Uma Reflexão Sobre a Segurança nas Comunicações

Tenente-coronel
António José Caessa Alves do Sacramento

Enquadramento da segurança das comunicações

A palavra "segurança" é empregue na língua portuguesa com múltiplos sentidos, pelo que a consideramos uma palavra delicada. Parece-nos assim adequado começar por apresentar uma breve introdução ao conceito de segurança sobre que nos propomos efectuar algumas considerações, ao longo deste artigo.

A palavra "segurança" é empregue, por exemplo, quando analisamos a capacidade de resistência à intrusão de um determinado edifício, por hipotéticos assaltantes. Diremos então que tal edifício será mais ou menos seguro, consoante o maior ou menor grau de resistência avaliada. Também empregamos o termo "segurança", ao analisarmos algumas características observadas na estrada de acesso a esse mesmo edifício e nos referimos, por exemplo, à ausência de sinalização específica que alerte da existência de curvas apertadas com bermas abruptas e não protegidas por *rails*. Estas "seguranças" são obviamente distintas.

No primeiro caso, exemplo da intrusão, estaremos a analisar a forma de impedir uma acção directa, uma intenção de um ou vários indivíduos terem acesso intencional a esse edifício e ao que de valor (humano, material ou de informação) nele possa ser obtido. No segundo caso, estaremos a falar de acções indirectas, sem intervenção intencional humana. No primeiro caso estamos a falar da segurança a que corresponde na língua inglesa o vocábulo *security* e, no segundo, ao vocábulo *safety*. A complementaridade dos dois conceitos pode ser exemplificado pela expressão seguinte:

(Segurança) $_{\text{Português}}$ = (*Safety* + *Security*) $_{\text{Inglês}}$

Safety pode traduzir-se por um conjunto de meios humanos, técnicos e de procedimentos que visam evitar acidentes/incidentes não originados pela acção humana intencional. *Security* será o conjunto de meios humanos, técnicos e de procedimentos que visam evitar acidentes/incidentes provocados intencionalmente pela acção humana.

A segurança militar enquadra-se tipicamente no conceito de *security*, mas não em exclusivo. Nos tempos mais recentes ela tem vindo a englobar algumas áreas conceptualmente enquadradas na *safety*, como se observa, por exemplo, quando as unidades militares elaboram planos de prevenção contra catástrofes naturais, ou naturalmente cumprem com as normas de prevenção de acidentes e segurança no trabalho nos diversos órgãos das suas instituições em que esta obrigatoriedade se enquadra.

A segurança militar é fundamentada em doutrina e gerida por normas e procedimentos e ao seu não cumprimento estão sempre associadas sanções que poderão vir a ser do foro disciplinar ou criminal. Tanto a quem cria as normas reguladoras da segurança como a quem observa o seu cumprimento (inspectores), são muitas vezes encarados como entidades que exercem "poder", o que, em nossa opinião, constitui um conceito errado. A segurança em si, não é poder. A segurança associada a um sistema de informação e comunicações (SIC)[1] militares, que apoia o comando, controlo, comunicações, informações e redes de computadores, conferindo-lhe confidencialidade, integridade, disponibilidade e não repúdio da comunicação, veicula a decisão e a capacidade de comando de quem efectivamente exerce o poder.

A função de inspecção da segurança, para além da supervisão técnica e disciplinar, deverá também possuir uma faceta de cariz didáctico, de aconselhamento e orientação, no sentido do cumprimento das normas, que devem ser naturalmente sempre exequíveis. Para o aperfeiçoamento do nível de segurança, é imprescindível a existência de uma consciência de segurança que só se alcança mediante a contínua prática da sensibilização para possíveis ameaças, a detecção de vulnerabilidades, a análise dos riscos com implementação das respectivas medidas correctivas e através de uma adequada e fundamental formação em segurança.

A segurança pode ser analisada e executada a vários níveis, também designados por escalões. O nível estratégico é o de maior dimensão, onde os intervenientes são estados ou nações e suas associações. Internamente aos estados, existe um nível inferior que constitui o domínio das polícias. A segurança militar é uma segurança protectiva, por vezes também referida como segurança "intra-muros" e engloba quatro áreas distintas: segurança física, segurança do pessoal, segurança da informação e segurança das matérias classificadas.

A segurança da informação designa-se em terminologia OTAN por INFOSEC (*Information Security*) e visa a aplicação de medidas de segurança para protecção da informação processada, armazenada ou transmitida nos sistemas de informação e comunicações, ou qualquer outro sistema electrónico (por exemplo, sistemas de sensores), contra a perda de confidencialidade, integridade, disponibilidade e para prevenir a perda de integridade ou disponibilidade dos próprios sistemas.

A segurança da informação compreende a segurança dos computadores (COMPUSEC - *Computer Security*) e a segurança das comunicações (COMSEC - *Communications*

Security).

A COMPUSEC visa a aplicação de medidas de segurança do hardware, software e firmware de um computador ou sistema de computadores, com a finalidade de proteger ou prevenir a ocorrência não autorizada da divulgação, manipulação, alteração, ou interrupção de acesso da informação.

A COMSEC visa a aplicação de medidas de segurança das comunicações, de forma a negar a pessoas não autorizadas o acesso a informação valiosa, que poderá derivar da sua posse ou estudo, ou assegurar a autenticidade dessas comunicações. Tais medidas incluem sistemas cripto.

A COMSEC subdivide-se em três áreas: a segurança da emissão (EMSEC - *Emition Security*), a segurança da transmissão (TRANSEC - *Transmition Security*) e a segurança criptográfica (CRYPTOSEC - *Cryptografic Security*). A EMSEC visa assegurar que a ocorrência de radiações comprometedoras fique confinada a certas áreas limitadas, pelo que serão áreas classificadas, aplicando técnicas específicas, contra a captura de informação, através da intercepção e análise, por parte de quem não esteja autorizado. A TRANSEC consiste na aplicação de medidas de segurança destinadas a proteger as transmissões da intercepção não autorizada, análise de tráfego e mistificação, evitando a exploração da informação, por outras técnicas que não a análise criptográfica. A CRYPTOSEC resulta da escolha, tecnicamente perfeita, dos sistemas criptográficos e da sua utilização apropriada.

As técnicas de transformar uma mensagem noutra representação sem significado, excepto para quem conheça o processo de reverter essa transformação, já existe há muito tempo. Os antigos espartanos já cifravam as suas mensagens militares. Uma das mais antigas cifras que se conhece é a cifra de César, cujo nome advém da sua utilização por Júlio César. A criptografia constitui a actividade da cifragem e da decifragem. Vem da palavra grega *kryptos* que significa "escondida" e *graphia* cujo significado é "escrever". À ciência que estuda a criptografia chama-se criptologia.

Os meios utilizados pela criptografia destinam-se à codificação (e descodificação) da informação, para o que lhe é aplicado um algoritmo de criptografia, de que resulta uma cifra. As cifras utilizadas antes do aparecimento dos computadores tinham como unidade de manipulação o caracter, ou seja, limitavam-se à substituição de um caracter por outro. Assim se processava na célebre máquina de cifra "Enigma" utilizada na Segunda Guerra Mundial (1939-45). Hoje em dia, com o recurso aos computadores, um caracter é codificado por vários bits (8, 16, 32, 64, ...) e os algoritmos de criptografia implementados mantêm as operações básicas de encriptação da informação para obtenção do criptograma e desencriptação deste, mas passou-se a ter como unidade de manipulação o "bit".

Se historicamente a criptografia tinha aplicação nas trocas de informação no campo da então chamada "espionagem" dos líderes militares e da diplomacia, a moderna criptografia fornece mecanismos que permitem muito mais a manutenção do "segredo".

Actualmente a criptografia fornece um conjunto de aplicações em novas áreas, tais como: autenticação, assinatura digital, e-Currency (dinheiro electrónico ou dinheiro digital), e-Voting (votação electrónica). A criptografia tem-se desenvolvido de tal forma que se tem vindo a impor como uma nova especialização da engenharia, constituindo uma arma poderosa para fornecer privacidade (confidencialidade), autenticidade e integridade à informação, permitindo a sua troca em links de comunicações não classificados do domínio público e com custos de utilização muito baixos, como os que hoje se verificam na utilização da WWW.

Tendo-nos já referido às áreas que tradicionalmente caracterizam a segurança militar, existe uma outra, que não sendo uma área especificamente militar, é também considerada tanto pelas normas e regulamentos da OTAN como pela legislação nacional relativa a segurança. Referimo-nos à segurança industrial. O SECNAC 2 aprovado pela Resolução do Conselho de Ministros nº 37/89 de 24 de Outubro define as *Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Industrial, Tecnológica e de Investigação.* A Autoridade Nacional de Segurança (ANS) Portuguesa tem competências relativamente à segurança industrial, à coordenação, credenciação e inspecção do cumprimento das normas de segurança, bem como quanto a propostas de alteração e revisão das mesmas.

No mundo competitivo dos diversos sectores industriais, são inúmeras as empresas que continuamente concorrem para objectivos comuns, pretendendo alcançar o seu sucesso empresarial (com objectivos de lucro financeiro) o que pode implicar a falência de outras. O não cumprimento das normas de segurança por determinada empresa, acabará por fornecer assinaláveis vantagens aos seus concorrentes. Quando uma empresa facilita informação, seja ela relativa aos seus objectivos a alcançar a curto, médio ou longo prazo, ou permite o acesso a dados importantes sobre as áreas de investigação ou intervenção, estará indubitavelmente a oferecer informação vital, que poderá vir a por em risco a sua própria existência.

Os ataques da espionagem industrial têm motivações precisas: ganhar vantagem competitiva sobre a concorrência, roubando segredos dos concorrentes. Empresas da China, França, Rússia, EUA e outros países roubam segredos tecnológicos aos concorrentes estrangeiros. Uma empresa amoral, mas racional, investe fundos na espionagem industrial, consciente do elevado retorno do investimento, porque tal pode representar apenas uma parte do investimento necessário à investigação e desenvolvimento. A tolerância ao risco é média, porque a reputação de uma empresa seria abalada se fosse apanhada a espiar uma concorrente [2].

Longe vão os tempos (tecnologicamente), em que se comunicava pelo telefone de Alexander Graham Bell[3]. Nos dias de hoje, os terminais para troca de informação baseiam-se em tecnologias digitais, ampla e profundamente estudadas, sendo desenvolvidas, produzidas e comercializadas por grandes grupos económicos, que colocam esses equipamentos a preços de mercado extremamente competitivos, encontrando-se ao alcance de praticamente todas as empresas e organizações, como de

grande parte dos cidadãos. Actualmente a troca de informação pode ser executada por equipamentos terminais de diversos tipos, como: um telefone; um computador que pode transmitir texto, voz, áudio, imagem parada ou vídeo; uma fotocopiadora ou um *scanner*; ou um equipamento que execute multi-funções.

O amplo acesso à informação e a sua capacidade de troca, a nível global, constitui uma característica bem marcante da sociedade em que vivemos.

> *O rápido desenvolvimento das Tecnologias da Informação e das Comunicações (TIC) tornando o mundo muito mais aberto, conduziu ao desenvolvimento e afirmação de um novo modelo de sociedade: a Sociedade da Informação, como um modo de desenvolvimento económico e social em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação da informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenham um papel central na vida dos cidadãos* [4].
>
> *A amplitude e o valor da informação, hoje, numa sociedade globalizante, têm impacto aos seus diversos níveis - económico, político, cultural, social e também militar. Há que considerar e reflectir os aspectos conflituais da informação, e que se enquadram no tipo da Guerra de Informação* [5].

Quem intercepta as comunicações?

No domínio dos padrões tecnológicos mais actualizados, a informação a trocar entre dois terminais, que indiferentemente poderão estar localizados em qualquer parte do mundo, começará por ser digitalizada (convertida em "bits") num dos terminais e a transmissão para o seu exterior inicia-se pelo envio dessa informação para uma LAN, normalmente constituída por uma rede "estruturada" da organização a que pertence, podendo o transporte dessa informação prosseguir através de uma MAN ou WAN. Normalmente os terminais ligam-se à LAN por um cabo tipo UTP e uma ficha RJ-45 através de uma tomada compatível. Esta tomada pode materializar, apenas simbolicamente, onde termina o domínio da COMPUSEC (aquém da tomada) e se inicia a COMSEC (além da tomada, prosseguindo na redes local e equipamentos e redes subsequentes) até alcançar a tomada de outro terminal onde se conecta por outra ficha RJ-45. Para estes links de comunicações, percebe-se ser perfeitamente indiferente que os bits transportem informação contendo texto, áudio ou imagem, cifrados ou "em claro".

A COMSEC e a INFOSEC enfrentam serviços e sistemas de informações (*intelligence*), vulgarmente designados por "secretas". Os utilizadores dos sistemas de informação e comunicações e os especialistas de tecnologias de COMSEC têm como adversários entidades existentes em diferentes domínios, sejam eles inimigos num teatro de guerra, antagonistas em conflitos regionais, ou empresas concorrentes em plataformas comerciais ou industriais. Pelo acesso facilitado às diversas tecnologias de ponta, por

quem tenha capacidade financeira, os adversários da COMSEC podem igualmente ser constituídos por grupos de criminalidade organizada, em permanente confronto com as polícias, não correspondendo, neste caso, às típicas organizações de serviços de informações pertencentes a determinado estado ou nação.

Tal como a segurança, as informações possuem várias subdivisões que implementam uma organização funcional de pesquisa e tratamento da informação, de acordo com as características da fonte. Com o desenvolvimento tecnológico existente, as fontes de aquisição de informação são muito diversificadas, como se pode verificar ao consultarmos uma enciclopédia com informação especializada nesta área[6]. As subdivisões das informações consideradas são:

- HUMINT (*Human Intelligence*) - aquisição de informação com origem em seres humanos, seja em entrevistas ou interrogatórios, na perseguição de suspeitos, ou utilizando outras técnicas para obtenção de confissões ou revelações involuntárias de informação;
    - GEOINT (Geospatial Intelligence) - aquisição de informação com origem na exploração e análise de imagens satélite, fotografia aérea, mapeamento e digitalização do terreno;
- IMINT (*Imagery Intelligence*) - aquisição de informação (imagem) via satélite e fotografia aérea;
- MASINT (*Measurement and Signature Intelligence*) - aquisição de informação cuja obtenção não se enquadra na SIGINT, IMINT ou HUMINT:
    - ACOUSTINT (*Acoustic Intelligence*) - aquisição de informação com origem acústica;
    - CBINT (*Chemical and Biological Intelligence*) - aquisição de informação com origem química e biológica;
    - DEWINT (*Directed Energy Weapon Intelligence*) - aquisição de informação com origem em armas de energia dirigida;
    - *Effluent/Debris Collection* - aquisição de informação com origem em efluentes atmosféricos e escombros;
    - EOINT (*Electro-Optical Intelligence*) - aquisição de informação com origem electro-óptica;
        - IRINT (*Infrared Intelligence*) - aquisição de informação com origem na banda do infravermelho;
        - LASINT (*Laser Intelligence*) - aquisição de informação com origem em sistemas laser;
    - MATINT (*Materials Intelligence*) - aquisição de informação com origem na análise de materiais;
    - NUCINT (*Nuclear Intelligence*) - aquisição de informação com origem na análise de radiação;
    - RADINT (*Radar Intelligence*) - aquisição de informação com origem em radares;
    - RF/EMPINT (*Radio Frequency/Electromagnetic Pulse Intelligence*) - aquisição de informação com origem em emissões de frequências rádio e impulsos na

banda do espectro electromagnético;

- OSINT (*Open Source Intelligence*) - aquisição de informação que está acessível publicamente. Inclui a informação que circula em jornais, na internet, livros, listas telefónicas, revistas científicas, emissoras rádio, televisão, etc.
- SIGINT (*Signals Intelligence*) - informação resultante da intercepção de sinais com origem em emissão de energia electromagnética;
    - COMINT (*Communications Intelligence*) - aquisição de informação com origem na intercepção de comunicações;
    - ELINT (*Electronic Intelligence*) - aquisição de informação com origem em sensores electrónicos;
- TECHINT (*Technical Intelligence*) - aquisição de informação resultante da análise de armas e equipamento utilizado por forças armadas de nações estrangeiras.

As subdivisões mais características das informações são a HUMINT, a SIGINT a IMINT e a OSINT, na medida em que as restantes resultam do desenvolvimento e aperfeiçoamento das tecnologias inerentes a estas. Existe por vezes alguma tendência para confundir COMINT com SIGINT, uma vez que esta tornou-se numa disciplina mais inserida no campo das informações militares e até certo ponto das diplomáticas, ao passo que a COMINT é transversal a todas as comunicações.

ECHELON, um sistema curioso

Nos dias seguintes ao tristemente célebre atentado ao World Trade Center, ocorrido em 11 de Setembro de 2001, os diversos órgãos de comunicação social internacionais interrogavam-se como teria sido possível um ataque de tal dimensão, sem conhecimento dos serviços de informações americanos. Veio a ser divulgado posteriormente que o treino e preparação dos elementos que pilotavam os aviões teriam sido realizados em território americano, nas suas próprias escolas de formação de pilotos. Ouvimos então algumas referências à existência de um sofisticado e recente sistema de aquisição de informação, designado ECHELON, que utilizando as tecnologias mais avançadas dos sistemas de informação e comunicações, com custos extremamente avultados e pagos pelo estado americano, pelos vistos não seriam justificados.

Também ouvimos então dizer que tal sistema estaria ao serviço das agências de informações e segurança americanas que andariam mais ocupadas com investigações da área industrial, a nível mundial, do que com as informações que visavam ameaças internas ao estado, propriamente dito. É um facto ser aquela uma actividade muito rentável e contribuir para o acompanhamento do nível e sentido da investigação das tecnologias de ponta de outros estados, mas qual será o preço social, económico e político resultante da morte dos milhares de cidadãos americanos, que naquele dia apenas se encontravam nas Twin Towers, num dia vulgar de trabalho?

As fragilidades da segurança podem ter custos economicamente não mensuráveis, que mais tarde ou mais cedo, podem mesmo vir a ferir os princípios dos estados

democráticos, especialmente quando enfrentam antagonistas de outros actores internacionais que regendo-se por princípios e conceitos verticalmente distintos terão para eles tanta ou maior importância que os princípios da democracia. Não nos será fácil alguma vez entendê-los à luz dos nossos conceitos socio-políticos e mais difícil será prever as futuras acções terroristas de grupos organizados.
Mas o que é então o ECHELON e qual foi a sua origem?

Uma aliança secreta de SIGINT teve a sua origem durante a Segunda Guerra Mundial, no sentido de conjugar esforços e tecnologias conjuntas dos Aliados, na intercepção e análise das mensagens cifradas, trocadas pelas tropas alemãs, japonesas e soviéticas. A continuação na pós-guerra desta aliança de informações foi formalizada por volta de 1947-48[7] com a assinatura de um acordo de cooperação e partilha de informação, entre o Reino Unido e os Estados Unidos da América. Segundo Patrick S. Poole[8], as agências constituintes dessa comunidade designada UKUSA, incluíam, para além da Agência Nacional de Segurança (*National Security Agency - NSA*) dos Estados Unidos, organizações de segurança das comunicações de Inglaterra (*Government Communications Headquarters - GCHQ*), do Canadá (*Communications Security Establishment - CSE*), da Austrália (*Defense Security Directorate - DSD*) e da Nova Zelândia (*General Communications Security Bureau - GCSB*). Estes são os cinco principais países anglófonos que assinaram o acordo UKUSA, e nos seus termos, cada um assumiria responsabilidades na superintendência da vigilância em diferentes partes do globo.

A rede ECHELON foi desenvolvida no final dos anos 60 e constitui uma parte fundamental do sistema global dirigido pela UKUSA, competindo às suas estações espalhadas pelo mundo interceptar e processar as comunicações retransmitidas via satélites de comunicações. Outras partes do mesmo sistema interceptam mensagens da Internet, dos cabos submarinos, das transmissões radiofónicas, dos equipamentos secretos instalados em embaixadas, ou utilizam satélites orbitais para monitorização de sinais vindos de qualquer ponto da superfície terrestre.

Outros países vieram posteriormente contribuir com as suas agências SIGINT para esta comunidade UKUSA. É o caso da Alemanha, Japão, Noruega, Coreia do Sul e Turquia, embora com um papel menor, sendo designados como membros de terceira linha *Third Party*[9]. Para além destes, existem ainda outros países, como é o caso da China, que possuem no seu território estações SIGINT da UKUSA, ou partilham SIGINT, mas em condições e termos muito mais limitados.

Embora sendo um sistema complexo, o ECHELON pode ser explicado sumariamente. São instaladas, espalhadas por todo o mundo, estações de intercepção, com a capacidade tecnológica de interceptar e capturar todo o tipo de sinais electromagnéticos, sejam eles provenientes de satélites, feixes hertzianos, ou tráfego de comunicações celulares (telemóveis) processando essa informação recorrendo às potentes capacidades de computadores que equipam as grandes agências mundiais de informações.

Fig 1 - Sistema de intercepção electrónica global - ECHELON[10]

Esses poderosos computadores possuem aplicações que efectuam o reconhecimento de voz e reconhecimento de caracteres ópticos (OCR), procurando na informação interceptada palavras ou frases constantes em listas designadas por "dicionários" do ECHELON. Estes "dicionários" são pré-estabelecidos, consoante o tipo de pesquisa que se pretende efectuar. Sempre que os sistemas informáticos detectam uma palavra do "dicionário" executam uma gravação da mensagem para posterior análise e processamento. Os analistas das informações, em cada uma das estações de escuta, mantêm as listas das palavras-chave de que foram encarregados de analisar, enviando posteriormente as matrizes de informação encontrada à agência que solicitou tal pesquisa. Esta actividade pode ser graficamente representada pela figura seguinte.

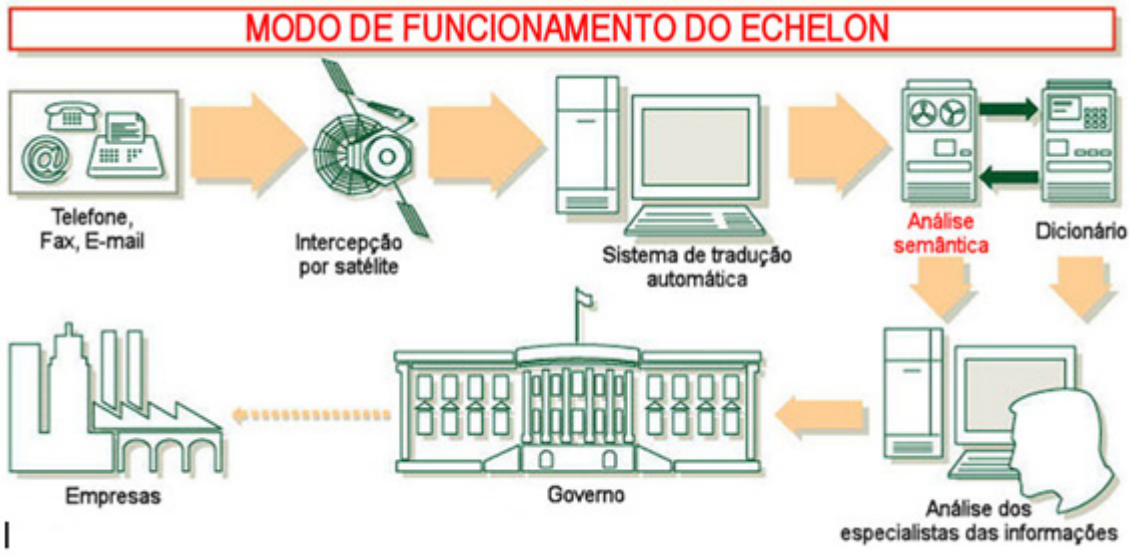


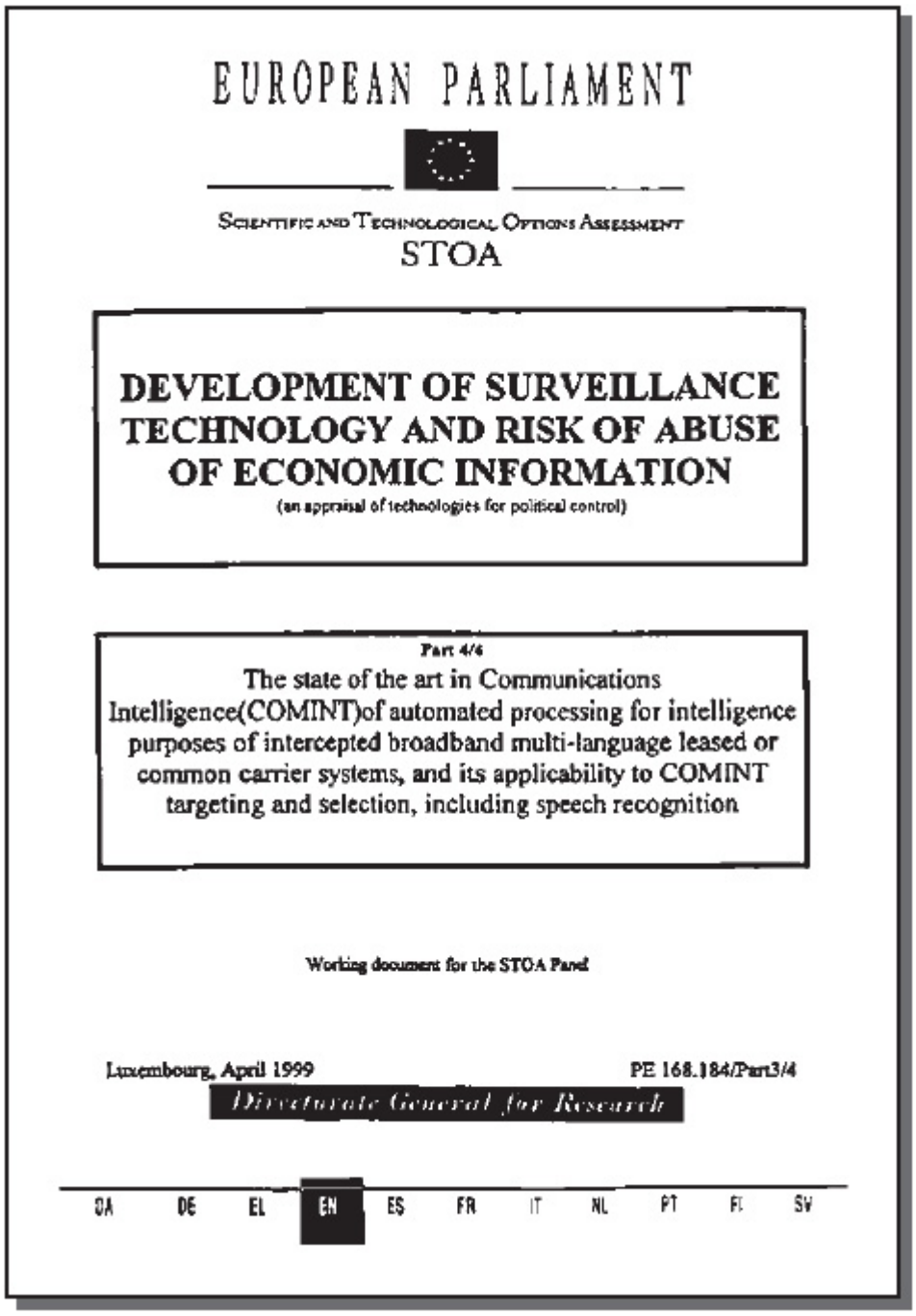
Fig 2 - Modo de funcionamento do Echelon[11]

Com esta explicação sumária, pensamos ter deixado mais claro não existir qualquer tipo de troca de informação transmitida "em claro", seja qual for o sistema de informação e comunicações utilizado, que não possa ser "escutada" e gravada, seja ela executada num telefonema (em telefone fixo ou móvel), uma transmissão por Fax, um e-mail, ou um teleimpressor.

Os sistemas pertencentes à comunidade UKUSA foram extremamente úteis na análise das comunicações do ex-Bloco de Leste, no período da Guerra-fria. Com o desaparecimento deste Bloco, este sistema passou a ser utilizado contra quem? A resposta a esta questão não é fácil pela delicadeza do assunto, mas não se poderá dizer tratar-se de uma falsa questão, vinda de espíritos permanentemente embrenhados na paranóia da segurança ou em constante busca das teorias da conspiração.

A maior discussão pública deste assunto ocorreu no Parlamento Europeu, no seguimento de vários relatórios elaborados, demonstrando como os serviços de informações de vários países no mundo, não exclusivamente anglófonos, vinham praticando a sistemática "pirataria da informação". Estas acções vieram a culminar num Plenário do Parlamento Europeu em 5 de Setembro de 2001.

Para que este acontecimento tivesse ocorrido, os documentos mais significativos apresentados foram relatórios preparados pelo gabinete do programa de Avaliação das Opções Técnicas e Científicas (STOA)[12], que vieram levantar sérias preocupações nos países europeus, acerca da natureza e tipo de vigilância praticada pelo ECHELON e potencial significado para as liberdades civis e económicas. Um dos relatórios STOA, cuja capa da versão original reproduzimos, serviu de base ao livro de Duncan Campbell "*O Mundo sob escuta*", de que existe uma versão em língua portuguesa, com uma introdução de Jorge P. Pires.



EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

(an appraisal of technologies for political control)

Part 4/4

The state of the art in Communications Intelligence(COMINT)of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition

Working document for the STOA Panel

Luxembourg, April 1999 PE 168.184/Part3/4

Directorate General for Research

DA DE EL EN ES FR IT NL PT FI SV

Quem ler este relatório, que posteriormente veio a designar-se *IC2000,* tomará conhecimento de provas documentais sobre a existência do ECHELON e as tecnologias utilizadas para intercepção de comunicações civis e comerciais, cobrindo questões técnicas, políticas e organizacionais relacionadas com a COMINT. Foi apresentado ao Parlamento Europeu a 5 de Julho de 2000, que votou favoravelmente a criação de uma comissão temporária de 36 Deputados, presidida pelo Deputado Português Carlos Coelho, com a finalidade de analisar as questões por ele levantadas.

A investigação terminou no Verão de 2001 e concluía indubitavelmente sobre a existência do ECHELON, a par de outros e mais amplos métodos de espionagem global das comunicações, que interceptam mensagens a partir da Internet, de cabos submarinos, de transmissões radiofónicos, de equipamentos secretos localizados no interior de embaixadas, ou utilizam satélites orbitais para monitorização de sinais em qualquer parte da superfície terrestre. A comissão avisava que estes sistemas constituíam uma ameaça ao comércio e à privacidade e que esse tipo de operações teria já infringido as convenções sobre os direitos humanos.

Segundo Campbell[13], a aliança UKUSA operando a maior rede de vigilância do mundo e os seus sistemas e métodos estão longe de serem únicos. Pelo menos trinta outras nações operam redes de SIGINT, a nível global ou regional. A Rússia, a China, a França e outras nações possuem redes mundiais. Mas nações europeias mais pequenas, como a Dinamarca, a Holanda ou a Suiça, construíram estações de intercepção de satélites para obtenção e processamento de informação mediante escuta das comunicações via satélite.

Onde um Estado adquire os equipamentos de COMSEC?

A segurança é, quase sempre, considerada incómoda. Especialmente por quem julga que procedimentos aligeirados, característicos de hipotéticas dinâmicas empreendedoras aparentam equivaler a elevados níveis de desembaraço de boa qualidade. Tememos que, na área da segurança, tal desembaraço associado ao aligeiramento de procedimentos, geralmente esqueça e ultrapasse algumas normas e procedimentos que conduzirão forçosa e fatidicamente a violações de segurança, em que não só matérias classificadas poderão ser comprometidas, violadas ou destruídas, mas também poderão ser destruídas informações valiosas ou pôr em causa algumas vidas humanas.

Para se tentar alcançar um estado satisfatório de segurança, é indispensável a prática, no dia a dia, do respeito e cumprimento de normas actualizadas, sedimentadas numa equilibrada e sensata cultura de segurança. Essas normas regulam os procedimentos de todas as vertentes da segurança: segurança do pessoal, segurança física, segurança da informação e segurança das matérias classificadas.

A segurança da informação, em geral, e a segurança das comunicações, em particular, não se restringem a regulamentar normas e procedimentos, mas englobam o recurso a sistemas de informação e comunicações, associados às respectivas tecnologias de segurança, tendo estes equipamentos de ser certificados para o nível de classificação de segurança da informação que neles será processada, armazenada e trocada, de forma a garantirem a confidencialidade, integridade e disponibilidade da sua informação, como garante do exercício da capacidade do comando e controlo.

Perante o ambiente de guerra tecnológica em que tentámos caracterizar o permanente conflito existente entre a segurança das comunicações e as informações, onde pode um Estado adquirir as tecnologias que protejam os seus sistemas de troca de informação

classificada, sejam eles destinados às suas forças armadas, às suas polícias, aos seus embaixadores ou a outros membros desse Estado?

Um Estado terá de ter o controlo sobre as suas tecnologias de segurança das comunicações. Deverá possuir a capacidade de estudar, desenvolver e produzir os meios específicos de segurança das comunicações, sob risco dos seus diversos sistemas de informação e comunicações serem a fonte de informação das informações de outros países ou do crime organizado, uma vez que as tecnologias de intercepção e escuta, cuja utilização estava antigamente restringida às forças militares e policiais, adquirem-se hoje nos mercados internacionais a reduzidos custos.

Esta área da segurança deverá ser uma das principais, se não a fundamental a ter em atenção, num país que já entendeu a indispensabilidade de um choque tecnológico como um dos pilares impulsionadores, rumo ao desenvolvimento nacional.

Num Estado de parcos recursos, não fará sentido que o investimento em investigação e produção tecnológica reverta, por exemplo, só para um ramo das forças armadas, mas ser executado numa perspectiva nacional. Esse esforço nacional deve incentivar a execução de vários projectos, baseados na exclusiva produção de tecnologias nacionais, como resultado do esforço conjunto entre as universidades e a investigação nacionais, que associados à nossa indústria produzam os necessários sistemas de segurança das comunicações, para utilização nas actividades específicas no âmbito exclusivo do Estado. Todos os projectos que venham a surgir deverão ser acompanhados ao mais alto nível, tanto sob o ponto de vista de acompanhamento tecnológico, como de todas as condições de segurança a respeitar em todas as actividades parcelares que no seu computo global culminarão na produção de diversos equipamentos que sirvam à política INFOSEC do Estado. O resultado deverá ser a produção de vários modelos de equipamentos que satisfaçam as características intrínsecas de todas as áreas do Estado, satisfazendo os requisitos específicos tanto das suas forças armadas, como das suas polícias, dos seus embaixadores e restantes organismos do estado que deles tenham necessidade.

Os equipamentos resultantes serão sempre, para o nosso Estado, tecnologicamente mais seguros que outros adquiridos a empresas internacionais, que provavelmente terão como grandes clientes as próprias agências SIGINT e as de outros países.

No passado, a indústria nacional já deu provas da capacidade de responder a desafios deste nível tecnológico, tendo produzido vários modelos de equipamentos de COMSEC que entraram ao serviço do Exército, nos anos oitenta e noventa.

Quando um Estado adquire a outro a capacidade tecnológica para garantir a segurança das suas comunicações, estará a dotá-lo da capacidade de ser invisível aos seus olhos e inaudível aos seus ouvidos, na intercepção e pesquisa às trocas de informação efectuadas nos seus sistemas de informação e comunicações, seja essa informação das áreas de interesse militar, político ou económico. E, assim, esse outro Estado, que ainda será remunerado para esse fim, ficará agradecido e deterá o destino daquele nas suas mãos!

Nestes termos já pensava Sun Tzu, conforme o escreveu no "*Capítulo VI. Pontos fracos e fortes*" do seu livro "*A arte da guerra*", em 500 AC:

"Ó arte divina da subtileza e segredo! Por ti aprendemos a ser invisíveis, por ti inaudíveis; e consequentemente detemos o destino do inimigo nas nossas mãos."[14]

Bibliografia

Bispo, António J. (2002). *A Sociedade de Informação e a Segurança Nacional.* Revista Estratégia, volume XIII. Instituto Português da Conjuntura Estratégica.
Costa, José Ribeirinha Diniz da (2004). *Segurança da Informação no Contexto das Novas Tecnologias. Um modelo para o Exército.* Curso Superior de Comando e Direcção 2003/2004 - Trabalho Individual de Longa Duração. Lisboa: Instituto de Altos Estudos Militares.
Campbell, Duncan (2001). *O Mundo sob escuta. As capacidades de intercepção no século XXI.* Tradução de Jorge P. Pires. Lisboa: Frenesi.
Dinis, José António Henriques (2005). *Guerra de Informação - Perspectivas de segurança e competitividade*. Lisboa: Edições Sílabo.
Giles, Lionel (2003). *Sun Tzu on the art of war - The oldest military treatise in the world.* http//www.kimsoft.com/powar.htm (acedido: 25 de Outubro de 2005).
Hager, Nick (1996). *Secret Power - New Zealand's role in the International Spy Network.* Craig Potton Publishing, Nelson, New Zealand.
http://fas.org/irp/eprint/sp/ (acedido: 30 de Outubro de 2005).

North Atlantic Council (2002). *Security within the North Atlantic Treaty Organization (NATO).* C-M(2000)49.
Presidência do Conselho de Ministros - Resolução nº 37 (1989). *Normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação - SEGNAC 2*. Diário da República - I Série Nº 245 (24-10-1989).
Supreme Headquarters Allied Powers EUROPE (1997). *ACE Security Directive - AD 70-1*. Belgium.

Glossário

Assinatura digital - Forma de autenticação digital de informação, em analogia com a assinatura manuscrita num documento escrito numa folha de papel. Baseia-se em tecnologias de software de criptografia de chave-pública e chave-privada.

Autenticação - Processo de associar um indivíduo, um computador ou uma aplicação (programa informático) com a sua única identidade, perante um sistema informático. A autenticação pode ser feita através do uso de *passwords* por parte do utilizador ou através da troca de chaves e poderá envolver uma terceira entidade de confiança

(entidade certificadora). Os utilizadores são identificados perante uma aplicação através de uma identificação do utilizador ou *user id*, ou por sistemas de reconhecimento biométrico.

Cabo UTP - Um cabo do tipo UTP (*Unshielded Twisted Pair*) é o tipo mais utilizado em redes de computadores. Constituindo uma variante dos cabos de pares entrelaçados, não possui nenhuma blindagem exterior.

COMPUSEC - *Computer Security* - A segurança dos computadores visa a aplicação de medidas de segurança do hardware, software e firmware3, de um computador ou sistema de computadores, com a finalidade de proteger ou prevenir a ocorrência não autorizada da divulgação, manipulação, alteração, ou interrupção de acesso da informação.

COMSEC - *Communications Security* - A segurança das comunicações visa a aplicação de medidas de segurança das comunicações, de forma a negar a pessoas não autorizadas o acesso a informação valiosa, que poderá derivar da sua posse ou estudo, ou assegurar a autenticidade dessas comunicações. Tais medidas incluem sistemas cripto.

Confidencialidade - Necessidade de protecção dos dados e informação classificada, de forma a poderem ser revelados apenas a quem estando autorizado, esteja credenciado e tenha necessidade de conhecer.

CRYPTOSEC - *Cryptografic Security* - A segurança criptográfica resulta da escolha, tecnicamente perfeita, dos sistemas criptográficos e da sua utilização apropriada.

Dinheiro digital - Transacções de negócios efectuado através de sistemas de informação e comunicações.

Disponibilidade - Assegurar que todos os recursos possam ser acedidos sempre que uma entidade autorizada o solicite.

EMSEC - *Emition Security* - A segurança da emissão visa assegurar que a ocorrência de radiações comprometedoras fique confinada a certas áreas limitadas, pelo que serão áreas classificadas, aplicando técnicas específicas, contra a captura de informação, através da intercepção e análise, por parte de quem não esteja autorizado.

INFOSEC - *Information Security* - A segurança da informação visa a aplicação de medidas de segurança para protecção da informação processada, armazenada ou transmitida nos sistemas de informação e comunicações, ou qualquer outro sistema electrónico (por exemplo, sistemas de sensores), contra a perda de confidencialidade, integridade, disponibilidade e para prevenir a perda de integridade ou disponibilidade dos próprios sistemas.

LAN - *Local Área Network* - Rede de comunicações local, que poderá estar ligada, ou não a uma WAN.

Firmware - Software que existe embebido em dispositivos de hardware. Como exemplo, podem-se referir os programas de arranque dos computadores, designados por BIOS (Basic Input Output System). Outro exemplo deste tipo de software embebido, hoje muito vulgarizado, pode-se encontrar nas *USB flash drives*, vulgarmente designadas por *pen's* (canetas-memória). Uma *flash* ROM deste tipo é constituido por uma EEPROM (*Electrical-Erased Programmable Read-Only Memory).*

Integridade - Comprovar que a informação não tenha sido alterada ou se modificada apenas por quem está autorizado.

MAN - *Metropolitan Area Network* - Constitui uma forma intermédia entre a WAN e a LAN, distribuindo-se por uma área geográfica localizada, por exemplo, numa cidade.

OCR - *Optical character recognition* - Reconhecimento de caracteres ópticos.

OTAN - Organização do Tratado do Atlântico Norte.

Rede estruturada - Rede de acesso e transporte de informação que pode englobar uma variedade de serviços analógicos e digitais, como: CATV (*Community Antenna Television* - televisão por cabo), VOIP (*Voice Over Internet Protocol* - voz sobre IP), transporte de Imagem, vídeo-conferência, ligações a LANs, etc. Para cada serviço é delimitado um canal, restando para os outros serviços uma grande parte da banda total. Estas redes são distribuídas em árvore ou anel, partindo de um ponto designado "sala de equipamentos", podendo chegar ao terminal de cada utilizador, por várias formas possíveis. Os meios mais utilizados em sistemas de cablagem estruturada são o cabo UTP nível 5 e o cabo de fibra óptica.

Segurança física - Parte da segurança que se preocupa com as medidas físicas destinadas a salvaguardar o pessoal e prevenir acessos não autorizados a informações, materiais e instalações, contra a espionagem, sabotagem, danificação e roubo, tanto nos locais de fabrico, armazenagem, ou utilização, como durante deslocações.

Segurança das matérias classificadas - Ocupa-se com a situação em que as matérias classificadas se encontram protegidas da possível concretização de ameaças contra a sua confidencialidade, integridade e disponibilidade.

Segurança do pessoal - Parte da segurança que se preocupa com todas as medidas relacionadas com o pessoal destinadas a neutralizar as ameaças postas pelos serviços de informação hostis, ou por pessoas ou organizações subversivas.

Segurança protectiva - Sistema organizado de medidas defensivas instituído e mantido a todos os níveis, com o objectivo de obter e manter a segurança.

TRANSEC - *Transmition Security* - A segurança da transmissão consiste na aplicação

de medidas de segurança destinadas a proteger as transmissões da intercepção não autorizada, análise de tráfego e mistificação, evitando a exploração da informação, por outras técnicas que não a análise criptográfica.

Votação electrónica - Inclui votação pela internet e outro tipo de votação *online*. Existem vários sistemas de informação e comunicações que permitem apurar o voto dos cidadãos. Essa votação electrónica pode ser efectuada por um quiosque electrónico, internet, telefone, cartão perfurado, sistemas de leitura óptica em cartões criados para esse fim.

WAN - *Wide area network* - Rede de comunicações geograficamente dispersa. Utiliza-se este termo por oposição a uma rede local (LAN).

WWW - *Wold Wide Web* - Constitui o universo de toda a informação acessível, através da rede global e uma personificação de todo o conhecimento humano na *Internet.*

---

1 Na terminologia inglesa designa-se CIS (Communications and Information Systems).
2 Cf. Costa (2004: 57).
3 Alexander Graham Bell registou a patente do seu telefone em 7 de Março de 1876, tendo no dia 10 do mesmo mês efectuado a apresentação pública da primeira transmissão telefónica.
4 Cf. Bispo (2002: 67).
5 Cf. Dinis (2005: 65-66). "A definição de Guerra de Informação, com base na doutrina militar conjunta americana (…), configura-se com «operações de informação conduzidas durante tempo de crise ou conflito para alcançar ou promover objectivos específicos sobre um adversário específico ou [vários] adversários. (…) se se fizer uma extensão deste conceito para além do âmbito essencialmente militar, com a sua aplicação a um nível mais alargado aos diversos sectores económicos, então toda esta doutrina se poderá expandir e aplicar ao tecido empresarial e outras organizações (…)".
6 Cf. http://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines (adaptado) (acedido: 3 de Dezembro de 2005).
7 Nessa época, a maior parte das comunicações de longa distância, civis, militares ou diplomáticas, eram estabelecidas via rádio, em frequências na banda da HF (High Frequency, 3 - 30 MHz), usualmente designadas "ondas curtas".
8 Cf. Pole, Patrick S. (1999/2000). America's Secret Global Surveillance Network. http://fly.hiwaay.net/~pspoole/echelon.html (acedido:24 de Outubro de 2005).
9 Cf. Richelson, Jeffrey. http://fas.org/irp/eprint/sp/sp_f2.htm (acedido: 30 de Outubro de 2005).
10 Cf. imagem (adaptada) obtida em http://www.seprin.com/echelon-g.jpg (acedido: 9 de Dezembro de 2005).
11 Cf. imagem (adaptada) obtida em: http://www.rfi.fr/Kiosque/Mfi/Guerre/Lundi/reseau.htm (acedido: 10 de Novembro de

2005).
12 Cf. STOA - Scientific and Technological Options Assessment. Relatórios STOA podem ser consultados em: http://cryptome.org/dst-1.htm; http://cryptome.org/dst-2.htm; http://cryptome.org/dst-3.htm; http://www.iptvreports.mcmail.com/stoa_cover.htm (acedidos: 31 de Outubro de 2005).
13 Cf. Campbell (2001:17).
14 Tradução livre de: O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence hold the enemy's fate in our hands. http://www.kimsoft.com/polwar6.htm (acedido: 25 de Outubro de 2005).

_____

* Tenente-Coronel de Transmissões. Comandante Interino do Regimento de Transmissões.