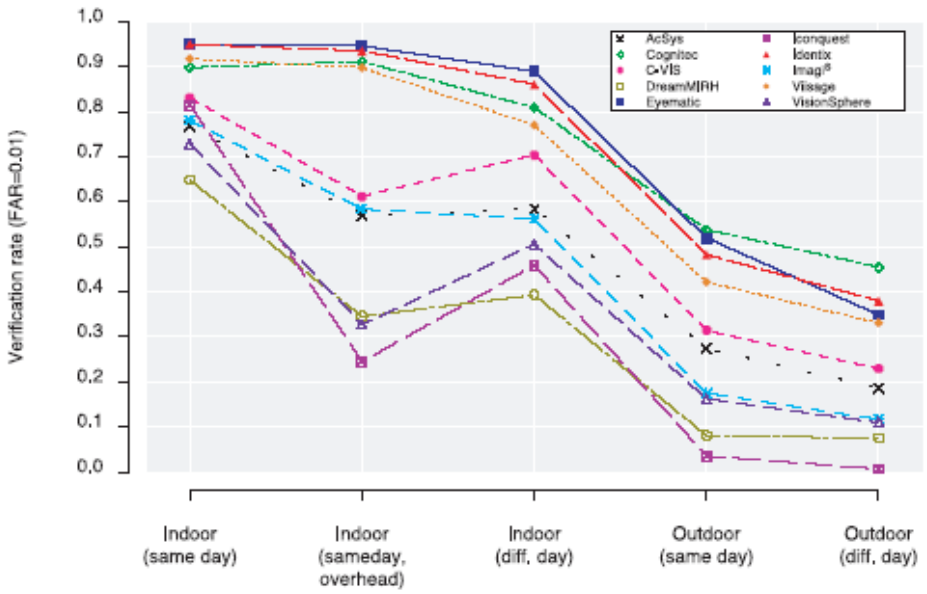



*Figura 39 – Performance de algoritmos de reconhecimento facial em diferentes contextos. Fonte: (Phillips et al., 2003)*

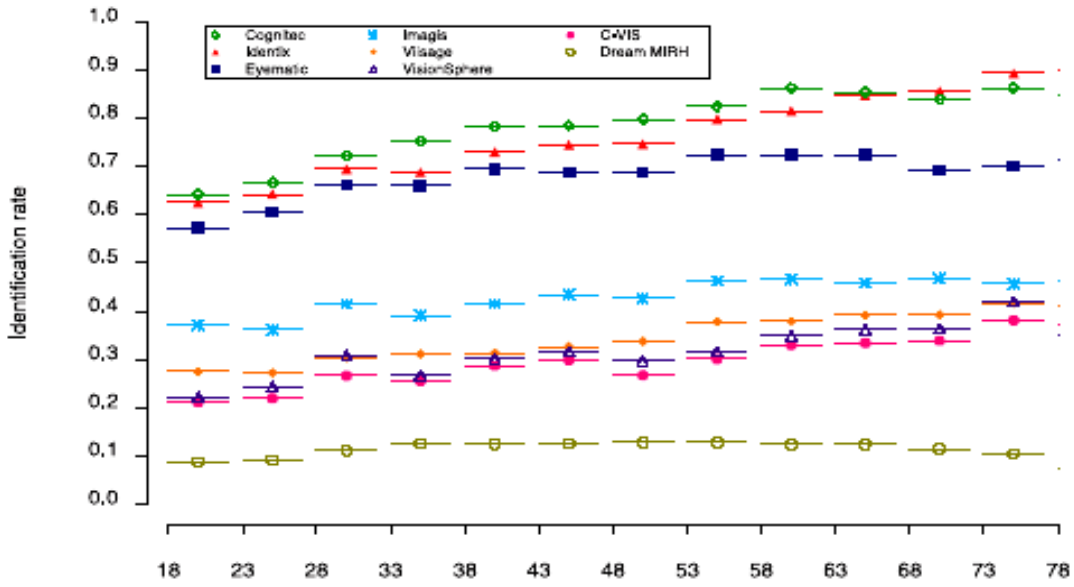



*Figura 40 – Performance de algoritmos de reconhecimento facial de acordo com a idade do utilizador. Fonte: (Phillips et al., 2003)*

A evolução da tecnologia de reconhecimento facial evoluiu de tal forma que os melhores algoritmos apresentados ao FRVT2006 superaram o desempenho dos seres humanos, que participaram no teste como se de um algoritmo se tratasse (Figura 43). Os dados disponibilizados pelo FRVT2006 usam um esquema gráfico de representação estatística descrito na Figura 41.

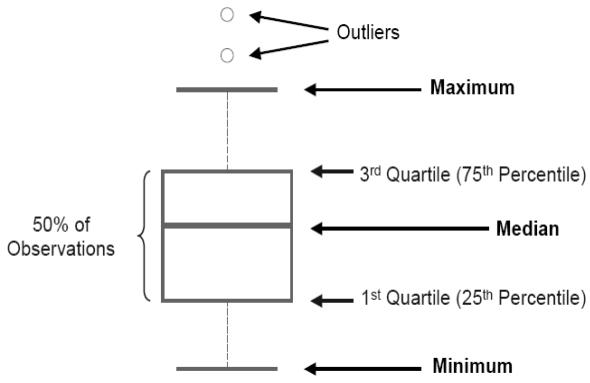



*Figura 41 – Esquema de representação estatística do FRVT2006. Fonte: (Phillips et al., 2007)*

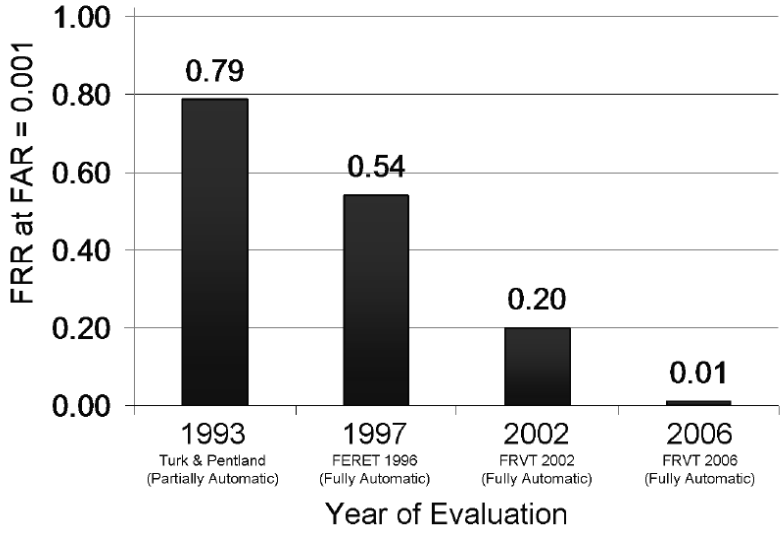



*Figura 42 – Evolução da precisão dos algoritmos de reconhecimento facial - fonte: (Phillips et al., 2007)*

Apesar do bom desempenho dos melhores algoritmos apresentados a concurso no FRVT2006, a tecnologia de reconhecimento facial não estava ainda em 2006 com um nível de maturidade que permita o reconhecimento público da tecnologia. Como se pode verificar na Figura 44 os algoritmos apresentam valores de precisão muito piores quando se passa do grupo de imagens de muito alta resolução (fotografias obtidas com uma *Nikon D70* de 6 megapixéis) para o grupo de alta resolução (fotografias obtidas com uma *Canon PowerShot G2* de 4 megapixéis) e ainda mais quando se passa para o grupo de baixa resolução (fotografias tiradas com condições de luz controladas, com uma dimensão de arquivo de 10000 bytes e aproximadamente 75 pixéis entre os centros dos olhos). Ainda assim, faltará algum tempo para que o equipamento informático disponha de forma generalizada de dispositivos de captação de imagem com capacidade adequada para um bom desempenho com os algoritmos existentes.

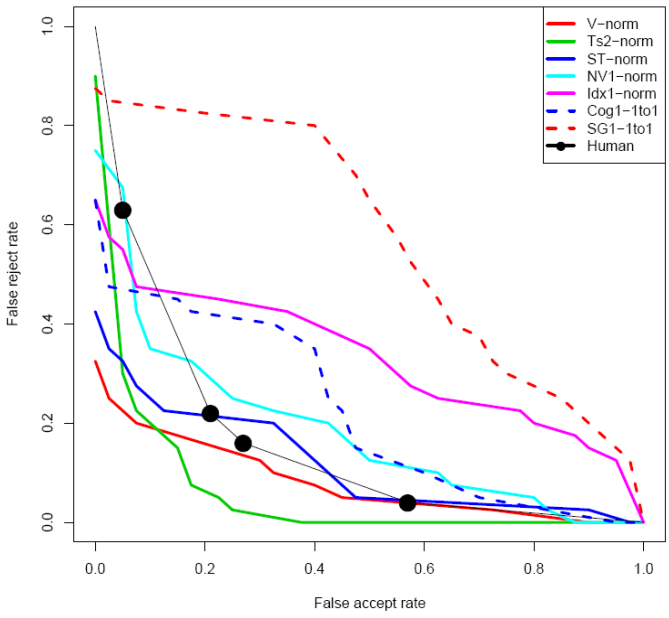



*Figura 43 – Comparação do desempenho dos algoritmos em comparação com o ser humano. Fonte: (Phillips, 2006)*

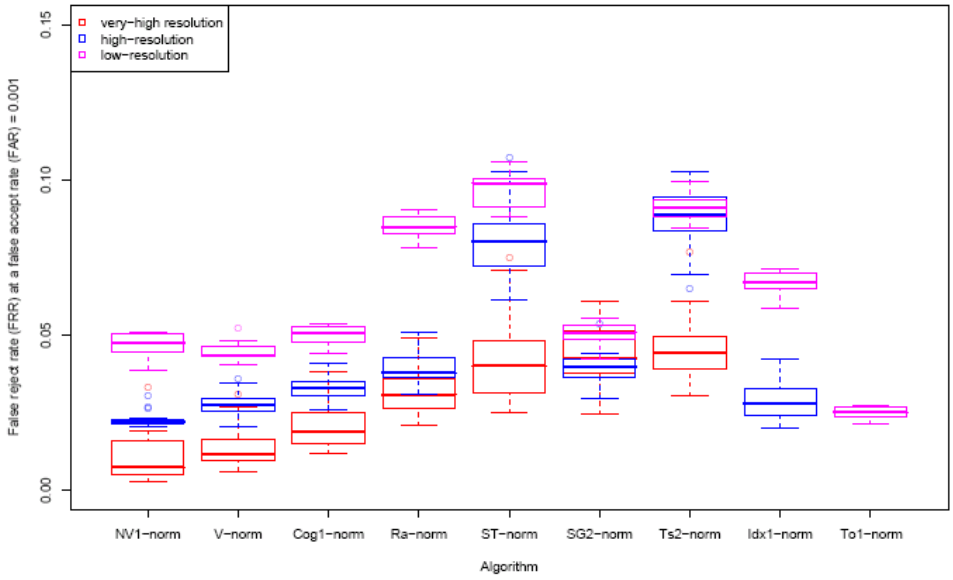



*Figura 44 – Desempenho dos melhores algoritmos de reconhecimento facial no FRVT2006. Fonte: (Phillips et al., 2007)*

Uma tecnologia emergente, derivada do reconhecimento facial tradicional, é o reconhecimento facial tridimensional. O FRVT2006 também contemplou este tipo de algoritmos, testados com um conjunto de imagens tridimensionais obtidas com um sensor Minolta Vivid 900/910. Também esta tecnologia está fortemente dependente da evolução das tecnologias de suporte, que neste caso são ainda mais recentes. Ainda assim, a Figura 45 mostra que os algoritmos submetidos à competição têm já um desempenho ao nível dos processos tradicionais com imagens de baixa/média resolução.

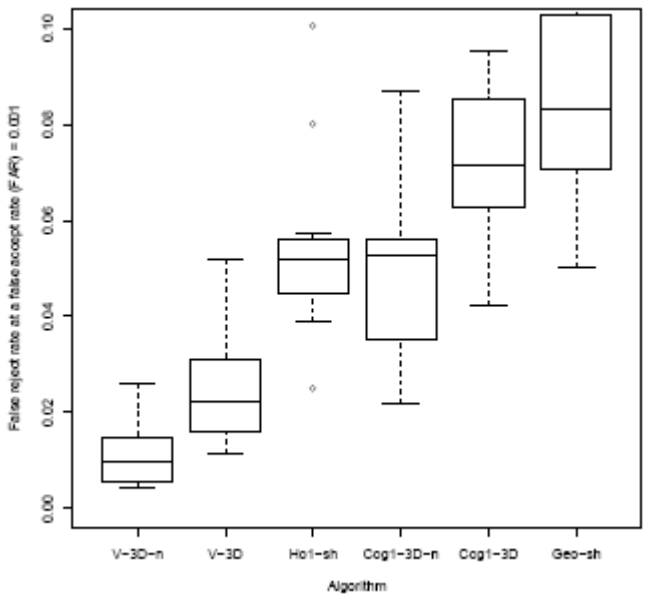



*Figura 45 – Desempenho dos algoritmos de reconhecimento facial por imagens tridimensionais. Fonte: (Phillips et al., 2007)*

## *3.2 Geometria da mão*

Em 1981 no livro publicado pelo *Office of Technology Assessment* do Congresso dos Estados Unidos da América sobre o uso da tecnologia e os correspondentes aspectos de política pública no uso de computadores nos sistemas de informação nacionais dizia-se:

> *A new and surprisingly effective form of physical identification is the geometry of the hand. Individual finger lengths vary from one person to another. This variance is sufficiently significant and unique to be the basis for a relatively inexpensive (around $3,000) identification device. It is based on the use of a high intensity light shining on a pattern of photocells. It is sensitive both to external geometry and to the translucence of the flesh near the fingertips. Thus, it is quite difficult to deceive it with any artificial device (Office of Technology Assessment, 2001).*

Quase trinta anos depois os algoritmos melhoraram, o preço foi reduzido, mas já não é fácil encontrar peritos que partilhem do entusiasmo que o texto

reflecte. Hoje, o reconhecimento da geometria da mão resulta de uma análise das características da mão combinadas entre si, como a forma, o comprimento dos dedos e as suas linhas características (Ross, 1999). Podemos ter diferentes níveis de segurança neste sistema consoante se utilizem as características em si, a posição das características relativamente a um ponto fixo ou a fixação de vários pontos e as distâncias das características relativamente a todos eles.

De realçar que a geometria da mão não é uma característica própria de cada indivíduo, mas tem a vantagem de facilmente ser combinada com outras biometrias como, por exemplo, a impressão digital (Ross, 1999).

Por outro lado, a geometria da mão, comparada com outras biometrias, não produz um grande conjunto de dados. Portanto, dado um grande número de registos, a geometria da mão pode não ser capaz de distinguir um indivíduo de outro com características da mão semelhantes (Thian, 2001).

Esta tecnologia está ainda longe da maturidade embora, quando combinada com outros factores inerentes à mão, como as linhas da palma, os valores possam melhorar consideravelmente, não pela precisão da representação mas por factores ligados aos algoritmos de decisão.

## *3.3 Impressão digital*

A impressão digital é, sem dúvida, a tecnologia biométrica mais utilizada actualmente. Embora a generalidade dos sistemas utilizados tenham um nível de fiabilidade ainda baixo, esta biometria tem um nível de aceitação muito satisfatório, provavelmente devido ao facto de a impressão digital ser há muito tempo utilizada nos registos civis, associada a documentos de autenticação/identificação.

Os equipamentos normalmente utilizados para a captura dos padrões não distinguem, eficientemente, um dedo vivo de um dedo morto (separado do utilizador legítimo ou replicado sinteticamente) sendo fácil produzir uma impressão digital sintética com ou sem a colaboração do seu proprietário. Existem leitores que tentam ultrapassar o “efeito dedo morto” recorrendo a

sensores de tensão arterial, condutividade, temperatura e leitura de padrões existentes em camadas inferiores à epiderme. No entanto, estas tecnologias são caras e ainda não atingiram o nível de maturidade desejado, além de que são frequentemente vulneráveis à utilização de uma prótese fina aplicada sobre um dedo vivo.

O FVC (*Fingerprint Verification Competition*) é um teste de grupo organizado pela Universidade de Bolonha, pela Universidade Estadual San Jose e pela Universidade Estadual do Michigan desde 2000. Enquanto o FVC 2000 contou com a participação a concurso de 11 algoritmos (Maio, Maltoni, Cappelli, Wayman, & Jain, 2001), o FVC2002 contou já com a participação de trinta e um algoritmos, entre produtos académicos, industriais e anónimos (Maltoni, Maio, Jain, & Prabhakar, 2003). Da informação disponibilizada por (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002) e (Maltoni et al., 2003) pode-se concluir (Tabela 4) da existência de um grau de maturidade já bastante elevado. No entanto, existem sistemas (mesmo comerciais) muito distantes dos valores desejados, com taxas médias de intersecção de erros (médias porque resultam do cálculo da média das taxas de intersecção de erros obtidas pelo algoritmo nas oito bases de dados utilizadas) superiores a 5%, isto é, taxas vinte e cinco vezes mais altas do que o produto melhor classificado. Devido ao grande número de métricas utilizadas, que dificultam a percepção da precisão dos sistemas avaliados, foram consideradas apenas as dez melhores taxas de intersecção de erros.

Os leitores de impressão digital vêm, frequentemente, incorporados em *hardware* de utilização comum como, por exemplo, o teclado. Torna-se então necessário conhecer o nível de precisão destes dispositivos. A única empresa que respondeu a esta questão indicou que a FAR é menor que 1% e a FRR é inferior a 2%. Aliás, a qualidade da impressão digital capturada pode variar imenso. Na Figura 46 podemos ver nove impressões digitais (de dedos diferentes) ordenadas pela sua qualidade.

| *Produto* | *EER* |
|---|---|
| *Bioscrypt Inc.* | 0,0019 |
| *Anónimo* | 0,0033 |
| *Anónimo* | 0,0041 |
| *Bioscrypt Inc.* | 0,0077 |
| *Siemens AG* | 0,0092 |
| *Neurotechnologija Ltd* | 0,0099 |
| *SAGEM* | 0,0118 |
| *Andrey Nikiforov (independente)* | 0,0131 |
| *SAGEM* | 0,0142 |
| *Deng Guoqiang (independente)* | 0,0218 |

*Tabela 4 – Fiabilidade do reconhecimento de impressão digital no FVC2002*

*Figura 46 – Impressões digitais com qualidade diferente. Fonte: (Maio et al., 2001)*

No FVC2004 obtiveram-se taxas médias de intersecção de erros com valores mais altos do que no FVC2002, denotando que o conjunto de dados biométricos agora em teste é mais exigente para os algoritmos do que o anterior. Todos os dados apresentados na Tabela 5 referem-se à competição aberta (Maio, Maltoni, Cappelli, Wayman, & Jain, 2004), isto é, com limites mais permissivos para o tempo de execução. Existem outros resultados referentes à competição *light* onde são exigidos tempos de processamento mais rápidos mas que, naturalmente, apresentam resultados, do ponto de vista da fiabilidade, mais fracos. Embora Maio (Maio *et al*., 2004) divulgue apenas os códigos de

referência dos algoritmos é possível verificar os seus criadores na página oficial do evento em http://bias.csr.unibo.it/fvc2004.

O FVC2006 veio confirmar o problema da heterogeneidade de resultados desta tecnologia. Embora ainda não seja conhecida a análise detalhada dos testes efectuados, já é do domínio público que, para as 4 bases de dados utilizadas na competição (onde foram avaliados 70 algoritmos), os melhores resultados de taxa de intersecção de erros foram 5.564%, 0.021%, 1.534% e 0.269% (Cappelli, Ferrara, Franco, & Maltoni, 2007).

| *Produto* | *EER* | *FRR para obtenção de uma FAR nula* |
|---|---|---|
| *Bioscrypt Inc. (Canadá)* | 0,0207 | 0,0621 |
| *Sonda, Ltd (Fed. Russa)* | 0,0210 | 0,0659 |
| *Institute of Automation, The Chinese Academy of Sciences (China)* | 0,023 | 0,1001 |
| *Gevarius (Rússia)* | 0,0245 | 0,0734 |
| *Jan Lunter (França)* | 0,029 | 0,03213 |

*Tabela 5 – Fiabilidade do reconhecimento da impressão digital segundo o FVC2004*

## *3.4 Leitura de Íris*

Esta tecnologia envolve a análise do anel colorido que cerca a pupila do olho humano e, sendo a menos intrusiva de todas já que funciona mesmo com óculos postos (Liu & Silverman, 2001), tem um baixo custo de implementação, já que uma câmara normal pode ser utilizada no processo, apesar da qualidade da imagem a utilizar no processo ser um factor importante a ter em conta (Thian, 2001).

A leitura de íris possui padrões de comparação com eficácia acima da média e é uma das poucas tecnologias biométricas que pode ser adequada para identificação. No entanto, a dificuldade de utilização e integração com os sistemas existentes é um obstáculo à sua utilização (Liu & Silverman, 2001).

Nos últimos anos vários investigadores e empresas dedicaram-se à investigação dos processos de reconhecimento da íris, uma vez que a patente do conceito, *Iris Recognition System*, registada por Flom e Safir (Flom & Safir, 1987) expirou em 2005 (Bowyer, Hollingsworth, & Flynn). O *Iris Challenge Evaluation 2005* – ICE2005 – e o *Iris Challenge Evaluation 2006* – ICE2006 – são uma consequência desse interesse generalizado e pretenderam avaliar a precisão dos algoritmos existentes. Este último evento foi realizado em simultâneo com o FRVT2006 pelo *National Institute of Standards and Technology* com o apoio do *Department of Homeland Security*, da *Transportation Security Administration*, do *Director of National Intelligence*, do *Federal Bureau of Investigation* e do *National Institute of Justice*. Além do objectivo fundamental do ICE2006 (a avaliação e promoção das tecnologias de reconhecimento da íris), foi ainda possível comparar o desempenho dos sistemas de reconhecimento de íris com os sistemas de reconhecimento facial (Phillips et al., 2007).

No ICE2006 participaram 8 algoritmos oriundos dos Estados Unidos da América, China, França, Japão e Reino Unido. Uma conclusão interessante do ICE2005, confirmada pelo ICE2006, é que a precisão destes algoritmos é melhor para o olho direito do que para o olho esquerdo (Phillips et al., 2007) como se verifica na Figura 47, uma informação a ter em conta na definição dos processos de utilização desta tecnologia. As imagens foram capturadas com um sensor *LG EOU2200.*

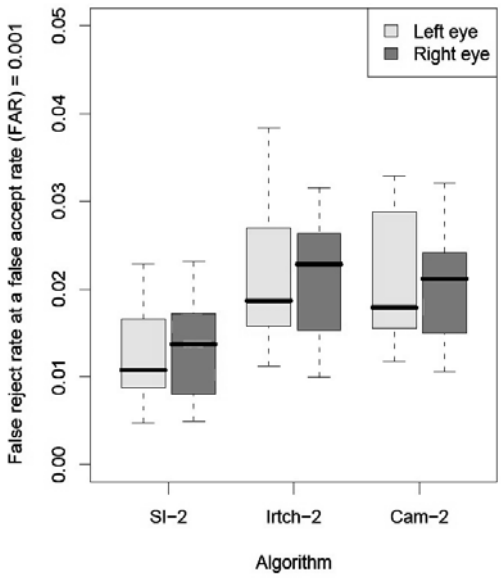



*Figura 47 – Desempenho dos algoritmos de autenticação por reconhecimento da íris. Fonte: (Phillips et al., 2007).*

## *3.5 Leitura de retina*

Os sistemas biométricos baseados na leitura de retina analisam a camada de vasos sanguíneos situada na parte de trás do olho, através da utilização de uma fonte de luz de baixa intensidade, obtendo assim padrões únicos. Esta tecnologia pode atingir altos níveis de precisão, mas requer que o utilizador olhe para dentro de um receptáculo e foque um determinado ponto, o que não é conveniente para utilizadores que usem óculos ou que receiem o contacto próximo com o leitor (Liu & Silverman, 2001).

## *3.6 Reconhecimento de voz*

Embora a informação capturável relativa à voz pareça não possuir informações suficientes para a identificação em larga escala (Jain, Hong, & Pankanti, 2000), esta tecnologia, baseada no facto de as características físicas de cada indivíduo, associadas a hábitos comportamentais, proporcionarem à sua

voz características únicas, pode ser bastante competitiva no que respeita aos protocolos de autenticação.

A voz é, antes de mais, um som. Os sons são vibrações do ar, normalmente representados pela adição de curvas sinusoidais (Figura 48) que representam os componentes de um som que têm uma determinada frequência – medida em Hertz, número de ciclos por segundo – e amplitude. Uma sequência de discurso humano é uma sequência de sons criados pelo corpo humano, começando pelas cordas vocais (excitadas pela injecção de ar enviado pelos pulmões) e moldados pela língua, pelos dentes e por outros factores da fisionomia do orador. Esta sequência, sendo a soma de diversas componentes, tem características muito irregulares. A Figura 49 mostra o espectro amplitude *versus* frequência da voz de Alanis Morissette construído com o Xanalyser, uma ferramenta de análise de frequência para o XWindow.

A abordagem tradicional no uso da voz é a modelação dos sons produzidos. Prova disso é o facto de encontrarmos os *Gaussian Mixture Models* (Modelos de Misturas Gaussianas) e os *Hidden Markov Models* (Cadeias de Markov com Estados Latentes) em vários contextos de autenticação (Fette, Broun, Campbell, & Jaskie, 2000).

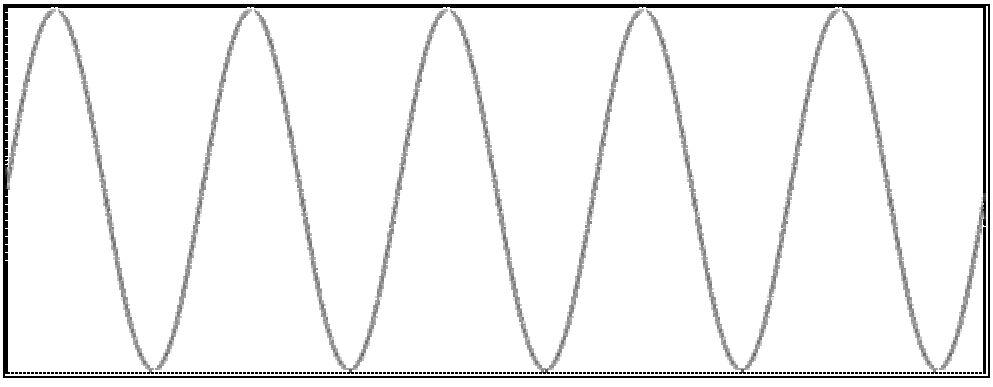


*Figura 48 – Representação sinusoidal de um som puro*

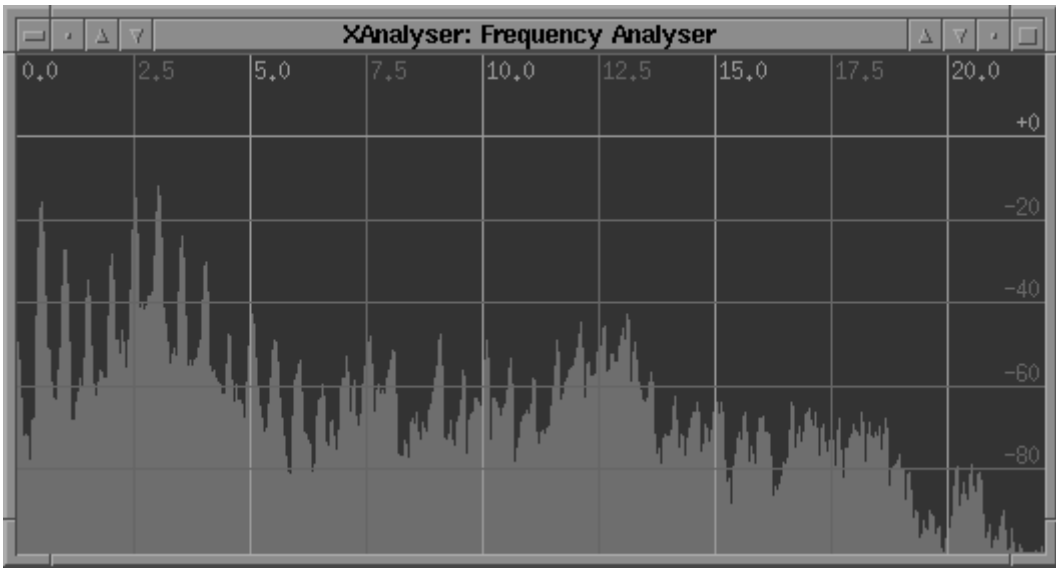



*Figura 49 – Gráfico amplitude vs frequência da voz de Alanis Morissette.*

*Fonte: http://www.suse.de/~arvin/xanalyser*

A qualidade da extracção das características da voz influência, como é fácil de perceber, o desempenho do sistema. Existem diversos parâmetros da voz que podem ser utilizados e no processo convencional de reconhecimento de voz os processos de captação da voz são independentes dos processos de classificação, sendo estes últimos os responsáveis por obter uma decisão relativa ao sucesso ou insucesso da autenticação. É também necessário considerar o ruído associado e que reduz a precisão de um sistema de autenticação por reconhecimento de voz (Zhen & Canwei, 2002).

As características de alto nível da voz, como padrões de acentuação e uso da linguagem, são resistentes à adição de ruído mas obrigam ao reconhecimento do conteúdo do discurso, recolhendo as sequências de palavras e uma imensidão de dados para criar uma estimativa acústica e gerar um modelo. Isto aumenta a complexidade do processo e, portanto, a escolha mais habitual recai nas características acústicas de baixo nível. Acresce o facto de que os sistemas recorrem, em geral, ao mesmo espectro de propriedades (*Mel-Frequency Cepstral Coefficients*, MFCC) para o reconhecimento do que é dito, uma vez que o método MFCC inclui, para além das distribuições de frequência

do som que permitem a sua identificação, também a forma e o comprimento de onda dos sons produzidos pelas cordas vocais, consideradas como identificadores dos indivíduos. Para além disto, verificou-se que a informação recolhida de uma forma dinâmica aumenta significativamente o desempenho do sistema de autenticação. Assim sendo, a energia especificada no MFCC, bem como a sua primeira e segunda derivadas têm sido características muito utilizadas (Zamalloa, Bordel, Rodriguez, & Penagarikano, 2006).

Estudos realizados em 2007 mostram que cada indivíduo não utiliza todo espectro de frequências e que aquelas que não são utilizadas são elementos distintivos dos utilizadores. Nesse estudo foram recolhidas a amplitude em mais de 1000 frequências da voz de 43 utilizadores voluntários que repetiram a palavra “análise” 11 vezes. A escolha desta palavra prende-se com a variedade de sons que apresenta, o que poderia fornecer alguma informação extra. Os sons recolhidos incluíam vários valores da região do infrasom (Figura 50) que foram ignorados, uma vez que eram relativos a ruído, aparecendo também numa “gravação de silêncio”. Após a remoção destes valores, obteve-se uma matriz tridimensional (amplitude, frequência, tempo) que pode ser representada graficamente como exposto na Figura 51. O estudo utilizou 8 voluntários para separar as representações gráficas obtidas a partir das gravações em 43 grupos distintos, de acordo com as semelhanças entre as faixas não utilizadas e todos eles associaram cada representação às restantes produzidas pelo mesmo utilizador (Figura 52). Ainda assim, o estudo não foi capaz de apresentar uma forma automática de proceder ao reconhecimento utilizando um sistema de computação (Tenreiro de Magalhães, Guimarães, Santos, Revett, & Jahankhani, 2008).

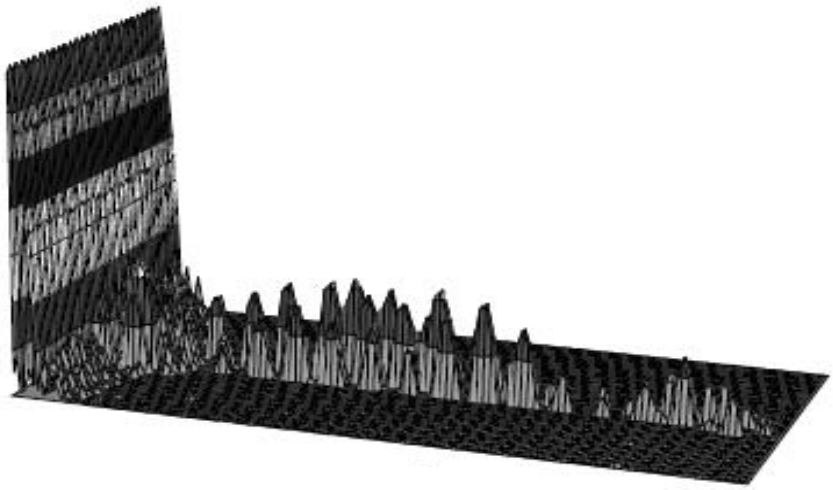


*Figura 50 – Amplitude (eixo vertical) versus frequência ao longo do tempo, quando um utilizador disse a palavra "análise"*

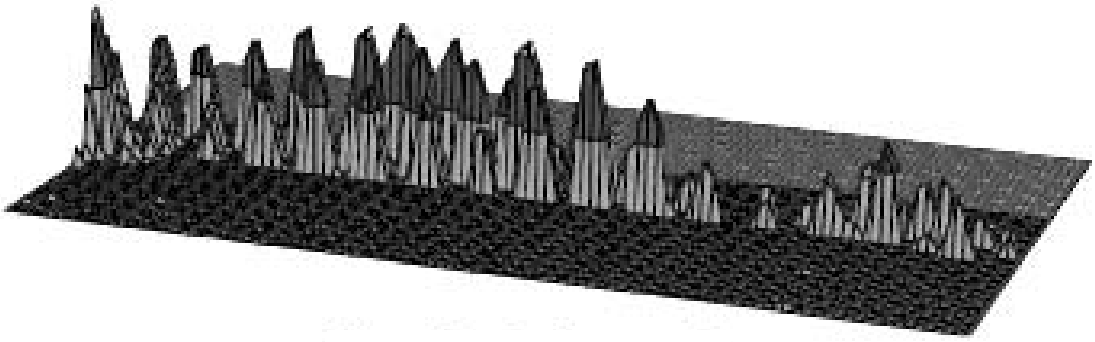


*Figura 51 – Amplitude (eixo vertical) vs frequência ao longo do tempo, quando um utilizador disse "análise", depois de retirados os valores da região de infra-som*

A descoberta de um processo de associação das frequências não utilizadas ao seu emissor, poderá, pelo menos, acrescentar um novo elemento aos algoritmos de reconhecimento de voz o que, além de acrescentar fiabilidade aos processos de autenticação, poderá vir a permitir taxas aceitáveis de sucesso no que respeita à identificação (Tenreiro de Magalhães et al., 2008).

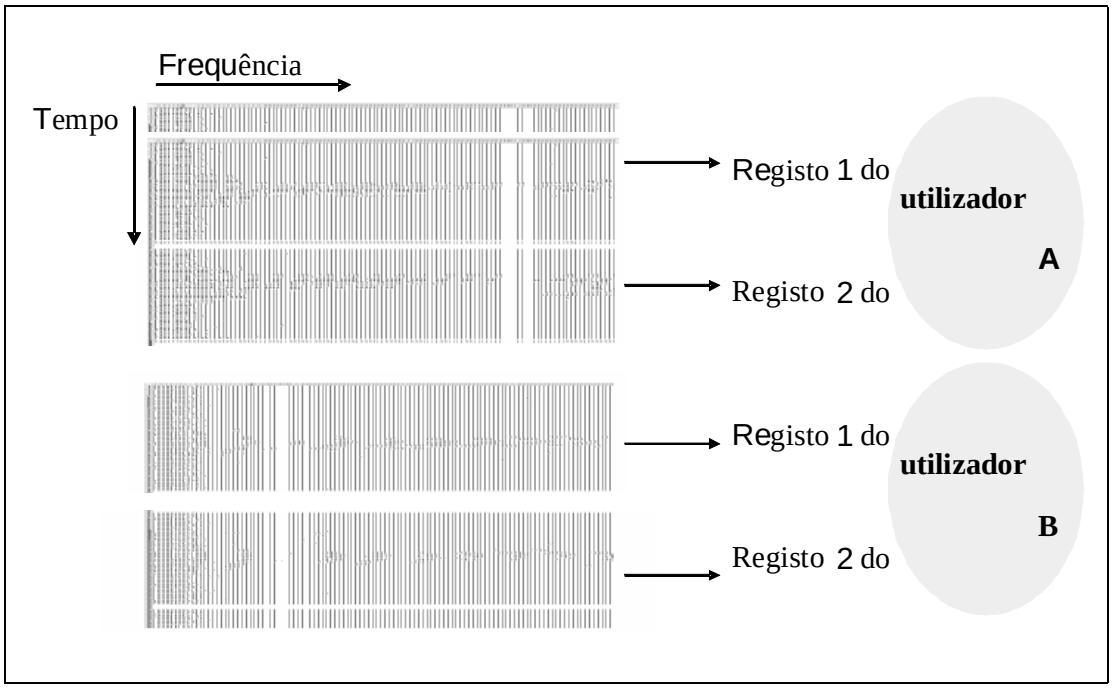



*Figura 52 – Aspectos gráficos de alguns registos de alguns utilizadores*[3]*. Adaptado de (Tenreiro de Magalhães et al., 2008)*

Apesar das limitações ainda existentes, o potencial destes sistemas é grande devido ao baixo custo do *hardware* necessário que, aliás, está já presente em grande parte dos computadores existentes: um microfone.

## *3.7 Assinatura manual recolhida de modo digital*

A assinatura tem sido utilizada como um elemento de autenticação e identificação largamente disseminado. É utilizada para comprometer indivíduos e organizações em contratos e para realizar pagamentos através de, por exemplo, cartões de crédito. A assinatura manual pode ser utilizada como uma biometria para autenticação/identificação desde que se possua um painel que capture a velocidade e a pressão dos movimentos que geram a assinatura, bem como a sua forma.

Segundo um inquérito realizado pela epaynews em Janeiro de 2004 (disponível em http://www.epaynews.com/poll/index.html#jan04), com a questão

3 As linhas brancas verticais correspondem às frequências não utilizadas

"*As a consumer, which of the following payment methods are you most comfortable with?"* (como consumidor, com qual dos seguintes métodos de pagamento se sente mais confortável?), os cartões de crédito e os cheques são os meios de pagamento preferidos por 43% dos utilizadores (Figura 53) e, uma vez que dependem da assinatura do seu proprietário, podem tornar esta tecnologia numa das mais disseminadas, atenuando as questões relacionadas com a sua utilização fraudulenta.

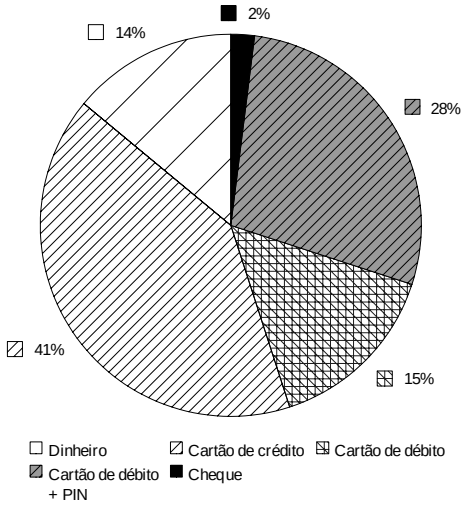



*Figura 53 – Resultado de um inquérito sobre as formas de pagamento (fonte: epaynews)*

Esta tecnologia tem poucos exemplos de aplicações comerciais (sendo a sua utilização pelo Leumi Bank of Israel emblemática) talvez por apresentar taxas de falsa aceitação e de falsa rejeição que variam entre 2% e 5% (Dimauro, Impedovo, Lucchese, Modugno, & Pirlo, 2004), porque os dispositivos de captura não fazem parte do equipamento normalmente disponível nos dispositivos de computação, ao contrário dos dispositivos de captura de som e vídeo e porque a sua inclusão não é viável em dispositivos portáteis, ao contrário, por exemplo, dos leitores de impressão digital.

## *3.8 Keystroke Dynamics*

A tecnologia habitualmente denominada *Keystrokes Dynamics*, também conhecida nos países de língua oficial portuguesa por dinâmica de digitação, é baseada na monitorização dos padrões comportamentais do utilizador ao digitar palavras/frases passe e/ou texto durante uma sessão. Regra geral, o sistema requer que o utilizador, na primeira utilização, digite a mesma frase um determinado número de vezes. Contudo, teoricamente, um sistema pode na primeira utilização recolher a informação necessária para encontrar um padrão sem o conhecimento do utilizador. É também possível ao sistema adaptar o modelo do padrão ao longo do tempo, de forma a ajustar-se à nova informação recolhida. Esta furtividade resulta, entre outros factores, do facto de esta tecnologia não exigir a utilização de equipamento dedicado, fazendo uso do teclado já disponível para a sua função habitual, o que torna a dinâmica de digitação numa tecnologia excelente para utilização em sistemas que se pretende que sejam utilizados pelo maior número de pessoas possível, como é o caso das aplicações de governo electrónico.

A monitorização dos padrões de digitação, com o objectivo da autenticação, teve início no final da década de setenta, quando Gaines e a sua equipa da Rand Corporation monitorizaram a actividade de sete dactilógrafas profissionais (Gaines, Lisowski, Press, & Shapiro, 1980). Esta experiência permitiu concluir da viabilidade desta forma de autenticação, muito embora os valores apresentados para os erros de tipo I e II (falsos positivos e falsos negativos) não fossem fiáveis, considerando que o número de utilizadores foi muito pequeno e que o algoritmo foi deduzido dos próprios dados, não tendo depois sido testado noutro conjunto de dados, ou mesmo num qualquer subconjunto dos mesmos dados.

Após um período de perto de duas décadas em que esta tecnologia não despertou um interesse relevante na comunidade científica, académica ou industrial, o tema ganhou um novo fôlego e foram várias as equipas que se

dedicaram ao estudo de novos algoritmos, primeiro recorrendo às abordagens das Probabilidades e Estatística mais tradicionais, depois recorrendo às tecnologias de Inteligência Artificial, usando diferentes abordagens do problema e recorrendo a diferentes técnicas e métodos para encontrar as regras de decisão do algoritmo.

Uma vez que. desde 1980, foram desenvolvidos e testados diversos algoritmos, tanto determinísticos como recorrendo à inteligência artificial. As descrições que se seguem pretendem apenas apresentar os princípios básicos dos algoritmos apresentados nos trabalhos mais relevante neste domínio e, portanto, não são matematicamente rigorosos. Os algoritmos descritos são apresentados por ordem cronológica dentro de cada grupo de investigação onde estão agrupados. Os grupos de investigação são apresentados por ordem cronológica do primeiro trabalho relevante publicado.

Em 1990, Joyce e Gupta apresentam um método baseado no cálculo de um valor representativo da distância dos tempos de latência entre os caracteres introduzidos e os tempos de latência previamente armazenados, recorrendo aos tempos registados na introdução do nome de utilizador, palavra passe, primeiro nome e último nome. Estes dados são encarados como um vector de dimensão 4 (os quatro campos), em que cada coordenada é um vector de tempos de latência. É então calculado o vector de médias, $M=<M_{nome\_de\_utilizador}, M_{palavra\_passe}, M_{primeiro\_nome}, M_{último\_nome}>$, dos tempos de latência do processo de registo no sistema (força à introdução dos dados 8 vezes) e a distância euclideana desta média a cada um dos vectores dos 8 registos. E o desvio padrão dessas médias de distâncias são usadas como margem para a aceitação de uma tentativa. Um vector de tentativas T, de dimensão 4, é aceite se estiver distante de M (distância euclideana) menos do que uma vez e meia a margem definida (Joyce & Gupta, 1990).

Em 1992 foi utilizada uma rede neuronal do tipo *perceptron*, com resultados muito positivos, já que teve uma taxa média de erro de classificação de 2%. No entanto, este estudo envolveu apenas 5 utilizadores, sendo, portanto,

pouco confiável. Ainda assim, trata-se do primeiro relato da aplicação de redes neuronais com sucesso efectivo (Bleha, Knopp, & Obaidat, 1992). Já em 1990 o mesmo grupo de investigação tinha recorrido a um classificador de Bayes para a autenticação de 26 voluntários, tendo obtido uma FAR de 2.8% e uma FRR de 8.1% (Bleha, Slivinsky, & Hussien, 1990).

Em 1995, Obaidat, que já tinha alguns trabalhos anteriores, pouco relevantes, na utilização de ferramentas de inteligência artificial para a autenticação com recurso à dinâmica de digitação, estuda o uso dos tempos de pressão das teclas como elemento de avaliação, verificando algumas melhorias nos resultados, que aumentam quando os tempos entre teclas e os tempos de pressão são combinados (Obaidat, 1995). Apesar da relevância desta nova forma de aquisição de dados, as taxas de erro apresentadas para o processo que recorre ao tempo entre teclas e às redes neuronais são demasiado altas se comparadas com os valores publicados nesse período (Bleha et al., 1992), superiores a 60%, indicando uma má parametrização do problema que põe em causa a descida dos valores com a inclusão dos novos dados. Em 1997, o autor publicou o mesmo estudo acrescido do uso de outros paradigmas de redes neuronais (*fuzzy ARTMAP*, *Radial Basis Function Networks* e *Learning Vector Quantization*) tendo apresentado o uso dos tempos de pressão como uma novidade (5 anos depois da publicação anterior) e indicando a obtenção de uma taxa de precisão de 100%. Este valor obtido numa experiência com 15 utilizadores não é, como se verifica pelos estudos posteriores, generalizável (Obaidat, & Sadoun, 1997).

De modo a apresentar um método de identificação baseado na dinâmica de digitação Monrose recorre, em 1997, à distância euclidiana e a cálculos probabilísticos baseados na presunção de que os tempos de latência para uma mesma sequência seguem uma distribuição normal. Monrose calcula a semelhança, denominada *Score(R, U)*, entre um perfil conhecido *R* e um perfil desconhecido *U* fazendo $Score(R,U)=\sum_{i=0}^{N}(\frac{1}{o_{u_i}}[\sum_{j=1}^{o_{u_i}} Prob\frac{X_{ij}^{(u)}-\mu_{r_i}}{\sigma_{r_i}}])$ , onde o

vector $<\mu, \sigma, o_i, X_i>$ contém, respectivamente, a média, o desvio padrão, o número de ocorrências e os valores para o i-ésimo elemento. Pesando esta fórmula na proporção do número de ocorrências de cada elemento, Monrose consegue uma taxa de identificação superior a 90% (Monrose & Rubin, 1997).

Mais tarde, Monrose apresenta um sistema baseado nos modelos de semelhança de Bayes, mais uma vez com o objectivo de permitir a identificação de um utilizador (Monrose & Rubin, 2000). Para tal, os utilizadores registados são agrupados de acordo com os grupos de caracteres em que têm ritmos de digitação semelhantes. Assim, por exemplo, os elementos do grupo correspondente ao conjunto {as, ta, mo, de} têm ritmos semelhantes ao digitar estas 4 sílabas, mas têm ritmos distintos (nestas sílabas) dos membros de todos os outros grupos. Quando um conjunto de dados é recolhido para identificação do seu utilizador, é constituído para cada grupo um vector *x* de dimensão *n* com os tempos correspondentes às suas *n* sílabas. Presumindo que estes vectores seguem uma distribuição Normal (ou de Gauss), o vector desconhecido é associado à pessoa que tem uma probabilidade maior de ser o seu "proprietário". A função de decisão, $\Delta$, para o cálculo da distância entre dois vectores *x* e *x'* é:

$$\Delta^{\alpha}(x, x') = \sum_{i=1}^{n} w_i \left( \frac{\sqrt{(x_i - x'_i)^2}}{\sigma_i} \right)^{\alpha}$$ onde $w_i$ é uma função ponderadora calculada dividindo a frequência absoluta da sílaba *i* (em todos os dados de todos os grupos), pela frequência absoluta de todas as sílabas (em todos os dados de todos os grupos); $\sigma_i$ é o desvio padrão dos tempos correspondentes à sílaba *i* no conjunto dos dados e $\alpha$ é uma constante que serve para ajustar a robustez do algoritmo (valores mais próximos de 1 do que de 2 aumentam ligeiramente a eficácia do algoritmo).

Em 2001, Monrose apresenta um algoritmo que recorre à Álgebra, nomeadamente aos polinómios e aos espaços vectoriais, para gerar palavras passe complexas partindo de uma palavra passe simples e do padrão de

digitação do utilizador, dando mais uma função à dinâmica de digitação (Monrose, Reiter, & Wetzel, 2001).

No ano 2000, Ord e Furnell testaram uma rede neuronal em 14 indivíduos para verificar se esta biometria pode também ser aplicada a teclados numéricos utilizados para introdução de números de identificação pessoal com 6 dígitos, conhecidos por PINs (*Personal Identification Numbers*). Os resultados apresentaram FAR promissoras (9.9%) mas a taxa de falsas rejeições obtida mostrou-se proibitiva (30%), rejeitando o utilizador legítimo em quase um terço das tentativas de autenticação (Ord & Furnell, 2000). Alguns elementos deste grupo de investigação continuaram as pesquisas e, em 2002, apresentaram os resultados do uso de uma rede neuronal (uma *Feed-Forward Back Propagation Network*) para a avaliação da dinâmica de digitação, quer na introdução de códigos PIN em dispositivos móveis (4 dígitos), quer na introdução de um número de telemóvel, fosse ele fixo, para efeitos de autenticação, ou fosse um qualquer número que se pretendesse ligar. A precisão do processo de autenticação com recurso a um qualquer número de telefone mostrou-se desastrosa, com uma FAR de 36.3% e uma FRR de 24.3%, e os restantes processos também não apresentaram resultado satisfatórios, com taxas de intersecção de erros de 15% (Clarke, Furnell, Lines, & Reynolds, 2002). Os mesmos autores apresentaram, um ano depois, um estudo comparativo que utiliza diversos algoritmos para avaliar o uso da dinâmica de digitação num sistema móvel, tanto com recurso ao PIN de 4 dígitos como com recurso à introdução de um número de telemóvel com 11 dígitos. Dos métodos utilizados, que incluíam algoritmos estatísticos clássicos e vários tipos de redes neuronais, os que obtiveram melhores resultados foram as redes neuronais GGRN (*Generalised Regression Neural Network*) para o PIN de 4 dígitos e as redes neuronais FF MLP (*Feed-Forward Multi-layered Perceptron*) para os códigos de 11 dígitos. Ainda assim, foram obtido resultados de FAR e FRR ligeiramente superiores a 10%. Estes resultados são claramente insuficientes para autenticação autónoma, como seria o caso na utilização dos dados recolhidos na

introdução do número de telefone que se deseja contactar, mas parecem razoáveis enquanto complemento dos métodos existentes, em especial do PIN (Clarke, Furnell, Lines, & Reynolds, 2003). Estes investigadores investigaram ainda a possibilidade de utilizarem as mensagens de texto enviadas a partir dos dispositivos móveis como fonte de dados para a autenticação por análise da dinâmica de digitação, recorrendo a redes neuronais. Embora os resultados divulgados em 2004 mostrem uma precisão muito baixa, com uma EER de 17.9%, este estudo mostrou que esta utilização da dinâmica de digitação parece ter resultados muito diferentes em utilizadores diferentes, sendo que para alguns é uma tecnologia com alguma fiabilidade, com EER inferiores a 10%, enquanto que para outros é uma tecnologia não só inútil mas até incómoda, com EER superiores a 30% (Clarke, Furnell, Lines, & Reynolds, 2004).

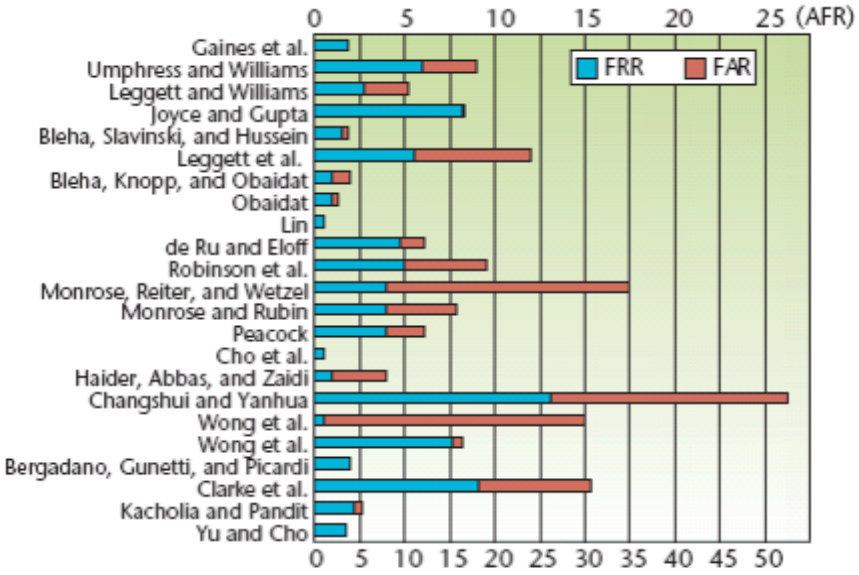
Em 2002, um grupo de investigadores da universidade de Torino apresentou um trabalho que utiliza os tempos entre o momento de pressão de uma tecla e o momento de pressão da terceira tecla de uma sequência de três caracteres, denominada trigrafo. Assim, uma palavra passe como "constantinopla" teria apenas 4 dados, correspondentes à introdução dos trigrafos "con", "sta", "nti" e "nop". O vector composto pelos pares (tempos de digitação dos trigrafos, trigrafo) é então ordenado por ordem crescente do tempo dispendido e é calculada a distância ao vector de referência. Esta distância é a soma das diferenças entre os indices de cada trigrafo e é normalizada através da divisão pela maior ordem de desordem possível num vector *V* de *n* elementos:

$\frac{V^2}{2} se\ n\acute{e}\ par, \frac{V^2-1}{2} se\ n\acute{e}\ \acute{i}mpar$ Este processo revelou-se muito preciso, com uma FAR de 0.01% e uma FRR de cerca de 4%, mas fica a dúvida se a qualidade da precisão resulta do uso de trigrafos, justificando-se por não ser tão sensível a pequenas variações dos padrões dos utilizadores, da comparação de vectores, ou se resulta do facto das amostras utilizadas terem 30 caracteres (10 tempos), o que é muito quando comparado com os estudos que recorrem a palavras passe, tipicamente mais curtas (Bergadano, Gunetti, & Picardi, 2002).

Os algoritmos apresentados são uma selecção, baseada na sua relevância, das várias aproximações utilizadas para encontrar algoritmos de *Keystroke Dynamics* que forneçam níveis de segurança, não reconhecimento, satisfatórios. Muitos outros podiam ser referidos, todos com métodos de avaliação diferentes, diferente número de utilizadores envolvidos (normalmente muito reduzido), diferente número de caracteres necessários para fazer o registo no sistema e diferente número de caracteres necessários para proceder à autenticação/identificação de um utilizador. Esta disparidade de parâmetros dos algoritmos e da sua avaliação tornam impossível a tarefa de os comparar. Além disso, não existe, neste contexto, um conceito de amostra representativa. O mesmo algoritmo apresenta resultados diferentes quando testado com diferentes grupos de voluntários e, portanto, a única forma de comparar dois algoritmos é testá-los com o mesmo grupo de dados e concluir qual é o melhor para o nosso caso. No que respeita a aplicações *Web*, onde este método de avaliação não é exequível, devemos considerar apenas os resultados que envolvam um número considerável de voluntários. O esforço computacional do algoritmo deve também ser tido em conta, uma vez que o tempo de execução é um factor crítico em qualquer aplicação.

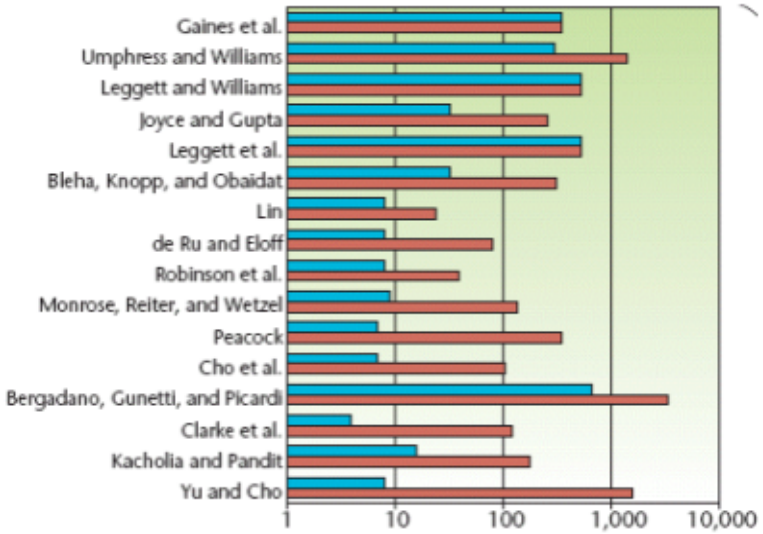
Ainda assim, é de registar que os valores anunciados da FAR variam desde os 0% até mais de 50%, a FRR varia de mais de 25% a menos de 1% e o número de utilizadores envolvidos na avaliação dos algoritmos está, geralmente, entre dez e cem (Peacock, Ke, & Wilkerson, 2004). As figuras 54, 55 e 56 foram extraídas de (Peacock *et al*., 2004) e sintetizam esses dados. A Figura 54 apresenta, para cada algoritmo, a FRR, a FAR e o valor EER (apresentado no eixo superior) correspondente à média entre a FRR e a FAR; a Figura 55 apresenta o número de caracteres necessários para fazer o registo no sistema (a vermelho) e para proceder à autenticação do utilizador (a azul). A Figura 56 apresenta o número de acessos utilizados na avaliação de cada algoritmo. Nos casos em que foram combinadas outras características para avaliação, como é o caso da pressão exercida no teclado, foram considerados apenas os resultados

relativos à componente que avalia os padrões temporais da forma de digitação, uma vez que nos interessa avaliar apenas algoritmos que mantenham a universalidade potencial do seu uso, não impondo restrições ao nível do hardware necessário.



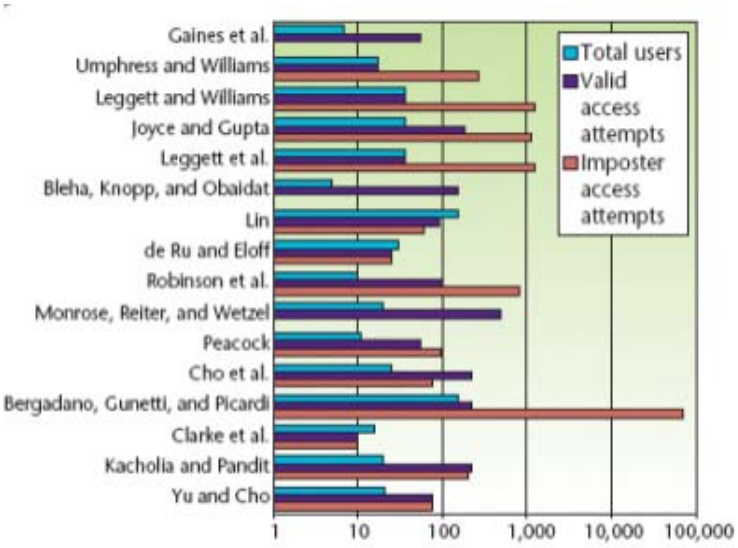

©IEEE

*Figura 54 – Precisão dos algoritmos de Keystroke Dynamics. (Peacock et al., 2004)*




©IEEE

*Figura 55 – Número de caracteres necessários em cada algoritmo para o registo (a vermelho) e para a autenticação (a azul). (Peacock et al., 2004)*




©IEEE

*Figura 56 – Número de ensaios realizados. (Peacock et al., 2004)*

## *3.9 Outras tecnologias biométricas*

As tecnologias biométricas de carácter físico têm evoluído imenso nos últimos anos, no que respeita à precisão, à sua integração com outros equipamentos e à sua integração com outras tecnologias biométricas, criando sistemas multimodais com um potencial interessante. No entanto, não têm aparecido tecnologias que avaliem biometricamente outras partes do corpo. Já no que respeita às biometrias comportamentais a inovação é imensa, embora ainda muito imatura. Os sistemas em desenvolvimento mais promissores são descritos nas secções seguintes.

### 3.9.1 Reconhecimento do "*grip-pattern*"

Esta tecnologia pretende reconhecer um utilizador pela avaliação da força e da distribuição da pressão exercida por ele sobre um objecto, de acordo com o conceito patenteado nos Estados Unidos da América por Michael Recce em 2003 (Recce, 2003).

A investigação nesta área tem estado relacionada essencialmente com a verificação da identidade dos utilizadores de armas de fogo, embora possa ser utilizada, pelo menos em teoria, para controlo de acesso físico a edifícios e a viaturas. As armas denominadas de inteligentes têm um mercado considerável, dadas as consequência de um disparo acidental ou do roubo e futura utilização de uma arma de fogo, e estão no mercado algumas soluções que tentam impedir o uso de uma arma por um utilizador que não seja o seu proprietário. A solução mais básica é a colocação de um aloquete no gatilho que impede a sua utilização sem a posse do código ou da chave que o abre. Mais tecnológica é a solução da *Armatix* (www.armatix.de) que bloqueia o cano da arma com um dispositivo que só pode ser retirado com recurso a um aparelho que irá exigir um código PIN ou a impressão digital de um utilizador legítimo. A *Armatix* também comercializa armas com activação/desactivação por comando remoto instalado num relógio.

No processo biométrico são incluídos sensores no punho da arma e o processo de disparo mantém-se bloqueado até que o sistema indique que a autenticação decorreu com sucesso. Para que estes processos possam ser aceites pelo mercado têm que apresentar taxas de falsa rejeição muito baixas (por exemplo, a Holanda exige que as armas utilizadas pelas forças policiais tenham uma probabilidade de não funcionarem inferior a 0.01%) o que ainda não acontece. Actualmente obtém-se taxas de intersecção de erros na ordem dos 5% (Veldhuis, Bazen, Kauffman, & Hartel, 2004).

### 3.9.2 Reconhecimento da forma de pisar

Uma outra característica individual, particularmente útil para o controlo de acesso, é a forma de pisar. Esta característica, em investigação desde o final do século passado (Orr & Abowd, 2000), além de apresentar taxas de falsa aceitação promissoras (±3%), embora com taxas de falsa rejeição ainda muito elevadas (±16%), não é afectada pelo calçado utilizado e, portanto, poderá obter algum sucesso no controlo de acesso físico a instalações (Mostayed, Kim, Mynuddin, Mazumder, & Park, 2008).

### 3.9.3 Gait Authentication

Esta tecnologia analisa as várias características particulares de um utilizador ao atravessar um corredor. Além de poder ser complementado com informação sobre a forma de pisar, caso a zona de reconhecimento disponha de um piso sensível à pressão, as imagens da forma como um utilizador caminha incluem diversas características mensuráveis como a amplitude do passo, a variação na altura (provocada pelos passos), a velocidade de deslocação e a oscilação dos braços (Boyd & Little, 2005).

Estes sistemas de identificação/autenticação estão muito dependentes da evolução das técnicas de tratamento de imagens, já que é necessário desambiguar as imagens obtidas que incluem sombras e outros elementos

perturbadores. Actualmente já existem sistemas que apresentam taxas de erro inferiores a 7% (Ben-Abdelkader, Cutler, Nanda, & Davis, 2001)

## *3.10 Autenticação gráfica*

A vulnerabilidade das palavras passe resulta da sua má utilização generalizada que, por sua vez, resulta daquilo que tem sido chamado de paradoxo da palavra passe: uma palavra passe deve ser facilmente memorizada, logo simples, e simultaneamente deve ser segura, logo complexa. Consequentemente, é virtualmente impossível conseguir uma "boa" palavra passe. Por outro lado, uma vez que os utilizadores ainda não interiorizaram a necessidade de manterem seguros os seus segredos de autenticação, mesmo as palavras passe com um nível aceitável de segurança transformam-se numa ameaça quando as políticas de segurança não são implementadas, isto se existirem. Os resultados de um inquérito realizado em 2004 (Tenreiro de Magalhães, Revett & Santos, 2006) a sessenta profissionais das tecnologias de informação indicaram que, mesmo naqueles com conhecimentos tecnológicos, a necessidade de garantir a segurança das palavras passe é subestimada, sendo este facto, provavelmente, uma das razões que levou os governos a aumentar o investimento nas tecnologias de autenticação biométrica depois dos atentados de 11 de Setembro de 2001 nos Estados Unidos da América. Como se pode verificar na Tabela 6, apenas 17% dos profissionais inquiridos utiliza códigos que incluem símbolos e 72% afirmou que raramente muda os seus códigos de acesso (Figura 57), apesar de 52% terem conhecimento de que pelo menos uma pessoa conhece pelo menos uma das suas palavras passe (Figura 58). Esta necessidade de manter a simplicidade dos códigos de autenticação e o princípio da confiança generalizada, oposto ao princípio da desconfiança generalizada que melhor serviria os objectivos da segurança dos sistemas, que permite que os códigos de acesso estejam afixados no monitor ou num *post-it* colocado debaixo do teclado, cria uma falha de segurança que é necessário resolver. Tanto mais

que 65% (Figura 59) dos inquiridos assumiu que usa apenas um ou dois códigos para aceder a todos os serviços com autenticação por palavra passe.

A questão da transmissibilidade do segredo assume uma importância acrescida, já que conhecer uma palavra passe de um sistema significa poder aceder a um conjunto de sistemas utilizados pelo legítimo proprietário do segredo de autenticação e permitindo que o intruso se faça passar por ele, tanto dentro dos sistemas como, frequentemente, perante outros sistemas que irão utilizar o facto de estar autenticado com sucesso nesse sistema para validar a identidade apresentada num novo registo. Por exemplo, é comum enviar uma mensagem de correio electrónico para validação da identidade de quem se regista. Se a autenticação no sistema de correio electrónico tiver sido fraudulenta, todo o processo fica em causa.

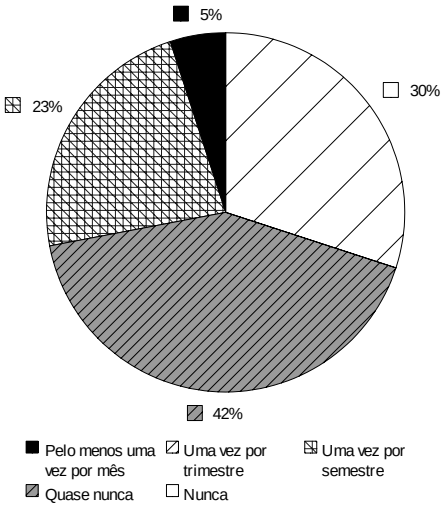



*Figura 57 – Frequência de alteração das palavras passe dos profissionais de tecnologias de informação inquiridos*

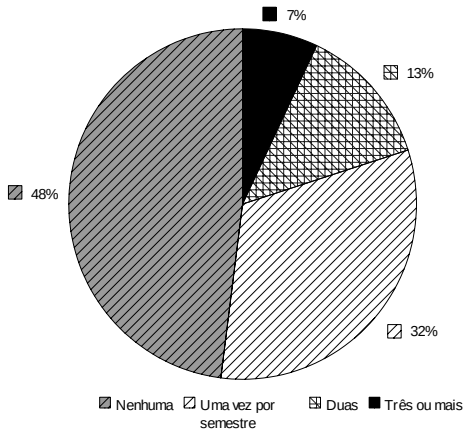



*Figura 58 – Número de pessoas que conhecem, pelo menos, uma das palavras passe dos profissionais de tecnologias de informação inquiridos*

| *Constituição das palavras passe* | *Percentagem de utilizadores* |
|---|---|
| *Letras e símbolos* | 0% |
| *Números e símbolos* | 0% |
| *Letras, números e símbolos* | 17% |
| *Apenas letras* | 23% |
| *Apenas números* | 17% |
| *Letras e números* | 43% |

*Tabela 6 – Constituição das palavras passe dos inquiridos*

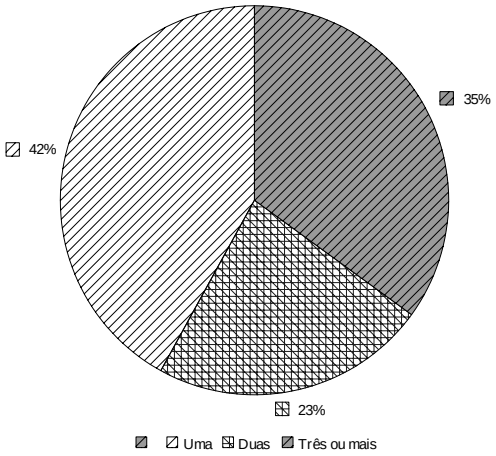



*Figura 59 – Número de palavras passe utilizadas com frequência pelos profissionais de tecnologias de informação inquiridos.*

Apesar do uso das tecnologias biométricas para aumentar a segurança dos sistemas ser um assunto muito discutido, não se alcançou um consenso. Enquanto os governos e as empresas exercem uma pressão constante para uma maior integração destas tecnologias com os sistemas de segurança já implementados (como os passaportes e os cartões de identificação), as associações de direitos humanos estão preocupados com as implicações éticas e sociais do seu uso. Esta situação cria um desafio para encontrar algoritmos menos intrusivos, mais fáceis de usar e mais precisos, enquanto outras soluções devem, em simultâneo, ser criadas/desenvolvidas. A fusão da avaliação biométrica com os processos gráficos de autenticação representa um caminho com potencial, em especial nos sistemas móveis, por fornecerem alguma protecção contra a visualização, acidental ou não, da introdução do código secreto, já que os ecrãs são, tipicamente, de dimensões reduzidas e/ou são utilizados próximo do corpo. As secções seguintes apresentam as tecnologias de autenticação gráfica existentes e alguns algoritmos que serviram de protótipo para a avaliação da precisão potencial destes sistemas.

Em determinados ambientes, em especial os móveis, as palavras passe podem ser substituídas por segredos de autenticação de carácter gráfico, tirando vantagens da habilidade humana para reconhecer informação visual de uma forma mais eficiente do que sequências de caracteres sem semântica (Nickerson, 1965; Shepard, 1967; Standing, 1973).

A autenticação gráfica é uma tecnologia em que o utilizador selecciona um conjunto de imagens de um conjunto maior, ou selecciona alguns pontos na imagem. O segredo possuído pelo utilizador legítimo é o conjunto de imagens/pontos seleccionados e a correspondente sequência. Estas tecnologias podem fornecer uma forma de gerar palavras passe, utilizando funções unidireccionais, a partir da sequência gráfica seleccionada e, desta forma, providenciar compatibilidade com os sistemas que actualmente recorrem a palavras passe. Apesar de Blonder ter patenteado a sua “palavra passe gráfica” em 1996 (Blonder, 1996), muitos sistemas gráficos foram propostos, como

veremos de seguida. No capítulo seguinte será apresentado um novo sistema que ultrapassa o âmbito da patente de Blonder ao integrar na autenticação gráfica os algoritmos de autenticação comportamental.

### 3.10.1 DAS - *Draw a secret* (Jermyn, Mayer, Monrose, Reiterand, & Rubin, 1999)

Este esquema de autenticação foi pensado para ser utilizado em PDAs (*Personal Digital Assistants*). Neste esquema o código pessoal é uma imagem desenhada pelo utilizador numa grelha (Figura 60). O desenho é convertido numa sequência de pares de coordenadas. O texto gerado a partir do desenho é transformado através de um função de *hash* unidireccional sendo o resultado armazenado e associado ao utilizador. O valor de *hash* gerado no processo de autenticação é comparado com o valor armazenado sempre que o utilizador tenta aceder ao sistema.

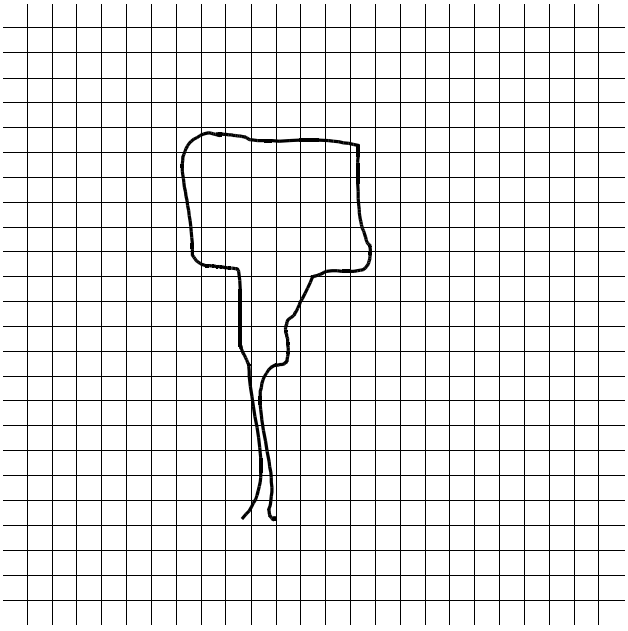


*Figura 60 – Exemplo de segredo de autenticação no sistema Draw-a-Secret*

A vantagem deste método é o facto de gerar códigos longos e o facto de ser difícil a terceiros imitar o desenho de autenticação. Apesar deste esquema ter sido projectado com o objectivo de ser utilizado num PDA, é possível utilizar o

*Draw-a-Secret* num computador e, neste caso, a utilização em locais públicos é desaconselhada uma vez que é fácil a qualquer transeunte memorizar um desenho visualizado num monitor.

### 3.10.2 *Déjà Vu*

A proposta de autenticação elaborada por Dhamija and Perrig (Dhamija & Perrig, 2000) é baseada na geração de imagens com base num grupo de imagens pré-seleccionadas. O esquema de autenticação é composto por três fases distintas: criação do portefólio, treino e, por fim, autenticação. A primeira consiste na selecção de um conjunto de imagens abstractas. Partindo das imagens seleccionadas é executado um processo de geração de novas imagens que serão utilizadas para compor o portefólio do utilizador. Na fase de treino o utilizador pratica durante algum tempo o processo de autenticação com o objectivo de melhorar a memorização das imagens. A última fase acontece sempre que o utilizador tenta aceder ao sistema. Nessa altura o sistema apresenta um grupo de imagens escolhidas aleatoriamente e que inclui as imagens do portefólio do utilizador e que este deve identificar para que lhe seja permitido o acesso.

A grande vantagem deste processo é a dificuldade de transmissão do segredo, já que é virtualmente impossível descrever as imagens seleccionadas e, uma vez mais, a desvantagem é a vulnerabilidade destes sistemas ao uso em locais públicos.

### 3.10.3PassFaces™ (Real User Corporation, 2001)

Este esquema de autenticação baseia-se no estudo empírico de Brostoff e Sasse (Brostoff & Sasse, 2000). Para criar um código de acesso o utilizador pré-selecciona um grupo de quarto fotografias de pessoas de um grupo de fotografias disponíveis. Depois deste processo, o utilizador passa por um processo de treino, tendo em vista a memorização. O processo de autenticação consiste em quatro fases, em cada uma delas é apresentada ao utilizador uma

grelha com nove fotografias. Em cada grelha existe uma fotografia do conjunto original do utilizador e oito escolhidas aleatoriamente para o confundir. Facilmente se reconhecem as semelhanças deste esquema com o anterior, o *Déjà Vu*, sendo que a diferença entre os sistemas, do ponto de vista do utilizador, é a escolha de imagens abstractas ou de fotografias de pessoas.

O uso de fotografias tem vantagens e desvantagens. A grande vantagem é a facilidade de memorização. As desvantagens são a facilidade de transmissão do segredo, já que é mais fácil descrever uma pessoa do que uma imagem abstracta, e a eventual redução do espaço de chaves, já que os estudos indicam que os utilizadores tendem a escolher fotografias de pessoas da mesma raça (Meissner & Brigham, 2001; Levin, 2000; Walker & Tanaka, 2003).

### 3.10.4*PassPoints* (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005)

O sistema *PassPoints* é baseado na escolha de um sequência de pontos pré-seleccionados numa imagem fixa. No esquema de autenticação o utilizador selecciona os pontos que escolheu, dentro de uma área de tolerância. Esta área de tolerância é necessária já que o ponto escolhido corresponde a um pixel, o que é demasiado preciso para um utilizador humano.

### 3.10.5 *Visual Identification Protocol* (VIP)

De Angeli (De Angeli, Coventry, Johnson, & Coutts, 2003) também propôs uma solução para a autenticação dos utilizadores baseada na memória visual. Foram criados, nesse sistema, três processos de autenticação que foram depois comparados com o processo de autenticação baseado em códigos numéricos, normalmente designados por PIN (*Personal Identification Number*). Os resultados dessa comparação estão apresentados na Tabela 7, de acordo com as interpretações dos autores. É claro que o conceito de desempenho “máximo” é muito relativo.

A primeira opção para autenticação, designada VIP1, consiste na selecção de quatro imagens de um grupo de dez pré-definidas, dispostas em posições fixas e introduzidas pela mesma sequência. A segunda opção, designada por VIP2, difere da primeira por apresentar as imagens por uma ordem aleatória. Com a terceira opção, a que os autores chamaram VIP3 e onde pretenderam estudar os limites do paradigma visual, o utilizador tem um portefólio de oito imagens e em cada tentativa de autenticação são apresentadas quatro delas em simultâneo com outras doze imagens escolhidas aleatoriamente de um outro conjunto de imagens. O utilizador tem, então, que identificar as imagens que são suas, sem preocupações com a sequência. O estudo de De Angeli mostrou que os erros mais comuns associados ao protocolo VIP1 estão relacionados com a escolha das imagens por uma ordem errada e que no caso do protocolo VIP2 os erros eram a escolha das imagens erradas ou da sequência. No protocolo VIP3, o mais exigente, era comum os utilizadores seleccionarem imagens que não constavam do seu portefólio como sendo suas. É claro que estes eram os tipos de erros esperados à partida, dadas as características de cada um dos três protocolos apresentados.

| *Protocolo* | *Tipo de código* | *Localização* | *Desempenho* |
|---|---|---|---|
| *VIP1* | 4 imagens de 10 por ordem fixa | fixa | Igual a um PIN |
| *VIP2* | 4 imagens de 10 por ordem fixa | aleatória | Intermédia |
| *VP3* | Baseado num portefólio | aleatória | Máxima |

*Tabela 7 – Processos de autenticação e resultados*

## *3.11 Enquadramento legal*

As preocupações sociais de segurança, privacidade e intrusão na esfera pessoal dos utilizadores levou muitos países a conflitos judiciais que pretendiam impedir determinadas implementações de tecnologias biométricas. Ainda assim, foram poucos os casos em que os legisladores sentiram necessidade de criar novos regulamentos que criassem um enquadramento jurídico específico para essas situações, sendo mais frequente o recurso a diversos aspectos das leis

civis e criminais em vigor no Estado do juízo em causa, resultando numa jurisprudência própria de cada Estado.

Em Portugal é a Comissão Nacional de Protecção de Dados (CNPD) que tem a responsabilidade de autorizar a instalação de sistemas biométricos (Assembleia da República, 1998) com base nas evidências de garantia da protecção dos direitos daqueles que os utilizam. Devido à grande utilização destes sistemas para controlo de acessos e pontualidade, a CNPD tem disponível um documento (Comissão Nacional de Protecção de Dados, 2004) com os princípios orientadores que devem reger a aplicação desta tecnologia, independentemente da obrigatoriedade de notificar a CNPD dos tratamentos de dados efectuados e de dispor de um parecer positivo desta instituição. Os próximos parágrafos baseiam-se nesse documento e pretendem sintetizar o contexto legal para a implementação de sistemas biométricos de controlo de assiduidade e pontualidade em Portugal, quer a nível social quer a nível técnico.

A utilização de sistemas biométricos no contexto de uma relação de trabalho deve ser precedida de um processo de esclarecimento e formação dos utentes de forma a obter a adesão voluntária dos trabalhadores e maximizar a eficácia do sistema. Só é exigível do trabalhador um dever de cooperação se existir um perfeito esclarecimento da forma como os dados recolhidos serão tratados e dos motivos que levam a entidade patronal a adoptar um sistema biométrico. Ainda assim, o trabalhador pode recusar o tratamento dos dados quando existirem “razões ponderosas e legítimas relacionadas com a sua situação particular”. Além disso não é admissível o uso de tecnologias biométricas furtivas no contexto de uma relação de trabalho, uma vez que o titular do padrão biométrico tem o direito de saber se este se encontra armazenado e para que fins, bem como o direito de testar a validade desse padrão através da execução do processo de autenticação e/ou identificação. Deve também existir um período de utilização experimental que permita avaliar o desempenho do sistema e deve ser possível ao trabalhador, de modo a satisfazer o disposto no artigo 17.º n.º4 do Código do Trabalho, a verificação do

resultado do algoritmo biométrico sempre que o utilize, por exemplo através da apresentação num monitor da identidade identificada ou da existência de um sistema de luzes que confirme a correcta autenticação.

Uma vez que os padrões biométricos armazenados são uma representação digital da característica medida e, portanto, não permitem a duplicação ou reconstituição desta, está actualmente aceite pela CNPD que "a recolha de dados biométricos (...) não tem qualquer implicação com a integridade física do trabalhador, não afectando, igualmente, o seu direito à identidade pessoal e à intimidade da vida privada". De forma a garantir que assim seja, os processos de pedido de autorização de aplicação de sistemas biométricos apresentados à CNPD devem incluir uma declaração dos fabricantes de que não cedem às entidades que fornecem ou adquirem os equipamentos as chaves das representações digitais armazenadas.

Do ponto de vista técnico, os sistemas devem possuir um grau de fiabilidade suficiente para não comprometer a finalidade para que está a ser utilizado e não criar dificuldades acrescidas ao trabalhador, violando os seus direitos. Devido ao perigo para a privacidade da centralização de informações em bases de dados, não é admissível o relacionamento das tecnologias biométricas com outras como, por exemplo, a videovigilância, sem prejuízo da utilização de sistemas multimodais que recorram à avaliação de mais do que uma característica do trabalhador, de modo a aumentar a fiabilidade do processo. Apesar de as bases de dados constituídas serem um repositório de características inferidas a partir dos dados biométricos e não de dados biométricos em si, a CNPD recomenda que os padrões biométricos (em especial no caso da impressão digital) sejam armazenados em cartões transportados pelos utilizadores. Por último, deve ser referido que os dados biométricos de um utilizador devem obrigatoriamente ser eliminados no momento em que cesse a relação contratual ou em que o trabalhador mude de local de trabalho.

Apesar do recurso a legislação comparativa cumprir os requisitos para as aplicações civis, o aumento da actividade de terrorista no ciberespaço está a

criar a necessidade de legislação específica. Franco Frattini, comissário europeu para a justiça e assuntos internos, em declarações à imprensa (“Bruxelas garante que ameaça de ataques terroristas na UE é 'elevada'”, 2007), anunciou que a União Europeia está a preparar propostas legislativas, uma vez que a Internet está a ser utilizada pelos terroristas para difundir propaganda terrorista, organizar atentados e recrutar novos membros.

Alguns processos de autenticação que recorrem à dinâmica de digitação e à autenticação gráfica estão protegidos por patentes em alguns países, em especial nos Estados Unidos da América. Uma vez que a existência de uma patente num determinado país é, normalmente, considerado como um factor de preferência para o registo de direitos noutro país, apresenta-se de seguida o essencial de cada uma das patentes com maior relevo nos domínios da autenticação biométrica apresentada nesta tese, ou nas tecnologias que a suporta. Na construção de uma solução específica para um sistema de autenticação do cidadão perante os sistemas informáticos do Estado, é aconselhável a utilização de métodos que não estejam abrangidos pelas patentes referidas, como é o caso de todas as soluções propostas.

- US4805222 (*Method and apparatus for verifying an individual's identity*):
  - Patente solicitada solicitada a 23 de Dezembro de 1985 pela *International Bioaccess Systems Corporation.*
  - A patente apresenta um sistema de autenticação em que os dados apresentados são comparados com o padrão armazenado recorrendo à comparação de vectores, através da distância euclideana. Os inventores sugerem também a fórmula: $D = \sqrt{\sum_{i=i} W(i) \frac{(X(i) - Y(i))^2}{(S_1(i) - S_2(i))^2}}$ para inclusão da variação interna de cada sujeito (recorrendo ao desvio padrão) na forma de cálculo da distância e para, caso se entenda necessário, pesar elementos distintos de forma distinta. São reclamados os processos em que um conjunto de tempos é recolhido

e, a partir dele, é criado um padrão que é comparado com os tempos de uma posterior inserção de dados. Tempos de distância acima do limite de tolerância estabelecido despoletarão um alarme que depende da vontade do proprietário do sistema (Young & Hammon, 1989).

- US5559961 (*Graphical Password*):
  - Patente pedida a 30 de Agosto de 1995 pela *Lucent Technologies Inc*.
  - A patente regista um sistema em que um conjunto de pontos numa imagem , ou uma sequência de pontos numa imagem constitui o segredo de autenticação (Blonder, 1996).

- US6192578B1 (*securing restricted operations of a computer program using a visual key feature*):
  - Patente pedida a 2 de Março de 1998 pela *Micron Electronics Inc*.
  - A patente protege um sistema em que uma figura decorativa possui, numa determinada região secreta, um controlo que tem que ser activado num determinado período de tempo para que a acção solicitada seja autorizada (Elledge, 2001).

- US6151593 (*Apparatus for authenticating an individual based on a typping pattern by using a neural network system*):
  - Patente pedida a 14 de Abril de 1998 pela *Postech Foundation*.
  - Esta patente reclama um utensílio para autenticação com recurso aos vectores temporais de uma palavra passe, utilizando uma rede neuronal para a obtenção do padrão (Cho & Han, 2000).

- US6327659B2 (*Generalized User Identification and Authentication System*) e US6332192B1 (*Generalized User Identification and Authentication System*):

- Patentes pedidas pela *Passlogix Inc*. respectivamente a 12 de Maio de 1998 e a 9 de Fevereiro de 2001.
- Estas patentes protegem um método de autenticação baseada num desafio gráfico que consiste na alteração da posição de um conjunto de objectos no ecrã, efectuados numa só etapa ou em várias, considerando a ordem das acções ou apenas a posição final dos objectos. A segunda patente é um complemento da primeira para incluir a possibilidade de utilização de cifragem dos dados secretos armazenados (Boroditsky & Manza, 2001, 2001A).

- US6209102B1 (*Method and apparatus for secure entry of access codes in a computer environment*):
  - Patente solicitada a 12 de Fevereiro de 1999 pela *Arcot Systems*.
  - Protege um método para a introdução de PINs através de um interface visual (Figura 61) onde a sequência dos caracteres visiveis no ecrã é alterada aleatoriamente em cada utilização do sistema. Trata-se, na realidade, de um sistema de autenticação gráfica onde a imagem é composta apenas por números (Hoover, 2001).

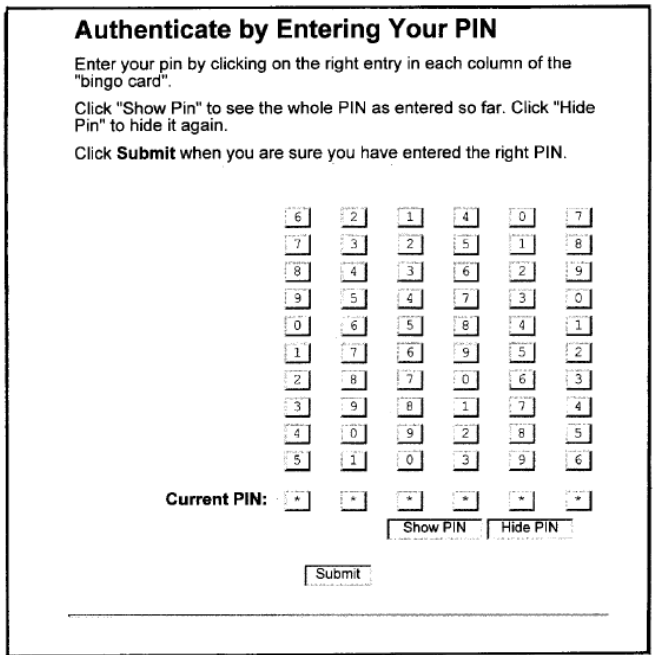



*Figura 61 – Sistema de introdução de PIN reivindicado por Hoover*

- US6895514B1 (*Method and apparatus for achieving secure password access*):
  - Patente pedida a 25 de Junho de 1999 pela *Lucent Technologies Inc*.
- Patente semelhante, no que respeita ao método, à de Young *et al.* (US4805222), propondo diversas formas de comparar os vectores mas reclamando o método em que a semelhança entre a palavra passe apresentada e a palavra passe proposta também entra no cálculo do valor de decisão, tal como a semelhança temporal, com um determinado peso. Este método prevê, portanto, a possibilidade de um utilizador conseguir o acesso ao sistema apesar de introduzir uma a palavra passe errada, desde que a palavra introduzida tenha um "nível suficiente de semelhança" com a original. É de salientar que decorreram quase seis anos entre o pedido da patente e a sua aprovação (Kermani, 2005).

- US7350078 (*User selection of computer login*):

- Patente solicitada pelo seu inventor, G. Odom, a 4 de Março de 2002.
- Esta patente protege um método onde o utilizador escolhe o tipo de processo de autenticação que pretende, seja proveniente apenas de um dispositivo ou de vários e tanto avaliando apenas um critério, como a exactidão da palavra chave, como vários, por exemplo para incluir uma avaliação dos tempos de introdução dos caracteres (Odom, 2008).

- US7243239B2 (*Click passwords*):
  - Patente pedida pela Microsoft Corporation a 28 de Junho de 2002.
  - Esta patente protege diversas formas de definição das áreas de tolerância, com recurso a uma grelha criada a partir de diversas formas geométricas, das selecções de pontos numa figura para constituição do segredo de autenticação do utilizador e diversas formas de armazenamento dos dados que representam as selecções (Kirovski, Jojic, & Roberts, 2007).

- US6954862B2 (*System and method for user authentication with enhanced password*):
  - Patente pedida pelo seu inventor, M. L. Serpa, a 27 de Agosto de 2002.
  - Esta patente propõe um método de autenticação em que a palavra passe tem que ser introduzida num ritmo previamente combinado com o sistema ou de acordo com a solicitação em cada entrada de acordo com uma sinalética secreta, mas conhecida do utilizador (Serpa, 2005).

- US7206938B2 (*Key sequence rhythm recognition system and method*):
  - Patente solicitada pela *iMagic Software Inc.* a 26 de Novembro de 2002.

- Esta patente protege o processo de autenticação por reconhecimento biométrico da forma de digitação. Os tempos recolhidos correspondem aos tempos de pressão das teclas utilizadas para introduzir um texto, bem como os tempos entre as teclas correspondentes (denominado tempo de voo). Os tempos são considerados válidos se estão dentro de uma vizinhança do tempo médio para esse par de caracteres, com amplitude dependente do correspondente desvio-padrão. Neste processo os textos de registo e o texto de autenticação podem ser distintos e só serão considerados os tempos que tenham valores médio conhecidos. O número de acertos necessários para aceitar o utilizador é um parâmetro ao dispôr do administrador (Bender & Postley, 2007).

- US7240367B2 (*User interface and method for inputting password and password system using the same*):
  - Patente pedida pela *Shinbitech Co., Ltd* e pelo seu inventor, S. Park, a 18 de Março de 2003.
  - Esta patente protege um método de autenticação gráfico que consiste em apresentar ao utilizador, em cada desafio, dois conjuntos de símbolos, A e B. Em cada desafio o utilizador deve associar um símbolo do conjunto A a um símbolo do conjunto B (Park, 2007).

- US7305559B2 (*Software method for improved password entry*):
  - Patente solicitada pela *Lenovo Singapure Pte Ltd*. a 4 de Dezembro de 2003.
  - O método protegido é uma versão da avaliação da dinâmica de digitação onde os intervalos de aceitação têm como centro o tempo relativo de cada tempo parcial em relação ao tempo total ou em relação a um dos tempos parciais que, após ser fizado, serve de unidade de medida (Schreiber & Knox, 2007).

- EP1469372A2 (*User Authentication using Rhythmic Passwords*):
  - Patente solicitada pela AT&T a 16 de Abril de 2004.
  - Trata-se de um sistema para acrescentar a avaliação do ritmo das introduções à avaliação dos dados introduzidos. A patente é pensada para sistemas DTMF (*Dual-Tone Multi-frequency*) mas é protegida a generalização do processo a qualquer "ponto de acesso" como computadores. A patente protege o método que consiste em proteger a comparação dos tempos de pressão e de latência com os armazenados, tanto por comparação exacta como recorrendo a um intervalo de aceitação, nomeadamente aquele que é resultado dos desvios padrão calculados. O método pode incluir a substituição de dados armazenados pelos agora introduzidos (Smith & Cheung, 2004).

- US7376899B2 (*Method and system for producing a graphical password, and a terminal device*):
  - Patente solicitada pela *Nokia Corporation* a 18 de Junho de 2004.
  - Esta patente protege um sistema de autenticação gráfica que propõe ao utilizador que constitua uma imagem, o seu segredo de autenticação, a partir de diversos blocos constituintes da mesma classe, por exemplo constituir a imagem de uma pessoa a partir de diversos cabelos, diversos olhos, diversos narizes, diversos troncos, etc. (Mäntylä, 2008).

É de referir também a existência de alguns pedidos de patentes relevantes que poderão vir a ser aprovados brevemente. É esse o caso dos seguintes pedidos de patente, mais uma vez apresentados por ordem de solicitação:

- US20060095789 (*Method and system for establishing a biometrically enabled password*):

- Patente pedida pela International *Business Machines Corporation* a 3 de Novembro de 2004.
- Esta patente reivindica o processo em que a autenticação é efectuado primeiro por palavra chave e só é utilizado o processo que recorre à dinâmica de digitação após um período de estabilização, correspondente a uma fase inicial, mais ou menos longa, do uso do sistema (Davis *et al*., 2006).

- US20060174339A1 (*An arrangement and method of graphical password authentication*):
  - Patente solicitada pelo seu inventor, Hai Tao, a 5 de Outubro de 2005.
  - Esta patente reivindica um método de autenticação gráfica onde a imagem apresentada ao utilizador é uma grelha e o segredo de autenticação é constituido por uma sequência de intersecções da grelha (Tao, 2006).

Além das patentes e dos pedidos de patentes apresentados, existe neste momento um pedido de patente internacional muito relevante no domínio da dinâmica de digitação. Trata-se do pedido WO2007128975A2, denominado *Biometric Security Systems*. Esta patente foi solicitada pela Universidade de Westminster a 5 de Abril de 2007 e reivindica o método de autenticação por dinâmica de digitação que submete os tempos avaliados a processos sucessivos de avaliação da sua adequação, cada um com uma tecnologia diferente, por exemplo passando sucessivamente por um teste estatístico, um teste baseado em sistemas imunes artificiais e um teste baseado numa rede neuronal (Revett, 2007). Uma vez que este pedido de patente reivindica um método que recorre a algoritmos mas não é em si mesmo um algoritmo, é provável que venha a ser aprovado, já que escapa à polémica em torno das patentes de algoritmos existente em algumas regiões, nomeadamente na Europa.

Da análise da legislação existente, incluindo os direitos garantidos, de facto ou em potência, pelas patentes e pelos pedidos de patente conhecidos, é especialmente relevante a não existência de qualquer entrave legal à associação da autenticação gráfica à avaliação dos padrões biométricos comportamentais que lhe estão associados e à associação desta tecnologia com a dinâmica de digitação, desde que sejam salvaguardados os direitos fundamentais do utilizador, em particular o seu direito à informação sobre o uso (o que impede a captação de dados biométricos sem o conhecimento do utilizador) e os objectivos da tecnologia utilizada.

# 4 Novos processos de autenticação e sua avaliação

## *4.1 Aplicação da teoria de Rough Sets na Dinâmica de Digitação*

A teoria dos *Rough Sets*, proposta por Pawlak (Pawlak, 1982) é uma tentativa de propor uma estrutura de transformação automática de informação em conhecimento. É baseada na ideia de que qualquer conceito inexacto pode ser aproximado por defeito ou por excesso usando uma relação gerada pela informação sobre os objectos. Pawlak salienta que uma das noções fundamentais no princípio dos *Rough Sets* é a necessidade de descobrir redundância e dependência entre os elementos. Desde então, esta filosofia tem sido utilizada com sucesso em diversas tarefas como, por exemplo, a construção de processos de classificação baseados em regras, identificação e avaliação de dependências entre dados e redução dos dados sem perda de conhecimento (Pawlak, 1982; Pawlak, 1991; Slezak, 2002).

Esta técnica foi usada como parte integrante de um algoritmo para reconhecimento de padrões para *Keystroke Dynamics*, desenvolvido na Universidade do Minho. A recolha de dados foi efectuada ao longo de um mês recorrendo a um *software* escrito em JAVA e executado num *browser* a partir de um portal *online*. A sequência escolhida tinha 14 caracteres correspondentes à expressão “EU SOU POPULAR”, resultando em 13 tempos recolhidos por frase. Participaram 96 utilizadores e todos utilizaram a mesma frase para que os seus tempos pudessem também ser considerados como tentativas de ataque às contas dos outros utilizadores. Para este ensaio, um utilizador introduziu 96 vezes a frase e foi considerado como o utilizador legítimo. Os restantes foram considerados como atacantes, um tempo de cada um. 70% dos dados foram considerados como grupo de treino e 30% como grupo de teste e a divisão, bem como as restantes operações, foi efectuada pelo *software Roseta*. Foi primeiro utilizada a ferramenta *Reduct* para tentar reduzir a complexidade dos dados sem

perda de conhecimento e, de seguida, geraram-se as regras o que, sem o uso de qualquer filtro, resultou em 1747 regras. Foram então eliminadas todas as regras com menos de 5 ocorrências de suporte, resultando num conjunto de 657 regras. O resultado permitiu uma precisão superior a 97% no discernimento das entradas legítimas. Este resultado aponta para uma possibilidade real de se utilizar a teoria de *Rough Sets* para a criação de regras individuais para classificação das tentativas de autenticação recorrendo à dinâmica de digitação .

Outros estudos, enquadrados com os trabalhos deste doutoramento, mostraram que é também possível utilizar com sucesso relativo (FAR e FRR ambas inferiores a 10%) redes neuronais probabilísticas na autenticação pela dinâmica de digitação (Revett et al., 2007).

## *4.2 Pointer Dynamics*

### 4.2.1 Uma proposta de autenticação gráfica

O sistema proposto consiste na escolha de uma imagem de entre quatro disponíveis. Cada uma das quatro imagens inclui uma grelha (20x15), onde a primeira linha contem letras e a primeira coluna contém números (Figura 62). Assim, cada uma das trezentas células pode ser identificada por um par letra/número. Neste sistema o utilizador que opte por uma autenticação gráfica deve escolher as células de uma ou mais imagens (só pode visualizar uma imagem de cada vez, mas pode alternar entre elas quantas vezes quiser), que passarão a constituir, incluindo a ordem por que foram escolhidas, o seu segredo gráfico de autenticação. Após a selecção das várias áreas, o sistema transforma-as numa cadeia alfanumérica complexa, utilizando funções unidireccionais, o que permite que este protocolo de autenticação possa ser utilizado em sistemas já implementados, criando a possibilidade de escolha entre o protocolo gráfico ou a palavra passe tradicional. Essa escolha pode ser deixada ao utilizador, ou ser feita pela instituição proprietária do sistema. No sistema implementado para

efectuar os testes, o utilizador pode escolher ou a palavra passe tradicional ou a palavra passe gerada a partir da sequência gráfica (Figura 63)

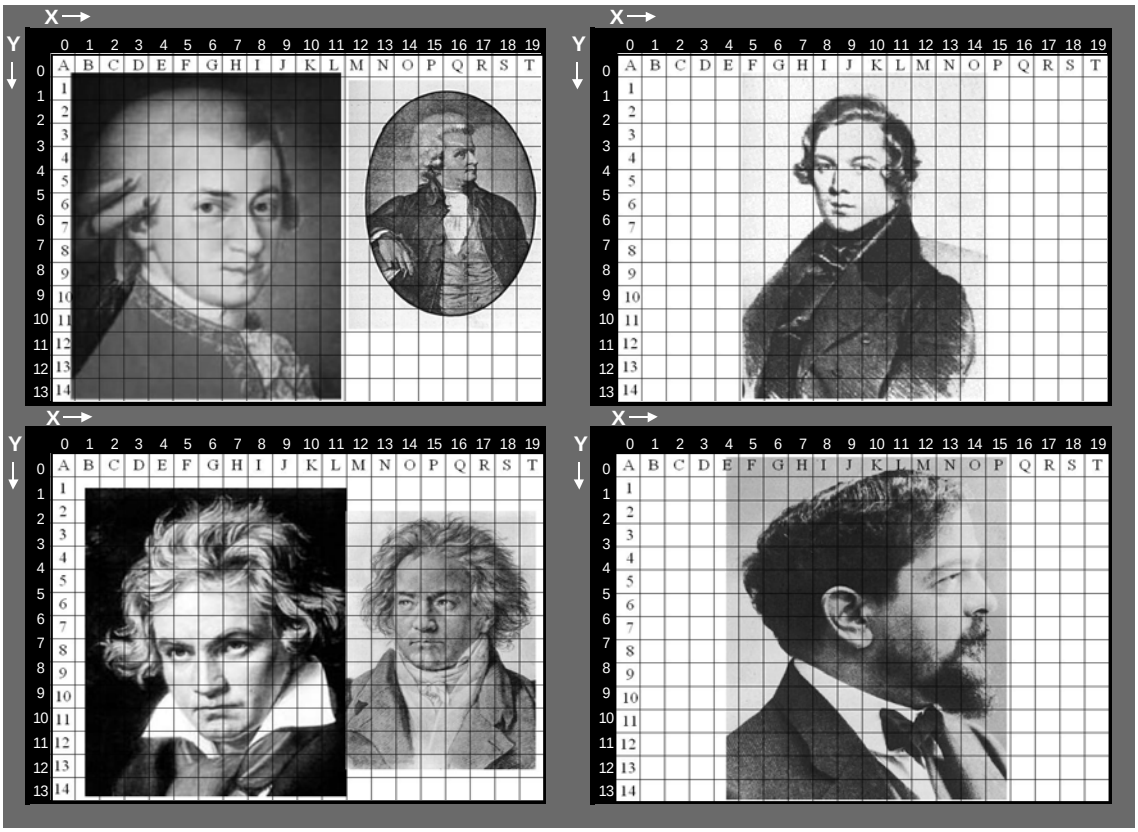


*Figura 62 – Imagens disponíveis para selecção das células de autenticação*

Este protocolo tem semelhanças com o *PassPoints* mas, neste caso, o utilizador não escolhe pontos, escolhe regiões/células e, portanto, conhece exactamente a região onde pode/deve clicar, enquanto que o sistema *PassPoints* pretende que o utilizador seleccione o mesmo ponto, dando-se-lhe uma margem de erro que pode ser maior ou menor, mas que é sempre desconhecida do utilizador. A existência de um sistema de coordenadas alfanuméricas apresentava-se, à partida, como uma vantagem potencial, por facilitar a memorização das células escolhidas, mas veio a revelar-se como demasiado condicionadora das opções de chaves, como se verificará na secção seguinte, se for implementado sem restrições na escolha do segredo de autenticação.

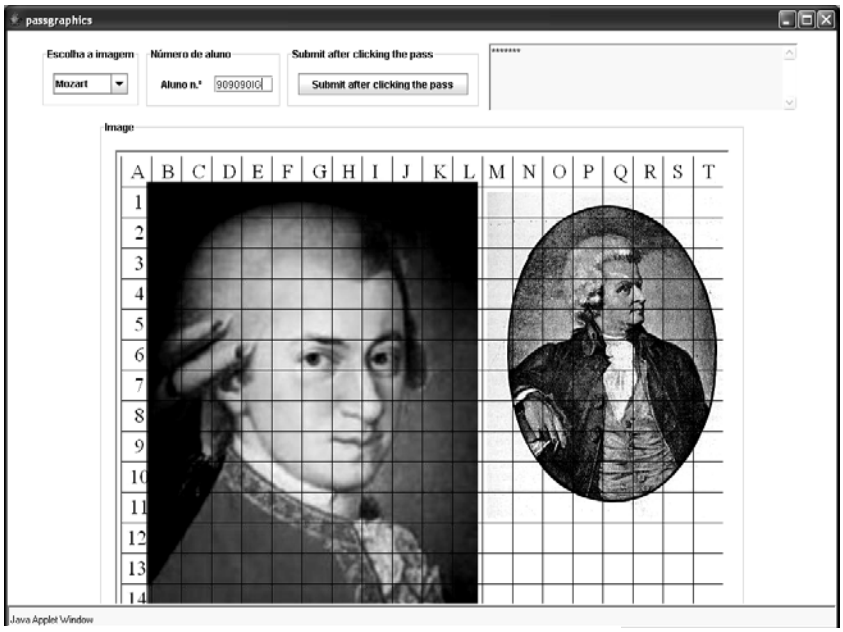



*Figura 63 – Aspecto visual do interface de autenticação*

### 4.2.2 Boas práticas na selecção das imagens

A utilização de sistemas gráficos de autenticação elimina alguns problemas relacionados com os códigos alfanuméricos, por exemplo o uso de palavras passe facilmente associadas ao utilizador como o seu nome ou a sua data de nascimento. No entanto, a escolha errada das imagens utilizadas nos sistemas gráficos de autenticação pode criar um ambiente propício a outros maus hábitos. Tendo em vista a compreensão dos mecanismos de escolha das células que constituem as sequências de autenticação, foi elaborado um estudo envolvendo cento e setenta e três utilizadores de um sistema real. Foi-lhes explicado o processo de autenticação descrito na secção anterior e foi-lhes pedido que escolhessem uma sequência gráfica de autenticação, deixando de utilizar a palavra passe convencional, sem que lhes fosse imposta qualquer regra adicional.

Os resultados mostraram que:

- 50% dos códigos escolhidos são constituídos por três ou menos células e 70% não têm mais do que 5 células (Figura 64). É também

digno de nota o facto de 21% dos utilizadores terem escolhido apenas 1 célula para servir de chave de autenticação.

- 75,9% das chaves de autenticação são constituídas por células de uma só linha (55,5%) ou de uma só coluna (20,4%). Destas destacam-se as 10,98% de chaves constituídas apenas por células da linha imediatamente abaixo das letras (Tabela 8).
- Da totalidade dos pontos escolhidos, a linha seguinte à das letras, as esquinas das imagens, os olhos de pessoas, as letras e os números obtiveram, respectivamente, 39.94%, 13.12%, 9.18%, 10.06% e 6.56% das escolhas, ao invés dos 6.67%, 2.11%, 0.83%, 6.67% e 5.26%, respectivamente, que seria de esperar se a escolha fosse aleatória (Tabela 9).
- Os utilizadores escolhem, normalmente, células da primeira imagem (64,36%), sendo que a probabilidade de uma célula ser escolhida é tanto menor quanto mais abaixo na lista de selecção está a figura que o contém (Figura 65).

As conclusões deste estudo mostraram que os analistas e programadores devem incluir nas suas políticas de segurança medidas que garantam que as sequências gráficas têm um nível de segurança adequado, nomeadamente:

- Forçar o utilizador a escolher no mínimo 5 células.
- Impedir a definição de chaves constituídas por células de um só linha ou coluna.
- Não propor imagens de pessoas e/ou com pontos muito destacados.

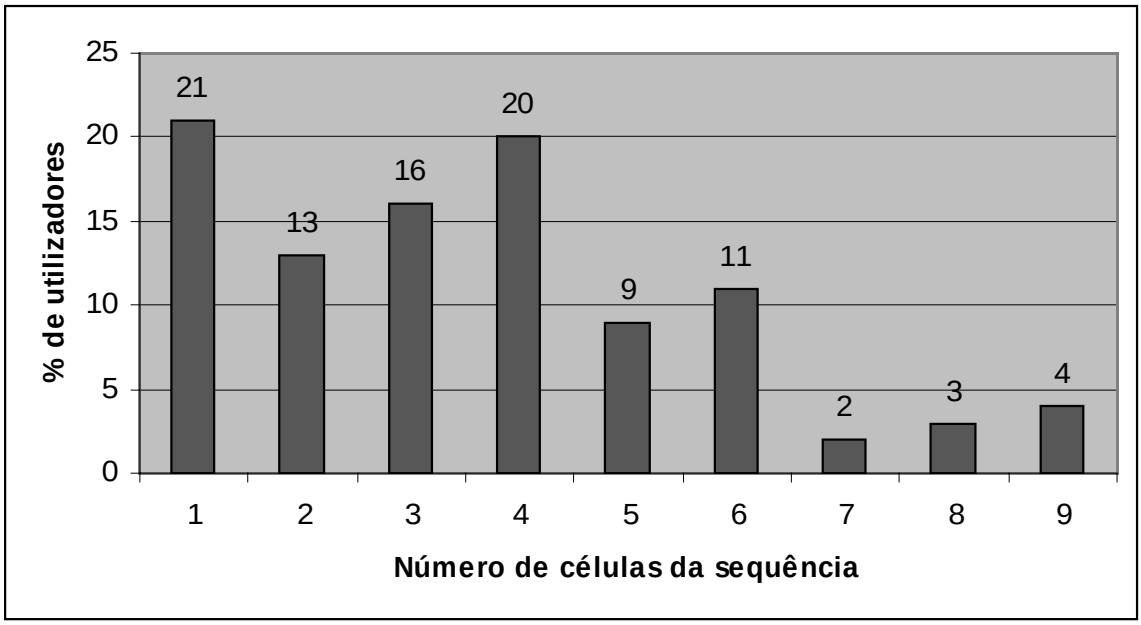



*Figura 64 – Número de células em cada sequência gráfica de autenticação*

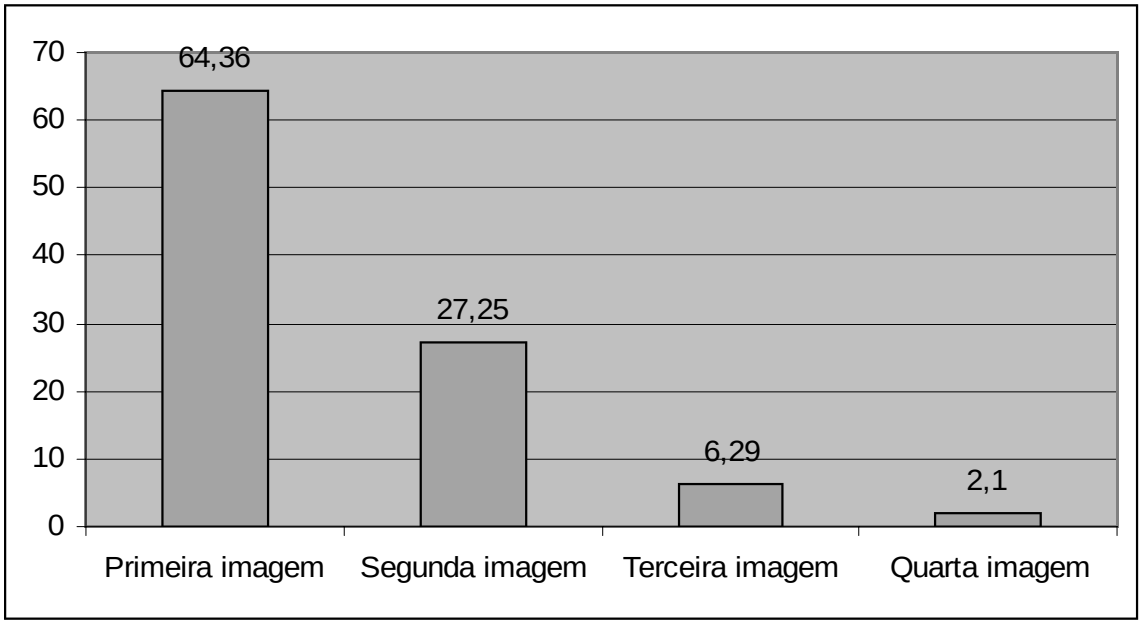



Figura 65 – Incidência de escolhas nas diversas imagens disponíveis, de acordo com a ordem por que foram apresentadas

| | *Utilizadores (%)* |
|---|---|
| *Palavras passe constituídas exclusivamente por caracteres* | 6.36 |
| *Palavras passe constituídas exclusivamente por números* | 2.89 |
| *Palavras passe constituídas exclusivamente por regiões na linha imediatamente abaixo das letras* | 10.98 |

*Tabela 8 – Constituição das sequências gráficas de autenticação*

| | *Expectável se aleatório* | *Percentagem verificada* |
|---|---|---|
| *Regiões na linha imediatamente abaixo das letras* | 6.67% | 39.94% |
| *Esquina* | 2.11% | 13.12% |
| *Olhos* | 0.83% | 9.18% |
| *Letras* | 6.67% | 10.06% |
| *Números* | 5.26% | 6.56% |

*Tabela 9 – Tipos de pontos seleccionados acima do expectável se o processo de escolha fosse aleatório*

### 4.2.3 Autenticação gráfica biométrica – *Pointer Dynamics*

O conceito de *Pointer Dynamics* resulta da junção da autenticação biométrica comportamental com a autenticação gráfica. Este conceito experimental pretende definir o padrão de um utilizador ao utilizar um dispositivo apontador (rato, *stylus*, *touch pad*, etc.) para se autenticar perante um sistema de autenticação gráfico. Em cada tentativa de autenticação, o acesso é permitido se e só se o padrão existente na forma como o segredo gráfico foi introduzido é semelhante ao padrão do utilizador legítimo previamente armazenado.

A utilização de um processo de autenticação que une a biometria comportamental e a autenticação gráfica permite o acesso a processos de autenticação forte mesmo a cidadãos analfabetos ou com grandes dificuldades

na escrita, por dispensar o uso de caracteres, substituídos por algo que é familiar, as imagens. Embora seja pouco provável que cidadãos analfabetos ou com grandes dificuldades na escrita recorram a serviços do Estado disponibilizados na Internet, é possível que isso aconteça em algumas situações específicas, como em balcões de apoio ao cidadão colocados em Juntas de Freguesia, ou no eventualidade de virem a ser adoptadas urnas electrónicas que disponham de processos electrónicos de autenticação. Esta tecnologia pode ser também utilizada nos processos de autenticação baseados nos chamados "teclados virtuais", tão comuns nas plataformas de banca electrónica e que não são mais do que uma forma de autenticação gráfica, onde a imagem é uma grelha de números (Figura 66 e Figura 67) ou uma representação de um teclado (Figura 68). Nestes sistemas, amplamente testados, a autenticação gráfica tem sido utilizada para a introdução dos códigos de identificação pessoal e, no caso da Caixa Geral de Depósitos, este processo é utilizado até para a introdução do número de utilizador.


*Figura 66 – Sistema de autenticação com teclado virtual numérico da plataforma de e-banking da Caixa Geral de Depósitos (número de utilizador e código de acesso)*

A junção de algoritmos biométricos aos actuais processos de autenticação gráfica utilizados por alguns bancos introduziria uma nova camada de segurança, que poderia substituir ou complementar os actuais códigos inscritos em cartões entregues aos clientes e que são solicitados para a realização de

determinadas operações. Estes cartões são vulneráveis a ataques por diversas formas, desde o *phishing* até ao uso de *software* malicioso instalado furtivamente no computador do utilizador, onde são solicitados os códigos constantes do cartão. Os bancos têm tentado sensibilizar os seus utilizadores para um comportamento seguro, nomeadamente com mensagens apresentadas sempre que o utilizador acede aos seus serviços (Figura 69), mas a introdução de um nível de segurança biométrico traria resultados imediatos, mesmo porque a captura de um vector biométrico pode, se o sistema assim o entender, não permitir a sua reutilização.


*Figura 67 – Sistema de autenticação com teclado virtual numérico da plataforma de e-banking do Banco Espírito Santo (só para o código de acesso)*

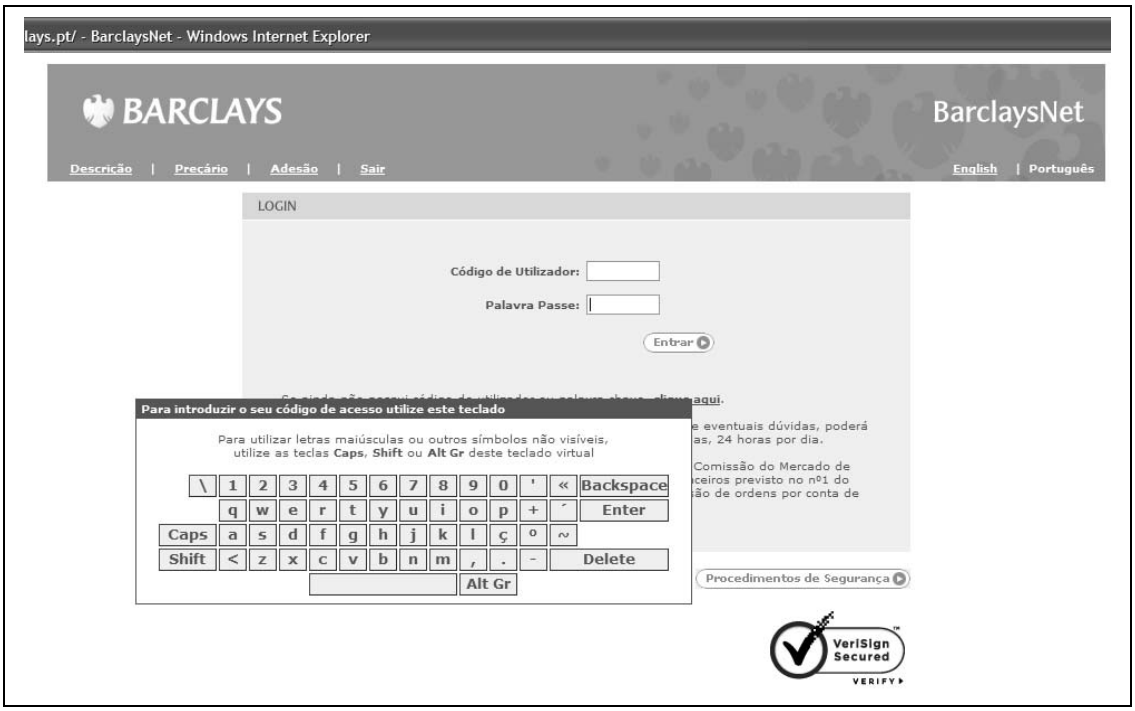



*Figura 68 – Sistema de autenticação com teclado virtual alfanumérico da plataforma de e-banking do Banco Barclays (só para o código de acesso)*


*Figura 69 – Mensagem de alerta anti-fraude exibida a cada acesso ao serviço Caixa Directa, o serviço de e-banking da Caixa Geral de Depósitos*

### 4.2.4 Um sistema de *Pointer Dynamics* experimental

#### 4.2.4.1 Descrição

Com o objectivo de testar a tecnologia *Pointer Dynamics*, integrou-se uma applet Java num software denominado Moodle, um Sistema de Gestão de Cursos *Online*. O processo de autenticação desta plataforma foi transformado de forma a substituir o sistema convencional de utilizador e palavra passe pela informação gerada pela *applet* desenvolvida. Para o funcionamento do Moodle foi instalado o pacote de software WAMP5 que inclui o sistema gestor de bases de dados MySQL, o servidor *Web* Apache e o PHP na versão 5.

Tanto o ambiente de registo como o ambiente de autenticação consistem numa janela com um campo para o nome de utilizador, um painel de diálogo, onde o utilizador recebe algum *feedback* do sistema, dois botões para apagar a palavra passe, um para apagar só a sequência actual e outro para apagar todas as sequências introduzidas, e um terceiro botão utilizado no processo de registo para avançar para a introdução seguinte (Figura 70). O processo de registo consiste em doze fases onde, em cada uma, o utilizador tem que repetir o segredo gráfico de autenticação para que o sistema tenha um conjunto de tempos necessário para estabelecer um padrão. A imagem estava dividida numa grelha de 11x16 células (Figura 70) mas não apresenta o sistema de referência por letras e números, representando uma evolução do sistema MRS que entra em consideração com as recomendações dos estudos relativos a uma boa escolha das imagens. A ausência de referências dificulta também a transmissão do segredo. Além desta alteração, foram também introduzidas na *applet* algumas limitações à escolha do segredo gráfico, de acordo com as boas práticas já descritas:

- As sequências de autenticação têm, obrigatoriamente, de possuir pelo menos quatro pontos e, no máximo dez (esta última limitação foi imposta por questões relacionadas com a arquitectura do Moodle).

- Os pontos das sequências não podem estar todos na mesma linha ou na mesma coluna.
- Os pontos das sequências não podem estar todos em esquinas.

Também a imagem utilizada respeita as boas práticas referidas, não apresentando pontos que se destaquem na figura.


*Figura 70 – O sistema de registo e autenticação*

### 4.2.4.2 Precisão obtida

Participaram nesta experiência nove utilizadores, provenientes de diferentes áreas profissionais, que se voluntariaram para fornecer a sua informação de autenticação (nome de utilizador e segredo gráfico) após o registo no sistema. Diversos alunos de diferentes anos da Licenciatura em Informática de Gestão da Universidade do Minho tentaram aceder ao sistema, usando a informação de autenticação destes utilizadores, tornada pública. Também os utilizadores legítimos continuaram a aceder naturalmente ao sistema, registando sempre a data e hora em que o fizeram, para que pudessem ser distinguidos de

tentativas de intrusão, para que fosse possível calcular a taxa de falsas rejeições.

Uma vez que o objectivo da experiência era compreender se a informação fornecida pelos tempos entre cliques era suficiente para que o sistema estabelecesse um padrão utilizável para verificar a legitimidade dos utilizadores (não se tratava de encontrar o melhor algoritmo, mas sim um algoritmo) utilizou-se um algoritmo desenvolvido e testado previamente na dinâmica de digitação, considerando as semelhanças entre os tipos de dados processados.

O processo utilizado tem duas fases distintas, como é habitual nas biometrias: o registo e a tentativa de autenticação. Na fase de registo, o utilizador insere, através do seu dispositivo apontador, a sua chave secreta doze vezes e o sistema grava os tempos entre os vários cliques, gerando uma matriz *n* x *12* e calculando a média, a mediana e o desvio padrão de cada um dos *n* tipos de tempos. A fase de autenticação consiste em, para cada dois pontos seleccionados, recolher o tempo decorrido (denominado tempo proposto, TP, por estar a ser proposto como um tempo legítimo) e compará-lo com o correspondente valor armazenado na fase de registo, usando um critério de verificação definido pela fórmula apresentada na Figura 71, onde $\alpha$ é uma variável parametrizável.

$$Minimo(média; mediana) * \left(1 - \alpha - \frac{DesvioPadrão}{média}\right) \leq TP \leq Máximo(média, mediana) * \left(1 + \alpha + \frac{DesvioPadrão}{média}\right)$$

*Figura 71 – Critério de decisão de aceitação de um determinado tempo de latência*

Uma vez classificados todos os tempos, correspondentes à sequência de selecções da chave secreta, cada um recebe o valor 0 (zero) se não satisfaz o critério, 1 (um) se satisfaz o critério mas o tempo anterior não, e 1.5 (um e meio) se tanto esse tempo como o anterior satisfazem o respectivo critério de aceitação. Este método valoriza os acertos consecutivos, em detrimento de acertos alternados. Esses valores são então adicionados e é obtido um valor final, denominado Soma A, que corresponde ao nível de confiança do padrão

apresentado. Se A não é menor que o valor definido (um parâmetro previamente definido) então o utilizador é aceite como legítimo e a matriz *n* x *12* é actualizada, passando a incluir os tempos registados neste acesso e eliminando a sequência de tempos mais antiga. Desta forma, permite-se ao utilizador uma evolução na sua forma de introduzir a chave secreta, o que pode acontecer por fenómenos relacionados com a habituação ao processo, ou à memorização do segredo, embora essa evolução tenha necessariamente que acontecer de forma lenta. A precisão obtida, com $\alpha$ definido a 0.6 (seis décimas), para os diferentes níveis de aceitação da *Soma A* são apresentados na Figura 72, bem como as respectivas linha de tendência (polinomiais de grau seis).

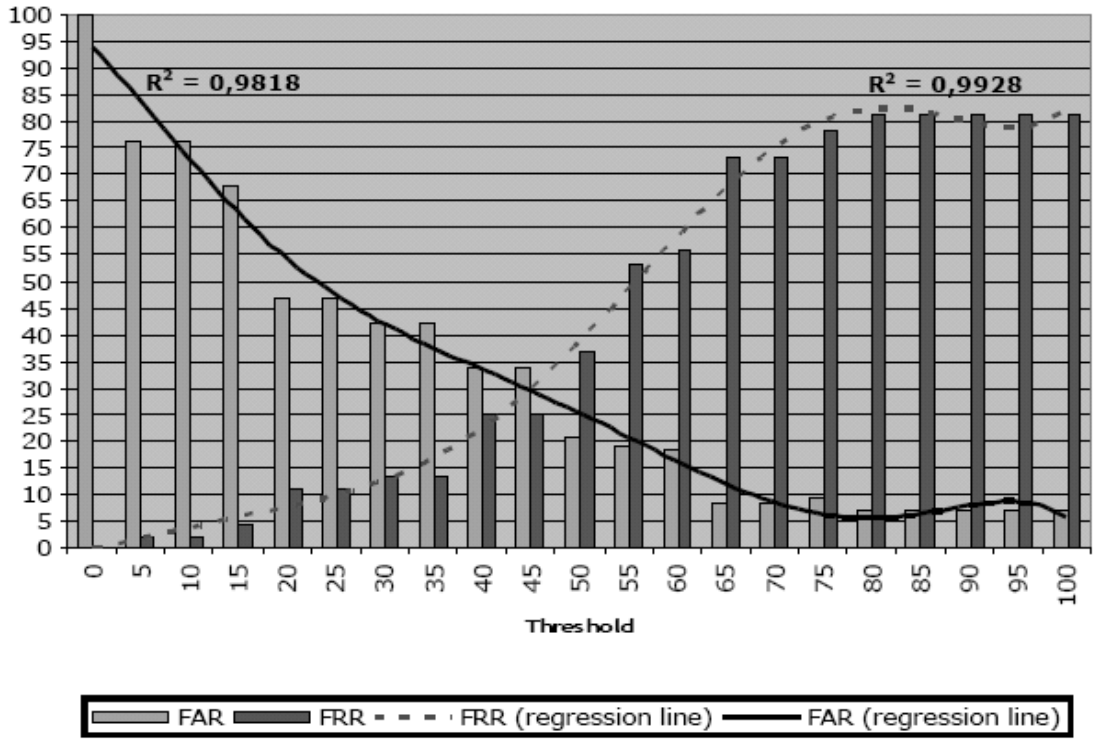



*Figura 72 – Precisão obtida com o algoritmo de testes, com $\alpha$ definido a 0.6, após o segredo de autenticação ter sido tornado público*

Estes valores correspondem aos erros de tipo I e tipo II, falsos positivos e falsos negativos, após o segredo de autenticação ter sido tornado público, o que sem biometria resultaria numa entrada no sistema sem oposição para qualquer

intruso, isto é, numa taxa de falsas aceitações (FAR – *False Acceptance Rate*) de 100 %, na provável alteração pelo intruso da chave legítima e, a partir daí, numa taxa de falsas rejeições (FRR – *False Rejection Rate*) de 100%. Assim sendo, é excelente obter um *Crossover Error Rate* (CER – taxa de intersecção de erros, também designado por *Equal Error Rate* - EER) de 30%. Embora esta taxa de intersecção de erros seja ainda um valor alto, aproximadamente dois terços dos intrusos que tenham obtido por outras vias o segredo de autenticação serão, ainda assim, impedidos de aceder ao sistema, enquanto que, para isso, o utilizador terá que se dispor a repetir a chave uma em cada três vezes que tente aceder ao sistema.

Também muito importante para a análise da viabilidade desta tecnologia, da perspectiva da precisão, é o facto de ser possível atingir taxas de falsas rejeições e taxas de falsas aceitações muito baixas (não simultaneamente). Este facto indica claramente que a tecnologia é utilizável, no que respeita à precisão, já que pode ser usada sem esforço por parte do utilizador bloqueando, ainda assim, algumas tentativas de acesso ilegítimo com a chave secreta correcta, e pode ser usada com um nível de segurança bastante elevado, exigindo um esforço maior ao utilizador que terá que repetir frequentemente a chave de autenticação. Ainda assim, esta tecnologia está numa fase embrionária e necessita de tempo para que possam surgir novos algoritmos que consigam obter valores menores de erros, nomeadamente com recurso às tecnologias de inteligência artificial.

Outro facto digno de registo é o facto de que, apesar de todos os esforços colocados nas limitações impostas aos tipos de sequências que os utilizadores podiam escolher, vários utilizadores apresentaram um padrão semelhante na escolha da sua chave de autenticação, nomeadamente recorrendo a formas geométricas formadas pelos pontos da sua selecção, por exemplo uma diagonal ou um quadrado. Considerando este facto, decidiu-se avaliar os níveis de precisão desta tecnologia considerando apenas os utilizadores que escolheram sequências de autenticação dependentes da imagem, descartando os

utilizadores que escolheram sequências de carácter geométrico. Os resultados melhoraram significativamente e o *Crossover Error Rate* (CER) desceu para 19%, como se pode verificar na Figura 73.

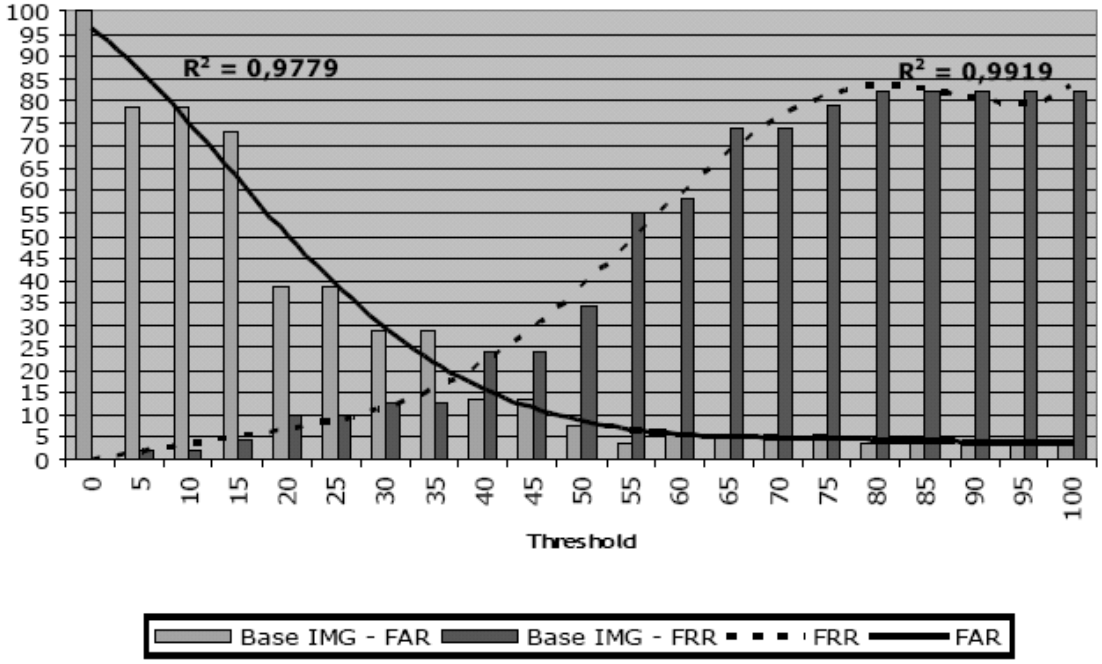



*Figura 73 – Nível de precisão para os utilizadores que escolheram uma sequência baseada na imagem e não na geometria (após divulgação pública do segredo de autenticação)*

Os resultados indicam, uma vez mais, que a implementação de políticas de segurança correctas e adequadas para a constituição dos segredos de autenticação pode representar um factor chave no sucesso do uso de uma tecnologia e nesta, em particular, também. Se as melhores regras de selecção do segredo de autenticação forem seguidas, é possível obter níveis satisfatórios de precisão, mesmo com um algoritmo que não foi ainda optimizado para esta tecnologia (Tenreiro de Magalhães et al., 2008).

## *4.3 Integração com outros sistemas*

A alteração do processo de autenticação deve, sempre que possível, evitar alterações significativas nos sistemas que protege, de forma a evitar longos tempos de implementação e elevados custos. Assim, as secções seguintes apresentam alguns métodos para integração dos sistemas apresentados nos sistemas convencionais.

### 4.3.1 Geração de palavras passe a partir de sequências gráficas

Uma sequência gráfica de autenticação de comprimento *n*, composta por células de uma imagem dividida em *K*x*S* células, pode ser encarada como um vector do tipo ($p_1$, $p_2$,…, $p_n$) onde $p \in \{(x, y) \mid 0 \le x \le K,\ 0 \le y \le S\}$, já que os valores de *x* e de *y* definem a região seleccionada na imagem bidimensional. De forma a manter a compatibilidade com os sistemas tradicionais de autenticação por palavra passe, é necessário gerar, a partir da sequência gráfica secreta, uma sequência de caracteres. Para o conseguir, iremos utilizar 15 tabelas (Tabela 13 a Tabela 27 do Anexo V), numeradas de 0 a 14, com 26 colunas e 20 linhas. Temos, assim, 7800 células, cada uma com uma sequência de três caracteres.

O processo de conversão começa com a escolha da primeira célula, que será encontrada da tabela de valor (*x*+*y*)mod15, linha *x*mod*K*, coluna *y*mod*S*. Então, para cada $p \in \{(x, y) \mid 0 \le x \le K,\ 0 \le y \le S\}$ consideremos que:

1. $\Omega$ toma o valor do código ANSI do primeiro carácter da última célula seleccionada.
2. $\Psi$ toma o valor do código ANSI do segundo carácter da última célula seleccionada.
3. $\Theta$ toma o valor do código ANSI do terceiro carácter da última célula seleccionada.
4. A tabela seguinte a ser usada é encontrada fazendo $x+y+\Omega$ mod 15
5. A próxima célula está na linha $x+y+\Psi$ mod 20 (20 é o número de linhas).

6. A próxima célula está na coluna $x+y+\Psi$ mod 26 (26 é o número de colunas).

Para prevenir a possibilidade da sequência de células escolhidas ser descoberta, por exemplo, através da captura dos pacotes transmitidos na rede sem protecção, num sistema implementado sem preocupações de segurança, é necessário efectuar algumas alterações finais à sequência de caracteres obtida, para aumentar exponencialmente o número de possibilidades obtidas numa tentativa de, partindo da sequência de caracteres obtida de forma ilegítima, obter a sequência gráfica de autenticação que, assim, permanece secreta. Consegue-se assim garantir que a violação de um determinado sistema não garantirá o acesso a outros sistemas, ou subsistemas, que utilizem outras tabelas de conversão e onde o utilizador utilize a mesma sequência gráfica. Para efectuar as transformações faremos:

1. $\alpha$ toma o valor do código ANSI do primeiro elemento da cadeia de caracteres já obtida.
2. *t* toma o valor de *x* mod *n* (*n* é o número de células seleccionadas na sequência gráfica)
3. Inverte-se a ordem dos primeiros *t* caracteres.
4. $\beta$ toma o valor do código ANSI do último elemento da cadeia de caracteres já obtida.
5. *s* toma o valor de *y* mod *n*
6. Inverte-se a ordem dos primeiros *s* caracteres.

Se no momento da autenticação o sistema permitir ao utilizador escolher o processo de autenticação que irá utilizar, considerando o ambiente envolvente e/ ou o equipamento usado, então é necessário que o sistema converta a sequência gráfica na palavra passe do utilizador. Isto pode ser obtido de duas formas: o sistema aceita duas palavras passe diferentes, a alfanumérica

escolhida pelo utilizador e a gerada a partir da sequência gráfica, ou é feita uma tabela de conversão, armazenada no servidor, que permite o processamento em ambiente seguro dos dados provenientes dos campos de autenticação que compara a cadeia recebida e a sua versão convertida com a sequência armazenada. Se uma delas for igual o utilizador é aceite. Assim, aceita-se tanto a sequência alfanumérica introduzida directamente, como a resultante da conversão da sequência gerada a partir da sequência gráfica. A tabela de conversão de cada utilizador associa cada caracter existente nas tabelas de geração (Tabela 13 a Tabela 27 do anexo V) a um outro caracter, de forma a que a conversão resulte na mesma palavra passe que a introduzida pelo utilizador directamente no campo numérico. Neste caso, o nível de segurança da palavra passe gerada é reduzido ao mesmo nível de segurança da palavra passe escolhida, uma vez que serão a mesma.

### 4.3.2 Alteração periódica da palavra passe

Uma das vulnerabilidades dos códigos secretos e até mesmo dos objectos usados para a autenticação, por exemplo *smart cards*, é a durabilidade da sua validade. Por um lado os utilizadores têm limitações de memória que os impedem de possuir boas palavras passe, já de si difíceis de memorizar, e de as alterar com muita frequência. Por outro lado, é custoso substituir com frequência e de forma segura os objectos de autenticação ou substituir, pelo menos, os elementos neles contidos. Assim, caso um potencial intruso se apodere dos recursos necessários para aceder a uma infra-estrutura, física ou lógica, é provável que mantenha a capacidade de lhe aceder por muito tempo. Aliás é até possível que tenha a oportunidade de inviabilizar o acesso do utilizador legítimo, por exemplo alterando-lhe a palavra passe.

O sistema gráfico de autenticação biométrica, *Pointer Dynamics*, contorna esse problema. É extremamente difícil transmitir o segredo de autenticação oralmente e mesmo recorrendo a esquemas. Por outro lado, caso essa violação

de segredo aconteça é muito difícil fazer a autenticação no padrão biométrico correcto. Resta, portanto, o perigo de a comunicação dos dados de autenticação ser interceptada, graças a uma infra-estrutura pouco segura. Nesse caso, os tempos de autenticação podem fornecer apenas uma pista dos tempos que será necessário fornecer ao sistema, já que um utilizador nunca repete completamente um vector de tempos medido ao milissegundo e não são imediatas as alterações a introduzir para manter a integridade do padrão. Acresce que essa informação tem um tempo limitado, já que a própria sequência de caracteres, gerada a partir da sequência gráfica, pode ter um período de vida limitado, mesmo sem que o utilizador mude de sequência gráfica. Basta para isso que as tabelas de conversão da sequência gráfica em sequência alfanumérica sejam frequentemente alteradas podendo ser utilizadas, no limite, apenas uma vez, sendo geradas tabelas diferentes para cada sessão (Tenreiro de Magalhães et al., 2008a).

### 4.3.3 Sistemas de Autenticação Gráfica na autenticação do servidor

A navegação na Internet exige com frequência a autenticação dos utilizadores para acesso a determinados conteúdos e/ou serviços, mas são poucos os recursos ao dispor do utilizador para validar a identidade as páginas de Internet que visita. Na verdade, um dos ataques mais comuns actualmente é o *phishing*, o processo de atrair para uma determinada página de Internet um utilizador convencido que está a visitar uma outra página de Internet de aparência semelhante. Este tipo de ataques tem gerado prejuízos muito avultados, estimando-se que só no período entre Maio de 2003 e Abril de 2004 tenham existido quase 2 milhões de vítimas de *phishing* que sofreram um prejuízo de 1200 milhões de dólares. Por outro lado, as empresas gastaram, no mesmo período, cerca de 100 milhões de dólares em tecnologia para prevenir o phishing e em campanhas de sensibilização/educação dos utilizadores (Geer, 2005).

As técnicas de *phishing* são muito variadas. Uma forma corrente de levar um utilizador a uma página de Internet falsa de uma entidade conhecida (tipicamente bancária) é o envio de uma mensagem de correio electrónico a solicitar que o utilizador siga um determinado *link* para executar uma tarefa na página de Internet da companhia bancária. A tarefa pode ser a actualização dos dados do cliente, sob alegada pena de ficar excluído do serviço, o preenchimento de um inquérito, com direito a uma recompensa, ou qualquer outra forma que a imaginação dos atacantes conceba. Na verdade, não só o número de mensagens de correio electrónico enviadas com o objectivo do *phishing* tem crescido muito rapidamente, como as formas de contacto social têm-se diversificado, recorrendo, por exemplo, a mensagens instantâneas e a *posts* em *blogues* com *links* para os sítios *Web* falsos. (Geer, 2005). No entanto, existem outras abordagens, menos sociais e mais tecnológicas, para levar um utilizador a introduzir as suas credenciais de autenticação numa página de Internet ilegítima.

Uma das técnicas conhecidas é o DNS *cache poisoning* ou DNS *hijacking* (Wüest, 2005). Nestas abordagens o servidor de DNS é utilizado como recurso para o ataque. No primeiro caso o sistema é enganado por receber uma indicação em que confia, com base na confiança que tem no servidor DNS, mas que na realidade é falsa e proveniente de outra fonte. Normalmente isto é conseguido provocando uma sobrecarga do servidor DNS legítimo de forma a que a resposta a um pedido de informação do endereço IP correspondente a um determinado domínio não possa ser dada em tempo útil. Uma vez que a associação entre um domínio e um endereço IP fica em cache durante algum tempo sem que nesse período seja feita nova verificação, o sistema acede a um servidor ilegítimo sem que exista qualquer alteração no endereço que usa. No segundo caso, através de uma ataque ao servidor DNS a informação é adulterada e, assim, é o servidor legítimo que dá uma informação ilegítima.

Outra técnica utilizada com algum sucesso é o recurso a vulnerabilidades relativas a XSS (*Cross-Site Scripting*), permitindo aos atacantes a introdução de

código próprio dentro das páginas legítimas. Assim sendo, o utilizador depara-se com um hiperligação ilegítima na página de Internet legítima. Os atacantes podem até incluir uma janela de autenticação extra na página de Internet ou apoderarem-se das *cookies* de sessão colocadas no disco do utilizador pelo servidor legítimo (Geer, 2005).

Também a introdução de código malicioso no computador do utilizador pode servir os propósitos do *phishing*. O *worm* Crowt.D demonstrou que este tipo de tecnologias pode alterar o ficheiro do sistema operativo que estabelece a relação entre os endereços de IP (*Internet Protocol*) e os servidores, levando os utilizadores a seguir para um IP diferente, mas mantendo o endereço textual correcto no *browser*. Esta técnica consegue um efeito, do ponto de vista do utilizador, semelhante ao DNS *Poisoning*, mas não exige um ataque a um servidor, o que é tipicamente mais difícil, mesmo porque há muitos mais utilizadores do que servidores DNS e podem-se sempre escolher os mais frágeis (Geer, 2005).

As abordagens *anti-phishing* têm uma capacidade limitada. A base da luta contra o *phishing* é o fecho dos sítios *Web* pelos fornecedores do serviço de Internet. No entanto, esta actividade é consumidora de recursos, humanos e financeiros, e é demorada. Além disso, os sites de phishing estão frequentemente alojados em países sem enquadramento legal para este tipo de actividades. Outra técnica utilizada é o envio de um conjunto imenso de dados para o servidor que está a realizar o *phishing*. Normalmente esta técnica não consegue neutralizar o servidor, como aconteceria num ataque tradicional do tipo *Denial-of-Service*, conseguindo apenas uma redução do seu desempenho e inundando as bases de dados com informação falsa (*poisoning*), diluindo a informação real que o sítio *Web* consiga obter de utilizadores legítimos do sistema legítimo.

Uma das primeiras entidades a perceber a necessidade de incrementar a segurança da autenticação dos seus sítios *Web* e a agir foi o *Bank of América* que, em 2005, apresentou o sistema *PassMark*, desenhado com o objectivo de

permitir que o utilizador autentique o sítio *Web* da instituição a que pretende aceder, ao reconhecer uma determinada marca (tipicamente uma imagem) que lhe é particular e que foi escolhida previamente (Bank of América, 2005). Se esta marca for a base para a introdução da sequência gráfica secreta de autenticação, então o sistema de autenticação biométrica gráfica, *Pointer Dynamics*, pode também ser utilizado para autenticar o sítio *Web* que presta o serviço ao utilizador.

Como prova de conceito, foi desenvolvido um protótipo neste doutoramento que, quando um utilizador pretende aceder ao serviço, solicita a introdução do seu nome de utilizador e, nessa altura, o sistema cria (do lado do servidor) a correspondente página de autenticação, que inclui a imagem específica do utilizador e, inserido na imagem, o endereço IP da máquina que solicitou a imagem (Figura 74) e a data/hora do pedido (para impedir que sites de phishing reutilizem a imagem de forma a enganar utilizadores que utilizem máquinas com endereço IP fixo). Se o sistema não apresentar a imagem correcta, a data/hora correcta ou o IP correcto, o utilizador sabe que é muito provável que esteja a ser vítima de um ataque. Caso a imagem esteja incorrecta, muito provavelmente o sítio *Web* é ilegítimo, caso os dados na imagem não estejam correctos, muito provavelmente o utilizador está a ser vítima de uma ataque do tipo *man in the middle*, onde uma máquina simula ao utilizador ser o servidor legítimo e simula ao servidor que é o utilizador legítimo, colocando-se a meio da comunicação e replicando ou alterando as mensagens transmitidas de acordo com a sua vontade. Desta forma, o *Pointer Dynamics* é utilizado para autenticar tanto o utilizador como o sítio *Web* (Tenreiro de Magalhães et al., 2008).

Infelizmente, o processo descrito não impede um outro tipo de ataque, do tipo do utilizado pelo código malicioso usado pelo PWSteal.Bancos.B (também conhecido como Infosteale.Bancos.B) que cria uma janela de autenticação sobre a janela original com o objectivo de capturar os dados de autenticação fora da protecção do protocolo SSL (*Secure Socket Layer*) apesar da presença do cadeado SSL contendo os detalhes do certificado correctos (Symantec

Corporation, 2003). Um *software* deste tipo poderia ser criado para também atacar um sistema com *Pointer Dynamics*, desde que fosse utilizada uma imagem transparente.

O sistema é também vulnerável a Cavalos de Tróia que, ao detectar o acesso a uma página de Internet conhecida, armazenam a sequência de cliques e uma imagem do ecrã (vulgarmente denominada *screenshot*), permitindo calcular os pixeis seleccionados.

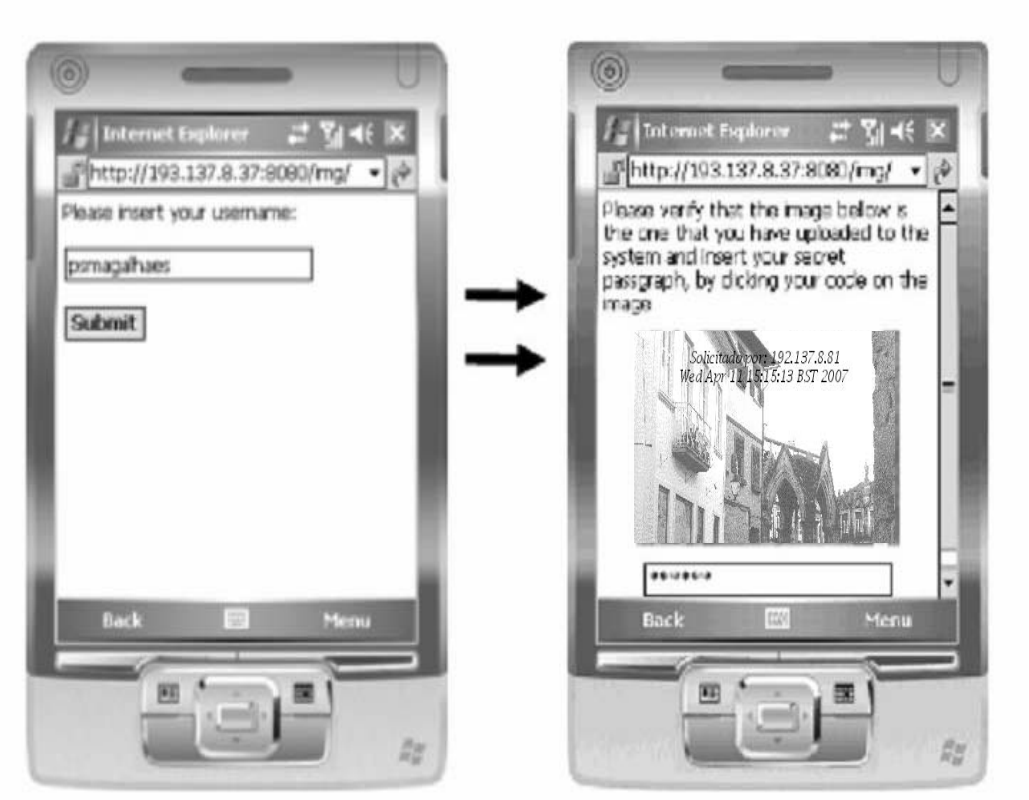



*Figura 74 – Sistema de autenticação com anti-phishing por Pointer Dynamics, utilizado num dispositivo móvel.*

Um aspecto negativo deste método é a possibilidade do endereço IP apresentado ao servidor ser diferente do endereço IP visto pelo utilizador, por este ter sido alterado ao longo da comunicação, situação normal em sub-redes, levando a uma informação enganadora na imagem. Uma implementação mais cuidada, deveria deixar a opção de visualização do endereço IP ao critério do utilizador, sendo por exemplo, uma informação do seu perfil. Uma vez que a

maioria dos utilizadores não domina os conceitos de redes, seria provavelmente mais indicado que as opções por defeito fossem a inclusão da data e hora e a exclusão do endereço IP.

## *4.4 Factores subjectivos de avaliação de qualidade*

### 4.4.1 Modelo adoptado

A adopção de uma tecnologia depende de diversos factores objectivos e subjectivos e do contexto em que a adopção ocorre. De acordo com o *Technology Adoption Model* (Modelo de adopção de tecnologia) defendido por Davis (Davis, Bagozzi, & Warshaw, 1989) os dois factores fundamentais que irão influenciar a atitude do utilizador perante a tecnologia são a percepção da utilidade e a percepção da facilidade de utilização, resultado da interpretação pessoal de um conjunto de factores externos (Figura 75). No entanto, em situações sujeitas a regulamentação, a tecnologia poderá ser imposta e, nesse caso, a intenção de comportamento resulta, segundo a *Theory of Reasoned Action* (Ajzen & Fishbein, 1975), da atitude perante o comportamento (resultado das suas avaliações e crenças) e das normas subjectivas que são o resultado das crenças normativas e da motivação para respeitar a regulamentação imposta (Figura 76). Em determinadas situações a ligação psicológica do utilizador à tecnologia pode contribuir para a adopção de uma tecnologia (Figura 77), conforme o modelo de adopção proposto por Malhotra e Galletta em 1999. A ligação psicológica contém a influência dos processos de influência social sobre as intenções e atitudes do indivíduo perante a tecnologia, resultando na interiorização, identificação ou cumprimento do comportamento induzido (Malhotra & Galletta, 1999).

A avaliação da percepção e da ligação psicológica, por se tratarem de factores subjectivos, só pode ser avaliada por sondagem. Assim, seleccionaram-se aleatoriamente 600 números de telefone, necessariamente de entidades particulares (cidadãos adultos), recorrendo às listas telefónicas da rede fixa, e

procedeu-se à sondagem por via telefónica. De acordo com o modelo adoptado e considerando que a tecnologia biométrica comportamental ainda não é usada, os grupos de questões avaliaram os factores potencialmente conducentes à futura adopção da tecnologia: a percepção da utilidade, a percepção da facilidade de uso e a ligação psicológica.

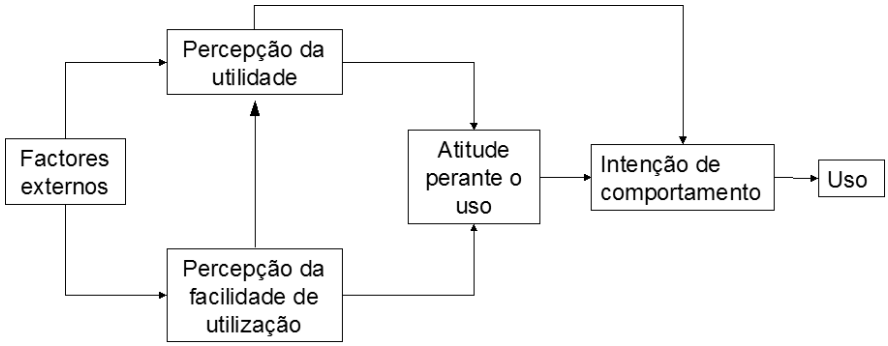



*Figura 75 – Technology Acceptance Model. Adaptado de (Davis, Bagozzi, & Warshaw, 1989)*

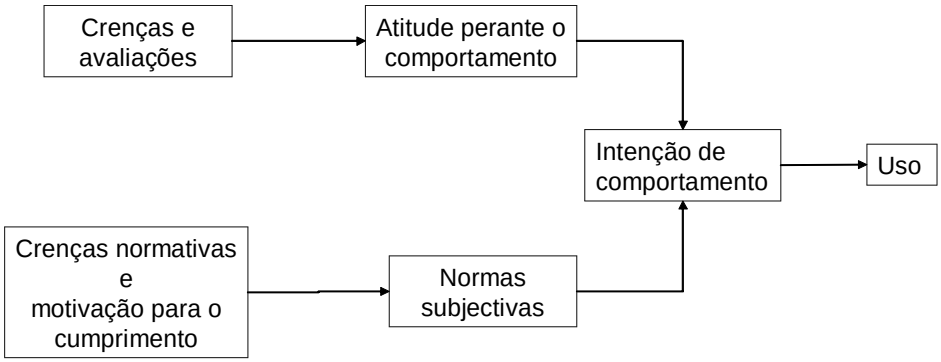



*Figura 76 – Theory of Reasoned Action. Adaptada de (Ajzen & Fishbein, 1975)*

A ligação psicológica é frequentemente decomposta em três factores: interiorização, identificação ou cumprimento, de acordo com os três processos de influência social propostos por Kelman (Kelman, 1958, 1961). O'Reilly e Chatman (O'Reilly, Chatman, & Caldwell, 1991) desenvolveram um modelo de

questionário com 12 itens posteriormente adaptada para os Sistemas de Informação por Malhotra e Galletta (Malhotra & Galletta, 1999). No entanto, uma vez que o objectivo não era avaliar o nível actual de adopção, mas o nível potencial de adopção, foi necessário propor ao inquirido a situação hipotética de a tecnologia ser adoptada pelo governo e aplicar os tempos verbais no modo condicional, o que levou a algumas adaptações ao questionário (Figura 78). Dos grupos de avaliação da percepção foram eliminadas as questões 4, 5, 8, 9 e 10 por não se adequarem ao contexto, já que as questões 8, 9 e 10 referem-se explicitamente e exclusivamente ao ambiente/local de trabalho e as questões 4 e 5 só podem ser respondidas após uma utilização real do sistema. Foram também eliminadas as perguntas 8 e 10 do grupo de avaliação da ligação psicológica por estarem exclusivamente relacionadas com o sucesso no local de trabalho.

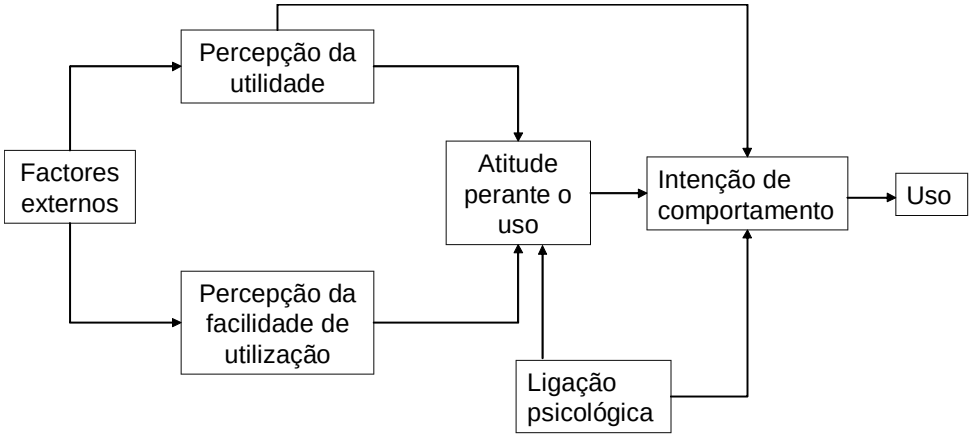



*Figura 77 – Technology Adoption Model. Adaptado de (Malhotra & Galletta, 1999).*

A utilização de um sistema que recorra à dinâmica de digitação não implica qualquer alteração de comportamento, apenas uma aceitação da captura acrescida de dados. Já o *Pointer Dynamics* implica a aprendizagem de um novo processo de autenticação, semelhante ao actualmente utilizado para autenticação nos bancos electrónicos e, portanto, não necessariamente estranho para o utilizador. As perguntas tiveram que ter esta diferença em consideração e, além disso, uma vez que o inquérito era universal, existia a possibilidade de encontrar indivíduos tecnologicamente inabilitados. Assim, a sondagem começa

com uma pergunta de filtro (pergunta zero) que foi utilizada para decidir se fazia sentido apresentar as perguntas 1 a 13, às quais o inquirido pôde responder escolhendo o seu nível de concordância com a afirmação. Para esse efeito foi utilizada uma escala de Likert de 7 pontos variando de “não, discordo totalmente” a “sim, concordo totalmente”.

As escalas de Likert permitem um tratamento quantitativo de opiniões qualitativas, sendo especialmente úteis para captar expressões extremas das reacções que se pretendem captar. Este facto é resultante da tendência para encarar cada pergunta isoladamente e responder próximo dos extremos, concordando ou discordando. Para acentuar este factor, permitindo aferir a tendência para comportamentos extremos, correspondentes à adopção ou rejeição da tecnologia, os exemplos apresentados para esclarecer uma qualquer questão, devem ser extremados (Brooke, 1996). O questionário utilizado apresenta um texto com alguma dificuldade de compreensão para pessoas com menos formação académica (a maioria dos inquiridos, como era de prever dada a realidade portuguesa). Assim, sempre que foi necessário foram prestados esclarecimentos aos inquiridos sobre o significado das questões ou mesmo de alguns dos termos utilizados. Estes esclarecimentos poderão ter influenciado os resultados da sondagem, levando as respostas para ambos os extremos já que a descrição das tecnologias, mesmo se enviesada (o que não foi o caso) leva, de acordo com os estudos de Brooke (Brooke, 1996), para uma reacção mais forte ao tema em estudo tanto na aceitação como na rejeição. Assim, os valores obtidos devem ser avaliados essencialmente na perspectiva de uma reacção positiva ou negativa à questão e, a partir daí, à tecnologia.

***Pergunta filtro***

0. Utiliza o e-mail, a Internet ou o cartão Multibanco?

***Avaliação da percepção da utilidade e da facilidade de utilização***

1. Seria fácil, para si, aprender a introduzir um código secreto carregando em partes de uma imagem, em vez de carregar em letras ou números.

2. Seria fácil, para si, introduzir uma sequência secreta através de um teclado ou de toques no ecrã.

3. A maneira como uma pessoa introduz um código secreto é o suficiente para confirmar que é mesmo ela, desde que a máquina armazene os tempos que a pessoa demora a introduzir os números ou as letras.
   a. Considera que essa tecnologia pode funcionar bem.
   b. Concorda que o facto de medirem os seus tempos não perturba o utilizador.
   c. Seria fácil, para si, habituar-se à ideia de que a máquina mede os seus tempos enquanto introduz a sua sequência secreta?

4. Considera que o uso de biometrias tornaria as suas tarefas mais seguras.

5. Considera que o aumento do uso de biometrias que medem os comportamentos seria útil para tornar as tecnologias mais seguras.

6. Considera que usar partes de uma imagem em vez das letras e dos números dos códigos secretos tornaria o uso das tecnologias mais fácil.

7. Considera que o aumento do uso de biometrias que medem os comportamentos tornaria o uso das tecnologias mais claro e compreensível.

***Avaliação da ligação psicológica***

8. Aquilo que o uso das biometrias representa, no aumento da segurança, é importante para si.

9. O motivo porque preferiria usar biometrias nos serviços electrónicos do Estado é por causa dos valores do seu país.

10. Gostaria de usar biometrias nos serviços electrónicos do Estado por causa da semelhança dos seus valores com os valores do seu país.

11. Sentiria orgulho em utilizar biometrias.

12. Aquilo que pensa das biometrias é diferente daquilo que diz às outras pessoas que pensa.

13. Se não sentir que é recompensado por usar biometrias não vê qualquer motivo para fazer esse esforço.

*Figura 78* – Questionário adaptado de acordo com o TAM

### 4.4.2 Resultados obtidos na sondagem

A primeira grande dificuldade na realização de uma sondagem por via telefónica é encontrar números que correspondam a residência em que esteja alguém em casa. Uma vez atendida uma chamada, a segunda dificuldade é conseguir que o cidadão se disponha a responder às questões. A grande quantidade de inquéritos telefónicos e, principalmente, as vendas por via telefónica têm saturado os utentes do telefone fixo.

O inquérito desenhado começava com uma pergunta de filtro que, quando respondida negativamente terminava o questionário. Tratava-se de compreender se o cidadão em causa já utiliza qualquer tipo de tecnologia que lhe permita compreender as restantes questões. Bastava que o cidadão tivesse alguma vez usado, ou soubesse como funciona, ou a Internet, ou o correio electrónico ou o cartão multibanco. Um dos elementos bastava e, dada a grande penetração anunciada pela SIBS e pelas entidades bancárias da tecnologia multibanco, esperava-se que a larga maioria dos inquiridos respondesse afirmativamente. Mas, infelizmente, não foi assim. 234 dos 600 inquiridos (39%), responderam negativamente, uns por total desuso, outros porque era o conjuge quem “tratava desse assuntos” (Figura 79).

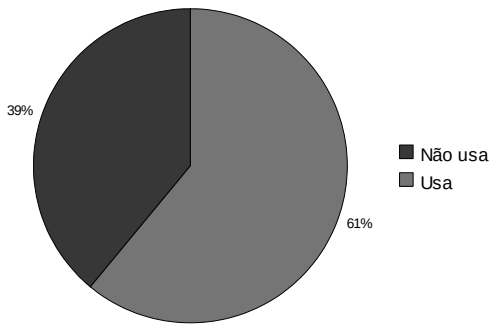



*Figura 79 – Respostas à questão zero: "Utiliza o e-mail, a Internet ou o cartão Multibanco?"*

mais valores positivos), denotando alguma satisfação com a usabilidade dos processos existentes actualmente.

O gráfico da (Figura 80) mostra os valores acumulados ao longo das 9 nove questões deste grupo, para cada uma das 7 respostas possíveis, sendo clara a tendência para a concordância e, portanto, para uma percepção positiva da utilidade e da facilidade de utilização das tecnologias em estudo.

| *Questão* | *Resposta* | | | | | | |
|---|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| *1* | 21 | 1 | 3 | 0 | 129 | 61 | 151 |
| *2* | 0 | 0 | 0 | 0 | 2 | 41 | 323 |
| *3A* | 99 | 59 | 36 | 31 | 32 | 32 | 77 |
| *3B* | 0 | 1 | 0 | 9 | 2 | 1 | 353 |
| *3C* | 0 | 0 | 0 | 0 | 1 | 34 | 331 |
| *4* | 4 | 0 | 0 | 0 | 21 | 39 | 302 |
| *5* | 0 | 0 | 0 | 0 | 51 | 3 | 311 |
| *6* | 37 | 43 | 35 | 39 | 71 | 44 | 92 |
| *7* | 0 | 3 | 0 | 1 | 23 | 44 | 295 |

*Tabela 10 – Respostas às questões 1 a 7 (grupo de avaliação da percepção da utilidade e da facilidade de utilização)*

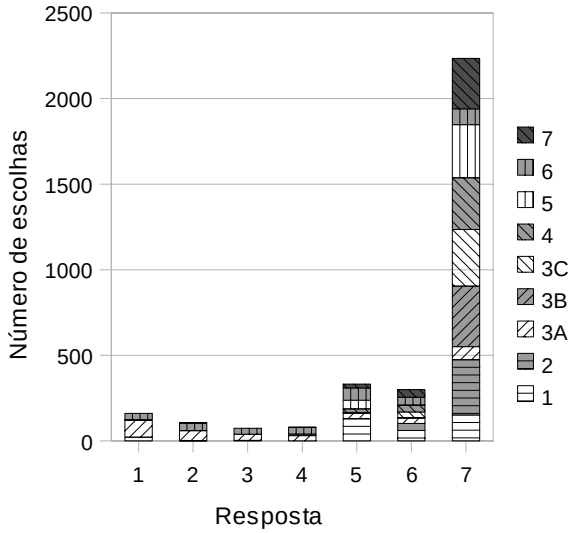



*Figura 80 – Acumulado das respostas ao grupo de avaliação da percepção da utilidade e da facilidade de utilização*

Na avaliação da ligação psicológica as perguntas 8 a 11 são efectuadas pela positiva e, portanto, cotações elevadas correspondem a factores positivos na adopção da tecnologia. Foi o que se verificou nas respostas obtidas (Tabela 11 e Figura 81). Já as perguntas 12 e 13 têm uma conotação negativa e, portanto, o ideal seria a obtenção de cotações baixas. Foi o que se verificou na questão 12, “Aquilo que pensa das biometrias é diferente daquilo que diz às outras pessoas que pensa” que, deixou muitos dos inquiridos ofendidos. Já na questão 13 há uma polarização das respostas, que se concentram essencialmente nos extremos como esperado (Brooke, 1996), denotando uma percentagem significativa de inquiridos que sentem a necessidade de uma recompensa para usarem biometrias (Tabela 12 e Figura 82). De modo a obter uma visão geral da ligação psicológica dos inquiridos foi então invertido o sentido da escala utilizada nas questões 12 e 13 e os valores obtidos foram adicionados aos resultantes das questões 8 a 11, mostrando claramente uma boa ligação psicológica às tecnologias em estudo (Figura 83).

Verifica-se, portanto, como resultado global da sondagem, que o cidadão português parece estar predisposto à introdução das biometrias comportamentais, em particular o *Pointer Dynamics* que esteva no centro deste estudo, como forma de autenticação do cidadão perante os serviços electrónicos do Estado. Esse resultado é especialmente visível no gráfico da Figura 84 que apresenta o número médio de respostas (depois de invertido o sentido das questões 12 e 13) para cada uma das 7 posições da escala de Likert utilizada. Assim, valores na área esquerda do gráfico da Figura 84 representam uma tendência para a resistência à adopção das tecnologias em estudo, enquanto que valores na área da direita do gráfico representam uma tendência para a aceitação e adopção dessas tecnologias.

| *Questão* | *Resposta* | | | | | | |
|---|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| *8* | 0 | 0 | 4 | 0 | 0 | 21 | 341 |
| *9* | 3 | 1 | 0 | 0 | 115 | 106 | 141 |
| *10* | 4 | 0 | 0 | 0 | 96 | 129 | 137 |
| *11* | 0 | 0 | 0 | 0 | 31 | 39 | 296 |

*Tabela 11 – Respostas às questões 8 a 11 (primeira parte do grupo de avaliação da ligação psicológica)*

| *Questão* | *Resposta* | | | | | | |
|---|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| *12* | 353 | 7 | 6 | 0 | 0 | 0 | 0 |
| *13* | 148 | 0 | 0 | 61 | 0 | 15 | 142 |

*Tabela 12 – Respostas às questões 12 e 13 (segunda parte do grupo de avaliação da ligação psicológica)*

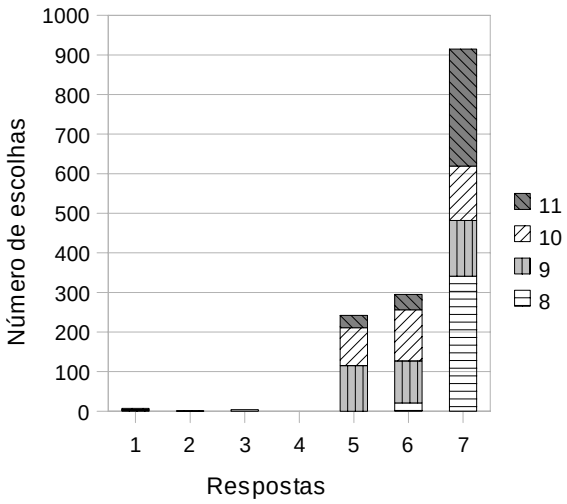



*Figura 81 – Acumulado das respostas às questões 8 a 11 grupo de avaliação da ligação psicológica*

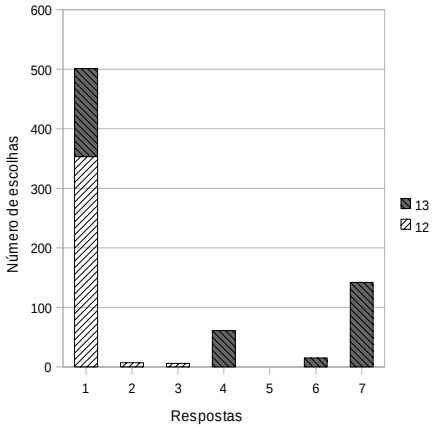



*Figura 82 – Acumulado das respostas às questões 12 e 13 do grupo de avaliação da ligação psicológica*

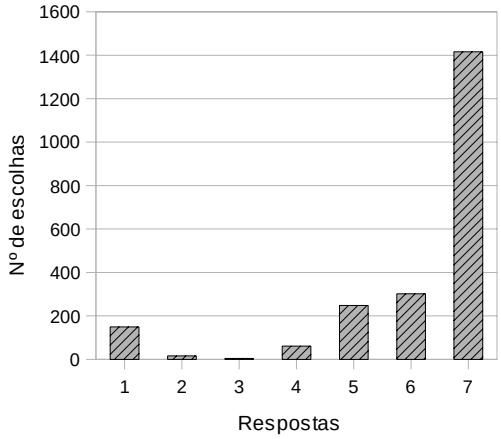



*Figura 83 – Avaliação da ligação psicológica (escala de Likert onde 1 corresponde a uma ligação inexistente e 7 a uma ligação muito forte)*

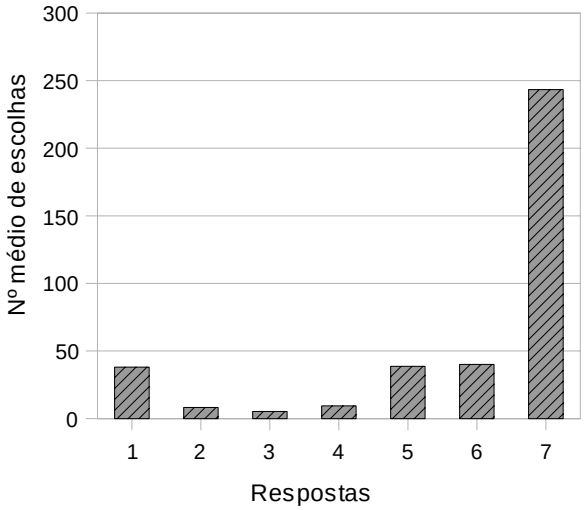



*Figura 84 – Avaliação da tendência de adopção das tecnologias em avaliação*

# Conclusões e propostas de trabalho futuro

## *Conclusões*

Este doutoramento teve como objectivo o estudo da viabilidade da utilização de tecnologias biométricas comportamentais na autenticação do cidadão perante os serviços electrónicos do Estado. Para demonstrar a tese que afirma ser viável essa utilização, era necessário demonstrar a necessidade de reforçar a segurança dos processos de autenticação, demonstrar a existência de algoritmos simultaneamente capazes de responder aos requisitos funcionais dos sistemas electrónicos do Estado e facilmente integráveis com os sistemas existentes, confirmar a sua aceitação pelo público e, por último, aferir da sua legalidade, à luz da legislação actual.

A revisão de literatura mostrou que o uso das biometrias por entidades governamentais é vasto e abrange diversas áreas de actuação. No entanto, a utilização das tecnologias biométricas nos processos de autenticação em sistemas operados pelos governos tem sido meramente pontual e sempre revestida de muitas precauções. Por outro lado, a revisão de literatura também mostrou que algumas das tecnologias têm evoluído consideravelmente e, embora existam discrepâncias preocupantes nos resultados dos testes de avaliação de desempenho (mesmo nos maiores e mais reputados) o nível de maturidade da autenticação biométrica é já considerável, pelo menos no que respeita à avaliação de algumas características, como a íris e a face. Ainda assim, as biometrias físicas exigem o recurso a *hardware* que, sendo mais ou menos comum, nem sempre está disponível nos equipamentos utilizados para acesso aos serviços electrónicos do Estado o que inviabiliza a sua utilização neste contexto.

Seguindo as recomendações do BEM, foi efectuada uma revisão da legislação existente, incluindo os direitos garantidos, de facto ou em potência,

pelas patentes e pelos pedidos de patente conhecidos, tendo ficado demonstrado que não existe qualquer entrave legal à associação da autenticação gráfica à avaliação dos padrões biométricos comportamentais que lhe estão associados e à associação desta tecnologia com a dinâmica de digitação, desde que sejam salvaguardados os direitos fundamentais do utilizador, em particular o seu direito à informação sobre o uso (o que impede a captação de dados biométricos sem o conhecimento do utilizador) e os objectivos da tecnologia utilizada.

Os casos-de-estudo apresentados demonstraram a existência de ameaças específicas aos sistemas de informação do Estado. Para além das ameaças comuns à generalidade dos sistemas de informação, os Estados apresentam-se como alvos potenciais de várias entidades.

O caso dos ciberataques à Estónia e à Geórgia mostraram que os ataques aos sistemas informáticos de um Estado podem ser utilizados por outros Estados ou por grupos nacionalistas de Estados rivais para paralizar os serviços públicos, nos países mais dependentes da tecnologia, ou para, pelo menos, impedir o recurso à Internet para divulgação de informações à comunidade internacional. Trata-se de um misto entre o conceito maoista de “Guerra do Povo” e a estratégia trotskista de combate. No primeiro, elementos da população envolvem-se em operações militares isoladas sob o consentimento e a aprovação tácita do Estado que, oficialmente, não se envolve no conflito. No segundo, grupos especializados atacam apenas os pontos críticos da região alvo (centrais eléctricas, postos de comunicações, etc.) contando com as massas para suportar a acção militar, *a posteriori*, não para a realizar. A actual versão desta estratégia inclui paralizar os sites fundamentais de um Estado, incluindo aqueles que se destinam à difusão de informação de carácter público. O Estado português tem investido na modernização da administração pública, nomeadamente no que respeita ao aproveitamento dos recursos disponibilizados pela Internet, o que torna os seus sistemas de informação um alvo especialmente apetecível para este tipo de acções. Os casos descritos teriam

consequências muito mais gravosas se tivessem tirado proveito das vulnerabilidades existentes nos processos de autenticação e, portanto, urge reforçar a sua segurança.

O estudo do uso das tecnologias de informação e de comunicação pelas organizações terroristas demonstrou a existência de grupos tecnologicamente evoluídos e com conhecimentos relevantes no domínio da informática. Para além disso, demonstrou que os grupos extremistas têm consciência da potencialidade dos sistemas de informação enquanto meio de divulgação de ideais, enquanto local de recrutamento, fonte de informação e até como suporte para o treino de actividades terroristas e mesmo para a sua execução. No entanto, não foram ainda desencadeados ataques terroristas reais[4] através da Internet, provavelmente porque, a avaliar pela documentação colocada na Internet, o grande objectivo das organizações terroristas activas é a aniquilação física dos seus inimigos. Os ataques a sistemas de informação causam danos económicos, mas só muito dificilmente causarão a morte de um elevado número de pessoas. Ainda assim, os grupos terroristas têm mostrado uma elevada capacidade de recrutamento de indivíduos altamente qualificados e, se a opção vier a ser pelo recurso a ataques a sistemas de informação com o objectivo de provocar a morte de um elevado número de pessoas, é provável que a escolha recaia no aproveitamento de uma vulnerabilidade na autenticação, uma vez que essa é uma das formas mais fáceis de dispor dos privilégios necessários para alcançar esses objectivos. O Estado português, fruto das suas alianças internacionais é um alvo potencial para estas organizações, como ficou demonstrado.

Os casos estudados mostraram também que muitos dos ataques aos serviços electrónicos dos Estados estão relacionados com a espionagem, nomeadamente a espionagem industrial com envolvimento estatal. Os estudos apresentados demonstraram que a redução das tensões militares no período pós Guerra Fria, permitiu o redirecionamento de meios, antes destinados aos

4 No Second Life aconteceram alguns ataques virtuais a instalações emblemáticas ocidentais que destruíram instalações por alguns dias, até à sua reposição com recurso às cópias de segurança.

serviços de informações militares, para a obtenção de informações que permitam obter uma posição favorável em diversas relações comerciais. Mais uma vez, a quantidade de informação confidencial que é potencialmente exposta, se os processos de autenticação dos serviços electrónicos do Estado forem vulneráveis, é suficiente para justificar o investimento no aumento da sua segurança.

O último caso-de-estudo apresentado refere-se ao crescente investimento da República Popular da China na potencialidade da Internet para a obtenção de uma vantagem significativa em caso de confronto militar assimétrico. Os estrategas chineses foram dos primeiros a reconhecer a potencialidade da Internet como meio para obter uma vantagem sobre Estados militarmente mais fortes e, enquanto aumentava significativamente o seu investimento em meios militares de combate, a República Popular da China preparava também unidades especializadas no combate no ciberespaço. Por outro lado, os estrategas chineses reconhecem também a potencialidade da "Guerra do Povo" em caso de conflito digital. As acções recentes demonstram que este país encara já a Internet como um espaço privilegiado para obtenção de vantagens comerciais e políticas e a existência de um número elevado de emigrantes chineses e de sino-descendentes nos países ocidentais (alguns em posições que requerem níveis de segurança consideráveis) com ligações culturais e afectivas ao *Império do Meio* deverá aumentar as preocupações dos Estados ocidentais com a transmissibilidade das credenciais de autenticação. Estas preocupações são ainda mais pertinentes se atendermos ao facto de que a espionagem recorre frequentemente ao suborno para obtenção de informações, nomeadamente credenciais de acesso. É, portanto, urgente que os sistemas electrónicos fornecidos pelos Estados aos seus cidadãos e aos seus funcionários passem a dispor de processos de autenticação disponíveis universalmente e que recorram a credenciais não transmissíveis, como é o caso das tecnologias biométricas comportamentais.

A existência de algoritmos biométricos adequados a plataformas diferentes (o *keystroke dynamics* em espaços públicos, com monitores vulneráveis à visualização, acidental ou não, dos segredos de autenticação; o *pointer dynamics* em espaços privados e/ou em equipamentos portáteis que assegurem alguma privacidade) ficou demonstrada pela sua apresentação (prova de conceito) e pela avaliação da sua precisão que, ainda assim, carece de algum trabalho futuro. Os parâmetros avaliados foram, de acordo com as recomendações do BEM, as taxas de falsa aceitação, de falsa rejeição e de intersecção de erros. Embora o BEM considere que uma tecnologia só é adequada para uso na autenticação se apresentar taxas de erro inferiores a 1%, essa indicação refere-se ao seu uso enquanto único elemento de autenticação. Uma vez que os algoritmos apresentados são indissociáveis dos respectivos segredos de autenticação, as taxas efectivas de erro, para comparação com os valores propostos pelo BEM, seriam a taxa de erro a multiplicar pela probabilidade (ínfima) de adivinhar o código secreto, o que coloca estas tecnologias num patamar de segurança considerável.

Os algoritmos apresentados demonstram que é possível integrar estas tecnologias com os sistemas existentes o que, embora não seja uma solução ao nível do desenho de raíz, permite poupanças significativas. A nova tecnologia apresentada, o *pointer dynamics*, além de possuir uma componente biométrica, o que naturalmente dificulta a transmissão do segredo de autenticação, recorre a sequências gráficas, o que aumenta o espaço de chaves, além de colocar mais um entrave à partilha do código secreto. Esta tecnologia permite ainda a substituição periódica das palavras chave alfanuméricas sem que o utilizador tenha que memorizar uma nova sequência de autenticação, o que garante que a obtenção, por intercepção de comunicações, do segredo de autenticação tem uma duração limitada, impedindo que a conta de um utilizador seja utilizada/monitorizada por terceiros sem o seu conhecimento durante longos períodos.

Para aferir do nível de aceitação das biometrias comportamentais foi elaborado um estudo por sondagem (foram inquiridas telefonicamente 600 pessoas, escolhidas aleatoriamente), seguindo o Technology Adoption Model. O estudo demonstrou que a população está receptiva à utilização de biometrias que avaliam a forma como os segredos de autenticação são introduzidos, nomeadamente para proceder à autenticação nos serviços electrónicos do Estado.

Da globalidade dos resultados obtidos resulta a confirmação de que é viável e desejável a implementação de processos de autenticação baseados em biometrias comportamentais nos serviços electrónicos do Estado.

### *Propostas de trabalho futuro*

O trabalho futuro no campo dos processos de autenticação nos serviços electrónicos do Estado estará sempre associado a três vertentes fundamentais: a política, a social e a tecnológica. Estes factores definem a necessidade de investimento nestas tecnologias, com como a sua usabilidade.

Na vertente política o foco do trabalho futuro deverá estar no acompanhamento e compreensão da evolução da estratégia e da capacidade tecnológica das organizações emergentes, estatais ou outras, em particular daquelas já estudadas neste doutoramento: a Federação Russa e seus aliados, a República Popular da China, as máfias, os grupos de extrema-direita e de extrema-esquerda e as organizações terroristas. A avaliar pelas acções recentes, será necessário continuar o estudo dos ciberconflitos que continuarão a surgir e das acções de espionagem e sabotagem que venham a ser detectadas. Estes estudos deverão permitir, a cada momento, a compreensão do nível de interesse que os serviços electrónicos do Estado têm para as organizações referidas e da capacidade dos sistemas existentes para resistir a um eventual ataque.

A investigação na vertente social está relacionada essencialmente com a compreensão da visão das massas populacionais no que respeita à necessidade

de aumento da segurança dos processos de autenticação *versus* a necessidade da protecção dos dados pessoais. Será especialmente pertinente acompanhar a evolução do enquadramento que o cidadão dá aos seus padrões biométricos comportamentais, isto é, procurar perceber se o cidadão comum tende a encarar os seus padrões biométricos comportamentais como um dado privado ou como um dado público.

A investigação tecnológica na área das biometrias comportamentais cresceu nos últimos anos, sobretudo devido ao potencial de qualquer processo de autenticação em larga escala que não requeira *hardware* dedicado. Esta característica, mais do que uma vantagem, é um requisito no contexto de um serviço prestado, através da Internet, ao maior conjunto possível de destinatários. Considerando a usabilidade das tecnologias já existentes, o trabalho futuro, no que respeita ao desenvolvimento tecnológico, deverá estar focado essencialmente em três aspectos essenciais: a precisão dos algoritmos de autenticação, a evolução da autenticação para a identificação e a protecção dos dados privados na utilização destas tecnologias em espaços públicos.

A tecnologia *pointer dynamics* ainda está numa fase embrionária e é necessário prosseguir os estudos com vista à obtenção de algoritmos com um nível de precisão mais satisfatório. Entretanto, com as constantes evoluções das teorias matemáticas que suportam a investigação dos algoritmos de autenticação biométrica, será necessário prosseguir os estudos que conduzam ao aumento da precisão dos algoritmos de *Keystroke Dynamics*. Simultaneamente, novas abordagens na utilização destas tecnologias poderão permitir a transição dos processos de autenticação para os processos de identificação, o que poderá ter como consequência colateral um aumento dos níveis de aceitação pelos utilizadores, já que são dispensados da tarefa de indicar a sua identidade para confirmação pelo sistema.

De forma a superar a dificuldade de utilização do *pointer dynamics* em equipamentos de maior dimensão nos espaços públicos, é necessário prosseguir com a investigação de formas alternativas de introdução dos segredos de

autenticação. Por um lado porque os avanços da robótica poderão a médio prazo permitir o controlo de dispositivos apontadores apenas com o olhar, permitindo o acesso a estas tecnologias a cidadãos com restrições de mobilidade e, simultaneamente, dificultando a obtenção do segredo de autenticação por observação da sua introdução (Hoanca & Mock, 2006); por outro lado, porque a evolução dos sistemas operativos e do *hardware* poderá criar novas formas de interacção homem-máquina, que dispensem o uso de dispositivos apontadores. Estes avanços implicarão sempre momentâneas reduções na precisão dos processos de autenticação, o que implica novos estudos para aperfeiçoamento dos algoritmos.

# Referências

Abdul-Aziz (1996). The Moujahideen Explosives Handbook, *Encyclopedia Jihad*, Organization for the Preparation of Moujahideen. Retrieved Julho, 2008, from http://volnyj-strelok.narod.ru/Moujahideen_explosive_book.pdf

Acharya, L. (2006). Biometrics and Government. In S. a. T. Division (Ed.): Library of Parliament.

Ajzen, I., & Fishbein, M. (1975). *elief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Alrafidha, G. (2006), Le rôle des sœurs dans le JIHAD. Sciences islamiques et jurispridence. Retrieved Janeiro de 2008 from http://www.minbar-sos.com/forum/sciences-islamiques-et-jurispridence/1359-le-role-des-soeurs-dans-le-jihad.html

Al-Salem, M. B. A. (2003). 39 wasila Li-Kidmat Al-Jihad Wa-Al-Musharaka Fihi: Al-faroq.

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is Coming! In J. Arquilla & D. Ronfeldt (Eds.), *Athena's Camps: Preparing for Conflit in the Information Age* (pp. 23-60). Santa Monica, California: RAND Corporation.

Assembleia da República. (1998). Lei da Protecção de Dados Pessoais (247 ed.): Diário da República, Série I-A.

Bank of America (2005). SiteKey at Bank of America. Retrieved in 2005 From http://www.bankofamerica.com/privacy/sitekey/

Ben-Abdelkader, C., R.Cutler, Nanda, H., & Davis, L. (2001). Eigengait: motion-based recognition of people using image self-similarity. *Audio- and Video-Based Biometric Person Authentication.* Halmstad, Sweden.

Bender, S. S. & Postley, H. J. (2007). U.S. Patent No. 7206938B2. Washington, DC: U.S. Patent and Trademark Office.

Bergadano, F., Gunetti, D., & Picardi, C. (2002). User Authentication through Keystroke Dynamics. ACM Transactions on Information and System Security. V. 5 (4). pp. 367–397.

Bezerra, E. K., Nakamura, E. T., Lima, M. B., & Ribeiro, S. L. (2004). O Espaço Cibernético e Seu Emprego Como Agente de Instabilidade de Uma Nação: Uma Visão Sobre Guerra Cibernética, *I Conferência Internacional de Perícias em Crimes Cibernéticos*. Brasília: Departamento de Polícia Federal.

Biometric Watch. (2006). from http://www.biometricwatch.com/news.htm – 05-09-2006

Blakely, R. Richards, J. Rossiter, & Beeston, R. (2007). "MI5 alert on China's cyberspace spy threat". The Times.

Bleha, S. A., Knopp, J., & Obaidat, M. S. (1992). Performance of the perceptron algorithm for the classification of computer users. In Proceedings of the 1992 ACM/SIGAPP Symposium on Applied Computing: Technological Challenges of the 1990's (Kansas City, Missouri, United States). H. Berghel, G. Hedrick, E. Deaton, D. Roach, and R. Wainwright, Eds. SAC '92. ACM, New York, NY, pp. 863-866.

Bleha, S., Slivinsky, C., & Hussien, B. (1990). Computer-Access Security Systems Using Keystroke Dynamics. IEEE Transactions on Pattern Analysis and Machine Intelligence. V. 12 (12). pp. 1217-1222.

Blonder, G.E. (1996). U.S. Patent No. 5559961. Washington, DC: U.S. Patent and Trademark Office.

Boroditsky, M. D., & Manza, M. B. (2001). U.S. Patent No. 6327659B2. Washington, DC: U.S. Patent and Trademark Office.

Boroditsky, M. D., & Manza, M. B. (2001). U.S. Patent No. 6332192B1. Washington, DC: U.S. Patent and Trademark Office.

Boyd, J. E., & Little, J. J. (2005). Biometric Gait Recognition. *Biometrics School 2003*. LNCS 3161. pp. 19-42.

Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2007). Image understanding for iris biometrics: A survey, *Department of Computer Science and Engineering*, U of Notre Dame, Tech. Rep.

Brooke, J. (1996). Usability Evaluation in Industry: Taylor & Francis

Brostoff, S., & Sasse, M. A. (2000) Are Passfaces more usable than passwords: A field trial investigation. *HCI 2000*. Springer.

"Bruxelas garante que ameaça de ataques terroristas na UE é 'elevada'" (2007, 5 de Setembro). Público.

Buckley, C. (2007, 12 de Setembro). "China says suffers 'massive' Internet spy damage". Reuters.

Campbell, D. (2001). O mundo sob escuta: as capacidades de intercepção no século XXI. Frenesi: Lisboa.

Cappelli, R., Ferrara, M., Franco, A., & Maltoni, D. (2007). Fingerprint verification competition 2006, *Biometric Technology TodayVolume,* Vol 15, 7-8, 7-9.

Central Intelligence Agency. (10 June 2008). *The World Fact Book*. Retrieved Junho, 2008, from https://www.cia.gov/library/publications/the-world-factbook/geos/en.html

Central Intelligence Agency. (10 June 2008). *The World Fact Book*. Retrieved Junho, 2008, from https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html

Cho, S., & Han, D. (2000). U.S. Patent No. 6151593. Washington, DC: U.S. Patent and Trademark Office.

Clarke, N.L., Furnell, S.M., Lines, B.L., & Reynolds, P.L. (2002). Biometric Authentication for Mobile Devices. *Proceedings of the 3rd Australian Information Warfare and Security Conference.* Perth, Western Australia. pp. 61-69.

Clarke, N.L., Furnell, S.M., Lines, B.L., & Reynolds, P.L. (2003). Using Keystroke Analysis as a mechanism for Subscriber Authentication on Mobile Handsets. *Proceedings of the IFIP SEC 2003 Conference.* Athens, Greece. Pp 97-108.

Clarke, N.L., Furnell, S.M., Lines, B.L., & Reynolds, P.L. (2004). Application of Keystroke Analysis to Mobile Text Messaging. *Proceedings of the 3rd Security Conference*, Las Vegas, USA.

Coll S., & Glasser, S. B. (2005, 7 de Agosto de 2005). Terrorists Turn to the Web as Base of Operations. Washington *Post*.

Comissão Nacional de Protecção de Dados (2004). *Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e assiduidade*, 2004, from http://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-BIOM-assiduidade-acesso.pdf

Comissão Temporária sobre o Sistema de Intercepção ECHELON (2001). Relatório sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção ECHELON) (2001/2098 (INI)). Parlamento Europeu. From http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//PT

Common Criteria Biometric Evaluation Methodology Working Group. (2002). Biometric Evaluation Methodology Supplement [BEM].

Common Criteria for Information Technology Security Evaluation (2006), Versão 3.1, Setembro 2006, Retrieved Janeiro 2007 from http://www.commoncriteriaportal.org/thecc.html

Commonwealth Observer Group (2006). Zambia Presidential, National Assembly and Local Government Elections - Report of the Commonwealth Observer Group. In C. Secretariat (Ed.).

Conselho de Ministros. (2003). Plano de Acção para o Governo Electrónico (185 ed.): Diário da República, Série I-B.

Cyberwarfare worries. (2007, 1 de Junho de 2007). *Washington Times*.

Davis, B. L. , Gandhi, S. B., Jaiswal, P., Lewis, J. R., & Wang, F. (2006). U.S. Patent Application Publication No. 20060095789. Washington, DC: U.S. Patent and Trademark Office.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science.* 35. pp. 982-1003.

De Angeli, A., Coventry, L., Johnson, G. I., & Coutts, M. (2003). Usability and user authentication: Pictorial passwords vs. PIN. In P.T.McCabe (Ed.), *Contemporary Ergonomics 2003* (pp. pp. 253-258). London: Taylor & Francis.

Department of Defense (2002). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2002.

Department of Defense (2003). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2003.

Department of Defense (2004). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2004

Department of Defense (2004). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2005

Department of Defense (2004). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2006

Department of Defense (2004). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2007

Department of Defense (2008). Annual Report to Congress – Military Power of the People's Republic of China 2008. Washington: DoD. 2008. .

Dhamija, R., & Perrig, A. (2000). Déjà vu: A user study using images for authentication, *9th USENIX Security Symposium*.

Dimauro, G., Impedovo, S., Lucchese, M.G., Modugno, R., & Pirlo, G. (2004) Recent advancements in automatic signature verification, *Frontiers in Handwriting Recognition, 2004. IWFHR-9 2004. Ninth International Workshop on* , pp. 179-184.

DSCINT. (2005). *Cyber Operations and Cyber Terrorism, DCSINT,* (Vol. 1). Fort Leavenworth, Kansas: DCSINT.

Elledge, D. D. (2001). U.S. Patent No. 6192578B1 . Washington, DC: U.S. Patent and Trademark Office.

Embaixada da República de Angola em Portugal (2008), Retrieved Junho, 2008 from http://www.embaixadadeangola.org/geografia.htm, 2008

"Estonia fines man for 'cyber war'" (2008, 25 de Janeiro de 2008). *BBC News*.

"Estonia hit by 'Moscow cyber war'" (2007, 17 de Maio de 2007). *BBC News*.

"Estonian hold suspect over 'cyber-attacks'" (2007, 6 de Maio de 2007). The Sidney Morning Herald.

*Estonian Information Society Strategy 2013*. (2006). 2007, from www.riso.ee/en/files/IYA_ENGLISH_v1.pdf

Fette, B. A., Broun, C. C., Campbell, W. M., & Jaskie, C. (2000). *2000 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2000. ICASSP '00.*

Flom, L., & Safir, A (1987). U.S. Patent No. 4641349. Washington, DC: U.S. Patent and Trademark Office.

Gaines, R. S., Lisowski, W., Press, S. J., & Shapiro, N. (1980). Authentication by Keystroke Timing: Some Preliminary Results (pp. 48): Rand Corporation.

Geer, D. (2005). Security Technologies Go Phishing. *IEEE Computer*. 38 (6). pp. 18-21

"Georgia accuses Russia of waging cyberwar" (2008, 12 de Agosto de 2008). CBC News.

Gourlay, C., & Taher, A. (2007, 5 de Agosto). "Virtual jihad hits Second Life website". The Sunday Times.

*Grande Enciclopédia Universal* (2004). Vol. 8: DURCLUB SA.

Grunwald, L. (2006). Security by Politics - Why it will never work, *DEFCON*. Las Vegas.

Halevi, J. D. (2003). The 39 Principles of Jihad. Center for Special Studies, Intelligence and Terrorism Information Center, Setembro de 2003, Retrieved Maio de 2006 from http://www.intelligence.org.il/eng/var/39p_e.htm

Haris, S. (2008, 31 de Maio). "China's Cyber-Militia". National Journal Magazine.

Hoanca, B., & Mock, K. (2006). Secure graphical password system for high traffic public areas, *Eye Tracking Research & Applications Symposium 2006*. San Diego: ACM SIGGRAPH.

Hoover, D. (2001). U.S. Patent No. 6209102B1. Washington, DC: U.S. Patent and Trademark Office.

IBG, I. B. G. (2003). *The Biometric Industry: One Year After 9/11*. Retrieved Novembro, 2004

"Is China attacking Belgian computers?" (2008, 3 de Maio). United Press International.

Jackson, P. (2007, 17 de Maio). The cyber raiders hitting Estonia*. BBC News*.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric Identification. *Comunications of the ACM, 43*(2).

Jermyn, I., Mayer, A., Monrose, F., Reiterand, M., & Rubin, A. (1999). The design and analysis of graphical passwords, *8th USENIX Security Symposium*.

Jincheng, W. (1997) “Information War: A New Form Of People's War.” In Michael Pillsbury (eds) (1997) Chinese Views Of Future Warfare. National Defense University Press, Washington, pp 409 - 412

Johnson, B. (2006, 7 de Agosto). Hackers crack new biometric passports*. The Guardian*.

Joyce, R., & Gupta, G. (1990). Identity authorization based on keystroke latencies. *Communications of the ACM, 33*(2), 168-176.

Kelman, H. C. (1958). Compliance, Identification, and Internalization: Three Processes of Attitude Change? *Journal of Conflict Resolution, 2*, 51-60.

Kelman, H. C. (1961). Processes of Opinion Change. *Public Opinion Quarterly, 2*, 51-60.

Kermani, B. G. (2005). U.S. Patent No. 6895514B1. Washington, DC: U.S. Patent and Trademark Office.

Kirovski, D., Jojic, N., & Roberts, P. (2007). U.S. Patent No. 7243239B2. Washington, DC: U.S. Patent and Trademark Office.

Kyodo News. (2005, 26 de Agosto). Inmates to be monitored with biometric info at new Yamaguchi prison*. Kyodo News*.

Laczko, F. (2003). Europe Attracts More Migrants from China. Migration Policy Institute. Retrieved January, 2008 from http://www.migrationinformation.org/Feature/print.cfm?ID=144

Levin, D. (2000). Race as a visual feature: using visual search and perceptual discrimination tasks to understand face categories and the cross race recognition deficit. *Quarterly Journal of Experimental Psychology: General.* 129 (4). pp. 559-574.

Liang, Q., & Xiangsui, X. (1999). Unrestricted Warfare. Pequim: PLA Literature and Arts Publishing House, 1999.

Liu, S.. & Silverman, M. (2001). A Practical Guide to Biometric Security Technology, *IEEE Computer Society*.

Magalhães, P. S., & Santos, H. D. (2003). Biometria e Autenticação, *4ª Conferência da Associação Portuguesa de Sistemas de Informação*. Porto. Portugal.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2001). *FVC2000: Fingerprint Verification Competition*. Retrieved Junho de 2004, from http://bias.csr.unibo.it/fvc2000

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., & Jain, A. K. (2002). FVC2002: Second Fingerprint Verification Competition, *International Conference on Pattern Recognition – ICPR2002*. Quebec, Canada: IEEE.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2004). FVC2004: Third Fingerprint Verification Competition, *International Conference on Biometric Authentication – ICBA*. Hong Kong.

Malhotra, Y., & Galletta, D. F. (1999). Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation, *32nd Hawaii International Conference on System Sciences*. Maui: IEEE.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of fingerprint recognition*. New York: Springer.

Mandraud, I. (2007, 9 de Setembro). “La France, cible de hackers chinois Après les Etats-Unis, l'Allemagne et le Royaume-Uni, la France victime d'intrusions”. Le Monde.

Mäntylä, J. (2008). U.S. Patent No. 7376899B2. Washington, DC: U.S. Patent and Trademark Office.

Mattis, J. (2008). Video of the Memorandum of Understanding signing ceremony on the NATO-accredited Cooperative Cyber Defence Centre of Excellence, in Estonia. Retrieved Junho de 2008, from http://www.nato.int/docu/comm/2008/0805-chod/0805-chod.htm

McAfee (2007). Virtual Criminology Report 2007: Cybercrime The Next Wave Retrieved Julho, 2008, from http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

Meissner, C., & Brigham, J. (2001). Thirty years of investigationthe own-race advantage in memory for faces: A meta-analytic review. *Psychology, Public Policy & Law.* 7. pp. 3-35.

Melander, I. (2007, 10 de Setembro). "Web search for bomb recipes should be blocked: EU". Reuters.

"Merkel's China Visit Marred by Hacking Allegations" (2007, 27 de Agosto). Spiegel.

Monrose, F., Reiter, M. K., & Wetzel, S. (2001). Password Hardening based on Keystroke Dynamics. *International Journal of Information Security, 1*(2), 69-83.

Monrose, F., & Rubin, A. D. (1997). Authentication via Keystroke Dynamics, *Fourth ACM Conference on Computer and Communication Security*. Zurich, Switzerland: ACM.

Monrose, F., & Rubin, A. D. (2000). Keystroke Dynamics as a Biometric for Authentication. *Future Generation Computing Systems, 16*, 351-359.

Mostayed, A., Kim, S., Mynuddin, M., Mazumder, G., & Park, S. J. (2008). Foot Step Based Person Identification Using Histogram Similarity and Wavelet Decomposition, *2008 International Conference on Information Security and Assurance.* pp. 307-311.

NATO, North Atlantic Treaty Organization (2008), from http://www.nato.int/issues/cyber_defence

Nickerson, R. S. (1965). Short-term memory for complex meaningful visual configurations: A demonstration of capacity. *Canadian Journal of Psychology, 19*, 155-160.

Nelson, B., Choi, R., Lacobucci, M., Mitchell, M, & Gagnon, G. (1999). Cyberterror – Prospects and Implications, Monterey, CA: Center for the Study of Terrorism and Irregular Warfare.

Obaidat, M. S. (1995). A verification methodology for computer systems users. In Proceedings of the 1995 ACM Symposium on Applied Computing. K. M. George, J. Carroll, and D. Oppenheim, Eds. SAC '95. ACM, New York. pp. 258-262.

Obaidat, M. S., & Sadoun, B. (1997). Verification of Computer Users Using Keystroke Dynamics. IEEE Transactions on systems, Man, and Cybernetics – Part B: Cybernetics, V. 27 (2). pp. 261-269.

Odom, G. (2008). U.S. Patent No. 7350078. Washington, DC: U.S. Patent and Trademark Office.

Office of Technology Assessment (1981). *Computer-Based National Information Systems: Technology and Public Policy Issues*. U. S. Government Printing Office: Washington, D.C.

O'Reilly, C., Chatman, J., & Caldwell, D. F. (1991). People and Organizational Culture: A Profile Comparison Approach to Assessing Person-Organization Fit. *Academy of Management Journal, 34*, 487-516.

Oliveira, F. N. S. C. (2004). Ações Maliciosas Sobre Redes e Sistemas de Informações, *I Conferência Internacional de Perícias em Crimes Cibernéticos*. Brasília: Departamento de Polícia Federal.

Ord, T., & Furnell, S. M. (2000). User authentication for keypad-based devices using keystroke analysis, *Second International Network Conference – INC 2000*. Plymouth, UK.

Orr, R. J., & Abowd, G. D. (2000). The Smart Floor: A Mechanism for Natural User Identification and Tracking*, The CHI 2000 Conference on Human Factors in Computing Systems.* pp. 275-276.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, *7th European Conference on Information Warfare and Security*. Plymouth, UK.

Paet, U. (2007). *Address by Minister of Foreign Affairs of Estonia Urmas Paet*. Retrieved Julho, 2007, from http://www.vm.ee/eng/kat_140/8467.html?arhiiv_kuup=kuup_2007

Park, S. (2007). U.S. Patent No. 7240367B2. Washington, DC: U.S. Patent and Trademark Office.

Parlamento Europeu. (2001). *Resolução do Parlamento Europeu sobre a existência de um sistema global de intercepção de comunicações privadas e comerciais (sistema de intercepção "ECHELON") (2001/2098 (INI))*, 2001, from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2001-0441+0+DOC+XML+V0//PT&language=PT

Parlamento Europeu. (2007). *Acta da sessão de 9 de Maio de 2007 do Parlamento Europeu*, Retrieved 2007, from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070509+ITEM-012+DOC+XML+V0//PT

Pawlak, Z. (1982), *Rough Sets*. *International Journal of Computer and Information Sciences.* 11. pp. 341- 356.

Pawlak, Z. (1991). *Rough Sets – Theoretical aspects of reasoning about data*. Kluwer.

Peacock, A., Ke, X., & Wilkerson, M. (2004). Typing Patterns: A Key to User Identification. *IEEE Security and Privacy*.

Perakslis, C., & Wolk, R. (2006). Social Acceptance of RFID as a Biometric Security Method. *IEEE Technology and Society Magazine, Fall 2006,* 34-42.

Phillips, P. J., Grother, P., Micheals, R. J., Blackburn, D. M., Tabassi, M., & Bone, M. (2003). *Face Recognition Vendor Test 2002: Evaluation Report*. Retrieved Abril, 2003, from www.frvt.org

Phillips, P. J., Scruggs, W. T., O'Toole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L., & Sharpe, M. (2007). FRVT 2006 and ICE 2006 Large-Scale Results. Retrieved from http://www.frvt.org/FRVT2006/Results.aspx in Setembro de 2007.

Poh, N., & Korczak, J. (2001). Hybrid Biometric Person Authentication Using Face and Voice Features, *Third International Conference, Audio- and Video-based Biometric Person Authentication AVBPA 2001*. Halmstad, Sweden.

Poston, D. L., Mao, M. X., & Yu, M.Y. (1994). The global distribution of the overseas Chinese around 1990. Population and Development Review, Vol. 20, 1994. pp 631-645.

Privacy International, Statewatch, & European Digital Rights. (2004). *An Open Letter to the ICAO A second report on 'Towards an International Infrastructure for Surveillance of Movement'*. Retrieved January, 2005, from www.privacyinternational.org

Privacy International, Statewatch, & European Digital Rigts. (2004). *An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents*. Retrieved January, 2005, from www.privacyinternational.org

Pufeng, W. (1995). China Military Science. Pequim: Academy of Military Science. 1995. Retrieved May, 2008 from http://ftp.fas.org/irp/world/china/docs/iw_mg_wang.htm

Real User Corporation. (2001). *The science behind Passfaces. Passfaces™*. Retrieved October 2005, from http://www.idarts.com/

Recce, M. (2003). U.S. Patent No. 0133598A1. Washington, DC: U.S. Patent and Trademark Office.

Revett, K (2007). International Publication Number WO2007128975A2. Geneva: World Intellectual Property Organization.

Revett, K., Gorunescu, F., Gorunescu, M., Ene, M., Tenreiro de Magalhães, S., & Santos, H. (2007). A machine learning approach to keystroke dynamics based user authentication. *International Journal of Electronic Security and Digital Forensics.* V. 1 (1). pp. 55 - 70.

Ross, A. (1999). *A Prototype Hand Geometry-based Verification System*. Retrieved Setembro, 2004, from http://biometrics.cse.msu.edu/RossHand_MS99.pdf

Schmidt, A. (2005, 6 de Outubro). A High Tech Experiment in Exclusion - Haiti's Biometric Elections*. CounterPunch*.

Schreiber, G. G. & Knox, A. R. (2007). U.S. Patent No. 7305559B2. Washington, DC: U.S. Patent and Trademark Office.

Serpa, M. L. (2005). U.S. Patent No. 6954862B2. Washington, DC: U.S. Patent and Trademark Office.

Sevastopulo, D. (2007, 3 de Setembro). “Chinese hacked into Pentagon”. Financial Times.

Shepard, R. N. (1967). Recognition memoryfor words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior, 6*, 156-163.

Shimeall, T., Williams, P., & Dunlevy, C. (2002). Countering cyber war. *Nato review*, 16-18.

Silcock, R. (2001). What is e-Government? *Parliamentary Affairs, 54*, 88-101.

Slezak, D. (2002). Approximate Entropy Reducts. *Fundamenta Informaticae*.

Smith, T. M., & Cheung, E. (2004). European Patent No. 1469372A2. European Patent Office.

Standing, L. (1973). Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology, 25*, 207-222.

Symantec Corp. (2003). Infostealer.Bancos.B. Retrieved Abril, 2007, from http://www.symantec.com/security_response/writeup.jsp?docid=2003-073117-3108-99

Tao, H. (2006). U.S. Patent Application Publication No. 20060174339A1. Washington, DC: U.S. Patent and Trademark Office.

Tari, F., Ozok, A. A., & Holden, S. H. (2006). A Comparison Between of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords., *Symposium on Usable Privacy and Security (SOUPS) 2006*. Pittsburgh, PA, USA.

Tenreiro de Magalhães, S., Revett, K., & Santos, H. D. (2006). Critical aspects In authentication graphic keys, *International Conference on Information Warfare and Security (ICIW2006)*. Maryland Eastern Shore, USA: Academic Conferences, Inc.

Tenreiro de Magalhães, S., Guimarães, C., Santos, H., Revett, K., & Jahankhani, H. (2008). Voice Based Authentication Using the Null Frequencies, *3rd International Conference on Information Warfare and Security*. Omaha, USA.

Tenreiro de Magalhães, S., Revett, K., Santos, H., Santos, L., Oliveira, A., & Ariza, C. (2008a). Using technology to overcome the password's contradiction. In *Handbook of Research on Social and Organizational Liabilities in Information Security*, IGI Global: USA.

Tenreiro de Magalhães, S., Santos, H., & Nunes, P. V. (2006). An International Governmental Mailing System: A Requirement To Prevent Web-enhanced Terrorism, *The 5th European Conference on Information Warfare and Security*. Helsinquia.

Terrazas, A. M., & Devani, B. (2008). Chinese Immigrants in the United States. Migration Policy Institute. Retrieved from http://www.migrationinformation.org/USfocus/print.cfm?ID=685

The Associated Press. (2007, 27 de Maio). First privately run prison opens in Yamaguchi*. The Japan Times*.

The Zimbabwe Election Support Network. (2006). Zambia 2006 Tripartite Elections Report.

Thian, N. (2001). Retrieved February, 2003 From http://hydria.u-strasbg.fr/~norman/BAS/publications.htm. *Biometric Authentication System.* Unpublished Tese de Mestrado, USM, Penang, Malásia.

Thornburgh, N. (2005, 29 de Agosto). "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)". Time Magazine.

U. S. Department of Homeland Security: Machine-Readable Passport Requirement, P. R., USA, 22 de Outubro, 2004. (2004). Machine-Readable Passport Requirement, Press Release. In D. o. H. Security (Ed.).

U. S. Department of State. (2004). Extension of Requirement for Biometric Passport Issuance by Visa Waiver Program Countries, Press Statement 2004/886. In D. o. State (Ed.).

U. S. General Accountability Office. (2005). Homeland Security Recommendations to Improve Management of Key Border Security Program Need to Be Implemented. In U. S. G. A. Office (Ed.).

Veldhuis, R., Bazen, A., Kauffman, J., & Hartel, P. (2004) Biometric Verification Based on Grip-pattern Recognition. *IS&T/SPIE 16th Annual Symp. on Electronic Imaging*, January 2004, San Jose, California, USA, pp. 19-22.

Walker, P., & Tanaka, W. (2003). An encoding advantage for own-race versus other-race faces. *Perception*, 23, pp. 1117-1125.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Basic results, *Human-Computer Interaction International (HCII 2005)*. Las Vegas.

Wei, J. (1996). Information War: A New Form of People's War, Pequim: Liberation Army Daily, 1996. Retrieved Junho, 2008 from: http://ftp.fas.org/irp/world/china/docs/iw_wei.htm

Wolf, F. R. (2008). "Wolf Reveals House Computers Compromised by Outside Source". P.R. Press Release. Retrieved 11 de Junho de 2008 from http://wolf.house.gov/index.cfm?sectionid=34&parentid=6&sectiontree=6,34&itemid=1174.

Wu, C. (2006). An Overview of the Research and Development of Information Warfare in China. In Edward Halpin *et al* (eds.) Cyberwar, Netwar and the Revolution in Military Affairs. Palgrave MacMillan, Hampshire, pp 173-195.

Wüest, C. (2005). "Phishing In The Middle Of The Stream" - Today's Threats To Online Banking. *Proceedings of the AVAR* 2005.

Young, J. R., & Hammon, R. W. (1989). U.S. Patent No. 4805222. Washington, DC: U.S. Patent and Trademark Office.

Zamalloa, M., Bordel, G., Rodriguez, L. J., & Penagarikano, M. (2006). Feature Selection Based on Genetic Algorithms for Speaker Recognition, *Speaker and Language Recognition Workshop, IEEE Odyssey 2006*.

Zhen, Y., & Canwei, L. (2002). A New Feature Extraction Based the Reliability of Speech in Speaker Recognition, *6th International Conference on Signal Processing*.

# Anexos

# ANEXO I – Perspectiva histórica da relação entre a Estónia e a Federação Russa

A Estónia é um país báltico membro da União Europeia com fronteiras terrestres com a Rússia e a Letónia e fronteiras marítimas com a Finlândia e a Suécia (Figura 85). Apesar de ter várias centenas de anos de história, a Estónia só alcançou a independência enquanto Estado organizado soberano em 1918, para a perder de novo em 1941. Esteve sob o domínio dinamarquês até 1346, altura em que o território foi vendido à ordem alemã dos Cavaleiros da Espada, colocou-se depois sob a protecção da Suécia em 1561 e em 1721 passou para a tutela da Rússia graças ao Tratado de Nystad. O país viveu diversos levantamentos contra a Rússia durante o século XIX e em 1918 declarou-se independente, situação que durou apenas até 1940, quando foi invadido pela União Soviética. Pouco depois, em 1941, foi invadido pelo exército alemão e após a II Guerra Mundial voltou para o domínio da União Soviética. Só em 1991 a Estónia regressa à independência (*Grande Enciclopédia Universal*, 2004).


**Figura 85 – Localização geográfica da Estónia**

Os quase três séculos de imposição do domínio russo geraram numa parte da população, principalmente nos descendentes de colonos russos, uma sensação de proximidade e ligação, noutros um sentimento de afirmação nacionalista e de ressentimento anti-russo. Esta tensão interna levou a conflitos no inicio de 2007 quando o governo da Estónia decidiu deslocar, de uma praça do centro da capital Tallinn para um cemitério próximo, um memorial aos soldados soviéticos mortos na II Guerra Mundial (Figura 86), bem como alguns restos mortais aí depositados. Este monumento do período soviético é, há vários anos, o centro dos conflitos entre os "estónios" e os "russos da Estónia". O monumento representava um ponto de encontro para todos os que a 9 de Maio celebravam a vitória da União Soviética sobre o nazismo, facto que não agrada a alguns estónios mais radicais que consideram os nazis como libertadores e os russos (associados com a União Soviética) como usurpadores. O monumento russo é visto por muitos como um elemento de provocação desde o dia em que foi colocado pelos soviéticos em Tallinn, ignorando o monumento que ali perto homenageia os soldados da Estónia que combateram ao lado das tropas nazis contra as forças soviéticas. Acresce a esta tensão as disputas por alguns territórios fronteiriços que, estando sob domínio russo, são reclamados pela Estónia com base no acordo de paz de Tartu estabelecido em 1920 (Central Intelligence Agency, 2008).

Figura 86 – A Estátua que gerou a ciberguerra entre a Estónia e a Federação Russa

# ANEXO II – A evolução das formas de combate

O conflito faz parte da História do Homem, seja por questões de sobrevivência, seja pela procura do domínio e da supremacia. Assim, é natural que a evolução da tecnologia tenha alterado a forma de combater e a passagem dos tempos alterou de forma muito significativa o modo como o conflito acontece no campo de batalha, reflectindo as quatro formas fundamentais de confronto: *the melee* (combates homem a homem, sem organização e onde cada um lutava tomando as suas próprias decisões de combate de acordo com os seus interesses estritamente pessoais), *massing* (ataques em massa com formações rígidas), *maneuver* (adopção de manobras e tácticas de combate) e *swarming* (ataque autónomo e disperso, literalmente "enxameado", exigindo um nível organizacional elevado de forma a manter a coerência estratégica) (Arquilla & Ronfeldt, 1997).

A evolução das formas de conflito corresponde também a uma evolução da quantidade de informação de qualidade, disponível no teatro de operações. Nas primeiras formas de confronto a transmissão de informação no teatro de operações era efectuada de forma deficiente através de acenos ou gritos e recebidas através da visão ou da audição. Assim sendo, era praticamente impossível manter o comando e o controlo durante as primeiras batalhas de qualquer um dos quatro palcos de conflitos: a terra, o mar, o ar e o social. Exemplos destes conflitos são, em terra, os combates do antigo império Persa, dos Sumérios e do período após a queda de Roma; no mar, todas as batalhas navais anteriores ao século XVI; no ar, as batalhas da I Guerra Mundial; no campo social, temos o caso de Paris durante a Revolução Francesa (Arquilla & Ronfeldt, 1997)

A evolução dos conhecimentos sobre tácticas de combate permitiu o aumento do comando e controlo de tropas cada vez mais numerosas, utilizando-se formações geométricas com frentes bem definidas, unidades de reserva e

vagas de ataques (fase de *massing*). Paralelamente foram instituídos os treinos militares regulares e foram definidas doutrinas que permitiram o estabelecimento de uma hierarquia bem definida. Também a informação passou a ser transmitida por formas mais evoluídas, com recurso às mensagens escritas e aos códigos de sinais. A transição para a fase de *massing* pode ser reconhecida, por exemplo, em terra na campanha militar de Alexandre o Grande contra o Império Persa; no mar, nas linhas de batalha inglesas e holandesas; no ar, nas formações de bombardeiros da II Guerra Mundial; no nível social, nos motins europeus de 1848 (Arquilla & Ronfeldt, 1997).

A fase seguinte, denominada *maneuver*, literalmente manobra, caracteriza-se pela complexidade e sincronização dos movimentos das tropas, normalmente realizadas de uma forma rápida e num curto espaço de tempo, tendo sido utilizado com sucesso pelos senhores da guerra japoneses, por Alexandre o Grande, por Genghis Khan, por Napoleão e por muitos outros. Exemplos clássicos nos quatro palcos de conflitos são: em terra, as campanhas militares romanas com a disposição e manobra dos seus manípulos (divisões), recorrendo a um tabuleiro de jogo para desenvolver as tácticas e as manobras a utilizar; no mar, a batalha de Trafalgar onde Lord Nelson utilizou uma formação oblíqua entre outras manobras para alcançar a vitória sobre a armada francesa; no ar, a utilização de caças *Stuka* como apoio à *blitzkrieg* (guerra relâmpago) alemã durante a II Guerra Mundial; no nível social, a revolução bolchevique do princípio do século XX (Arquilla & Ronfeldt, 1997).

A forma mais complexa de organização do combate é o *swarming*. Neste modelo existe a necessidade de uma organização complexa e de uma elevada capacidade de processamento da informação. Esta estratégia foi poucas vezes utilizada por exércitos regulares, havendo notícia de muito poucas ocorrências, como são o caso, em terra, dos ataques vietnamitas durante a ofensiva do Tet e, no mar, da acção dos *Unterseeboot* (submarinos conhecidos como *U-Boot ou, pelos aliados, como U-Boat*) contra os comboios marítimos (Arquilla & Ronfeldt, 1997). No entanto, as estruturas não convencionais parecem ter agora

mecanismos para actuar desta forma. Se até à década de 90 do século XX as organizações armadas não associadas a Estados não dispunham de formas eficientes de comunicação e/ou não tinham formação militar que lhes permitissem actuar de forma descentralizada mas organizada e concertada, a massificação das tecnologias de informação e de comunicação garantiu-lhes o acesso aos recursos que lhes faltavam. Aliando o acesso à tecnologia com a formação obtida em países ideologicamente próximos, foi possível a estruturas como a *Al-Qaeda* transitar directamente da forma mais desorganizada de actuação em célula autogerida, para a forma mais complexa: a célula autónoma perfeitamente coordenada com as restantes células do grupo.

A informação mostra-se como uma condicionante da evolução da forma de combate, como se verifica na forma desorganizada como aconteciam os primeiros combates aéreos que, embora em parte justificada pela falta de estudos sobre as melhores formas de organização de combate aéreo, se deve essencialmente à falta de meios de comunicação entre os pilotos, tornando a hierarquia e a organização das forças armadas inútil perante uma situação de alteração das premissas do combate. Por outro lado, o alargamento das frentes de combate a vastas extensões de território, por vezes intercontinentais, não permite o estabelecimento de formas eficientes de comando e controlo sem formas eficientes de comunicação. Os desenvolvimentos tecnológicos, como o rádio foram, por isso, fundamentais para a evolução dos modelos de combate.

A importância da informação e das tecnologias de informação e de comunicação na forma de organização do combate tradicional, no seu comando e controlo e até na forma de actuação das forças de combate não convencionais como as organizações terroristas, criou um novo palco de conflito: o ciberespaço.

O final do século XX foi, por força da revolução dos meios de comunicação provocada pela introdução dos meios digitais, um período de revolução nas formas de combate ideológico, tanto legais como ilegais. As escaramuças tecnológicas representaram uma extensão dos conflitos armados e diplomáticos existentes mas pela sua desorganização ou pela independência de

cada acção tomada, pelo menos aparente, não podem ainda ser encaradas como frentes de combate. Foi assim no conflito entre a Índia e o Paquistão e na questão entre a região da Palestina e o Estado de Israel.

# ANEXO III – Os efeitos do ciberconflito da Estónia nas alianças internacionais

O impacto dos eventos ocorridos na Estónia, a tensão entre a Europa ocidental e a Federação Russa e a incapacidade de criar em tempo útil uma força capaz de neutralizar o ciberataque, levaram a uma discussão sobre a real capacidade dos Estados, em particular dos membros da NATO, para proteger as infra-estruturas tecnológicas que são, cada vez mais, o suporte do modo de vida ocidental. Ainda assim, não é fácil perceber o que realmente mudou a nível internacional após o conflito da Estónia.

A NATO tem desde 2002 um plano para a protecção dos recursos informáticos tendo criado, como consequência da Cimeira de Praga (2002), um organismo denominado NATO *Computer Incident Response Capability* (NCIRC) para assegurar a sua implementação. Até Maio de 2007 este organismo era a única entidade com preocupações de carácter informático e tinha como função essencial proteger a infra-estrutura de comunicação cifrada entre os membros da aliança (NATO, 2008).

Durante os incidentes de Abril e Maio de 2007 gerou-se alguma controvérsia sobre se os incidentes consubstanciavam um ataque que caía no âmbito dos acordos de protecção mútua na NATO. A NATO enviou especialistas para a Estónia mas que, dado o seu desconhecimento dos sistemas, puderam apenas actuar como observadores e, possivelmente, como consultores, embora de forma limitada. O fim dos ataques resolveu, para já, as dúvidas quanto à forma de resposta adequada pelos organismos internacionais, mas forçou a NATO a reconhecer a necessidade de mais do que um organismo de protecção de uma infra-estrutura militar de comunicações.

A NATO reconhece actualmente a necessidade de proteger infraestruturas críticas de carácter civil e o *Cooperative Cyber Defence*, promovido pela Estónia

e que incluía outros países há alguns anos, foi anunciado como um Centro de Excelência NATO, tal como tinha sido proposto por este país em 2003 ainda antes da sua adesão a esta organização. Na assinatura do memorando de entendimento que criou o agora denominado NATO *Cooperative Cyber Defence Centre of Excellence* (NCCDCE), o General James Mattis, chefe do Comando de Forças Combinadas dos EUA e Comandante Supremo da NATO, afirmar: "*Cyberspace must be protected just as we protect Land, Air and Sea*" (o ciberespaço deve ser protegido tal como protegemos Terra, Ar e Mar). Por outro lado, o General Mattis assumiu também que a Estónia previu a necessidade de concentrar as atenções na cibersegurança desde o primeiro ano de participação na aliança e que, passados quatro anos, é a Estónia quem assume a liderança do processo de criação de uma ciberdefesa da coligação (Mattis, 2008), juntando no NCCDCE a Estónia, a Alemanha, a Itália, a Letónia, a Lituânia, a Eslováquia e a Espanha sob a direcção do Tenente Coronel Ilmar Tamm. Mas, na realidade, o CCDCE ainda não é um Centro de Excelência NATO e o memorando sinaliza apenas a vontade conjunta de que tal venha a acontecer, o que está previsto para o final de 2008 ou início de 2009 se o processo decorrer com normalidade e obtiver aprovação na Comissão Militar e no Conselho do Atlântico Norte, como se pode ler no sítio Web do CCDCE já sediado nos servidores na NATO (http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD).

No que respeita à União Europeia, não parece haver alterações provocadas pelo ciberconflito da Estónia. Esta instituição dispõe de um organismo para a segurança da informação denominado ENISA (*European Network and Information Security Agency*), sediado na ilha grega de Creta, desde 2004. Este organismo dispõe de quadros próprios mas assume-se principalmente como um organismo coordenador das agências de segurança da informação dos 25 estados-membros. A União Europeia tem-se mostrado mais célere na colaboração económica e policial do que militar e também no ciberespaço parece ser assim, já que as preocupações da ENISA e da Comissão Europeia têm estado relacionadas com o cibercrime e não com a ciberguerra.

# ANEXO IV – Imagens na versão original (em Russo)

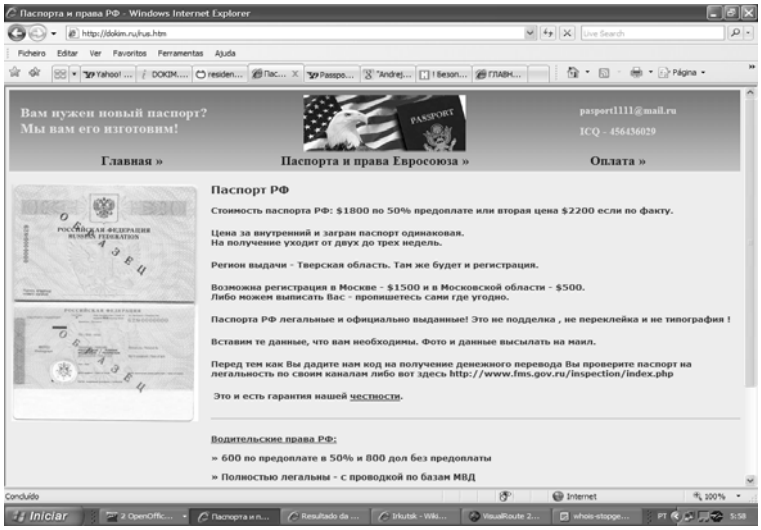



*Figura 87 – Tráfico de passaportes russos (dokim.ru)*


*Figura 88 – Tráfico de passaportes da União Europeia (dokim.ru)*

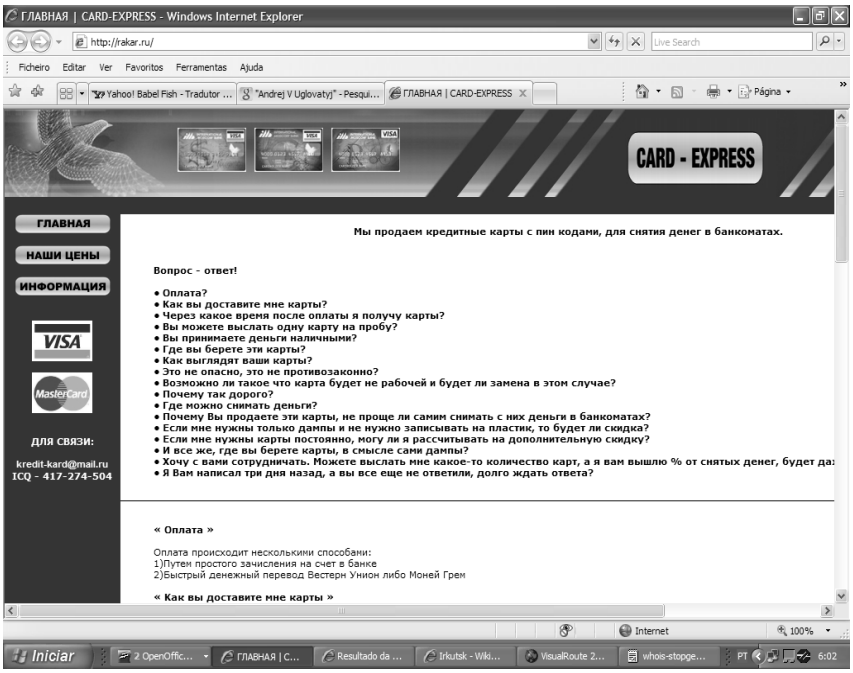



*Figura 89 – Tráfico de cartões de crédito (rakar.ru)*

# Anexo V – Tabelas de conversão de sequências gráficas em sequências alfanuméricas

| 0 | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4kQ | v9; | D't | ~\' | M'p | K"] | .n. | @8v | (!p | LQi | H=p | j.6 | h$m | „;] | q;_ | ]h8 | D-[ | -Yh | `Rj | T^- | evf | y6: | i*f | jJH | ^sI | {{T |
| E6W | xnf | ;}V | Sx8 | e(r | XT0 | ;8u | aWA | x6w | pd/ | #,T | t4j | EwB | ,!^ | ElX | VOU | PjE | br4 | wc\ | ;!I | A:/ | "eb | D,S | 8R1 | 8%| | dQi |
| B`o | }5N | yDv | y$U | ;3t | F`] | [+- | X!g | yvd | HdF | 9XQ | Wcp | 2-u | pEB | }Tj | jZl | mx | f#I | 5Df | &)^ | ?d$ | up6 | 3:@ | u=_ | r< | yjK |
| T~3 | LZM | hF7 | .'V | ]`d | C}{ | -5% | ];3 | qwn | &!n | -vf | sTr | IrV | X3d | aZn | zs4 | HqV | I1U | @v> | AUs | L[a | ?/n | OkA | |S/ | =s/ | j<6 |
| ZU8 | xtx | yT2 | ekN | Evy | V^# | )l2 | 2Fv | <w& | u{= | l6L | ?f0 | \r. | Jew | 6l/ | zL] | `Oc | zJk | Ati | Y&h | xG\ | O]^ | L3E | P#D | 8.d | tfx |
| !Z[ | He$ | 'Ot | HdS | QB( | >,y | ewC | }{d | ayq | %+" | a"} | 0LY | _DE | NjD | 53I | xXV | ry6 | ~,Y | ;l6 | ((e | $,8 | D~2 | ,Mp | lL9 | -zI | Ad~ |
| aC& | @,H | jos | Hg4 | e$Q | (i? | 0f| | k;n | hpS | Dx$ | z0& | ?P3 | W#f | k:B | &k` | v#^ | O/t | 0)q | 48a | 4~! | sv\ | N.! | gZb | ~"J | ?{< | zaL |
| ~t | 0lp | :%S | %$K | bUb | `f- | `9( | 3"" | u<W | HKI | @m= | CTQ | O)H | no; | A-t | {l# | Q\) | rGc | 1TX | |Vy | `<o | I7B | ~Np | "," | 3^$ | gYr |
| P?p | x7U | &^" | FLn | F|. | .\b | 1jo | 4{E | L$4 | _## | 6Bv | h8] | e@J | KFP | cO& | }SN | $kS | fN! | b(! | -%w | i]/ | c7` | #P: | ;an | 2=! | q^4 |
| k2" | v0n | z$S | v4j | W?, | ,yL | $#u | -q) | &O} | wZt | \G| | ]5B | k\a | BK6 | Xhp | m=c | [(Q | Tkd | +!r | !Y^ | IMf | KVf | jjM | rjJ | tF# | +v( |
| -md | eYY | t4Y | ali | .vl! | cT6 | Ml@ | wsk | 8Bo | jES | |9R | #&. | N.k | ;?? | (*V | h*i | 0@^ | ^1" | xB$ | -lv | <.t | Kb/ | V9< | &2m | ;,0 | D#r |
| ZVW | j.W | X~O | /f3 | g@5 | p%h | rAM | kuv | B[9 | xzb | UQR | 4"b | gIN | S6* | @6} | j]6 | UMr | z*H | n.K | O-H | 8el | <>r | 4H2 | t[/ | p;P | ZVw |
| WKA | ,y> | ?"B | XDw | +q, | OQ" | DNL | ]d1 | 9!f | A[7 | /Y' | j8\ | hj1 | CF* | DV: | tot | (>~ | }4H | y%3 | V[o | *s | !5Q | ey& | $o\ | d(% | o(@ |
| ]04 | e5Y | $rB | &q@ | ~~E | ?<! | 3[/ | ZG_ | "MD | 9t[ | {DF | |zU | D`d | 6B~ | Z?| | tjI | 8o+ | RFi | ~W3 | s7F | ?Sj | ]V[ | `RS | .5q | xke | dgQ |
| "M: | OCn | G%k | wyv | R~o | 9kb | 7uM | gCa | ,|, | 2G1 | 'Ew | CFi | Ljz | v+d | #1& | /e$ | oxG | -o2 | U`j | 3k! | <2q | #wE | <ub | Z2T | lg$ | zK' |
| ggz | t4% | \a: | J\2 | {[_ | ky> | |kI | K07 | &6x | :N: | >5V | }eg | >L2 | 2su | Cb^ | M)( | 3?T | Z]* | -^D | gUr | >LI | =C: | rMS | b^~ | >6/ | pte |
| W&H | !bQ | :Ww | dbX | P6U | AkE | `7K | G#% | u6V | TN9 | A:3 | 1Q( | :L5 | Gm- | @HA | 'jc | Zs[ | >N/ | c;? | n,> | 0rW | 5}} | qQ( | B3I | *Bh | #Ti |
| !~z | UxU | veV | H~? | ;b# | S80 | :=? | HXd | ^H~ | y!1 | Tt* | .db | V}7 | Ff! | XYt | P=W | iKO | t-3 | w1| | ubN | Wsk | \Ko | W8x | vbu | +q2 | ]), |
| Ud. | @yL | cc[ | tba | 1wP | sXB | LGk | -'A | sSC | dxU | ~6Z | A6r | 7[m | 1v% | R'M | "7| | ~`k | W&5 | lXl | 62] | tDn | V#R | LLj | pHp | XHm | v=G |
| }C! | a:E | <qM | QG# | w(@ | M&, | [<@ | !QP | yn* | *D~ | s2W | y4@ | 'VJ' | do* | TU" | ,<B | SRA | x9t | K,I | DzC | _6- | S,8 | ~Q] | ),? | N^} | hVY |

*Tabela 13 – Tabela 0 de conversão de sequências gráficas em sequências alfanuméricas*

| E&b | 2E8 | Jz# | P(7 | T]% | 2HI | zRf | Uv+ | zA[ | &/' | o2t | M"I | x)8 | k{P | Zz_ | 9jo | @]1 | ZV | T47 | ^+C | ^UA | 7@8 | Sw} | W]I | ~g- | _L2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SuE | LW8 | V6@ | uo* | X_u | aU? | qto | vv8 | [AE | 0}? | 4+s | ~bY | wD/ | #h# | Q(G | <Hz | @g{ | an| | 1J< | -nX | FS_ | lig | k> | =Jm | [m1 | >+g |
| z/9 | AD$ | k?$ | ~$| | Ru} | #BD | |IX | bm! | !^h | "9| | (YZ | u[# | >D0 | 8hr | GiB | :6b | }ly | PhL | nl> | k;A | Jts | RO" | j2L | "!( | 6;F | F"& |
| z*V | uO9 | )VD | A+U | Qb0 | i?z | *4v | h_l | J=# | E3G | yq@ | *# | %q[ | C*+ | _)C | 3IU | 7p2 | #[7 | eK' | z:E | [;4 | 1)c | ~X2 | v%1 | 7G\ | D") |
| x$S | /TJ | 4*o | 83` | X!9 | 5vR | X}c | .qd | Bwu | jW> | jQH | +97 | J#` | &0. | XSK | P/6 | r;F | `2K | Yau | w3; | le1 | ]<= | 47B | $U> | Op' | `Q< |
| Z}O | PX@ | j_ | de\ | flO | +KM | Kkz | Bmi | an[ | hua | Gg. | "Jp | 34/ | =`t | y&z | OLr | }d: | rKr | GM; | xxh | ."& | F;7 | &:1 | g<I | +"d | |Qc |
| uH. | ,%[ | &mC | {M{ | aO{ | Jlw | fz, | XF} | T.& | O/m | 3(N | +M@ | OVK | mey | S{O | ,*: | zPx | %8= | $BS | *X$ | =:y | o>7 | )#R | 9k" | If, | :c? |
| mk] | 0J^ | 0C/ | [+n | U:S | 8i8 | v;@ | 4Jb | 1F9 | Q#s | .%; | 8Df | =VR | .fM | c/? | tYU | Jd* | Hw: | :s$ | (R? | Uif | |m) | t:[ | ]?n | $VM | ^5c |
| Z@i | ).1 | H(K | h6R | I;b | B,d | mhl | j4@ | d5, | n,O | 2)S | _|( | i2f | (5v | Iok | ZdO | Vp+ | Fgb | A&g | q2j | #`F | ?O. | )wY | eV, | Zul | d0L |
| 9Af | |%I | k1_ | B5F | ~]~ | :OX | ]V? | O!x | @xe | Y4} | ZvK | Be_ | 40f | ,R_ | 8AJ | K?L | &:~ | BH@ | PnE | <mF | V]n | ,b< | ,>R | Twc | z9q | [{5 |
| <|+ | T,= | TCl | YE? | _~G | ~gv | V4B | >59 | CUz | &-G | |0o | nv] | N:I | Sj' | T>q | _%| | 9_{ | Z^[ | /;a | >ot | Iz~ | 5lb | 6\6 | KHm | V@| | d^o |
| f$U | \ZO | *BF | ([h | >sI | 8A] | ?2\ | ;0C | <N, | 6+; | T*| | !}U | Dt7 | h2l | llt | kp~ | d@c | Q]C | tT1 | P(@ | %/] | (qv | 9RE | TX" | INO | |zV |
| z!< | ]7B | <t[ | n}d | 8*= | )vD | )9k | esF | 1], | &%+ | iBN | PF4 | |>' | /d8 | J%S | sb' | +C; | c-g | vM5 | 0|* | h/a | p<& | 1x7 | "|; | 02w | E0a |
| `>T | `]o | +|Z | 6(i | +%u | +9@ | HnX | 1D} | _0k | u+y | ])T | =Tx | jjc | 1d6 | ?uf | I[O | hy+ | Zzg | >e- | =K| | \6] | tK> | `]q | Zbe | \<c | 'Ez |
| UHY | KL7 | oZF | ]Rc | HUX | I2c | rdu | tI9 | e6e | k%5 | c<Y | ')? | *tl | x+w | 7:{ | EL2 | `?j | S/J | %KA | R$2 | ((4 | _PD | gT3 | Lk~ | P"4 | }Pb |
| SrT | 4jY | 8zH | ;P( | mqW | mJ> | XUZ | 1_r | `w] | n<k | &~Z | #E% | y>J | ej+ | QT2 | PJf | G"+ | nJp | FNg | {!D | _O. | =hv | MC. | s\A | `P< | H>@ |
| cuG | ,x9 | ^/3 | DO2 | i3* | F)s | \~l | ?7` | PR> | <ry | `4' | ZFf | H?M | J/g | BxP | M0W | -t@ | WYP | nQF | &FS | D|# | .$} | 1#3 | L4^ | dR% | C[Y |
| |@X | /hP | /LS | qV* | Kk} | 3ZQ | 9yQ | 0-d | G)f | M]W | kr= | Vm# | H)H | .vM | 3SP | [$_ | $pK | kC/ | WIU | %r{ | >J4 | N50 | +Ej | Lh7 | Qy` | {t5 |
| En~ | >gM | =Cq | Y9/ | (AT | 2'Y | InL | AIp | R#- | s{V | MaV | Btp | ?O3 | {*[ | )W7 | MIP | UUJ | fFS | wQ0 | Ath | =V9 | t4E | 'Pz | tp. | H[{ | s}4 |
| ZKH | @^D | V^E | q34 | Noo | &KA | jVK | hWG | b4w | bi( | t$+ | 5T! | _.g | eYq | k"N | nq5 | ajX | n\d | Y02 | 5Vr | s8_ | N>- | xd@ | p}s | ?D- | 3(? |

*Tabela 14 – Tabela 1 de conversão de sequências gráficas em sequências alfanuméricas*

| tH! | 8>C | UW5 | DX& | =gK | [V~ | G9t | SL. | j%z | <.9 | F%N | !3o | OLi | i`O | p(o | 0D/ | Mi: | qc# | &F< | UX. | t`c | ivS | r!> | 3U} | w[@ | H)Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| '#4 | e_o | :6? | )C1 | X\L | 6zI | vB" | {95 | Cn3 | KOT | O+G | ~6W | sni | 5E, | Ctm | l"G | oq] | K'd | R/A | E$I | NC3 | vpg | |_> | Obs | z'a | =A( |
| L4[ | e,K | @ng | p$" | /:o | |_M | 1@{ | pT` | [=* | V`t | .:r | :)3 | ;]E | ]2H | yGW | CQ9 | mc^ | [hG | >Cw | PS& | gv( | G%e | Xoz | /I) | [K[ | Z-Z |
| lF0 | Y^Z | 2[- | .{E | \"^ | a\q | i!r | I>E | K6( | Hmi | Tse | k,, | ,Jq | bRM | <E: | "-k | Q)# | =3n | EWC | !Ox | u^< | QR0 | "'g | CTj | z|A | \q\ |
| -GT | z5) | RV/ | .vb | rPy | rCr | %(e | Q-q | !~# | N"% | JC? | n0h | N+z | (cw | x+9 | Jbf | ~jC | c^7 | 3F' | utR | j!9 | Gqf | ,;> | I_B | N4K | %|b |
| U}f | yYO | qWI | 6^A | EA} | OX] | yHd | 0*5 | Z9I | S}9 | }x+ | -7Q | MvH | HUS | _d+ | _t8 | VvD | mK8 | 0$$ | z>R | bi# | yAK | )u- | ]#& | $tM | #51 |
| 4~o | dlv | n{B | $d6 | m*" | xb{ | r&: | nj1 | ![Q | J"= | x]1 | 9P= | rEy | gcv | ,rd | 1nc | !A& | ,Yr | ~fS | op{ | /q~ | iJ7 | (f' | 9up | ];! | CO1 |
| _"A | WCp | A,+ | Yy! | kDq | PA3 | $aD | fd_ | EzE | \U0 | -Y= | 1"- | 7%O | gat | oX. | wOX | _>[ | |Sh | mJW | S^I | -c< | (mf | LgO | T5& | <IN | q:T |
| tpW | ;>U | ]Ey | $5k | P^Z | =tr | O&- | >6N | #* | v(\ | ]VD | o\( | ."% | lA; | 'BD | OQ~ | hpL | h.! | *tI | _?a | 8uE | =0B | 3M* | 60c | #x[ | o{k |
| *sZ | eTx | .-: | Yz< | ci/ | JS) | {xH | L{~ | l(D | d_2 | SiK | yyf | _Je | K65 | q#= | J%> | kv* | #0_ | Q_K | D8# | cJs | =%4 | Z'c | E'= | o+~ | 5o} |
| <+9 | o45 | b"R | +{~ | L1I | bQC | l?4 | `~Q | z|G | ='( | hMD | ZLX | :2v | o)z | xoi | F/{ | zLr | A0. | =/g | 0gM | ]?u | 0Iy | "tc | 0_v | N]F | /$M |
| ba^ | Pd\ | *59 | 2(S | F}r | WBI | E?) | NR! | Ek! | 7pG | HDp | cyx | /Sm | %ET | ,sj | o"K | :JF | \Vg | ^8^ | Jjh | }pm | Tj3 | p+> | {QV | RH[ | )(, |
| (!, | B4I | QEn | p.L | S1e | Drp | 0oV | dhT | 5$: | /ls | yn} | 3B, | c)q | #[< | !@Q | t+= | F4) | 9pw | *v% | 8\N | zkg | AWC | P*< | z/4 | \&K | ^O] |
| g{p | |:x | 03( | Yq{ | $s% | |d, | =[v | $;* | |:U | DD) | WAp | |q2 | DkN | /Y> | cDE | ?k} | dQ_ | ",9 | -k` | p^Y | F!i | qK[ | dR0 | EfV | #{[ | *C< |
| <QT | <-k | itg | [z> | J=x | {q+ | WE" | ;yH | d!) | B-z | ,C! | MpL | k.% | 8Vi | *b< | lDP | &Ws | 3@w | Ce5 | YAw | )>~ | 4&3 | >E+ | G~c | GB< | 3WL |
| h}} | }") | czt | H+y | G29 | DxF | 0=Z | ~}! | #6R | ;hi | YFp | Si~ | RY& | \jx | s)b | AL} | .$y | HR/ | FRr | Ade | 7Y/ | *.1 | Ypp | yqG | ;Dq | -T| |
| Qef | he+ | i\e | smN | CDx | d%= | T+3 | )de | ,I- | ul> | TC9 | *@s | (n8 | z/m | s_j | QN# | D>I | b6U | wx" | &3e | gDb | ZsU | 'Tp | }cX | p^\ | }#X |
| (H5 | x_f | @2# | ]`M | R7- | h%_ | 8a! | cG0 | %N9 | 1J" | x[ | B[C | @9J | {r, | _Ks | >cs | 0Ku | }!$ | zLC | Z$s | <", | *#r | _q? | Z~M | YF` | Lou |
| +he | [u^ | `vH | &<K | 706 | q^c | nW\ | EMU | XF` | Phv | 7li | RTZ | n)N | Vjm | x+S | @00 | rTC | ,g` | U_D | ~k$ | lu, | |dV | 1Ge | _[? | *~/ | h:_ |
| E[5 | ;HZ | *`G | =xA | =(V | 13U | hqN | dx* | j^s | RoC | ]`x | 5w` | tO] | Q+W | JL$ | U.W | .:f | c~0 | -S? | r:? | ger | \H` | m]e | .;?p | so~ | -{+ |

*Tabela 15 – Tabela 2 de conversão de sequências gráficas em sequências alfanuméricas*

| zta | MeM | r.3 | 1|1 | *-+ | u]y | oRo | YEK | F$E | |r` | q}' | gtS | uH' | SR) | E)7 | zV) | a<P | ]n" | b9P | 6xX | 4|W | }8@ | A/@ | J[k | z@B | 2,O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| sWo | Zrq | "5x | Q$; | L;R | L_r | x;F | s85 | x\M | 7nP | %AN | Co1 | u}, | U4@ | NZ5 | _7h | 02T | #M* | 0O` | IB1 | ^/I | IAQ | 7q% | kIW | ,\} | @|] |
| E`s | &yI | {i[ | u9P | XLt | EOb | O}H | 1~^ | U{3 | %/Q | *[b | 'e8 | =&v | %2x | 81. | #|7 | my} | 7YV | 5t9 | I$# | !7; | YIV | hv8 | V|% | v(E | .cy |
| SCN | yJ? | q<E | kvd | |U= | X/4 | [Vb | i(& | 1"k | P^# | |X> | W1e | p-E | -I1 | =J+ | uX' | G|O | q(2 | *$y | %{G | 1d8 | C4, | @Ko | M;B | _6x | )(6 |
| [^L | E.Y | t"` | :7C | 'ly | Vr` | {T" | _5> | rm] | Y!8 | .&+ | M<7 | hi* | 0uC | 'Wz | >>q | f3R | EXQ | Ol% | %u+ | >}7 | id} | OzE | t$& | igN | <Wm |
| i>E | =J0 | +rt | r!G | (C[ | tzb | A8+ | Mj7 | v7E | E"x | 2/W | ZSD | }]K | PAC | !x' | g=g | A76 | q/~ | `UV | tn] | eb? | Ut` | _UH | BR* | ?LP | koE | |
| h/: | \3D | xVG | U5V | 6vS | X@f | D47 | (t] | 2Y- | Nw5 | um\ | k5u | |Lx | .[+ | /o9 | -I% | R^t | _wR | G)! | |E. | <kj | ;dy | ;4k | Y<i | ogU | VIk |
| <>a | Yal | i`S | k)E | 'N] | c6- | O&} | aPs | 6GA | P&z | \L* | rt1 | y*\ | cW+ | 'tS | 4Q* | ?{| | Oba | 9Z/ | +(v | 2G[ | MOR | M!1 | (oq | t#m | y,m |
| /\N | 1D/ | %:C | yJ4 | k?0 | CZd | i6{ | \cT | LQ8 | ORv | `?k | _*f | :i` | VMv | [PR | Mm7 | 65o | +Ji | 8-O | kw_ | j:0 | a5N | '2B | h=f | G]$ | M?] |
| T_z | T8% | k-g | t[3 | 2LI | RKo | Lc{ | !Nj | T._ | "#( | Nn{ | 5~B | 8l[ | YAh | =1A | ~/} | WUa | *I% | ?[, | sYa | _K# | Fc5 | IDf | /GQ | zhj | u)" |
| x9Q | -SQ | -au | qp> | +8S | rP6 | -AL | n0a | WLf | 7,s | O)= | !#^ | K&p | ]V1 | Ug> | \.> | m0# | sG< | wnd | y\P | Ev[ | k$& | pdE | ?yh | ~iN | ?` |
| [H4 | 5N# | 5*o | U+d | nv8 | OhI | Lhr | uP: | f]3 | 5'D | 0,. | _)' | 9:\ | S!p | =u0 | VS? | (m% | 1fe | Nt, | @.) | SKZ | U2z | "{+ | N_^ | 1d@ | G1# |
| T(< | #>( | [tb | 9sI | 00o | ~ZE | ~u6 | 2fJ | q"[ | .:_ | /i1 | CLt | <04 | $7, | bLq | G4W | -G< | 0V/ | 8,| | --< | ugn | 5F= | QD9 | Q5q | 9u= | [@^ |
| p-! | 8"& | >`o | o$& | Em- | s[N | n2. | -m| | A4O | )tb | [nD | S:m | ]dg | F1U | ?bP | 6K_ | B+Z | {{Y | @{& | I^J | UWw | }D[ | `oP | }nW | OEA | F7p |
| t=b | #!/ | Avt | !]v | <*1 | O>L | J\# | ZVg | j[K | P7W | Jsm | ?/k | bM( | b'; | ,9g | hwd | D}! | ^8C | #HN | #]W | >bb | !"= | e=U | Jh4 | 3}D | ?Q$ |
| jNt | :d} | Wk| | oH' | qz8 | *%x | 74. | vfk | Z)F | ^nU | uGf | )Vt | Sz( | px( | 9MF | J8` | ... | hoo | "P[ | hZq | YAr | 2=$ | bi9 | Qm- | Xg7 | ?V~ |
| m8[ | Hum | ^tM | D9@ | n(t | b;H | b75 | J*{ | Sv$ | |)) | Rc` | 1p/ | 4!z | 8*t | pk` | Xse | H]| | ]lS | Go2 | Py{ | u]V | -wS | ~v{ | uHl | JR8 | `Z0 |
| p%5 | |^X | TxN | .CK | H|k | 0b1 | \8L | 8&@ | 69} | 1<b | ^q1 | q1) | 8L' | Mr[ | <O; | a)n | t!w | &ix | #g( | dV! | M67 | gJ; | T`Q | v,I | rmO | @HF |
| &&# | R'n | i}Z | PMK | OD6 | 3gY | "[* | )&c | e6w | 6LO | ('J | 94C | ^rZ | 5R) | GVF | LTh | Moz | DQm | ayz | 3^H | p{W | 0ss | =qf | i33 | jk` | LHW |
| ;eS | Xip | jOz | \A~ | e\r | ~?R | 5Si | A^| | _UA | ":K | tw% | W~# | gQZ | KAh | C&n | QFg | (?? | 'pR | h:W | f|) | n6N | \Q` | o`$ | uD= | *K\ | [zw |

*Tabela 16 – Tabela 3 de conversão de sequências gráficas em sequências alfanuméricas*

| n7* | $;8 | 4+0 | Wx[ | *1" | _OG | ]'C | |m; | GX| | *6A | Ypx | 8-C | |4d | ZsP | !~8 | FY1 | y]] | Yp: | '4) | %Nn | m:w | mzx | E+' | eE' | #Ey | }>B |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pt+ | Y"0 | F1g | nC' | yW" | +f@ | s}R | 4(0 | Z$J | 1'L | GX{ | 2Rb | |#c | TP0 | ^fd | v.| | {%L | #55 | R3} | pnh | c-y | vc[ | $qh | hs& | UmI | .FH |
| ?Rm | /in | }]L | bd( | p)] | {4, | SQ. | 688 | lMe | :1I | [:B | ggD | q:# | ()a | Hb! | F$u | DFc | Er6 | sP~ | FuO | Hp\ | u/Z | r2e | -op | *^I | dqe | |
| +2] | ,/d | qDG | =o~ | `)`b | [6G | qrs | u@r | 2@l | oAD | DlT | R&{ | G*H | e!V | ?F4 | /8k | 9RK | FvH | g#o | <:I | *Pw | :^. | hg# | wtu | 0gx | T%( | |
| U7G | 0)9 | b/& | @&x | l@R | -*a | d'% | rI$ | 5H8 | @Gg | =K@ | p-7 | ~dI | Rq@ | o?q | #nt | #,& | N~6 | \,: | 5&h | 4zn | "T7 | O> | 6ZT | ?H4 | 1rP | |
| r]@ | K`! | JUr | Ffj | +xe | $|+ | ")+ | \|[ | 8W| | <>& | WIO | A>$ | N\/ | h2; | v&3 | >r6 | =mR | ]oK | :bo | =xc | liY | uFu | 8ie | <&h | /Da | |
| H<: | Q#s | M9+ | vzf | +,q | 'Rn | %"n | BT) | ^SY | *o& | <V; | I>X | <]E | gF& | 30^ | LT" | eUh | !,< | /d` | "e[ | VN8 | ^6k | pIj | bm3 | djC | * _z | |
| ),K | rk, | ~WH | cpZ | 1{C | $[9 | vba | eIP | ?m\ | `WC | < _z | fo+ | x#Q | ITw | ER' | Q|# | D(| 6M_ | ?pG | TC@ | A(_ | 6;u | o4& | _X# | EUG | <qR | |
| 7e/ | c#E | !$f | 6a4 | XH@ | Yl& | r8W | L+> | I2] | 0Cx | (,b | E`( | C4t | xRy | "Qn | U5; | Xzx | MOq | k7` | nqT | sUG | [GC | I!% | *w? | I2P | g#2 | |
| m*. | OZ_ | R;> | Lt; | @Df | 6li | +#e | A3U | eSX | ^k- | {"a | +s< | G)a | "5I | r#; | Uny | S!5 | -dH | R}n | oE5 | FJ/ | QC# | t][ | VWd | jN" | P=^ | |
| OdY | xcv | ^WI | g82 | hLg | R!j | 4W~ | dr% | ?tW | rgN | gQm | r>& | zPt | &Kf | q7E | ~q] | 4^n | wd8 | Uki | _t+ | WV* | V;b | =sD | H][ | i8< | twH | |
| bw4 | >}k | m5% | "T, | I<4 | 'g8 | q[t | 'Qs | ^Z@ | TwW | /14 | RD$ | >H& | $yp | 45W | ATS | T!8 | ;<y | UbM | @)C | _1) | .ba | nPx | [gC | irJ | sA{ | |
| H}8 | 6\n | #E' | Oz( | uk, | c`C | GzZ | 4P1 | hV; | g.O | }MV | 5Bn | 'D_ | <E_ | j'2 | oa= | ?;Q | 1IW | `iR | Fjv | -sr | hXJ | 7?Y | H5e | ZHD | ZCo | |
| 3Wr | q8H | *PL | &3| | twY | ~*2 | MFV | c_I | USs | 3BM | $z= | *K' | v$\ | Ga5 | /+9 | @2? | ylP | 08n | r[: | Wpq | wjj | RS2 | F>v | /k+ | 1Kc | e(j | |
| Vg3 | X*0 | wno | O$H | p}L | 4HW | QKv | Eja | cvw | t)7 | gHT | 5Qr | 1,* | ;/< | o0f | arm | M{& | FtF | nDN | 93* | _gZ | 2l+ | Pg} | `96 | @Mf | nQG | |
| mEj | KY5 | `s~ | y<2 | ;JE | -K! | caw | xbC | L-[ | v\s | ebY | EoC | #@r | LSH | S(u | [jo | l"c | tIK | j7N | Q'G | 7'& | GLK | e+H | N+G | 590 | #H3 | |
| -L> | ,'# | :1= | JOA | =Dh | Z{m | ,me | bwl | l@: | Fv< | <`7 | bC% | &nk | =4k | TIT | zg( | fUC | 9h. | <ml | DN} | uR^ | #)7 | yxC | #|= | iwj | j*W | |
| Yf& | 3_s | Q/n | +A@ | D"j | /#C | [<N | LS\ | Mb\ | 9J` | !x+ | QI? | {6# | s)5 | ha3 | GQ@ | 3*~ | MIt | W?m | -VC | Sz1 | `0X | Pbt | Co" | 8E? | fjJ | |
| Ts( | ==V | ysb | Sfe | %qr | ]EE | LBi | Bb? | _fb | ^7( | qs@ | X}3 | >;} | ~YP | ]]o | Om( | 7:# | F|r | R9~ | 2Z3 | ?v7 | e8Q | _zv | ]j0 | Xsm | &q5 | |
| C9e | X\+ | Rb< | PvA | *q! | (=% | _Z | C$u | vQ8 | x\W | e}O | Ip4 | m&' | +Yf | ~~1 | wyI | &'] | %v] | BAQ | kL/ | [d: | 9HB | Hi> | @07 | Rs+ | 6p@ | |

*Tabela 17 – Tabela 4 de conversão de sequências gráficas em sequências alfanuméricas*

| teB | 4g= | Ws. | keZ | N/2 | >xn | ~/B | :7Q | n%5 | Z0q | CPS | :G@ | cif | ^RJ | \.w | ~O7 | ?uz | 8^@ | ]q7 | i[m | ]wU | .w_ | _B. | f9~ | Kq] | ,WV |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| r?V | /V? | >R& | (:- | dL^ | Tr+ | x.K | Q<6 | \U( | cgB | W@s | 4Ei | )Dk | "0h | %?9 | `vZ | US! | !Xg | Ad) | YNS | C"} | ;2G | c'/ | _.] | Wu; | K&= |
| |o= | 3<3 | ]?6 | Qy% | n@' | ;`S | vHs | sDJ | ::1 | <&j | c&. | a/o | oBD | CFb | <2c | \G: | W21 | s9B | '(D | WY} | ~1( | vN> | Mot | H/d | >;O | v(# |
| 42R | ]HU | gJ} | >lv | FI% | cQ; | ]vN | Q"Y | <!A | 7AO | (rG | sWp | Aa@ | {"8 | w:` | 2BW | Wy> | 2J_ | Z[% | C+& | W<` | u}> | @-q | &m= | >P6 | tCf |
| Aqp | ]%1 | QQ! | sq` | SRX | Sqv | e5P | Phb | 3*} | lSa | dSk | ^]} | *B| | K-~ | Fp2 | .8# | ~L# | "UK | ~D/ | 2[# | t{V | !Bp | -I7 | `yp | _\Z | R-^ |
| Qp6 | ow0 | [|* | vlS | Z#l | c`R | {bT | Yt> | ?gG | uP$ | UU` | t}) | ksZ | spn | /0j | Gsr | `3| | 4Nj | Ws| | {:J | vRH | E/w | HpE | EyF | i[_ | m}w |
| @vc | Jg: | k1+ | or> | lyx | sY- | 9sb | `1L | $8( | ^5b | "yK | )M& | OV' | -q( | hE4 | k}N | C+1 | `5{ | Xp` | jfv | J*( | M9j | (v@ | ':H | Nmj | +Kb |
| LH} | wZy | d7s | ,sL | iFy | c&D | U"Z | JV\ | ~s9 | c?o | B%r | wdh | 1@! | Sbe | $D) | `&V | =qy | }D$ | T*- | fcu | nrj | Je, | fl? | 7@f | I/q | 3e4 |
| gYV | nB: | .Py | =I7 | O>| | 63Z | Ul4 | -3; | +j1 | ,JM | ~hm | LjF | 'A0 | spY | bd! | Ib\ | @(J | U~r | h-P | H$d | 9Up | S?v | <3% | udj | 's$ | k<N |
| G;& | [8i | 9O5 | G1" | D5P | gN, | `~P | 1WP | LdV | b@5 | &%# | ~^C | -6Q | #\s | ^Z4 | Mwk | .~d | V&0 | b~X | nf\ | 'MJ | 5{k | >^i | Ec; | 'Ye | ar$ |
| )>e | 9;{ | t%x | (sz | [kn | zn, | j0V | i;I | J*L | +Fx | =iF | %6[ | cM\ | ;D~ | @2D | `j6 | -lj | XW& | >U. | 4W| | 4>0 | DWw | y-d | o&r | 6jc | i2m |
| Xvd | S/u | neS | >4\ | "d: | z=r | SRl | B4/ | Z:m | l`R | XN^ | 4h~ | :Gn | #A2 | At4 | IfR | )!: | wOY | 1,0 | ]b4 | j%= | :6{ | zr( | w^O | [i# | {}S |
| ='n | #&5 | :$= | eVK | 'W | <=\ | ]LM | >Y] | gPO | 8qJ | +]y | +[1 | 6qC | DNC | 1}, | x*& | O<p | %Hq | !1# | $[0 | ]"v | ozS | _26 | 4KF | Bq$ | A@Q |
| \yn | !^Q | MPC | ~0$ | h]E | Aat | Fu= | +ja | Er4 | @)V | &A( | yvq | <n! | 3K< | eu? | ~XQ | l:} | LrB | P#{ | (<l | qG= | ]1T | /xx | ZXl | 2{n | T8. |
| $T9 | :*| | n]3 | /t] | r^E | B"B | &V0 | ovs | 0v$ | gPV | :Tj | uXS | P(M | Au7 | *6* | (C6 | Q## | vxU | l.s | }KP | X,n | Yj^ | [B! | h[T | h~U | <#7 |
| d?O | "(A | jr) | v\> | OKg | Snk | 5Ul | fii | l,B | uQH | 8eF | nGz | au* | |4% | qb3 | f=^ | R}P | _gq | zvx | -;H | `2] | {^y | xKG | x12 | =]N | z<d |
| OMN | {}( | dfV | _E" | ?F9 | m,N | p"# | e?F | 9p\ | Eo! | +Yx | uWI | X(! | jr+ | ^+W | Ez| | fj> | YB- | *U| | Z'D | >,T | MT. | )1H | Qlu | 71< | )J< |
| )w, | eOa | hC= | gJ( | A2/ | C*- | ,MP | 7H> | C4k | ee" | X.3 | .:| | 3^{ | lEk | .2S | #Gh | X;{ | pG? | GsJ | wq$ | fz, | OZ1 | k(5 | #\H | Q\x | Y82 |
| &/H | oDM | m9] | QO! | *)A | KO* | D2? | T~6 | Qsh | zGM | Cuk | f0^ | Go] | ?b* | 5rR | ?RI | YSp | eX] | .Lk | A|1 | 13( | Lpi | F&S | :GF | R2{ | a." |
| jFx | uR- | $w^ | H^T | Lo< | 05> | 3jW | '8o | ?~Y | ~X1 | zS& | mRS | i<. | *VR | !P# | o=% | }U! | Nw! | v-m | i;F | 9;8 | -ZC | $i$ | 7pQ | =y8 | ,!i |

*Tabela 18 – Tabela 5 de conversão de sequências gráficas em sequências alfanuméricas*

| MS} | (]9 | Zld | +e- | `?0 | ;~x | O<P | e2r | W^" | KRj | ^<0 | !j{ | 6/e | \<k | fn! | 979 | S\H | 2F, | ,M| | klK | 'm{ | T3, | I20 | b!" | <(M | VEg |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| riu | YN7 | ySi | 3xY | #J. | ^F+ | ])? | fIC | Cz+ | w[\ | AV6 | RK6 | Y]u | k,< | zbw | eC0 | x3( | hm< | Vp< | @x# | 2tp | R.w | K`a | }mk | 2;k | 1kc |
| U){ | K8H | 8]9 | .q% | #K# | b+C | 4,D | 1Ad | LQ> | k#s | ^Z" | !*H | #ie | F09 | [4L | vMm | bio | 'Nl | \'y | y@N | wE` | 9ys | rGH | -tx | pEn | ju\ |
| foY | dus | 4r8 | CcJ | +4% | ]G; | Mdu | JAI | LsR | G+X | bra | tl7 | nq# | i3H | KDa | 4:' | O"F | =Rz | p5k | :Sv | osH | OS6 | ;=6 | #GV | a"; | M=F |
| jE& | ouS | KB# | "eB | rdz | b4% | 6Z& | ycG | ^1D | C50 | ih] | RdY | n4% | uh] | <Y( | "*Q | m0o | SU@ | bYb | wZ& | tVu | + _p | ")2 | 3F= | ;UL | ;K< |
| AN, | C1$ | tBy | .,X | WZ& | #ub | D$x | 7<9 | 7t^ | +p` | "vE | @Tg | Bwc | b-x | XGK | MFd | nv} | %yU | @e' | K,7 | 3K8 | _q~ | ol\ | ohM | :DG | lZR |
| 9C9 | !|^ | %um | 2J: | mL* | gfg | F%c | tsq | (&8 | J`Q | z." | E=~ | P47 | R%H | \d: | _\Z | nf+ | JUs | /7O | u=" | $#h | w&' | Ms- | {|O | @<` | h=D |
| H?) | o@# | f^| | ZN= | $/W | )6& | ENW | nA_ | Tg+ | wAc | [fP | Wqh | 00> | e~h | -&4 | @`d | )&k | [&; | P'8 | /Lq | yc9 | pQ/ | L7Z | nq1 | ~?# | 70L |
| '5$ | iZ< | NR~ | Fq2 | l#D | D>[ | ryl | l2\ | mx8 | uq> | yCT | wX% | ikE | dda | Ail | @yX | dya | /?V | hV8 | g!X | Q2H | ^pO | X&b | <E9 | n.\ | ual |
| o?Z | _*` | Uoe | xxr | PGd | 9EA | 'V_ | M,g | wOv | F,8 | o-Z | j=h | ^Ww | [/H | +fQ | Nfr | 7I3 | \+/ | H!+ | f)@ | m(S | i%& | (MI | =,x | :S{ | fp$ |
| 'Th | (';  | %LC | Y%. | M@E | }}} | t=) | kLF | Abs | pW_ | gJ# | |E, | ^Rp | nG0 | lt2 | N|H | >7E | U|8 | 'O+ | <z~ | Hv8 | hd0 | 'z[ | ]q| | R9l | KxB |
| 269 | [,% | edN | m6C | p^u | 5z1 | g~i | ~pa | NA` | 1t7 | 2#3 | A}" | /Gf | P3D | .[k | W|^ | YQS | Q-m | MD* | Iu" | 1L) | ZnT | u") | {=] | *02 | ;"3 |
| O`b | yT" | ..) | M.i | 2`u | oyY | mg] | mgm | WTL | fAC | [/O | %H0 | Rn1 | u6" | g]( | ICx | >y] | \P: | `v] | @%T | M}] | %@~ | lVi | E{) | \nD | u1! |
| li1 | h;" | h@x | }lc | 'h+ | jK{ | s/G | /D, | `(q | 2;Q | [E` | DH, | :2B | [#E | )w\ | ~=J | V%K | iK_ | i9W | 3Ri | _X* | *G | '?a | CD9 | 4g( | ]<b |
| C;i | zj" | &f{ | ]K^ | {Z= | rIR | Lh# | D%- | }v{ | +vk | {0~ | 5u1 | (J$ | D[W | ~t' | P:3 | zUj | =1P | 2MG | jW3 | @yN | p!Z | rAr | pMJ | w_m | rI^ |
| lkc | 4dk | g?A | 6He | k8m | {/M | !z< | lRx | k}, | x=h | 5J> | zUl | Gs. | 4sl | F.q | kRu | BAP | I_Y | :uH | mM# | k{/ | l:L | 0G@ | xd8 | 5Bt | Cak |
| KK_ | Kz% | X$r | P-H | J%8 | XRi | "dJ | L'} | {{l | a>P | I^J | m-f | Dy9 | ;c) | ZZ$ | eMW | Vu/ | @XQ | ;ot | tvY | wMU | r@e | W]f | 3d) | (H^ | k`B |
| #<, | 8SB | U}U | 8H4 | Wm0 | 6>D | 9$4 | :GD | k%\ | ZJR | <Ze | =`$ | +%' | dO] | ^&? | =hm | OX( | :Su | 00f | (El | JC4 | {%8 | ,'J | '#E | yl0 | Lp& |
| i/? | \<> | I4B | abv | hhb | ofN | _%: | ONB | L>1 | Xcq | Z_O | %Ha | jCF | 89( | i8P | kLd | mRF | R&_ | V(~ | PjS | ^vG | .g] | eia | qu> | ,MY | 5eS |
| #&7 | rP( | 4lX | .RF | dz: | S.+ | +U= | EZa | Y{# | izS | +OS | PCE | ${@ | B6+ | (N" | 19; | >Ot | hN! | i"r | 1+J | dWO | bR] | Lx0 | g'G | PW* | "w9 |

*Tabela 19 – Tabela 6 de conversão de sequências gráficas em sequências alfanuméricas*

| Q.5 | jtA | ;h= | Zb~ | QBj | Of0 | f}G | tqs | Tt~ | ##, | rN- | >,~ | ;?~ | 694 | B^M | [3w | k(M | }E' | gVJ | ZBq | NgO | x8b | p>W | F[| | uBm | ^42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [+. | Z(^ | $H] | 3%} | Aly | U*H | OXu | M*w | 3in | `[F | .L# | U@[ | P=! | *[# | 7wD | v"K | t?q | kqF | PcG | N![ | 9"` | u{B | d'R | HQF | AQ5 | \2W |
| w|C | 8s} | 4Vm | U~& | l|O | E!, | 45j | D;` | mRj | %F| | 9TH | ()G | RDj | <N' | F-W | RIk | }nV | XP8 | =g' | F0& | BFk | xdC | m2o | c~B | v|@ | v[% |
| -#H | tb( | mhq | Gsc | gki | 6j! | +mG | >Uh | 'd@ | 7~B | FMa | 7<0 | 5;f | %1p | {(? | 2"E | QoS | &8? | !a" | P^Q | V32 | A|8 | z)' | Q<L | jJ~ | np, |
| 9+B | aIE | /_9 | Lnd | {n| | z(D | `G! | \9* | 9rL | C_@ | lxB | x,= | 5K7 | v+/ | ,x9 | 9\: | ul= | y~] | 5-k | $6= | 7%` | X[! | rJf | $]i | w+0 | :_G |
| .Nm | Wux | a![ | "Yo | s$N | ]O` | h\` | ]N0 | 4.? | &G? | VP3 | {E_ | j4? | :x8 | NK; | JR8 | ]1+ | "/ | #*% | pya | 2!/ | 0hp | N$X | N/X | ^I# | ~ui |
| _lb | fr@ | j|- | p7Z | l=6 | uvs | =\d | ={\ | j(p | :Km | #R0 | h+R | 5]= | Q#( | ZW[ | E5> | @_7 | ^^O | r!$ | &\t | 5bm | {@G | m)_ | 9Z: | =]O | #t1 |
| <^P | !hA | zM{ | a;8 | D~l | giR | v[U | l6U | E0c | &-` | lN~ | ^.s | ,xQ | <^: | o9L | 9!6 | j#Q | KH1 | #g% | W,! | gGp | ,gN | bla | Zm~ | 1u$ | iK) |
| <9% | GcY | IK^ | [,( | *~^ | w5e | :]\ | 7R* | Kr_ | TQ3 | ,!- | ]NU | A;j | AaM | BrD | Qp* | y,F | i"( | iE; | Hho | 4l@ | `5` | ['k | i-K | E`# | 'P+ |
| co' | ee+ | ;bp | -H~ | 7E^ | ,cH | {ay | $3) | O{K | TfP | 7.& | s.u | "g= | ]^= | 8aa | Wj6 | )Zt | RdG | qfD | q~- | ox1 | }Zp | }cK | `n_ | *"/ | na1 |
| h.[ | -]. | hO9 | POg | k@U | JnD | }F: | R}G | HiX | 3,! | S;( | [0\ | _RH | S2[ | fyQ | 5XA | d|G | 0!' | DR\ | wqP | Zao | ~!9 | O,~ | >R( | 45N | l~t |
| %Z# | BhI | ew1 | @cy | 4KT | P,\ | /Da | g37 | gQ" | n%Z | 8rK | t2F | *,$ | bB] | xSI | t8P | cQV | mP> | NSj | PQj | BJQ | ;/ | /*V | EqF | @4; | 128 |
| b") | C$f | s8{ | RP; | +q* | Y9* | Wd! | Y5- | xs@ | kBu | ^!? | G/G | !C) | |%W | S3m | *b& | ?4L | #xU | XTj | i-` | .v* | Vfu | G=\ | uJL | jm; | w8G |
| #3q | w?M | G10 | ]BQ | -j{ | {hJ | aa} | js5 | S], | p-i | Zw( | /[0 | 0IQ | yrZ | /=T | %@# | 812 | LGl | 390 | KmE | !bD | RmX | .9r | }Zf | *mi | /.] |
| Bfl | wBr | 1:m | 7BW | 2n) | kEx | 7p, | DnZ | $9~ | 6d5 | Kh; | V9] | rhZ | jOC | lBI | Xd{ | qYR | 01K | P?~ | %[! | Ds8 | W+; | GiN | 1)W | }Yo | h[1 |
| 6Ky | D(< | 4H" | g*w | V,@ | 1+4 | HB\ | {/m | 0]5 | @s^ | Q#" | $5: | \9e | _5F | w"= | 8+r | mMN | a,+ | "L# | eG7 | ,!4 | TvH | id& | uwy | g0, | !h& |
| 6K6 | 9pD | '\d | <dv | 0Sm | gC@ | 2<E | 8gW | OfO | rq) | 'R} | ueZ | jZ$ | A;g | `T( | ZIR | MJ& | }o" | `C{ | &c* | ha5 | )" | JK7 | B%; | hAN | k'J |
| ZU# | (g& | _ac | GJF | 2>u | ?K~ | 7uM | *2x | ~zy | MPJ | H/P | HEj | n1z | Ny- | TPF | S]y | a-^ | @$/ | -at | GPI | W;[ | f3G | =tZ | g#{ | G"C | Scl |
| zBG | N/S | )d3 | HU: | k&$ | k]~ | OFU | juN | V*r | MzY | 9Q4 | l.o | `O* | o\b | <+Z | TlN | `uw | DiA | 83i | cZC | g7F | 4][ | ;]y | `:X | LLr | A_; |
| *tt | @;@ | Az, | "AU | ;EF | Rf% | D<4 | zoM | q~+ | [;H | I18 | GP0 | )%M | Q0X | 7s> | 4bj | Nr@ | YiA | 6=: | T0P | qqD | ]Dj | `Tb | w:3 | q|{ | 6BR |

*Tabela 20 – Tabela 7 de conversão de sequências gráficas em sequências alfanuméricas*

| 'N$ | pXa | a9e | >#j | JK* | 76\ | S"{ | KiO | +l1 | b_F | #oM | y3f | 5$m | Dwk | }$T | 2{a | K8x | @%A | e~g | "LA | 3m^ | d@m | PPN | %jh | @4+ | ^z7 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| _NC | qB_ | LN_ | [lH | 0}b | W<` | I(Z | bCv | <yC | K]M | .;^ | >6s | Vp% | =]w | `}8 | o/9 | ]aY | ~Bc | oo" | i`% | _b0 | 3pM | 33D | %0< | 2'2 | ]^Y |
| 1>R | e57 | _t5 | cGH | #:J | evW | q;> | W+E | /JQ | 3!S | XWW | ]5' | ORc | O\j | T!G | 4J$ | 'W5 | )ss | mmG | ?s} | 0D_ | vW7 | p7n | bTu | 8M{ | Ej? |
| t#q | X"! | N8S | yq3 | `4^ | l9g | wFt | _@ | N!h | "/c | o1* | `;a | ]&M | C{$ | X=; | q?X | *7X | GUT | ~ei | uQ< | VQ4 | gb/ | Z`t | Vyw | Mw5 | -$\| |
| O)6 | P:K | asi | d$K | I[( | AOg | MM( | L)P | {Vd | btt | P/v | T?% | '_7 | q03 | ~Q? | q]F | WjP | 9$T | OIh | \h? | a8N | <uB | LNR | )&H | W6{ | {xX |
| %KQ | \\|@ | ZS\| | 4Ym | i4* | 9hA | V*g | S<R | PH= | >{C | NeW | ~+e | @?k | 5,m | Gs` | p~M | ~h1 | {fe | {9l | npu | ;KB | SMA | g~b | g@k | "S= | tJy |
| WgY | !o8 | 6kn | 9Vx | jKe | cI7 | =0R | 5vM | ^I{ | YKf | o<J | !Z^ | )*` | Kq5 | fo[ | &K$ | 5\} | Y7~ | <jL | ^xA | xn6 | 7_7 | xS[ | Rx0 | r#} | K;1 |
| 4~2 | c2B | cFS | 6y$ | P1N | eIW | Q5y | >}X | 8-S | %qR | v4x | w\|C | !Tb | `>u | xf9 | B$u | :q3 | 5Cx | <>W | *Vq | oc. | h3n | S]? | =1( | wfA | :m& |
| Q{P | nAn | gQc | 2U5 | .B1 | 0#q | 3;i | ]\|W | ['@ | B:Z | hMC | 35! | %bo | *?L | %lk | Z-d | jfc | `-r | ub# | _R] | 64- | l[8 | #&d | IM5 | xHE | '!{ |
| !*Y | @yZ | Nv6 | 7x- | Ub | 6[o | r3J | ,#- | U;& | <Eg | CJP | _.4 | DhG | rGW | $2( | G_A | U@n | P/j | 6W" | -PJ | {hI | eY@ | @*e | 1jU | K&v | \>Z |
| ~Jt | I)$ | 'Kr | a?m | i[9 | 4\|F | .\|9 | 299 | \k' | 3Sr | m2* | cMv | y#M | 7i6 | >C~ | Zb2 | kdb | :"8 | Z@u | n?R | 6>D | kRE | L5^ | cQ. | q\|j | UPd |
| x4< | v,g | b~5 | rA$ | 5b! | Q!9 | wjA | Tu# | t98 | 8(% | ~bO | dL* | ptA | +Uu | ynA | EHr | U96 | yoV | s75 | +Qd | Bq} | wN# | 9Rr | )m$ | \|Rg | v2y |
| u_J | 5N& | Q0w | r`1 | =}S | mM= | mY9 | \\j | rER | EV/ | `(. | N]7 | E2% | D< | 6lx | o%e | TxD | WKR | !;9 | "Oa | m8( | VM4 | "9h | ]ZI | 4L/ | I4W |
| ;[g | IAF | Tr% | Vjc | [t: | 7T@ | -Ty | 5kt | ,qJ | p=^ | \zo | ]{c | c*6 | ~SJ | G'Y | ou= | ,<v | .ML | FA$ | hc( | FmO | y\` | &'Y | .uz | *%b | -s@ |
| zs> | 3>Y | i%( | ^HJ | L/b | Fz( | 9KC | H^q | tH- | ?k[ | s]! | C\|T | y!3 | zr4 | deu | Q'G | Rlx | -;C | h?W | ^,o | +$& | /3S | yDV | f7q | 9,} | ?8J |
| pUB | =P+ | ^>3 | !Aa | O=: | g#d | PPw | S}? | ?K) | 120 | BT8 | \|WJ | S7w | aD* | !4( | 3I# | ]'y | u[_ | le_ | .+f | coI | (!- | <]W | {/3 | qGP | w`[ |
| !Ba | gJS | Zks | .4d | P2D | kD" | `.L | As+ | l"& | $kt | `C6 | M(X | z8u | {0u | d^U | AwE | !Y% | ]8R | +zO | >4Z | f8W | OGi | e/M | Z]: | ;B& | cH% |
| P{Q | U._ | br2 | Y5o | s{o | sm} | )nj | e2L | R?z | a(N | 2dj | lz4 | ]e> | `n> | $LV | ILV | fc' | FMH | 9Gb | $nZ | 9S. | ;gG | 3A0 | Ou" | &`T | /Uh |
| 23t | hOc | oo: | ).O | h(G | @tc | Nff | Iwr | !pE | ir- | ^9$ | Yzj | ~y< | {Ht | "8, | I+8 | *& | &-H | xJ$ | ?:o | pQ, | F2- | fo* | XR9 | XE^ | Q`P |
| @s> | b@3 | WwM | qy~ | \#] | xDU | Ta# | GVC | K7i | {&6 | Z~S | CH3 | Ir~ | Exk | APp | fSI | RR` | @Dm | !?B | g;j | G8@ | F$\| | A!# | B$2 | ?@+ | (-q |

*Tabela 21 – Tabela 8 de conversão de sequências gráficas em sequências alfanuméricas*

| }sf | '.+ | kgV | FJ0 | u$c | -ZT | aL9 | ~m> | =Y7 | u#? | aZr | :sZ | KzU | Fl# | HzY | K" | {f~ | i3m | *$* | ^jh | 'YQ | 1*4 | lHq | p\|c | &zR | <yl |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| QZL | (xi | :x" | 55# | ?+V | MXA | X28 | NO+ | imW | Bwk | q\|u | s>9 | dUr | gBQ | !RP | 0st | YmO | +ng | O#a | QUK | .}& | s.R | vdQ | f3R | ^uP | xk4 |
| WKS | %\|$ | >m[ | zt@ | $[a | %z) | Rw# | R&Q | -{u | (Y5 | x%E | Hc+ | ;s& | !(% | x]i | [J7 | ^"m | _;- | R5N | GH# | %a~ | xRT | jeT | um8 | QPw | z^p |
| \~Y | x4: | *s | f/= | Vp/ | %Ha | it, | :8F | Avm | Cv- | v~M | VNM | #7/ | 9L5 | 7B_ | HI5 | 3Dw | B!* | 7N4 | rc~ | R]a | 5BS | ]4Z | *69 | 6Y8 | S[e |
| '^y | T~{ | [3) | y:; | N`r | ;MP | N#U | ?=K | tlY | -KN | )?g | \([ | w6} | !%M | yb; | U_T | nxi | c,C | V8\ | %Ww | ~'Q | NDM | 73] | $Dj | U`j | 03J |
| NLE | jr: | qjj | %fx | o@* | *>. | s?p | tN/ | ^^n | RHe | -$y | MM[ | 'g: | T6! | YOz | *_: | NKU | 5z< | o!k | (@L | 3y. | lY^ | O;% | slf | tdq | /g3 |
| -n- | JR_ | 27u | /Em | bMn | $(t | yGN | 5J6 | 3\l | #y` | I], | \>p | c#l | X<w | u7d | !gM | gl8 | S{G | FhG | PRb | ]fL | >P5 | q`K | Sr+ | `k' | 5Q+ |
| 5:s | LKO | p/A | V'c | 1,Q | ,u` | c8) | po_ | `.w | 25r | ,Y? | 3QA | q?b | />t | U(U | MY: | 7L2 | 6p8 | =Pa | d}t | >)' | {h= | V!, | _UP | ~nW | y=8 |
| j`G | CuL | vn4 | PXh | uZn | A=] | Us} | R(c | 8Gd | j@4 | ?rv | =js | EuG | P^( | jkr | Q^* | >ZK | U:a | p#; | ]U5 | y:M | 5[r | ]u? | o?j | zhO | _=9 |
| i:h | \|_B | 'Gr | :9I | H.. | ,qi | 024 | r~4 | `x4 | <sE | hV\ | "'+ | 8a* | }*w | ]a? | Xv/ | M0K | o0; | >HV | lot | $Ru | @$C | ^Z* | W&L | 5^ | Yl= |
| qmS | #1" | @=S | rza | >L{ | T9G | ;BE | k+1 | eE9 | =2p | N"? | kK] | \CF | YP} | hNI | 53~ | )!I | 71M | j4~ | CXm | oaa | [*' | T&p | @lz | 7q% | #Y8 |
| $mY | 6t{ | tJ< | `~$ | Icu | 2Su | ry~ | ;qn | (EY | sKj | 8#\| | $_$ | 1G* | 3,7 | &oo | R;% | JzZ | TL} | NxK | {*b | a(n | ^yG | Hwl | d\|A | STS | 13M |
| >b: | ;oS | nxF | oTH | %Cj | H.o | &UP | [E$ | 7^, | `t4 | M4d | tT> | Vnx | *hs | 4k5 | 5~> | .i: | mMD | ro- | Mdm | *#, | C{v | dJ; | s6- | ";` | 'UB |
| eB# | z=0 | Atk | $RL | /No | '/1 | 03Y | J[; | .7g | JXo | 5\m | cQm | DQx | j,p | /k7 | Bs\| | cYf | ^UV | /$p | d([ | +U/ | _X? | lo: | _KE | qf* | 5Ku |
| 3xb | Wno | XsE | CdW | 2(i | P~X | g+p | }K& | DuM | -%- | 3]m | -n7 | Jo' | U*3 | gW3 | :\6 | !O{ | Qj} | {YV | SBj | <<\| | @[& | 9mx | wmr | 6l> | @L[ |
| F=g | gio | +>m | +~P | Wli | [7# | +[a | X0; | Kc' | .!^ | #jF | $LD | QAJ | VPh | ~Qh | hmn | /k\| | IIX | E8W | H;> | MD9 | FK) | _(, | `X# | +?X | -92 |
| 8WM | [@f | !lw | BkH | mrK | &6m | S4# | e~h | X!n | _J4 | adK | "57 | [v+ | b6c | [D[ | WC~ | 2\|- | F4` | wJn | !W- | hrU | sFk | 6{D | 2Kt | '8_ | R{b |
| -82 | B\|, | LZ" | r(- | 87s | Je2 | X9@ | P$n | $Yb | <I& | eGS | k?" | L9b | QWP | ,H! | v;U | LA! | T^U | Kk} | P<i | Y{$ | F1g | 7p= | 5KJ | ":f | ~T; |
| dIc | z:E | &A" | fVu | +2j | ~R@ | \c{ | `PS | Yds | <d5 | M1, | e]q | KA" | }]9 | 51T | Afd | VEB | INe | <Em | yE, | PN. | CYr | U*U | ed{ | Z_4 | {m7 |
| F^( | 0^Z | bwW | [E. | sz& | 6IP | I>y | {3; | {8& | $@O | QGi | 3:p | QBc | 746 | e'y | 1*_ | `q& | ]j6 | Eg& | uBi | N@m | %<. | J.X | H/1 | 'b8 | ~VW |

*Tabela 22 – Tabela 9 de conversão de sequências gráficas em sequências alfanuméricas*

| 0n} | g@6 | `90 | w6W | GW! | }mJ | D_^ | kcP | +e. | %bh | S3w | ypi | Zt[ | h{9 | S~\ | 2bn | GHU | '$3 | %,k | V/q | P\|X | >\A | ist | UfR | w,J | goB |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \|pr | $ZL | @5F | "75 | }x\| | ]`Y | <uG | EV> | O=C | NA> | lda | 8e5 | U@) | m#t | uRg | H4r | ]kg | igX | M9\| | "Ss | ^ol | `l& | Gm: | qJ# | _7" | f01 |
| Qb\ | usd | !oi | +fW | f)s | jMP | B}5 | OEU | S&7 | =S< | 3eu | #3' | j&E | 8%m | Lc2 | {\|m | OO' | V&3 | 7@8 | 1ij | Z$} | !}Z | 3@M | \|lD | U:* | \|Yb |
| 5.i | Jy3 | *G+ | "@X | 5;4 | hf_ | vQp | EsS | aSj | Z[m | WB[ | :_T | )lO | 6Hc | _:9 | !(L | /#$ | pty | TT( | (.? | *A5 | Mdt | i_; | 2YH | =m~ | '0? |
| dUl | Q[N | nZJ | g>$ | ^qn | 'gm | >PK | opd | !R! | C4' | '/t | I>G | =iE | m$2 | tpu | NY0 | !Nr | (>_ | ,\|] | -AA | &<; | i~9 | ytc | R71 | wH0 | LKf |
| LGb | cyK | "Q} | fat | y>U | A&J | {Xw | Z88 | [#- | \7k | <ZF | K-Z | X)r | -v9 | o5X | 1B6 | 3l\ | ^<A | *K& | U$* | )G5 | Pn/ | /tp | [l) | pu- | !hP |
| #CW | &+3 | 6ik | S.g | lV[ | o\|M | f\|[ | gs` | wN_ | =oE | VF\ | 9%+ | \-e | G4- | 2%K | 0nA | @R$ | `-v | 5tn | 9H. | [++ | =DL | B`` | =Mo | ]*p | aog |
| LKU | ^jn | )n8 | $TL | Dwi | (]e | o~- | $5N | e>\| | a"f | "5x | aCM | mw8 | 8O{ | ~9\ | fW~ | 1.X | hI> | ^u+ | 3YY | &@6 | fFs | >X0 | P8_ | e!; | Mm. |
| qs~ | n36 | u}\ | vCV | %9. | v7U | %Cs | c#x | Ek" | !zC | ??b | sDX | Oo. | H1\ | b$O | -Zx | NF. | Hn^ | mIP | :b, | 2+L | -?" | 7HP | 6(" | FX5 | $@p |
| E?S | (GB | D#8 | JC. | ma] | '#8 | wZ@ | ]~t | Wtm | ;[6 | #W; | [T6 | 3'% | o~J | Y*: | UJL | 'lt | DF# | @4Y | o$: | [ll | Xhs | 6@" | h]v | NHY | j4s |
| "8M | 6K: | "JD | +tm | n@? | ;)/ | Zb% | ]`( | N)1 | 5:4 | =mO | /.1 | hlK | yS] | :Z/ | DS\| | q/; | {c6 | )Fn | (BY | &OT | j\d | -%g | ;2D | v!u | *bJ |
| ?C< | Ug% | F-: | ^e- | Q[L | ]>; | PkO | hg~ | <1~ | EN> | <~d | 3@u | jX0 | eX; | ou; | J}v | s^a | =:O | -.x | Q$: | {GC | P^L | uF= | =na | HLU | =)B |
| Yss | }'! | dR: | !sW | $;9 | eq= | ~0` | bn. | tOt | de+ | PP\ | Kyt | _1_ | D]` | <&, | @zv | c8[ | ~Mo | m^: | hNX | Fo- | jR} | e)d | 0i+ | O=P | `3n |
| _(U | 2^H | 3c\ | {Yi | f;[ | h"[ | ;_N | ig. | $kU | z2l | (W& | PhI | "cu | {dO | ;$Z | oVR | C~T | 7E2 | F[ | M@D | `Je | MXa | C69 | L,* | =bA | %\1 |
| =g/ | f+C | {D5 | ihP | j2Z | FIN | tYy | v^- | d1z | G~z | q!t | e#) | UCy | ZJx | =O* | [z_ | p~c | jQf | lK+ | vq~ | _R' | Dj. | YQT | Z-d | X2* | BPV |
| (yU | r_b | )NH | fFn | jI~ | 11c | M+g | fc} | :_v | -ov | f8= | e-b | 4"Z | 7/% | :'@ | u\|] | P:j | iYL | X8T | QA6 | JOt | !@b | Zus | %y: | /[x | gwt |
| ndX | I=` | cx, | g%` | tk6 | }SK | M^I | (`0 | z4O | NUg | GtP | GB} | Db[ | Y*- | (mX | ~Qx | 6rX | ZX+ | 8Bz | PJ1 | )-( | %J0 | iCk | W+V | }@: | xVj |
| @ad | AH= | z$4 | +eI | i&H | [#( | iTT | 8Os | :{! | Q/< | q3= | Bo9 | n-I | !I? | I`4 | ZK6 | hO] | ;\|q | oPP | q1> | KG1 | UU& | 3j' | o"m | &mN | )ng |
| @iv | N[@ | ;2% | =+i | 7@z | @^a | 8]a | kwo | !p! | =pZ | <+U | "N! | iHi | Isg | Tx^ | V-N | Mj: | Ku_ | "a) | pSN | dMu | gTX | 0IA | !Uo | [5i | ;!\| |
| %;# | .K+ | J*B | WIR | t-O | ,5E | @w- | `Xv | ->& | G3i | $zF | >LW | yCD | #J^ | Np9 | 61) | 't, | gA, | }e- | <X4 | ]_? | Sf9 | N\9 | :.{ | gL[ | "6/ |

*Tabela 23 – Tabela 10 de conversão de sequências gráficas em sequências alfanuméricas*

| L;z | CP" | %}z | -i& | ki: | z`$ | 9:' | \Ls | 'y< | lMs | pQK | ZB} | wma | `CZ | `!C | X1+ | qM: | Z+V | Tzx | 5k; | kBN | rw< | pyx | O)n | .8p | BtA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| #+# | SjU | }EX | mHg | -dH | BKd | Fiu | mC( | !#5 | T!3 | skO | TB\ | oyf | C;$ | n{Y | !~y | "}, | J[! | Vkg | _n. | TR% | q"o | F=t | 2\q | F:r | ;?0 |
| 197 | h!d | ,dF | W%e | t`E | Fi; | !Hf | d3i | .I, | [Ew | #&} | YzN | +CL | 'o` | sR: | l#X | D)D | )cQ | \VM | 9UD | {{W | #qH | *5J | b\A | 0:g | `@$ |
| 8mS | Ar_ | XQ\ | 37v | ]e. | -B] | m"Q | :vY | IP4 | zAB | in( | yup | =zK | f\c | G22 | c-p | ^[! | e3$ | \B; | D6U | a~< | 1gV | sVK | ~J; | q>N | rO\ |
| oKx | ,^N | H:! | {`k | ^{\ | :h$ | _P$ | e#u | qfk | rwu | n-5 | kEY | y9T | M6{ | <tW | 1J+ | A]" | 4`I | M^N | Z4d | bZ9 | E.. | B5t | u#a | MiC | hKz |
| /B1 | J_2 | y1w | )6r | !(5 | M<P | .w$ | ZED | M]g | M)/ | x~h | Pcy | ,.r | w^P | oAN | gq} | \|BU | c+\| | f{S | :z4 | G(B | o\Y | Y6` | RAi | Sa* | z#t |
| 0(S | "uW | g<. | U'/ | P\K | fV8 | k"p | V-C | mRg | ohY | L]: | ueL | 6^[ | FG5 | p0; | uN} | UbJ | ..: | zhv | hw4 | T3> | &8W | ~ _F | h[- | j3< | 5m0 |
| )\/ | }S* | wB~ | \Dq | >U? | "rZ | /0< | J8? | Ohn | EXc | b<E | (ZP | pf; | $\m | $/? | %`` | lUx | (!" | 7CE | '=o | y02 | `+d | &$( | w^! | qWR | ]"x |
| {8x | J_' | k!S | <pE | 7Y3 | j?R | U.v | y,S | SkP | z2j | ~]> | (q) | NVx | >Jx | 4l< | X,r | BIO | f?, | n/F | wCK | [e! | em~ | Jm> | a8o | T)> | .nm |
| VuL | M_4 | t2! | c=: | >6Y | V94 | Ve" | zS@ | \X[ | g]b | `VP | o^q | 8?" | [8M | 7i? | u1% | [?G | @FW | RG$ | rUU | cHt | fA" | *MW | gN, | @?$ | ESr |
| DUZ | a\| | .-% | U?: | pOa | &a5 | ?Qn | "jy | X@~ | HR2 | g(6 | I=^ | ^[C | MeV | ;.n | ~~# | ;#5 | NHO | m&f | a{x | {s< | $# | HI= | h3' | XO+ | 2#O |
| k]T | [13 | 5}} | (k> | {[K | GU] | Gf) | eNI | jw! | i/i | ov' | s/- | SL_ | Y-- | i:P | -$m | yw^ | 5IT | (Cm | _3U | ~%( | <w\ | 09h | /]j | 8fp | wR: |
| tX~ | rAa | Q\c | ^`} | <[x | A>A | qTs | Y< | /WD | pjK | -Ky | e3E | Cep | fZZ | ~@, | O(2 | sWT | kV= | V^C | k\J | JJO | 3@< | SAg | []F | 0}\| | Cg" |
| lRX | ne# | 9m] | jA\ | ,@k | +Vr | ]&, | OMZ | n{j | 9". | WD' | 7LO | pq5 | C`i | 9fe | l6j | >+" | 2[\| | oB_ | d)= | ?:J | Au\ | i{G | 9=. | onp | N+z |
| CSV | 0oS | $5/ | No1 | GJj | YZF | ?Ub | m?7 | ssx | @kj | 5b> | 7(` | w{K | V=u | ?sS | v+g | J_w | 5Dp | MtX | xSJ | njm | fcO | O5z | 8iZ | W%p | #H2 |
| [3} | uFM | '^J | UTC | ZAU | *$) | AIZ | ;~= | RuR | #rO | .\m | >h` | ,UY | HEc | ]X% | j;0 | r#@ | RJY | AEz | gV' | $n | STS | l{/ | g9Y | w=B | d*w |
| -xj | 68G | ]g1 | Poz | K0x | c?s | &<\ | A.$ | FJH | 5LI | V?H | kBZ | 9Z! | _ZY | L}y | Y.e | P.) | E.& | "O\| | @?D | FLU | []$ | $xC | ^-S | Tc3 | >00 |
| ~t\ | X(M | D/# | PED | u?@ | 01+ | ?DX | e-t | VJi | 4`] | !06 | WP} | Izu | %q< | 1es | !m1 | ^0; | F:j | zEq | h6_ | k7# | 1&v | hB% | 5^" | .F3 | u+L |
| rB, | ep+ | IDi | B1% | /<. | -]" | } j | C^~ | GhT | F{? | Ma\| | %x0 | H]? | `IP | ^(1 | k[P | jg\| | i<I | 8Zy | &"U | Q:A | .mO | p+B | (jn | g,a |
| Kr) | tXa | 5%H | @0E | Tf# | !Ty | O_z | 6u/ | X[x | I}; | M-; | ?k- | kMy | 9KA | )T; | SI- | ?F8 | sh' | %@\| | rcK | O^n | >H; | {Q1 | L\|^ | $'+ | eLu |

*Tabela 24 – Tabela 11 de conversão de sequências gráficas em sequências alfanuméricas*

| /6L | j>y | Ibd | (ww | x+P | ;[S | ^p] | HNy | tRY | p1~ | Mjv | Z"5 | UtJ | 1(a | 3!+ | Knh | yoi | Yk; | *H} | lEm | v7Q | &~$ | Zt5 | a]8 | `&z | pDi |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *]n | wr\| | @G. | h1} | 7,D | T0G | g;s | <Z@ | jLd | UT5 | \|zc | b=^ | xiF | `]v | 'JW | 3WC | =in | kdm | [8I | qsL | ?f# | Q?t | GO1 | R^W | Sdf | *6' |
| qFd | Qq_ | d]; | KD& | YN3 | !m/ | 7TC | Yzx | >4I | xpl | ^/e | vla | 5Yv | 7]a | C;= | HO_ | HgC | !zw | XCg | 4R+ | kw* | 49b | \o! | i_} | 9@n | ywl |
| vxj | jdx | Hb* | 5y? | gq. | eo. | ?0v | f"K | C&j | E{[ | YUx | UfO | ~7P | b,K | g6m | Y2R | >zH | ysr | y#F | 9M~ | j6d | $8k | XVY | P8f | 0y% | cl) |
| 1m$ | Kn+ | =9' | STm | Hg^ | R#7 | cpm | 1${ | 5`g | do= | :V | Q/\ | MX% | sDA | 8\g | dK< | 1i` | To[ | a,; | {<% | *31 | U37 | a>C | JQV | uAM | py+ |
| W?) | oX[ | P5k | ~G, | T/d | huC | ->R | ,ba | a2" | v95 | S5s | k\q | m*@ | /Bf | +>I | *5c | {3@ | 2tB | _*c | (uc | }^m | #6a | 'Yx | gd3 | Mz` | {}E |
| H:W | Ve- | x3l | <'k | /ez | UGO | UV. | ejQ | ^-[ | {<f | hkh | UNz | m"\ | PA+ | eN@ | G+: | O\|0 | ={0 | {<_ | OT: | la? | +L\ | A<B | 4h> | w)+ | $$a |
| 3BP | W$e | T[t | G(3 | U_L | (tO | f(F | ~Dq | -\w | okn | Y4< | ed= | mkx | ?:Y | t_\| | s+5 | X5s | TNz | _uO | mgJ | Ux- | _7y | /&Y | Hp2 | >h@ | )y% |
| l5N | TLG | Z(v | f,6 | .b5 | %ce | ,_F | c>_ | h!p | ,a. | C.H | MO] | K~N | 3z\ | j-3 | ^'T | $"\| | Kz* | 98: | Q~* | vdV | kf~ | 2G[ | 8$r | A7s | O%e |
| 9j" | %^% | N{. | dab | K]I | "Bl | wT. | 22$ | keI | )! | =`z | "JO | v\i | Ibl | {M~ | [VF | lO3 | STp | Y'6 | pE# | (bn | i-& | U}V | qFp | ]v` | hU4 |
| H_G | (#c | VXS | '6u | %Ys | $^ | {o[ | p6X | >@k | e>U | /"\| | b;e | 4vg | k\Y | Q;v | x/j | /CU | @0F | Kr: | F}r | #et | fw: | 81P | $bQ | :/u | V'S |
| K;@ | %!u | @~A | ~?% | =Ct | oYD | D^z | Aa~ | <J6 | /d= | ylV | rHG | 9Pf | 5C; | w;$ | c;~ | NVm | 8}p | 7]Z | KMB | >2k | skd | @)L | cpx | 34^ | ~j4 |
| n,b | 7`3 | L\? | iY* | zOJ | $JQ | A)d | BL2 | X*u | g#X | 0`g | R_Q | l"I | r'1 | )8@ | !;V | 23- | sM\ | * M | 1wU | AWV | 4Tq | (d: | CH& | Ylg | >E3 |
| 5WT | I>Z | J$; | xSu | \Y# | m=+ | F}A | 2(T | LBh | {e. | J!X | 3*2 | GCt | `q | w+i | W7M | ;wY | X5t | I<m | !?` | %VB | D\O | xh< | B7H | +Yx | bw: |
| bZ0 | {{? | t;% | 5Mp | m%v | '* | y;< | [[\| | PMB | W-b | \80 | $T= | O/9 | H0i | [aS | WO' | 29a | $zT | <'@ | R^! | fxo | ,$i | i"f | PB< | -'x | KUX |
| >~* | $bv | g8Q | ewk | KWc | Qrl | K:B | )W( | Ov< | i<j | X4I | 6;N | *Dj | 86e | *6> | 6c} | l,y | jXF | _Ud | d}e | roL | \uk | Y4. | !mb | \aq | z8B |
| 94_ | Ff' | L33 | DkM | `2j | i6v | !S0 | >[* | $>B | 4*\| | @&_ | Sx8 | 1O7 | suI | -C( | !fD | 5:. | qA= | gnm | TY& | "Va | AC$ | F54 | G>P | 'aa | .jR |
| E`@ | JjQ | y#` | _+/ | Q9t | -z' | D\O | ]nd | rF; | &9y | X-] | TJ* | _s7 | M!+ | }"2 | fAe | `bc | CsO | YL\ | ^f6 | bD0 | up2 | ar- | ~Dy | Oe^ | dpP |
| \|i, | NRt | <H" | `f[ | UA) | UNL | 'F= | MHf | RMo | Dm$ | ov! | QDa | k\2 | 1I< | pPk | \ol | MkG | U&0 | 5Qu | h\|F | "J{ | K'Y | e8W | T.a | dn_ | bac |
| Zi" | VQ^ | f4n | &zt | Q4U | H&> | G<h | &8; | {ZB | fnv | Mc% | _N~ | \|n5 | [-p | xM! | 7t/ | Tol | -\o | (si | G#9 | _h8 | d~k | V;z | C68 | 2h: | -EO |

*Tabela 25 – Tabela 12 de conversão de sequências gráficas em sequências alfanuméricas*

| aas | )<J | W"c | FoK | O+d | e{x | Jp7 | `ra | ,n' | g[` | K~P | ];g | 'Jn | [~r | lsd | vzF | #(D | a}V | ?x( | l`J | #!O | TUL | qvD | fQ] | t0? | gnC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kor | ,:n | 3)N | c,' | U6B | H9_ | i*S | +wv | Z?Z | :$f | nAr | 2v+ | :6J | [*- | -g% | RxD | 2k* | gm8 | {>x | X:U | 8Gg | A'g | u9c | 6dL | /dB | mKZ |
| e)O | FAe | HKL | zZ0 | V+C | KUp | `2T | m?( | ,GQ | ke; | D[R | 9NY | D7t | ]Yd | #^9 | iZf | !?= | ]UJ | h)L | QrA | K*2 | @G. | ]{. | UmD | =yk | a<? |
| %s# | A%z | %e4 | 91Q | 903 | 9M- | pbJ | jOG | .~D | J7R | 2"6 | z%M | #_% | .KT | SxM | K,_ | RCH | ,c? | *tW | T%0 | ?1/ | OSw | V[_ | [Ji | <Bw | #_6 |
| Bc" | Ux9 | SJp | ]9A | @yk | p}6 | -FP | \`i | @b0 | '3v | p&n | )vs | "5G | GP, | e`m | h^\| | 9fW | :aS | yfO | 8.p | kmD | lh& | rbp | m~G | (Gp | dOe |
| 0r> | 53@ | c]] | .^d | (/u | TmP | tx& | Gv[ | J2g | -1= | #f( | w/s | `J/ | -E- | lU% | P,Q | W/6 | /'$ | s6[ | a- | `}P | Gb( | GF" | .k~ | Q5C | cWa |
| E9v | Q,J | R6m | '0$ | jRq | 4SU | sd% | tc0 | nwS | 5mS | uFs | 5xf | {MG | 6i[ | YB; | ]Y7 | ;%X | ]n` | HCN | 53w | @o* | -Gv | \o# | Nr\ | TXT | J/a |
| U9: | q{. | Jo} | [Iq | Ke; | :P/ | K\= | ky_ | B0P | H0f | HRX | _4- | l5$ | ga7 | 6t; | eR@ | \|5} | C"= | i_# | ~=/ | xHO | U&M | xh} | \|N3 | /`_ | LY> |
| r[H | sQE | T<i | %u= | <{. | F72 | NU@ | }_p | 25" | K@y | fnT | kcp | -(c | g9c | =<k | KQ` | mS_ | %2j | xo0 | d15 | 1rV | &+% | ^57 | o") | Sgr | }w~ |
| `y_ | 'Mu | FY( | rkc | E!B | Y/= | W3] | phG | E<A | [8A | aZD | Q$: | mb# | :{# | "xk | K:e | evn | #80 | wF5 | XPA | rAX | nR1 | J>8 | 'rd | ;eo | DfR |
| Siz | .=! | i52 | KRI | {$= | e#\ | 6i6 | #s_ | s_$ | !`X | nZ_ | ,VY | ~ti | (3q | llG | SzW | aWp | `[D | y/: | Hr# | v^Q | ^N? | @}R | [$] | \A` | \MR |
| P[x | W9h | 0A' | x(" | SYU | 7=[ | MmU | Fa8 | 6L+ | UVO | ]:w | dx1 | 0yK | V10 | w@p | F.+ | Ed% | nz* | `G- | 8I} | @23 | yO} | E3R | f,0 | GTl | NUv |
| "$ | Mhh | `^[ | ^c> | y:Q | w?, | XGO | gWi | 5&Y | jXx | 47F | `.o | \6U | RqK | v){ | -4` | (S- | :22 | m=@ | !{z | vsV | )d( | /UJ | s]@ | Xeq | NbN |
| s16 | V3= | ?O> | fH0 | Tf` | bjX | sMQ | ]1N | "L, | [30 | nIb | x1! | qu} | UMV | ^Na | FkL | zi[ | F2. | "bY | p+, | Y;2 | GLv | NcP | `BV | tG@ | yzJ |
| yaf | Cu? | y@r | BE= | "MX | Jar | YKd | Q`\| | 9m[ | 5=G | cfO | [li | $Xr | )#M | G3L | fD8 | s67 | FiR | Vmq | *yY | 7Co | Gg_ | X.~ | }?) | @[( | 1_f |
| j;! | KcE | 3JK | _}y | *"1 | z&Q | `UP | B3M | ^R< | q#9 | ^`d | `5c | Z;T | O>- | Rfz | //J | z;W | )*T | ynQ | lgO | &[V | @b6 | GG6 | (v_ | wu: | /uF |
| AI) | k~c | Y7e | TjE | QP1 | =31 | 5yp | ip` | Mjs | &Ms | h^n | XLU | 5+T | }:[ | }36 | nO> | Z)l | :_h | 0;K | !<V | axw | 4C> | ^]9 | )\= | v`) | ~)]y |
| JRk | W*C | ]+g | Rf& | \|L. | yHQ | yTq | oq> | X#< | O1b | nN> | KcX | tK+ | 9), | `u" | KH\ | ^Em | [>- | ZDH | A]< | f\* | 2\e | uz` | z`c | x)7 | s$Q |
| jr5 | WUN | @!p | ;\4 | Wk- | h2$ | _:z | 3'c | XNz | +X< | s-p | N^\ | BP^ | ^J) | p/x | s"S | 6[p | J/, | m~u | ~+= | o`@ | r@j | _7c | (v9 | m>L | "b\| |
| T8h | KbR | *9< | z4S | 6V. | AB> | A'o | 1^C | (%@ | W%N | %CH | {)B | MZv | aPd | /1h | B_\| | ?S> | u\|N | %4; | ao" | P${ | _Wk | bu3 | r%9 | trR | Jhd |

*Tabela 26 – Tabela 13 de conversão de sequências gráficas em sequências alfanuméricas*