Defesa

Cyberwar-Netwar - A segurança na idade da informação

Eduardo Mateus da Silva

Nas novas formas de guerra a informação desempenha um papel cada vez mais importante. A superioridade na aquisição, no tratamento e na utilização da informação assim como a sua denegação ao adversário, conjugado com a utilização de armas inteligentes que também dependem totalmente da informação na aquisição de objectivos e no guiamento, traduziram-se em guerras rápidas, com destruições controladas e muito poucas baixas para os que detêm a superioridade da informação. A noção clássica da superioridade de meios, de três para um para iniciar um ataque, deixou de fazer sentido. Actualmente, forças muito mais ligeiras e ágeis podem superiorizar-se a efectivos muito maiores e maciçamente armados que apenas dispõem de informação limitada. Em contraponto com esta situação o novo cenário do terrorismo internacional sem pátria e sem rosto, pós 11 de Setembro, veio mostrar que os mais sofisticados meios de obtenção e interpretação da informação não foram e não têm sido capazes de recolher a informação necessária para prever, detectar e evitar esses ataques terroristas. Num caso provou-se a eficácia da superioridade da informação, no outro a incapacidade de obter a informação necessária, apesar dos meios colossais dos sistemas de escuta e intercepção de comunicações e dos equipamentos de análise e tratamento da informação, em particular supercomputadores de grande capacidade. Esta situação de contraste entre Forças Armadas eficazes, num mundo inseguro onde a informação desempenha papeis opostos, resulta da própria natureza da informação. A informação, embora seja a expressão de uma realidade, depende dos sensores que a detectam, dos observadores que a apreendem ou intuem, dos códigos que a exprimem e da forma como é comunicada, transmitida, interpretada e tratada. A informação é, por isso, fluida, susceptível de diferentes interpretações e vulnerável a deformações, intencionais ou não, da forma e do conteúdo. No caso do combate moderno entre Forças Armadas a guerra tende a fazer-se mais não entre homens mas entre máquinas (sistemas de armas) possuidoras de sistemas automáticos que assumem a parte mais significativa do processo de decisão e de acção. A aquisição, o processamento e a transmissão da informação entre máquinas utiliza códigos (linguagens) que são extremamente precisos e concretos e insusceptíveis de

diferentes interpretações e, por isso, completamente diferentes da comunicação entre os seres humanos, onde as diferentes línguas e o significado das palavras faladas ou escritas é susceptível de várias interpretações. Convém acrescentar que a inflexão da voz, o gesto e o olhar podem alterar ou enviesar o significado da mensagem que queremos transmitir. Assim, a circulação da informação entre as máquinas é rigorosa e não perde tempo com estados de alma ou hesitações. Por outro lado, é muito mais fácil proteger e securizar a informação que nelas circula por se tratar de redes fechadas onde o acesso do exterior é impedido e onde, além disso, se utilizam sistemas complementares automáticos de cifra, redundância de meios e sistemas de certificação e comprovação da informação. Este é o domínio da guerra electrónica onde os grandes exércitos dos países tecnologicamente mais desenvolvidos possuem toda a vantagem. É muito difícil a uma organização com poucos recursos ou a um *hacker* individual interferir com esse tipo de informação e mesmo quando o consegue normalmente trata-se de casos esporádicos com consequências limitadas. O problema da securização e do tratamento desta informação estratégica e táctica é mais crítico no sentido de como gerir e tratar a enorme quantidade de informação que circula e cresce exponencialmente. O problema é como diferenciar a qualidade dentro da quantidade e como criar informação/conhecimento, eliminando a redundância e a ganga ou lixo que apenas introduzem ruído de fundo. Como obter a informação necessária para combater e neutralizar o terrorismo internacional? Trata-se aqui, fundamentalmente, da circulação da informação entre seres humanos, que combinam a utilização dos meios tecnológicos mais sofisticados com formas rudimentares e toscas de comunicação e que podem utilizar uma miríade de linguagens humanas que mesmo os serviços de informações mais eficazes podem não conhecer. Por outro lado, a informação que se detecta, é, na prática, sempre imprecisa. Não se sabe qual é a origem (que organização, que rede), o local onde pode acontecer (país, cidade, ponto exacto), quando (data/hora) e a probabilidade de acontecer ou não. Perante esta imprecisão hesita-se entre avisar ou não os potenciais alvos, criando o medo ou até o pânico ou ser acusado de não se ter avisado e assim ter aumentado o número de vítimas. Mesmo a famosa rede "Echelon" não consegue resolver este problema. A rede Echelon começou com a rede UKUSA em 1948 (EUA, Canadá, Reino Unido, Austrália e Nova Zelândia) e foi reforçada com a criação da National Security Agency (NSA) por uma directiva secreta do Presidente Harry Truman (Communications Intelligence Activities) em Outubro de 1952 e tinha como missão proteger as comunicações governamentais e militares americanas, graças à criptologia. A NSA evoluiu rapidamente para uma agência

de espionagem. A sua divisa é claramente significativa: “In God we trust, all the rest we monitor”. Durante a guerra fria ficou famosa a intercepção das comunicações telefónicas entre o Kremlin e o Zil de Leonid Brejnev. Contudo, actualmente, as chamadas telefónicas de Sadam Hussein foram muito mais complexas a descriptar. A realidade é que hoje um telefone móvel pode varrer mil frequências diferentes durante uma conversação, o acesso à informática e mesmo à Internet explodiu. Existem no mundo centenas de milhões de computadores, centenas de milhões de telefones celulares e de faxes e a Internet duplica de dimensão todos os 90 dias. Com a rede Echelon calcula-se que são analisadas mensalmente cem milhões de mensagens, o que parece bem pouco perante o volume de informação que lhe chega e que se calcula em mil biliões de bits todas as doze horas. Apesar do orçamento da NSA ser de quatro mil milhões de dólares anuais e a rede dispor de 20 000 técnicos, não consegue satisfazer as necessidades e responder aos desafios que as ameaças à estabilidade do mundo actualmente colocam. Também é verdade que a comunidade internacional não pode estar dependente de uma rede de informações anglo-saxónica e, por outro lado, uma vez que parece existir acordo para todos os países cooperarem na luta contra o terrorismo, todos não são de mais para, no domínio da *Human Intelligence*, darem o seu contributo. Como isso poderá ser possível, ultrapassa-nos completamente. O problema que colocamos pode sintetizar-se da seguinte forma: como encontrar respostas viáveis para garantir a segurança da informação perante o extraordinário crescimento da produção, tratamento, difusão e circulação da informação, tendo em conta a cada vez maior dependência dos computadores, da Internet e a explosão das comunicações móveis. Tem também de ser entendido que a garantia da segurança tem a ver com todos os níveis de utilização da informação como seja ao nível estratégico/militar, ao nível económico/empresarial, ao nível comunitário/social e ao nível pessoal/individual. Ou seja, só faz sentido se conseguirmos gerir de forma inteligente e operacional o gigantesco volume de informação circulante e garantir o funcionamento do sistema mundial em todos os sectores e domínios de forma harmoniosa e estável. Devemos, por um lado, encontrar novas formas e métodos de tratar a informação de forma racional, encontrar novas ferramentas que permitam descriminar, seleccionar e transformar a informação em conhecimento, eliminando a redundância, a ganga e o lixo. Por outro lado, ao mesmo tempo, proteger e securizar a informação, garantir a sua integridade e qualidade. Referimo-nos inicialmente à dicotomia entre a informação que circula nas máquinas e aquela que liga os seres humanos. São situações diferentes que requerem soluções diferentes. Porque as linguagens e as formas de

comunicação são diferentes. Contudo, tanto num caso como noutro se põe o problema de como gerir o excesso de informação e garantir a segurança mas, embora o problema seja o mesmo, as soluções serão diferentes num e noutro caso. Se bem que as tecnologias utilizadas na circulação da informação entre máquinas sejam sofisticadas, consideramos que na gestão, no tratamento e na análise da informação circulante entre os humanos, o problema é ainda de mais difícil solução porque os parâmetros em jogo são muito mais diversificados e porque se misturam as mais altas tecnologias com sistemas mais toscos e rudimentares e, ainda, porque os comportamentos humanos são muito mais diversos, imprevistos e imprecisos do que os comportamentos, ou melhor, as relações entre as máquinas. Quais as formas de analisar fluxos enormes de informação, descriminar o que é que tem significado para uma determinada finalidade? Criar conjuntos de palavras (em que línguas) ou termos que as mascaram, estabelecer algoritmos significativos, comprimir textos mantendo o significado essencial, reconstruir um conteúdo usando apenas partes, enfim, um mundo de possibilidades em aberto, algumas ainda por explorar e que exigem investigações mais aprofundadas. Temos ainda de ter em consideração os seguintes factos:

- Que a informação pode circular instantaneamente em todo o planeta;
- Que a informação operacional ubíqua tem de ser tratada e securizada ao mesmo tempo em todo o lado;
- Que a informação/conhecimento com carácter estratégico tem prioridade e maior exigência no tratamento e na garantia de segurança.

Temos, assim, um amplo campo a explorar para encontrar novas formas de tratar e gerir a informação. Informação, que, no fundo, é um conceito virtual fluído e impreciso mas que, apesar disso, constitui o bem mais preci