Ciberguerra

Mestre
Nuno Manuel Oliveira Luz de Almeida

Problemática

É objeto deste pequeno "*paper*" contribuir para uma reflexão relacionada com a chamada ciberguerra no que ao seu perímetro diz respeito, nomeadamente, quanto à necessidade do setor bancário dever ou não nele ser incluído.

Enquadramento

Com a saída do Despacho nº 13692/2013, publicado em Diário da República, 2ª série, no dia 28 de Outubro, relativo à "Orientação Política para a Ciberdefesa", vindo na sequência de um conjunto de outras resoluções[1] e despachos[2], enquadrados pela Política Comum de Segurança e Defesa da União Europeia[3], é dado mais um passo no sentido de preencher o vazio existente no nosso país relativamente à prevenção e resposta às ameaças cibernéticas que ponham em risco a soberania e a segurança nacional (ciberguerra).

Envolvendo o conjunto de sistemas informáticos, redes de comunicação e informação neles processada e armazenada, o ciberespaço distingue-se, conceptualmente, quando comparado com as ameaças ditas convencionais, por não dispor de fronteiras físicas ou lógicas, possibilitar o tráfego "booleano" a uma velocidade quase igual à da luz (tempo zero), atomizar os atores do ciberespaço com objetivos de vida muitas vezes conflituantes entre si, tornar imprevisível os mecanismos de causa-efeito e, com isso, alterar por completo o paradigma da guerra e seus subconceitos de ataque, defesa, criminalidade e segurança, de entre outros.

Se, até ao início do nosso século, eram, essencialmente, de cariz físico as principais ameaças, de que o ataque às torres gémeas, por ser o mais terrível na sua espetacularidade recente, constitui o seu exemplo mais acabado, hoje, devido ao

exponencial desenvolvimento dos chamados sistemas e tecnologias de informação, há que lhes adicionar as ameaças lógicas, do mundo digital (veja-se, a esse propósito, o caso Edward Snowden).

A complexização do chamado "internet time" ao caminhar para uma convergência tecnológica materializada em telecomunicações digitais suportadas em elevadíssimas larguras de banda por onde tudo passa (texto, imagens, vídeo), equipamentos miniaturizados de facílimo transporte (telemóveis, pens) e "media" com acesso em real time a todo e qualquer recurso informativo (Google Earth), assim como a proliferação de serviços, aplicações, ferramentas, bases de dados, sistemas e protocolos usados, ao mesmo tempo que os experts nestas matérias são jovens com natural menor maturidade, obriga a olhar transversalmente para todos os intervenientes no ciberespaço, independentemente de pertencerem à sociedade militar ou civil.

A desmilitarização da informação (Wikileaks, espionagem setorial e institucional), se não for gerida de forma local, e mesmo individual, por cada cidadão, impossibilitará uma verdadeira cultura de segurança no ciberespaço. Na sociedade civil tornou-se clássico, talvez até pelo imediatismo cinematográfico, apontar-se o setor elétrico como aquele que, sendo objeto de uma disrupção, poderia conduzir uma sociedade da ordem ao caos num ápice. Também sem comunicações, a era da eletrónica em que vivemos desapareceria e, com ela, todo e qualquer sistema de transporte físico ou lógico. Sem que se negue a sua importância gostaríamos, contudo, de relevar um outro setor, o bancário, para o qual, neste âmbito da ciberdefesa, se tem olhado de forma bem menos exuberante quando não mesmo descuidada.

Para que não haja dúvidas, a afirmação feita não se refere ao trabalho que cada instituição tem vindo a desenvolver – coordenado pelo Conselho Nacional de Supervisores Financeiros (CNSP) – que se considera notável a todos os títulos podendo e devendo, até, ser exportável enquanto conhecimento específico, mas sim à importância que lhe tem sido dedicada pelas altas esferas governativas.

Alguém disse que a sociedade é uma rede de redes e um sistema de sistemas em que cada cidadão é um nó dessa rede. Imagine-se, pois, um cidadão que acorda pacatamente e se dirige para um supermercado para comprar o almoço e no ato do pagamento lhe dizem que o cartão não está ativo. Nesse mesmo momento vai ocorrendo a mesma situação com todos os clientes. Daí, o "nosso" homem dirige-se ao multibanco mais próximo e verifica que o saldo da sua conta não corresponde, minimamente, ao que esperaria apresentando-se a negativo. Quer telefonar para o banco mas, verifica que não o consegue fazer pela falta de saldo. A pé, dirige-se ao seu balcão pois começa a desconfiar que poderá haver um problema sério. Já no balcão, dizem-lhe que o sistema está com problemas e que deverá voltar mais tarde. Dirigindo-se à sua empresa começa a verificar que existe algum nervosismo, dado as contas da mesma se encontrarem em situação precária ou por falta de saldo ou por mensagem de encerramento. Como é fim do mês não poderão ser pagos os salários dos seus colaboradores nem honrar o pagamento aos fornecedores. Ao mesmo tempo, repara num som ensurdecedor que vem da bomba de gasolina fronteiriça ao prédio da sede da empresa. Abeira-se da janela e

constata haver discussões entre os automobilistas e o responsável da gasolineira. Apercebendo-se das conversas conclui não estar só na desdita. Uns anos antes, lembrava-se do apagão da EDP devido a uma cegonha. Agora, o apagão era do seu banco. E se não conseguissem reparar a situação? Regressar a um mercado de troca direta não seria solução.

Este cenário relatado poderia ser bem real se houvesse da parte de um governo ou de um conjunto de ciberterroristas fundamentalistas a vontade explícita de "emudecer" de forma aparentemente pacífica os cidadãos de um outro país ou parte de um setor chave desse mesmo estado. Sabe-se hoje que uma situação continuada de caos numa instituição bancária causará, ao fim de cinco dias, danos irreparáveis que a obrigarão a encerrar as portas causando, com isso, um impacto sistémico de dimensão superior ao da sua quota de mercado.

É importante, neste ponto, dizer que todos os anos há bancos que fecham por gestão danosa conducente à bancarrota, não havendo, contudo, nota de algum que o tenha feito devido a uma disrupção terrorista. Até hoje, há muitos ataques ao setor, mas sempre dominados pelos perímetros de segurança estabelecidos e controlados pelos profissionais da cibersegurança. Significa isso que deveremos estar tranquilos? Não, significa apenas que a banca tem encabeçado, com altíssimo aproveitamento, a luta contra essa cibercriminalidade não havendo nota de movimentos envolvendo ciberterrorismo concertado a uma escala de média/grande dimensão. Enquanto os primeiros procuram abrir brechas no sistema através de uma aplicação web escrita recorrendo a ASPs[4] e configurada no Internet Information Services acessível através de um endereço HTTP[5] instalado num servidor remoto que possibilita pesquisar, ou alterar conteúdos localizados numa base de dados por ligação OLEDB[6] e ODBC[7] e, com isso, desviar quantias das contas de um cliente para as suas próprias, os segundos procuram destruir a disponibilidade, a integridade, a sincronicidade e a confidencialidade dos dados através da destruição física de um ou vários equipamentos, da criação de um resíduo na frequência da transmissão destes, ou por intrusão, de um vírus nas aplicações, com isso prejudicando a sua recuperação.

Proposta

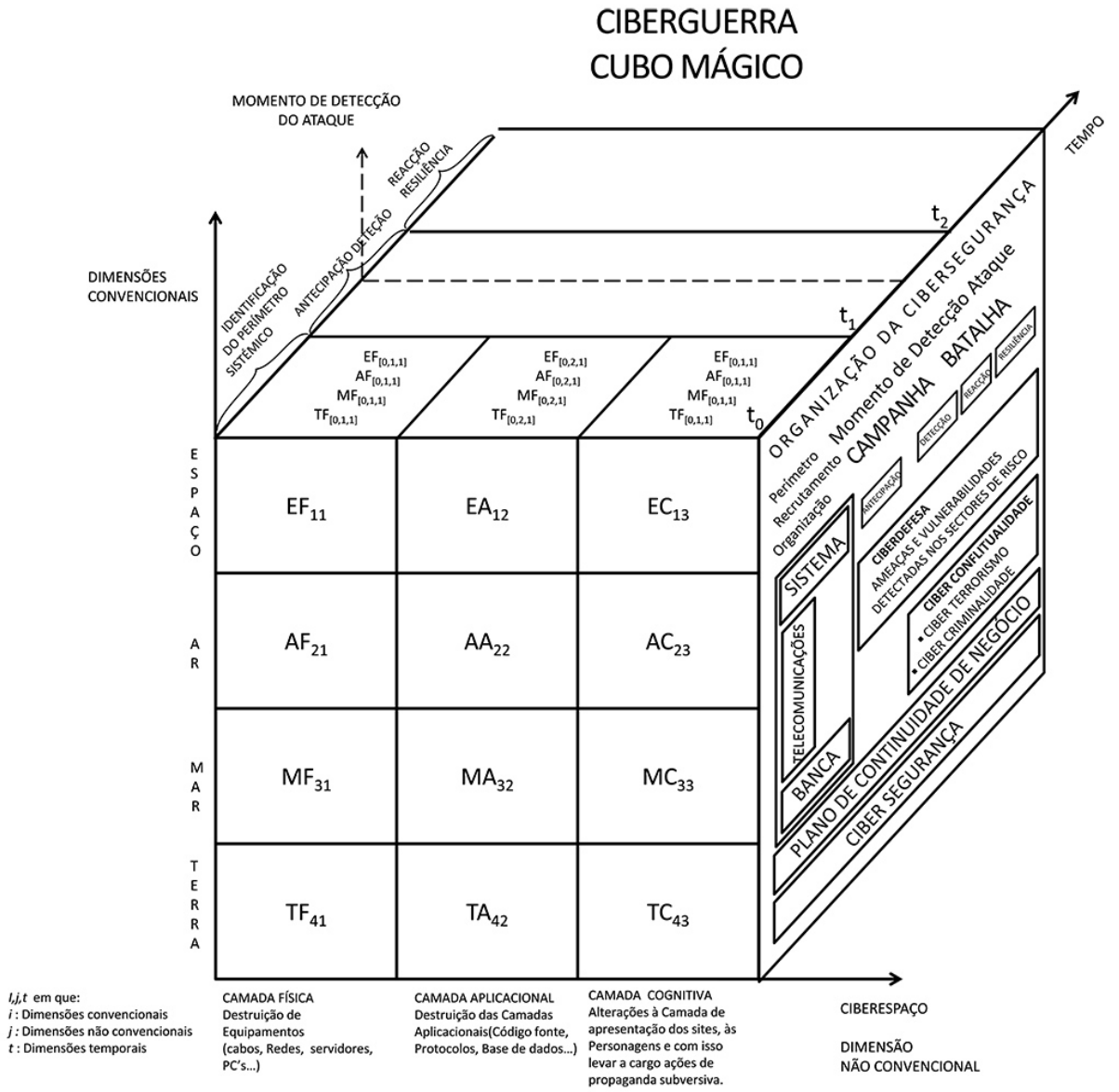
Sendo um perigo real, a banca, já há muito tempo[8] que se vem preparando para situações desta natureza, através do que se convencionou chamar Plano de Contingência de Negócio (PCN), o qual entronca no chamado Risco Operacional que é uma das três matérias que se encontra consignada, por sua vez, num dos três pilares que configuram o Acordo de Capital de Basileia II[9]. Para que o capital exigido ao nível de cada banco seja minimizado, deverá cada instituição mitigar o seu risco operacional através da comprovação da existência de um PCN devidamente testado. A gestão da continuidade de negócio compreende, assim[10], "o conjunto integrado de políticas e procedimentos que visam assegurar o funcionamento contínuo de uma organização, ou a recuperação atempada de uma atividade, no caso de ocorrência de eventos suscetíveis de perturbar o

normal desenrolar do negócio, nomeadamente, por implicarem a indisponibilidade das infraestruturas físicas, dos sistemas informáticos ou dos recursos humanos, de forma isolada ou em simultâneo.

Este tipo de eventos abrange, entre outros, cenários como catástrofes naturais, pandemias, atos de terrorismo, falhas nos sistemas informáticos". Significa isto que o setor detém na sua cultura, no seu ADN, uma filosofia de vida envolvendo os seus quadros e colaboradores, suportada na planificação de situações de risco antecipando-as, simulando cenários, medindo consequências sobre clientes, fornecedores e acionistas, hierarquizando tarefas de recuperação e mitigação, garantindo a existência de infraestruturas alternativas incluindo as físicas, as informáticas e as de comunicação, reportando à entidade de supervisão, possibilitando a auditabilidade a entidades terceiras e, sobretudo, imputando responsabilidades a cada um dos intervenientes. Os testes, sistematicamente efetuados com esse propósito, comprovam-no.

Este agregado de aspetos torna clara a importância que o setor financeiro detém quer enquanto alvo a atingir pelo ciberterrorismo, pela forma cirúrgica como se pode fazer parar um país, sem sangue, sem uma generalizada destruição física e às mãos de uma equipa "pequena e civil", quer enquanto conhecimento prático, detido e continuado, há já vários anos, que pode contribuir para o enriquecimento da Política de Ciberdefesa.

Atento ao propósito inicial e confirmando-se pela afirmativa a sua dupla importância, conclui-se o presente tema com uma sugestão de modelo macro integrador de atuação face a ataques no ciberespaço.



Por definição (ver figura), o ciberespaço varre um espetro eletrónico que é comum às chamadas dimensões convencionais da guerra, na sua geografia física – a terra, o mar, o ar e o espaço – mas numa nova variante, a dos sistemas de informação, que se encontram por facilidade académica subdivididos nas camadas: cognitiva ou do utilizador onde o cidadão comum navega através de *écrans*; física, onde se acomodam os programas, as ferramentas e os serviços usados; e na técnica ou aplicacional onde se recolhem as funcionalidades, se transformam os dados através do desenho técnico e da programação e se descarregam, devidamente formatados, os resultados obtidos.

É destas quatro por três dimensões que nasce o "nosso" ciberespaço constituído por doze nós sobre os quais se deve atuar de forma orquestrada, planeada, no tempo. Definida a estratégia de ciberdefesa, há que saber recrutar os profissionais, organizá-los, armá-los, desenhar taticamente a campanha e a batalha a travar, perspetivando as consequências.

É, exatamente, nesta sucessão de passos, aquilo a que chamamos o desenrolar da ação, que sugerimos a participação do setor bancário, à semelhança das elétricas e das *telco*[11]. Se estas últimas são consideradas parte integrante dos meios logísticos que importa salvaguardar, o primeiro deverá ser visto como o "grude" do sistema. Podemos "ver" com geradores alternativos, comunicar com equipamentos portáteis mas, sem moeda, invenção com mais de dois mil anos, retrocederíamos à Idade da Pedra. Integrada no seu conjunto, permitirá ao comando da ciberdefesa incrementar o seu poder de decisão, enquadrar, de forma homogénea, a abordagem de cada um dos setores civis (banca, elétricas e *telcos* em t=1), coordenar o sistema de um ponto de vista militar como um todo (i, j, t=2), identificar quem é quem na cadeia de responsabilidades do plano de continuidade em cada um dos setores e estabelecer o perímetro de risco de destruição (momento i, j, t=1) e respetiva defesa.

Postas as vantagens, o que fazer em primeiro lugar? Construir uma taxonomia de incidentes, de acordo, na componente civil, com o "*National Institute of Standards and Technology*" (interdição de acessos, código malicioso, "*denial of service*" e usos inapropriados), escolher ferramentas de classificação de dados de acordo com níveis de risco de perdas (classificação de ativos), identificar KPI's (*Key Performance Indicators*) a atingir em caso de perdas (serviços, aplicações, infraestruturas de base classificadas por grau de importância), definir modelos e equipas de ação a integrar na sala de guerra (papéis a desempenhar individual e coletivamente, escalonamento de problemas, protocolos da "*war room*", (…)), identificar os pontos de falha robustecendo-os e implementar, como corolário, o plano de continuidade.

Nova pergunta se impõe. Em que deve consistir o P.C.[12]? Sugerem-se oito fases: uma introdução, com o propósito, âmbito e pilotagem do próprio plano; um segundo bloco, de como o usar, explicando o modo de funcionamento da sala de guerra de acordo com as diversas escalas de problemas às crises; um terceiro capítulo, com a caracterização de problemas e respetiva atuação em função da sua dimensão; uma quarta parte, com a classificação dos ativos por níveis de risco de perda; uma quinta subdivisão, com as equipas envolvidas e suas respetivas responsabilidades, e formas de organizar os processos de trabalho; uma sexta, com os subplanos por tipologia de incidente, de ativos implicados e processos atingidos pelo ciberataque; um sétimo, capaz de efetuar o rescaldo da guerra tratando da documentação dos detalhes dos incidentes e respetivas ações de mitigação; culminando num oitavo, com as lições aprendidas, de molde a serem incorporadas em semelhantes situações futuras, no pressuposto de se ter sobrevivido (i, j, t=3). O que se acabou de descrever não é teoria, mas antes uma prática continuada no setor bancário que se acredita seja útil integrar neste processo.

Conclusão

A ciberguerra travada no ciberespaço, obrigando a uma aproximação diferenciada não convencional, obriga-nos a considerar cada vez mais "*players*" no tabuleiro das Políticas de Defesa Nacional. A banca, em particular, com o seu histórico, de quase vinte anos, de

Planos de Contingência ao nível das TIC, deverá inserir-se nessa operacionalização sistémica, quer enquanto alvo quer enquanto prestador de experiências a que se encontra sujeito no seu dia-a-dia combatendo a cibercriminalidade. De que forma? Passando a fazer parte do perímetro definido pela Política Comum de Segurança e Defesa da União Europeia.

---

[1] Resolução do Conselho de Ministros nº 19/2013, de 21 de março, que refere a necessidade de identificar o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários num ambiente de segurança global; Resolução do Conselho de Ministros nº 26/2013, de 19 de abril, relativa à Reforma "Defesa 2020", onde se fala dos passos necessários à criação de um Centro de Ciberdefesa.

[2] Despacho nº 5590/2012, de 11 de abril, relativo à definição e implementação da Estratégia Nacional da Informação englobando a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança.

[3] Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité de Regiões [Join (2013) 1 final], relativa à Estratégia da União Europeia para a Cibersegurança, de 7 de fevereiro de 2013.

[4] *Active Server Pages* – Estrutura de bibliotecas para processamento de linguagens de *"script"* capazes de gerar conteúdos dinâmicos ao nível da *Web.*

[5] *Hypertext Transfer Protocol* – Protocolo de comunicação ao nível da camada de aplicação de acordo com o modelo OSI *(International Organization for Standardization)* e que serve para transmitir dados da WWW *(World Wide Web).*

[6] *Object Linking and Embedding Database* – Interface de Programação de Aplicações que permite aceder de forma universal a diversas fontes de dados.

[7] *Open Database Connectivity* – Modelo de acesso padronizado a sistemas de gestão de bases de dados (SGBD).

[8] Carta Circular nº 75/2010/DSB, de 3 de dezembro, que revogou as recomendações publicadas por Carta-Circular nº 100/2005/DSB, de 26 de agosto.

[9] O Acordo de Capital de Basileia II, ou simplesmente chamado de B II, assente em três pilares, o de Capital, o de Mercado e o de Supervisão.

[10] Citação da página 2 da Carta Circular nº 75/2010/DSB, de 3 de novembro.

[11] Companhias de telecomunicações.

[12] Plano de Contingência.