

Inevitabilidade Digital: O Poder dos Laços Fracos, Convergência e Curiosidade na Disseminação do Stuxnet

Digital Inevitability: The Power of Weak Ties, Convergence and Curiosity in Stuxnet's Dissemination

Hugo Ramos*

*ISCTE-IUL - Instituto Universitário de Lisboa

Resumo

Este artigo debate o conceito da inevitabilidade digital no contexto da ciberguerra e está organizado em quatro partes. Os quatro temas discutidos são: o enquadramento internacional do novo tipo de guerra, a contextualização histórica do Stuxnet, os conceitos e princípios da análise de redes em ciências sociais e, por fim, a apresentação do conceito de inevitabilidade digital.

O conceito de inevitabilidade digital envolve três princípios: a força dos laços fracos, a convergência das redes na rede e o poder motivador da curiosidade como motor do comportamento humano. A análise deste conceito é feita sobre o caso real da rede de disseminação do Stuxnet, desde a sua concepção até à entrada na rede privada e segura da central nuclear de Natanz.

Palavras-Chave: inevitabilidade digital, laços fracos, convergência, curiosidade.

Abstract

This article argues about the concept of digital inevitability, in the cyber war framing, and it is organised in four parts. The four topics discussed are: the new kind of war in the international context, Stuxnet's historical context, the concepts and principles of network analysis in social sciences and the introduction of the digital inevitability concept.

The concept of digital inevitability involves three main principles: the strength of weak ties, the convergence of networks into the network and the motivating power of curiosity as a drive for human behaviour. The analysis of this concept is made on the real case of Stuxnet's network of dissemination, since its conception until its entrance in Natanz nuclear facility's private and secure network.

Keywords: digital inevitability, weak ties, convergence, curiosity.

"...information-gap perspective (...) can account for the observed motivating power of curiosity."

— George Loewenstein, 1994

A Era da Informação revolucionou os comportamentos e o método como se desenvolve o conflito no século XXI. Quando referimos conflito, reportamo-nos ao sentido tradicional de conflito entre Estados-nação que se desenvolve sob a forma de guerra.

De acordo com o general e teórico prussiano Carl Von Clausewitz, a guerra define-se como: "an act of force to compel our enemy to do our will" (Howard e Paret, 1984, p.75). Estes actos têm sido repetidos ao longo da história e envolveram sempre o exercício de soberania de um Estado sobre outro. Esta forma de guerra, aquela que se desenrola no plano físico e geográfico, envolvendo soldados humanos munidos de armas, sempre foi designada como convencional¹.

Os princípios que regem o estado de pré-guerra e guerra estão considerados em regras e limitações reconhecidas internacionalmente, na forma de teoria da guerra justa (*justum bellum*), em duas partes essenciais: (1) o direito a declarar guerra (*jus ad bellum*) e (2) as normas de conduta a observar durante o conflito (*jus in bello*) (Boylan, 2013, p.11).

O ponto (1) é geralmente parte integrante da Constituição de um país e a sua decisão é atribuída à "autoridade pública legítima" (Mushkat, 1987, p.98). O ponto (2) é regido pelo documento vulgarmente designado como Convenção de Genebra, mas que, na realidade, contém quatro tratados e três protocolos, chamando-se, oficialmente, Convenções de Genebra.

O seu precursor foi Jean Henri Dunant que, em 1863, elaborou duas propostas: a criação de uma agência internacional com fins humanitários em período de guerra e um tratado governamental, reconhecendo a neutralidade desta agência e permitindo-lhe o acesso a zonas de guerra com o propósito de proteger e respeitar a vida e saúde humanas e ajudar a aliviar o sofrimento provocado pelo conflito. A primeira proposta culminou na fundação da Cruz Vermelha, ainda em 1863, e a segunda, já em 1864, resultou na primeira Convenção de Genebra. Estas acções valeram a Dunant o primeiro Prémio Nobel da Paz em 1901.

Depois da primeira Convenção de Genebra, seguiram-se mais três, em 1906, 1929 e 1949, depois do final da II Guerra Mundial, onde foram sendo actualizadas as disposições criadas em 1864.

¹ A guerra convencional é uma forma de guerra conduzida pela utilização de armas vulgares (nos tempos recentes por armas de fogo) e tácticas militares no campo de batalha, entre dois ou mais estados, em confronto aberto e directo. As forças de cada lado são bem definidas e lutam com armas que visam o exército inimigo.

No entanto, as Convenções de Genebra regem, apenas, a condição humana em tempo de guerra, não mencionando qualquer disposição (com excepção do protocolo sobre guerra bioquímica de 1925) sobre o material bélico usado nos conflitos, o qual é abrangido pelas Convenções de Haia. Estas convenções realizaram-se em 1899 e 1907 e produziram um conjunto de declarações e tratados internacionais que resultaram nas leis da guerra, definindo um conjunto de regras que devem ser observadas pelos actores do conflito relativamente às armas por estes utilizadas.

Tendo em conta as Convenções de Genebra e Haia, existe um conjunto de tratados e regras internacionais que regulamentam o uso de armas em estado de guerra, mas muitos especialistas e académicos reclamam actualizações, devido ao facto de estes estarem desactualizados e não abrangerem a situação actual relativamente ao tipo de armas usadas em conflito. O seu principal argumento baseia-se no facto da ciberguerra e das ciber-armas não estarem, ainda, contempladas.

Porém, em virtude da rápida proliferação deste novo tipo de guerra e novas armas e, também, devido ao exemplo verificado na Estónia, em 2007, e ao Stuxnet² no Irão, em 2010, considerados, respectivamente, como a primeira ciberguerra e a primeira ciber-arma da história (Ramos, (in press)a, pp.5-7), a NATO, no relatório anual de 2011, elaborado pelo seu Secretário Geral Anders Fogh Rasmussen, clarificou a sua posição relativamente aos ataques cibernéticos, elevando-os ao mesmo nível dos ataques com armas nucleares:

“The security environment continues to change at a rapid rate and NATO has invested in 2011 to ensure that the Alliance is capable of meeting these emerging security challenges. Cyber attacks, the proliferation of weapons of mass destruction, terrorism and other emerging threats such as energy vulnerabilities increasingly affect the security of NATO's almost 900 million citizens” (Rasmussen, 2012).

O enquadramento desta temática chega mesmo a ser relevante na perspectiva da lei internacional relativamente aos direitos de auto-defesa, por parte de um Estado atacado ou aos direitos de auto-defesa colectiva, no caso de Estados que decidam participar na guerra em auxílio de um Estado atacado, o chamado princípio “*attack-on-one-attack-on-all*”.

Segundo a Carta das Nações Unidas, este princípio está consagrado no seu artigo 51º, mas, o que inicialmente era visto como um problema linguístico, assumiu outras proporções no mundo político ou ideológico relativamente à aplicação desta instituição. Segundo Mushkat (1987, pp.146-150), existem três posições predominantes nesta matéria: (1) os Estados que invoquem o princípio da auto-defesa colectiva

² *Malware*, descoberto em 2010, que atacou o programa nuclear iraniano na Central Nuclear de Natanz.

não o podem fazer sem que exista uma pretensão individual que, na mesma circunstância, poderia ser invocada usando o princípio da auto-defesa individual. (2) O princípio da auto-defesa colectiva define, essencialmente, a defesa de outro Estado por parte de Estados que vão em seu auxílio perante um ataque armado. E que (3) apenas no caso do ataque ao Estado visado constituir um potencial risco de segurança ao Estado que vai em seu auxílio, pode, este último, actuar no conflito.

Então para que servirão todos estes tratados, convenções e regras internacionais, se o Estado atacado desconhecer a proveniência de um ataque? Como podem estes princípios ser invocados, se o agressor estiver escondido por detrás de uma rede informática que não conhece fronteiras nem espaços soberanos e anular qualquer evidência da sua participação? Qual pode ser a reacção de um Estado perante a participação, mesmo que inconsciente, de um dos seus cidadãos na ligação do último elo que falta entre a esfera da rede pública e a rede segura de instalações militares ou outras, também de carácter sensível?

Em virtude destas e outras perguntas pertinentes, da relevância adquirida pelo uso de *malware*³ como arma de guerra e, também, devido à abertura de uma precedência com os factos ocorridos em Natanz, no Irão, impõe-se um estudo ontológico mais detalhado do Stuxnet e das circunstâncias que envolveram a sua criação, disseminação e utilização.

Este artigo discute a utilização das novas TIC como meio de disseminação do Stuxnet numa perspectiva Castelliana de *network society*, invocando conceitos como *network theory*, *network theory of power*, *network multidimensionality* e *digital inevitability*, sendo que, este último, será introduzido e clarificado, mais adiante, neste texto.

Contextualização Histórica do Stuxnet

No verão de 2010, várias empresas fabricantes de anti-vírus detectaram uma nova infecção no sistema operativo Windows que se espalhava lentamente pelos computadores dos seus clientes, em todo o mundo. O primeiro especialista em vírus informáticos a detectar o Stuxnet foi Sergey Ulasen (Kaspersky, 2011) que, em 12 de Junho desse ano, quando o primeiro indício da existência deste *malware* lhe foi reportada por um cliente, trabalhava na empresa bielorrussa produtora de software anti-vírus VirusBlokAda.

Ulasen recebeu um telefonema de um amigo e parceiro de trabalho, localizado no Irão, que dá assistência local a um cliente daquele país. Segundo informações iniciais deste parceiro, mais tarde actualizadas, o que

³ *Malware* é a designação curta de malicious software e abrange todos os tipos de software que podem provocar a quebra da operação normal de um computador, a recolha de informação sensível ou a administração de sistemas informáticos privados para os quais não teriam autorização de administração.

aparentava ser apenas um problema de configurações nos computadores afectados, revelou-se mais complicado e suspeito após as análises subsequentes. Ulasen estabeleceu um acesso remoto ao computador afectado no Irão e, juntamente com o seu parceiro local de investigação, conseguiram identificar o *malware* que estava a afectar os sistemas, a sua natureza camuflada, o estranho *payload*⁴ e as técnicas de propagação que utilizava. No entanto, o que mais preocupou Ulasen foi o facto de este *malware* estar a utilizar certificados digitais de uma empresa bastante reconhecida no mercado e, com isso, passar despercebido ao sistema de verificações do sistema operativo. Ulasen concluiu que os agentes por detrás do Stuxnet roubaram os certificados digitais desta empresa e introduziram-nos no seu *malware*, para que este não fosse identificado como potencial ameaça ao infectar os computadores por onde passava.

Como consequência desta extensa análise, a equipa liderada por Ulasen chegou à conclusão de que o Stuxnet usava quatro falhas no sistema operativo Windows (situação inédita até 2010. Todos os vírus, até então, usavam uma ou, no máximo, duas falhas do sistema operativo que infectavam) (Symantec, 2010), o que, *per se*, demonstrava as capacidades dos actores envolvidos na sua concepção. A equipa acabou por concluir que

“this malware was a fearsome beast with nothing else like it in the world, and that we needed to inform the infosec industry and community of the details” (Kaspersky, 2011).

Chegados a este ponto, e em virtude da gravidade dos factos, os investigadores decidiram informar a indústria informática desta descoberta. Em particular, informaram a Realtek, empresa cujos certificados digitais teriam sido roubados, e a Microsoft, empresa produtora do sistema operativo afectado, o Windows. Em virtude de não obterem qualquer resposta destas duas empresas, no dia 17 de Junho de 2010 decidiram que o caso não poderia permanecer mais tempo em segredo e Ulasen publicou as informações até então conhecidas sobre o Stuxnet no site da empresa VirusBlokAda. Nesta publicação podemos ler o seguinte:

“Modules of current malware were first time detected by "VirusBlokAda" company specialists on the **17th of June, 2010** and were added to the anti-virus bases as **Trojan-Spy.0485** and **Malware-Cryptor.Win32.Inject.gen.2**. During the analysis of malware there was revealed that it uses USB storage device for propagation. You should take into consideration that virus infects Operation System in unusual way through vulnerability in processing lnk-files (without usage of

⁴ No contexto da segurança informática, *payload* refere-se às acções maliciosas que um *malware* pode executar no computador que infectou e os consequentes resultados dessas acções.

autorun.inf file). So you just have to open infected USB storage device using Microsoft Explorer or any other file manager which can display icons (for i.e. Total Commander) to infect your Operating System and allow execution of the malware. Malware installs two drivers: mrxnet.sys and mrxcls.sys. They are used to inject code into systems processes and hide malware itself. That's the reason why you can't see malware files on the infected USB storage device. We have added those drivers to anti-virus bases as **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2**. Note that both drivers are signed with digital signature of Realtek Semiconductor Corp. (www.realtek.com).

Thus, current malware should be added to very dangerous category causes the risk of the virus epidemic at the current moment. After we have added a new records to the anti-virus bases we are admitting a lot of detections of **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2** all over the world.”⁵ (Ulasen, 2010).

A publicação desta informação iniciou uma reacção em cadeia que acabou por levar a Microsoft a analisar o caso Stuxnet através de uma equipa de engenheiros de *software* liderada por Bruce Dang (Borland, 2010). No entanto, a informação mais relevante para este artigo, que podemos retirar da publicação citada, é o modo como o Stuxnet infecta e se propaga nas redes de computadores afectadas: obviamente, além do uso das próprias redes informáticas às quais os computadores já infectados estão ligados, através de uma caneta USB⁶ (designada a partir daqui como CUSB), quando a rede ainda não foi afectada pelo *malware* e se encontra isolada de outras redes infectadas. A existência da CUSB neste contexto é um dos tópicos fundamentais na introdução dos conceitos de *digital inevitability* e *network multidimensionality* de que falaremos mais adiante. De acordo com Ulasen, a reacção das autoridades iranianas relativamente aos factos descritos foi surpreendente. Não existiu qualquer tipo de resposta ou comunicado oficial. O parceiro de Ulasen que, localizado no Irão, ajudou na recolha inicial de informação sobre as acções e resultados provocados pelo Stuxnet, pediu ao seu colega que não divulgasse o seu nome em qualquer tipo de relatório ou comunicado produzido pela empresa VirusBlokAda e absteve-se de qualquer tipo de comentário sobre os factos ocorridos no Irão. Mais tarde, em Minsk, o próprio Ulasen esteve presencialmente com alguns responsáveis iranianos de tecnologias de informação, com elevadas patentes e, quando confrontados com os factos ocorridos relativamente ao Stuxnet, estes afirmaram desconhecer qualquer tipo de infecção ou problema, no Irão, provocado por esse *malware*, como o próprio refere na sua entrevista:

⁵ Negritos pelo autor do texto citado.

⁶ Vulgarmente designada pelo nome original em inglês: *USB pen*, *USB stick* ou *USB flash drive*.

“Interestingly, later I met some high-ranking IT-dedicated Iranian officials in Minsk. They made like they didn’t know anything at all about the incident. Yeah, right” (Kaspersky, 2011).

Por seu lado, a Microsoft que, inicialmente, tal como Ulasen, esteve quase a desistir da investigação por pensar tratar-se de um caso vulgar ou já conhecido, decidiu organizar uma equipa de engenheiros e estudar o caso. As conclusões a que chegaram provam que Ulasen estava correcto desde o início, assegurando que o meio de infecção deste *malware* consistia na exploração de uma vulnerabilidade relacionada com o sistema de leitura de ícones dos ficheiros contidos numa CUSB, que dava privilégios de escrita ao Stuxnet no sistema do computador em questão. Perante a simplicidade de exploração desta vulnerabilidade e a pressão colocada sobre a Microsoft por um grande número de clientes, a equipa disponibilizou vários ficheiros com correcções que, supostamente, iriam resolver o problema. Dang referiu:

“A 7-year-old could exploit this. It’s bad news. Of course it turned out that this vulnerability had been known for several years by some people, but no one told me” (Borland, 2010).

No entanto, quando Dang pensava que a sua equipa tinha resolvido o problema, depois de alguma análise posterior, chegaram à conclusão que o *malware* estava a obter privilégios de administração nos computadores infectados e a continuar a sua actividade. O problema parecia não ter fim e, porque em teoria o código fonte de um vírus não é perfeito, Dang chegou a acreditar que, deixando-o executar as suas acções continuamente, o Stuxnet acabaria por provocar uma falha nas chamadas de memória e o sistema cairia num *blue screen*⁷ que mostraria mais detalhes sobre o problema. Infelizmente, o código fonte do Stuxnet era tão perfeito que foi executado dez vezes seguidas sem nunca provocar a desejada falha no sistema. Para piorar ainda mais o curso desta investigação, Dang recebeu uma chamada telefónica da empresa Kaspersky⁸, durante a qual foi informado de que os computadores infectados estariam a efectuar ligações em rede a outros computadores, dando-lhes instruções para efectuar acções ordenadas por este *malware*.

Para verificar a veracidade desta informação, Dang decidiu montar uma pequena rede de computadores, infectar um deles através de uma CUSB e abandonar a sala por algum tempo. Quando a equipa voltou, todos os computadores dessa rede estavam infectados. Este teste permitiu-lhes descobrir que o Stuxnet se

⁷ Nome atribuído ao ecrã de falha do sistema operativo Windows quando ocorre uma falha nas chamadas de memória feitas por um programa em execução.

⁸ Empresa russa que desenvolve *software* anti-vírus.

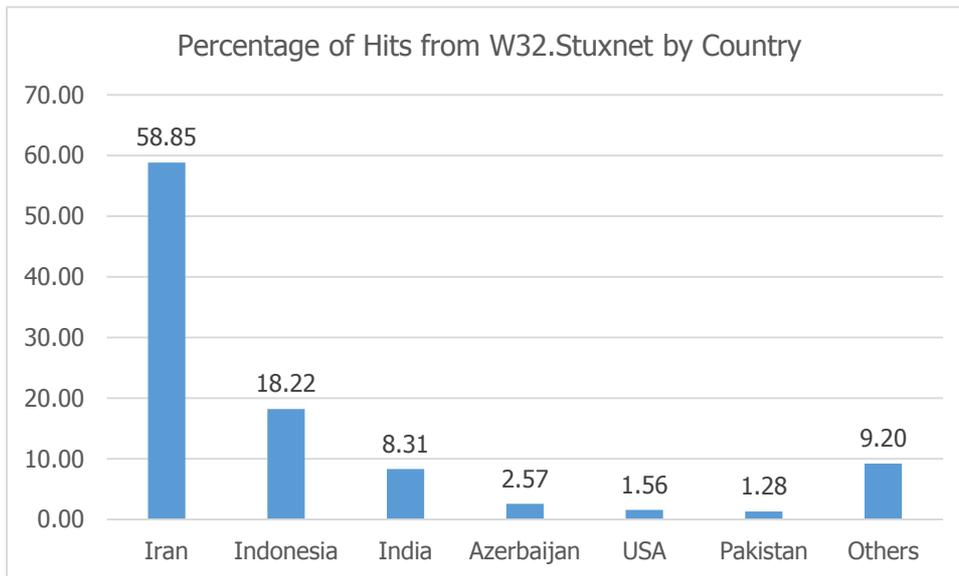
aproveitava de outra falha no sistema de impressão em rede do Windows, tendo este sido rapidamente corrigido. Relativamente ao trabalho da Microsoft na identificação das vulnerabilidades que o Stuxnet usava para infectar o computador inicial e os computadores ligados na mesma rede, o seu trabalho estava terminado. As falhas foram corrigidas e disponibilizados novos ficheiros para que os clientes afectados corrigissem o problema nos seus computadores.

Porém, ao final de quatro dias de intensa investigação, Dang não deixou de afirmar que:

“several things are clear from the reading of the code. It was written by at least several people, with the different components bearing the fingerprints of different authors. And the creators were careful to make sure that it ran perfectly, with high impact and 100 percent reliability. That’s a goal even commercial software developers often fail to meet” (Borland, 2010).

Estava descoberto o Stuxnet, as falhas do Windows que este aproveitava para expandir a sua acção, mas ainda não se conhecia, exactamente, a sua origem e os seus objectivos. A maioria do *malware* que circula pela Internet tem objectivos relacionados com o lucro fácil e muitos analistas e especialistas em segurança informática já conhecem o método para chegar à origem do mesmo: seguir o rasto do dinheiro. No entanto, o Stuxnet não persegue o lucro fácil, dificultando a descoberta da sua origem. Além deste problema, a propagação parece ser direccionada e não indiscriminada, forma como, geralmente, muitos *malwares* se propagam.

Através da figura 1, podemos ver como as infecções são localizadas maioritariamente num país: o Irão. A indicação, *per se*, da natureza localizada das infecções, poderia não dar nenhuma evidência relativamente aos objectivos do Stuxnet contudo, no dia 25 de Setembro de 2010, a agência noticiosa Associated Press lançou um comunicado (Karimi, 2010), referindo que as autoridades iranianas tinham denunciado um ataque informático, na forma de *malware*, que estaria a afectar algumas centrais de produção de material nuclear no país. Por medida de precaução, este tipo de instalações está sempre desligada de qualquer acesso à Internet ou outras redes públicas para evitar que um vírus possa afectar sistemas tão críticos. Este facto justifica a utilização da CUSB como forma de infectar o primeiro computador da rede interna, sendo que a vulnerabilidade do sistema de impressão em rede do Windows permitiria a infecção dos restantes computadores.

Figura 1: Percentagem de infeções por país. (Fonte: Symantec, 2010)

Porém, foi Ralph Langner, um especialista em segurança informática, que juntou as diversas evidências já descritas e, juntamente com a sua análise do código fonte do Stuxnet, descobriu os objectivos deste *malware*: através da infeção de computadores PLC da Siemens, provocar a aceleração e consequente explosão das centrifugadoras de enriquecimento de urânio, existentes no Irão, e provocar o atraso do programa nuclear iraniano (Langner, 2013). Como o próprio refere:

“the idea behind the Stuxnet computer worm is actually quite simple: we don’t want Iran to get the bomb” (TED, 2011).

Mas Langner vai ainda mais longe nas suas afirmações:

“My opinion is that the MOSSAD is involved but that the leading force is not Israel. The leading force behind that is the cyber super-power. There is only one and that’s the United States” (TED, 2011).

O Stuxnet foi um marco na história da ciberguerra e considerado a primeira ciber-armas, visto que, pela primeira vez, um *malware* passou do plano virtual para as consequências no plano físico, atacando

centrifugadoras de urânio e provocando a sua explosão, atrasando, assim, o programa nuclear iraniano. Um objectivo puramente militar.

Dos Conceitos e Princípios na Análise de Redes Sociais

Hoje, as redes são um componente essencial no estudo das ciências sociais. Desde o final do século XX, quando a presença da Internet se propagou exponencialmente, que as redes são, cada vez mais, objecto de teorias em variadas áreas de estudo das ciências sociais e constituem o fundamento de muitos conceitos que relacionam a prática social com o tempo e o espaço.

Na teoria social, o espaço pode ser definido como o suporte material de práticas sociais compartilhadas no tempo e o tempo podia ser definido como a sequência dessas práticas sociais (Castells, 2009, p.34). O uso intencional da palavra "podia", por Castells, justifica-se pelo facto de ter havido grandes mudanças relativamente à definição deste componente da teoria social. Enquanto que o espaço sofreu diferenças nas dinâmicas de abrangência e materialidade, mas não sofreu alterações de definição de conceito, o tempo, por outro lado, sofreu alterações ao nível do conceito, não tendo perdido muito da sua materialidade sequencial de eventos.

A introdução de toda uma nova teoria social, baseada no efeito combinado das novas tecnologias de informação e comunicação (designadas a partir daqui como TIC), surgidas na segunda metade do século XX, com as novas formas e processos sociais e as alterações comportamentais verificadas empiricamente na sociedade global, trouxe, também, redefinições de espaço e tempo. Castells introduziu as novas formas sociais de espaço e tempo, relacionando-as com as relações de poder que constituem a fundação da construção social desse mesmo espaço-tempo, como *space of flows* e *timeless time* (Castells, 2010).

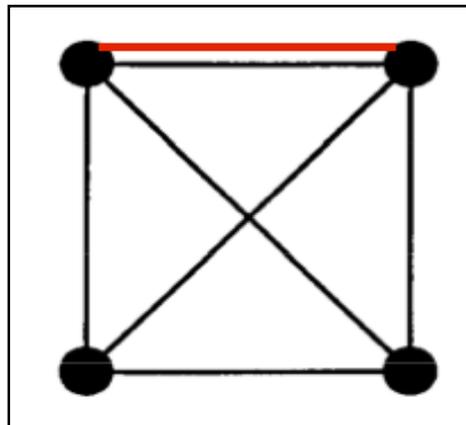
No entanto o que é uma rede? Antes de qualquer avanço no campo teórico das redes, é necessário clarificar o conceito de rede.

Uma rede é um conjunto de nós e interligações que unem esses nós. Um nó é o ponto onde as interligações se cruzam e uma interligação é a relação existente entre dois nós. Por outras palavras, para que uma rede possa existir, necessita obrigatoriamente de três nós e duas interligações. Dois nós e uma interligação constituem uma relação (Dijk, 2006, p.24) e um nó isolado sem interligações constitui um indivíduo, não havendo, então, em nenhum destes dois últimos casos, uma rede. Personificando esta definição, consideremos uma família tradicional de quatro elementos (pai, mãe, filho e filha) (figura 2), em que os pais são casados e os filhos maiores de idade, constituem uma rede de quatro nós e sete interligações. Aparentemente, poder-se-ia pensar que são seis interligações mas, se considerarmos as condições descritas, os quatro nós são constituídos pelos quatro humanos desta família e existem seis interligações de natureza biológica, sendo elas as relações directas existentes entre cada um deles. O pai e a mãe têm uma relação

biológica como progenitores dos filhos, cada um dos filhos tem uma relação biológica com cada um dos progenitores e os filhos, entre si, têm mais uma relação biológica de irmãos. O total resulta em seis interligações (relações) de natureza biológica. Mas onde está a sétima interligação neste exemplo? Na relação de natureza legal que une os pais através do casamento (interligação a vermelho). A não existência de mais interligações desta natureza resulta da maioridade dos filhos que, já não têm este tipo de relação legal com os pais, nem entre si.

Este exemplo demonstra bem o conceito de rede numa das suas formas mais simples, mas introduz, também, o exemplo da possível diferença de natureza dos dois tipos de interligações (relação legal e relação biológica).

Figura 2: Rede Familiar de 4 nós (Fonte: Haythornthwaite, 1996; editado pelo autor)



Do ponto de vista Castelliano da *network society* (2010) e, no âmbito das novas TIC, esta rede poderia ser analisada de inúmeras perspectivas. Por exemplo, se cada um dos elementos desta família tiver um telemóvel e o usar para comunicar com os restantes elementos da família, exactamente com a mesma tipologia das relações biológicas, temos uma rede que pode ser analisada da perspectiva da frequência com que cada elemento comunica com os restantes, chegando a conclusões, tais como quão forte ou fraca é a interligação que une os diferentes nós desta rede. Se o pai ligar à mãe sete vezes por semana, e ligar ao filho apenas uma vez por semana, temos uma interligação pai-mãe com mais intensidade do que a interligação pai-filho. Porém, ao apresentarmos este novo exemplo, apresentámos também mais alguns conceitos relacionados com o estudo das redes sociais. Por um lado, introduzimos o conceito de intensidade da interligação que, por definição, consiste numa análise quantitativa das relações existentes dentro de uma rede. Por outro lado, introduzimos o conceito de multidimensionalidade da rede. No exemplo acima, este conceito está patente na

utilização de telemóveis (objectos tecnológicos) para estabelecer interligações de comunicação entre os nós, mas, sobretudo, interligações entre os nós humanos e os nós tecnológicos (telemóveis), introduzindo, assim, uma nova dimensão (de natureza tecnológica) na análise. Enquanto na análise tradicional e unidimensional das redes sociais, o pai e o seu telemóvel constituem um único nó, na perspectiva da análise multidimensional, existe uma ruptura nodal entre o pai e o seu telemóvel, passando, cada um deles, a ser um nó da rede em análise. A rede de quatro nós passa a uma rede de oito nós e o objecto tecnológico deixa de ser um elemento passivo, tornando-se actor. Temos, então, a tecnologia endógena à rede, potenciando uma série de novos tipos de elementos passíveis de análise no estudo das redes sociais como, por exemplo, pessoas, telemóveis, computadores, livros, *etc.*. A entrada da multidimensionalidade no estudo das redes sociais permitiu o estudo, não apenas das relações entre indivíduos, como também das relações dos indivíduos com os objectos tecnológicos e dos objectos tecnológicos entre si.

Por fim, introduzimos, também, os conceitos de *space of flows* e *timeless time*. A inserção dos telemóveis na rede familiar veio provocar alterações de abrangência espacial no processo comunicativo familiar. Se, antes das TIC, o processo comunicativo da família se restringia, sobretudo, ao espaço do lar ou ao espaço onde os nós da rede se encontravam fisicamente numa perspectiva de relativa proximidade auditiva, depois das TIC, este espaço foi praticamente anulado ou substituído pelo *space of flows*. O *space of flows* é o novo espaço por onde se desenrola o mesmo processo comunicativo do passado. É a rede por onde passa a corrente de informação entre os nós da família. O "sítio" físico da reunião familiar é substituído pelo espectro rádio da rede de telemóvel ou pela rede da Internet, quando um nó distante usa o telemóvel ou o Skype para comunicar com a restante família. O *space of flows* é a conceptualização da substituição do espaço físico pelo espaço compreendido nos meios por onde a comunicação é, hoje, efectuada (Castells, 2010, pp.407-459). Temos, portanto, um espaço social que é dinâmico e constantemente mutável.

Contudo, não foi apenas o espaço social que sofreu alterações. Também o tempo social foi atingido pela influência das TIC. Castells denominou o tempo da *network society* como *timeless time* depois de observar a forma como as sequências de eventos ou processos sociais, num determinado contexto, deixaram de ter uma sucessão lógica ou cronológica. O exemplo que Castells observou primeiro ocorreu nas redes financeiras, mas apontou outros exemplos, como a capacidade que a ciência médica tem de controlar o relógio biológico do corpo humano e permitir, a uma mulher, a concepção de uma criança numa idade da sua escolha ou a cada vez menor clivagem entre o tempo pessoal, o tempo familiar e o tempo de trabalho, num contexto sócio-profissional, desde sempre governado, numa perspectiva muito Foucaultiana, pelo tempo industrial (2010, p.xli). Outro exemplo, aplicável, também, no exemplo da nossa rede familiar de quatro nós, é a permeabilidade de todos os tempos e espaços pela rede wireless que chega aos dispositivos tecnológicos que usamos nos dias de hoje. O facto de recebermos um telefonema ou um comentário no Facebook, durante

o jantar de família, provoca uma quebra no espaço-tempo desta prática social que, antes das novas TIC, era impermeável e determinado. Castells define, assim, o *timeless time* como o tempo do curto "agora", sem relação com o passado nem com o presente:

"Timeless time, the time of the network society, has no past and no future. Not even the short-term past. It is the cancellation of sequence, thus of time, by either the compression or blurring of the sequence. So, power relationships are constructed around the opposition between timeless time and all other forms of time. Timeless time, which is the time of the short "now," with no sequence or cycle, is the time of the powerful, of those who saturate their time to the limit because their activity is so valuable." (Castells, 2009, p.50).

De acordo com Haythornthwaite (1996), a análise de redes sociais difere de outros tipos de análise, porque se foca na observação empírica dos padrões emergentes nas relações de troca de recursos entre actores. Haythornthwaite apresenta diversos princípios da análise das redes sociais focados na natureza das interligações. Um deles é o (1) **conteúdo ou recursos**. As relações entre nós implicam troca, partilha ou entrega de uma variedade de recursos. Estes recursos podem assumir diversas formas e servir variados objectivos. Um dos mais comuns é a partilha de informação. Um estudo focado no tipo de conteúdo que é partilhado numa rede deve ter em conta a filtragem e selecção da informação relevante para o estudo em questão. Por exemplo, um estudo que pretenda responder à pergunta: "o email da empresa é mais usado para comunicação profissional ou pessoal?" deve concentrar-se em todas as interligações que representam uma troca de email e descartar os restantes tipos de comunicação, fazendo depois uma análise qualitativa dos temas observados nas trocas de informação.

Um outro princípio é a (2) **direcção**. As relações entre nós podem ser unidireccionais ou bidireccionais. Isto significa que a informação pode, por exemplo, circular apenas numa estrutura hierárquica *top-down* sem que haja resposta (*bottom-up*). Este exemplo verifica-se na rede comunicativa de muitas organizações institucionais ou profissionais, constituindo uma comunicação assimétrica. Por outro lado, a comunicação pode ser completamente bidireccional como, por exemplo, na rede familiar do nosso exemplo durante um jantar em que todos falam com todos e obtêm resposta, constituindo uma comunicação simétrica.

A (3) **intensidade** é outro princípio da análise de redes sociais focado na natureza das interligações. Este princípio refere-se ao grau de actividade numa determinada interligação, tendo sido clarificado através do exemplo do número de ligações telefónicas que podem existir entre dois nós em detrimento do número de ligações que podem existir entre outros nós.

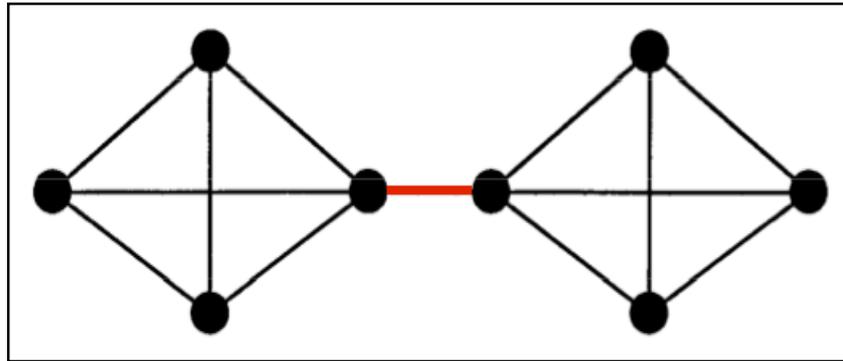
Por último, mas não menos importante, a (4) **força dos laços** que interligam os nós de uma rede. O laço que une dois nós depende directamente do número e tipo das relações existentes entre os dois, mas também da intensidade de cada relação individualmente. No entanto, segundo Haythornthwaite, para que uma distinção entre laços fracos e fortes possa ser feita, existe a necessidade de contextualizar a relação entre os nós, determinando, assim, o nível de "proximidade" entre os actores unidos por esse laço. Na figura 3, podemos ver um exemplo de uma rede com a existência de um laço fraco (identificado a vermelho). Este tipo de laço é, normalmente, identificado pela existência de dois nós que unem, apenas entre si, duas sub-redes mais coesas, sendo a coesão dos actores determinada por fortes relacionamentos e interesses em comum. Por exemplo, duas sub-redes, constituindo cada uma delas uma família de quatro pessoas, unidas pelo relacionamento amoroso de dois dos seus filhos ou, também comum no mundo profissional, duas equipas de trabalho, de empresas distintas, cada uma delas com um ponto único de contacto para troca de informação e tarefas.

Logicamente, poderíamos pensar que a probabilidade de circulação de informação é mais alta e mais redundante em relações de laços fortes, sendo, estes, importantes para uma maior fluidez de conteúdo. No exemplo da figura 3, é lógico pensar que a informação flui mais rapidamente e com menos possibilidade de impedimentos dentro de cada sub-rede isoladamente do que de uma sub-rede para a outra. Porém, nem sempre é o caso.

Granovetter (1973), através da polémica frase "the strength of weak ties", demonstrou que não é sempre assim. Este sociólogo realizou um estudo em que perguntou a indivíduos, recentemente empregados através de contactos na sua rede de contactos, que tipo de relacionamento existia entre eles e a pessoa que foi determinante para conseguirem esse emprego.

A ideia generalizada de que a probabilidade de obter informações para conseguir emprego é mais alta dentro da rede de contactos mais coesos da pessoa que procura trabalho, foi desfeita. Granovetter demonstrou que, do total de entrevistados, 55,6% conseguiu emprego através de pessoas com as quais mantinha contacto ocasional (mais de 1 vez /ano e menos de 2 vezes /semana), 27,8% conseguiu emprego através de pessoas com as quais raramente mantinha contacto (1 vez /ano ou menos) e apenas 16,7% conseguiu emprego através de pessoas com as quais mantinha contacto regular (2 vezes /semana ou mais).

Figura 3: Rede exemplificativa de um laço fraco. (Fonte: Haythornthwaite, 1996; editado pelo autor)



Granovetter demonstrou que a possibilidade de acedermos a informação mais diversificada e diferente daquela a que acedemos nos círculos mais próximos é maior se mantivermos relacionamentos com laços fracos, acedendo a outros círculos de conteúdo distantes do nosso, sugerindo a “primazia da estrutura sobre a motivação”. O próprio refere:

“A natural a priori idea is that those with whom one has strong ties are more motivated to help with job information. Opposed to this greater motivation are the structural arguments I have been making: those to whom we are weakly tied are more likely to move in circles different from our own and will thus have access to information different from that which we receive.” (Granovetter, 1973, p.1371).

Granovetter demonstrou, assim, que a eficácia da concretização de um objectivo é mais provável através do relacionamento com laços fracos da nossa rede, enquanto um todo (estrutura), do que através do relacionamento com os membros mais próximos e coesos da rede (motivação).

Este princípio é importante, não apenas porque permite determinar quão conectados estão dois nós, mas também, porque ajuda a compreender o nível probabilístico da circulação de informação na rede, servindo para clarificar o conceito de inevitabilidade digital.

Inevitabilidade Digital ou Como o Stuxnet Atingiu o Objectivo

O conceito que pretendemos introduzir neste tópico prende-se com a junção de três ideias fundamentais: a curiosidade como forte condicionante do comportamento humano, o poder dos laços fracos e a convergência tecnológica das redes na rede. Tentaremos demonstrar a sua aplicabilidade através do caso real do Stuxnet.

Antes de avançarmos na clarificação do conceito da inevitabilidade digital, é necessário dar a conhecer e explicar a constituição da rede que permitiu a este *malware* circular desde a sub-rede onde foi produzido até à sub-rede do seu objectivo final (figura 4).

Relativamente aos actores que participaram neste caso, temos os círculos azuis (à esquerda), representando o grupo de actores que desenvolveu o Stuxnet, sendo que o elemento isolado junto à interligação a preto é o actor que transportou a CUSB para um local próximo da central nuclear de Natanz ou para a área de abrangência do grupo de consultores externos que implementaram o sistema nestas instalações.

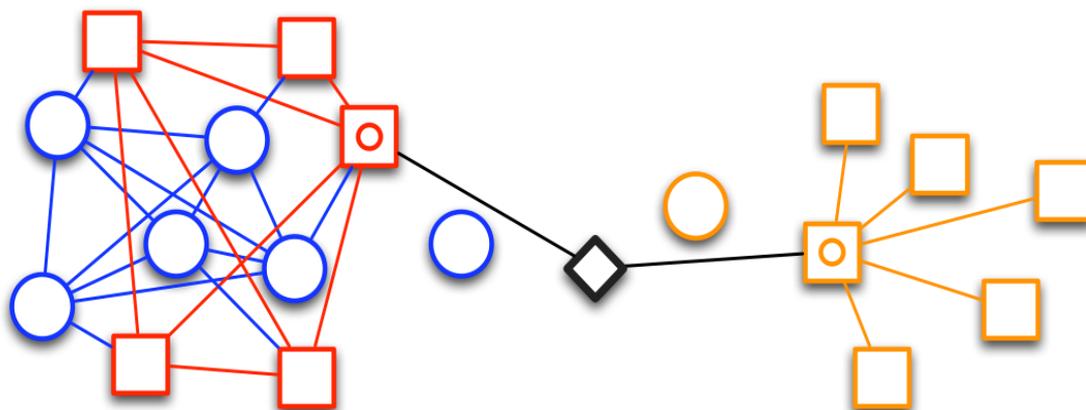
Os quadrados vermelhos (à esquerda), representam a rede de computadores usada no desenvolvimento do Stuxnet e estão ligados, cada um, respectivamente, aos seus utilizadores.

Os quadrados de cor laranja (à direita), representam a rede privada e isolada de computadores dentro da central de Natanz e o círculo laranja é o actor que transportou a CUSB para dentro destas instalações nucleares.

Por fim, o quadrado preto (ao centro), representa a CUSB dentro da qual o Stuxnet foi transportado.

Relativamente às interligações entre os diversos nós, temos as interligações azuis que representam as trocas de informação entre os actores que desenvolveram o Stuxnet e a utilização dos seus computadores, respectivamente. As interligações vermelhas, representam a rede informática que liga os computadores envolvidos na produção deste *malware*. As interligações a laranja representam a rede informática que liga os computadores da central nuclear.

Figura 4: Representação da rede de disseminação do Stuxnet (pelo autor)



Finalmente, a interligação a preto, representa o laço fraco que uniu as duas sub-redes informáticas, mediado pela CUSB.

Na figura 4, existem dois computadores assinalados com um círculo no seu interior. Estes representam o ponto de saída e de entrada de informação (o Stuxnet e as suas comunicações) e, conseqüentemente são os únicos nós que estabelecem a ligação entre as duas sub-redes, constituindo, assim, um laço fraco.

À esquerda da figura, temos uma rede multidimensional (Contractor, Monge e Leonardi, 2011, pp.685-706) e densa (Boase e Wellman, 2001, pp.4-5) e à direita temos uma rede egocêntrica (Haythornthwaite, 1996, pp.328-329) e ramificada (Boase e Wellman, 2001, pp.4-5).⁹

O que se pretende demonstrar é a seguinte ideia: na *network society* de Castells, onde as diversas redes são programadas para actuarem, cada vez mais, de forma autónoma, convergindo tendencialmente para uma rede global e onde a curiosidade humana é um poderoso condicionante do comportamento social, é impossível evitar a ciberguerra — aquilo a que chamamos a “inevitabilidade digital”. Por outras palavras, a impossibilidade de interromper o fluxo contínuo de informação digital na rede global. Castells refere, a propósito da programação das redes e da autonomia do fluxo de informação nos *space flows*, que:

“On-line communication, combined with flexibility of text, allows for ubiquitous, asynchronous space/time programming. (...) The space of flows is the material organization of time-sharing social practices that work through flows. By flows I understand purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in the economic, political, and symbolic structures of society.” (Castells, 2010, pp.30,442).

Tal como referimos anteriormente, o Stuxnet foi desenvolvido na sub-rede à esquerda (chamemos-lhe “rede A”) e chegou à sub-rede da direita (chamemos-lhe “rede B”), estando esta última completamente isolada e sem contacto com outras redes no exterior. Mas como chega informação digital a uma rede que está isolada por motivos de segurança? Através da existência, mesmo que temporária, de um laço fraco, materializado pelo uso de uma CUSB que, como já vimos em (Ramos, (in press)b, p.6) é um objecto tecnológico especificamente concebido para transporte de informação digital. Existiu, assim, a apropriação de uma tecnologia com o fim específico de criar o laço fraco assinalado a preto na figura 4 (Ramos (in press)b).

⁹ A rede egocêntrica também tem actores humanos envolvidos que interagem com os actores tecnológicos mas, para o claro entendimento deste artigo e, porque, no contexto do Stuxnet estes actores humanos não têm influência na rede tecnológica, vamos manter a designação de rede egocêntrica e ramificada, tal como é apresentada na figura 4.

A decisão de criar um laço fraco, neste contexto, não parece ser casual. O baixo volume de infecções detectadas fora do Irão, a natureza do próprio Stuxnet e o objectivo com que foi concebido, indiciam um ataque localizado e direccionado. A teoria da força dos laços fracos, de Granovetter, suporta esta interpretação através da função da força relativa da transitividade. Consideremos o computador vermelho com o círculo como nó "1", o quadrado preto como nó "2" e o computador laranja com o círculo nó "3". Segundo Granovetter, se 1 se interliga a 2 e 2 se interliga a 3, então a transitividade (1 interligado a 3) é mais provável, quando ambos os laços, entre 1-2 e 2-3, são fortes, como o próprio argumenta:

"More significant is the difference in the application of my argument to transitivity. Let P choose O and O choose X (or equivalently, let X choose O and O choose P): then I assert that transitivity — P choosing X (or X, P) — is most likely when both ties — P-O and O-X — are strong, least likely when both are weak, and of intermediate probability if one is strong and one weak. Transitivity, then, is claimed to be a function of the strength of ties, rather than a general feature of social structure." (Granovetter, 1973, pp.1376-1377).

Parece, assim, de grande relevância, o papel dos nós isolados (azul e laranja) junto às interligações a preto. Estes nós conferem a relativa força necessária aos laços entre 1-2 e 2-3 para que a transitividade seja estabelecida. Ambos, não demonstram interferência directa no fluxo de informação, mas, certamente têm influência indirecta no funcionamento estrutural da rede como um todo. Embora os laços temporários entre 1-2 e 2-3 sejam fortes, pela conferência temporária dessa força relativa por parte dos actores isolados, o verdadeiro laço que liga as duas sub-redes entre 1-3 é fraco. Para que esta ideia possa ser considerada de forma correcta, devemos pensar no trajecto da CUSB como um *space of flows* misto (geográfico e digital). Geográfico porque a CUSB viaja através do espaço físico e digital porque transporta informação em formato digital. Na realidade, os laços 1-2 e 2-3 são temporários e condicionais para a existência do laço 1-3, mas não interagem com a informação no fluxo, sendo meros portadores. Devemos pensar, também, que a interligação é intermitente e, teoricamente, muito instável, assumindo o papel de uma local bridge de grau 3 (Granovetter, 1973, pp.1364-1365). Grau 3, porque a rota mais próxima entre 1 e 3, não sendo a mesma representada a preto, seria entre 3 outros nós (o que na prática nunca aconteceria neste contexto). De facto, temos um laço fraco 1-3, porque a substância contextual das duas sub-redes A e B é completamente diferente, a interligação não existe continuamente, não existe bidireccionalidade e não existe, sequer, interacção entre 1 e 3. O laço fraco só existe, porque existiu passagem de informação de 1 para 3.

Outro ponto, que parece consubstanciar a eficácia atingida pelo uso do laço fraco 1-3, é a importância do princípio da difusão. Segundo Granovetter, em redes onde existem mais de três nós e não existindo qualquer

condição anormal nas interligações, nenhum laço forte é uma ponte (*bridge* nas palavras do próprio), mas todos as pontes são laços fracos:

“Now, if the stipulated triad is absent, it follows that, except under unlikely conditions, no strong tie is a bridge. Consider the strong tie A-B: if A has another strong tie to C, then forbidding the triad of figure 1 implies that a tie exists between C and B, so that the path A-C-B exists between A and B; hence, A-B is not a bridge. A strong tie can be a bridge, therefore, only if neither party to it has any other strong ties, unlikely in a social network of any size (though possible in a small group). Weak ties suffer no such restriction, though they are certainly not automatically bridges. What is important, rather, is that all bridges are weak ties.” (Granovetter, 1973, p.1363).

Assumimos, então, que uma ponte (*local bridge*) é sempre a rota (ou o *space of flows*) mais curta entre dois nós. Esta assumpção permite suportar o facto do ataque do Stuxnet ter sido especialmente direccionado e localizado. A pretensão dos seus autores não era infectar milhões de computadores pelo mundo, mas sim, atingir a central nuclear de Natanz e destruir as suas centrifugadoras de urânio. Na verdade, o *malware* foi desenhado e concebido por forma a apagar-se automaticamente do sistema, ao final de alguns dias, se não encontrasse a presença dos equipamentos alvo que deveria controlar e destruir. À semelhança de uma operação militar secreta, onde o objectivo deve ser rapidamente atingido e destruído sem chamar as atenções, o Stuxnet deveria entrar em acção rapidamente, sem que tivesse que passar por milhões de nós pelo mundo até chegar à sub-rede B (denunciando a sua presença). Verifica-se, assim, que um laço fraco é o *space of flows* mais reduzido entre dois nós que não pertencem à mesma sub-rede densa (com laços fortes) e aquele que atinge o propósito do “*now*” de Castells — o *timeless time*. Podemos concluir, então, que um laço fraco é a configuração mais pequena e mais rápida do espaço-tempo social da informação.

Por outro lado, Granovetter argumenta que as interligações em forma de laços fracos assumem uma posição fulcral de centralidade nas redes, porque permitem suportar a conceptualização de paradoxos na teoria social (1973, p.1378). A designação de “força dos laços fracos” é, em si mesma, um paradoxo, mas um de extrema importância, porque permite explicar o *modus operandi* da equipa na sub-rede A ao tentar atingir a sub-rede B com informação não autorizada, forçando a resistência a qualquer penetração exterior nos equipamentos da rede privada/interna de Natanz. De facto, segundo Foucault, qualquer forma de poder gera uma forma de contra-poder, assumindo, esta última, o papel de resistência que serve o propósito de equilibrar as forças em constante dinâmica:

“[the power] must also master all the forces that are formed from the very constitution of an organised multiplicity; it must neutralise the effects of counter-power that spring from them and which form a resistance to the power that wishes to dominate it: agitations, revolts, spontaneous organisations, coalitions - anything that may establish horizontal conjunctions” (Foucault, 1979, p.219).

Mas Foucault vai ainda mais longe:

“I would suggest [...] that there are no relations of power without resistances; the latter are all the more real and effective because they are formed right at the point where relations of power are exercised; resistance to power does not have to come from elsewhere to be real, nor is it inexorably frustrated through being the compatriot of power. It exists all the more by being in the same place as power; hence, like power, resistance is multiple and can be integrated in global strategies” (Gordon, 1980, p.142).

É visível o papel central deste laço fraco e o poder que representou na sua acção, visando consequências físicas no programa nuclear iraniano. A capacidade de mudar comportamentos e ter consequências no plano físico (por este motivo o Stuxnet é considerado a primeira ciber-arma da história) conferem ao laço fraco 1-3 um poder detalhadamente descrito por Castells. De facto, este conjunto de acções configura as quatro formas de poder em constante exercício na sociedade em rede (2011): (1) *Networking Power*, definida por Castells como o poder que é exercido por actores de diversas naturezas, que existem no núcleo da sociedade em rede, sobre outros actores não incluídos na mesma sociedade em rede. A observação empírica deste caso permite-nos estabelecer que, esta forma de poder, está patente na influência que os agentes na sub-rede A exerceram sobre o sujeito isolado de cor laranja e, também, sobre os sujeitos (computadores e outros equipamentos) da sub-rede B que não está ligada à sociedade em rede. (2) *Network Power*, definido como o poder resultante dos padrões necessários à coordenação das interacções sociais nas redes. Por outras palavras, as regras de inclusão de actores na rede. O paralelismo é, também, evidente. Aqui, os padrões são representados pelos protocolos usados nos *space of flows* para comunicação digital em rede. Todos os computadores usam o TCP/IP como protocolo base de comunicação em rede e o USB (*Universal Serial Bus*) para comunicação com objectos tecnológicos do tipo da CUSB. Estas regras ditam a inclusão ou exclusão desses actores da rede. A sua inclusão, sujeita a estas regras, possibilitou a passagem da informação (o *malware*), afectando o seu funcionamento. (3) *Networked Power*, definido, simplesmente, como o poder exercido por actores específicos sobre outros actores na rede social. Esta forma ficou patente pelo modo

como o poder da curiosidade condicionou a acção do sujeito isolado laranja, levando-o a contornar a resistência das normas de segurança da central nuclear e introduzir uma CUSB nos computadores da rede privada. Iremos clarificar mais sobre o poder da curiosidade já de seguida. Por último, (4) *Network-making Power*, definido como o poder de programar redes específicas de acordo com os interesses, objectivos e valores dos programadores. A evidência desta forma de poder não poderia ser mais clara. Existiu, definitivamente, um conteúdo em forma de software que, sendo introduzido na rede privada de Natanz, programou os computadores e diversos outros equipamentos por forma a satisfazer os interesses e objectivos dos programadores, levando-os a agir de acordo com os valores dos actores da sub-rede A.

Mas o que potenciou esta sequência de eventos e o consequente estabelecimento de um laço fraco entre 1 e 3? Nada teria sido possível sem um motor condicionante do comportamento humano suficientemente forte para o fazer circundar as formas de resistência impostas pelas regras de segurança das instalações nucleares de Natanz. Este motor chama-se curiosidade.

No ponto (3), *Networked Power*, falámos da curiosidade como uma força poderosa capaz de modificar o comportamento social. Clarifiquemos, agora, esta ideia.

O que é a curiosidade? Segundo refere Loewenstein (1994), a curiosidade tem sido constantemente reconhecida como um motivo central condicionante do comportamento humano, durante todo o seu ciclo de vida, tanto pela positiva como pela negativa. Tem sido, também, descrita como um dos factores por detrás da descoberta científica, possivelmente ofuscando a vontade de sucesso económico. Em muitas áreas da nossa sociedade, a curiosidade tem sido usada como factor de impulso da vontade humana, tais como, na publicidade e marketing, literatura e, até, descrita como a origem de comportamentos menos socialmente aceites, como o "voyeurismo" e o abuso de álcool ou substâncias ilícitas. No entanto, qual é a substância e no que consiste exactamente a curiosidade humana?

Loewenstein apresenta um estudo onde refere que as primeiras discussões e definições surgiram através de pensadores religiosos e filósofos da antiguidade clássica. Uma das primeiras definições de curiosidade diz-nos que é o desejo, intrinsecamente motivado, de informação. Uma segunda definição aponta para paixão, estando a intensidade da sua motivação directamente relacionada com o próprio termo. Por último, uma terceira definição refere a curiosidade como um "apetite da mente" ou "apetite cognitivo". Algumas definições mais recentes apontam para reflexos exploratórios, busca de novidade em detrimento do tédio, busca de uma determinada informação ou preenchimento de um espaço informativo vazio (1994, pp.76-77,88).

No âmbito deste artigo, não procuramos atingir uma nova definição científica de curiosidade, mas, por outro lado, estabelecer um paralelo entre a curiosidade, o facto de uma CUSB ter sido usada para criar o laço fraco 1-3 e a intencionalidade, intrínseca aos actores da sub-rede A, do uso da curiosidade para atingir o objectivo.

Peguemos nas definições que apontam para o preenchimento de um vazio informativo e um apetite da mente e podemos resumir o poder motivador da curiosidade, no conceito da inevitabilidade digital, através das palavras de Loewenstein:

“...drive theories and the information-gap perspective, which view curiosity as driven by the pain of not having information rather than by the pleasure of obtaining it, can account for the observed motivating power of curiosity.” (Loewenstein, 1994, p.92).

Uma observação empírica pode facilmente comprovar que uma CUSB encontrada num qualquer local, na maioria dos casos, será inserida no computador para verificação do seu conteúdo. Este é o poder da curiosidade, assumindo um papel fundamental na convergência das redes a nível global e, também, no caso do Stuxnet.

O poder motivador da curiosidade, juntamente com o panorama convergente das redes na rede global e o poder dos laços fracos, fazem-nos acreditar num futuro totalmente interligado da *network society*, com uma configuração e estrutura multidimensional, onde o fluxo de informação será contínuo entre sociedade e tecnologia, ocupando todos os *space of flows* com uma natureza *timeless time*. Nesse futuro, onde a interacção humana é falaciosa, é possível que a única forma de manter um actor tecnológico seguro e distante da ciberguerra, seja desligá-lo da tomada eléctrica.

Conclusão

Na introdução deste artigo, observámos como a problemática do surgimento da ciberguerra pode afectar as instituições existentes que regulamentam e promovem a “guerra justa” (Boylan, 2013). A necessidade de actualizar estas convenções e tratados é, agora, maior do que nunca. A NATO já se adiantou e declarou que os ataques cibernéticos estão ao mesmo nível dos ataques nucleares e do terrorismo. No entanto, sem regulamentação internacional neste sentido, actos de ciberguerra não podem ser julgados no mesmo âmbito da guerra convencional. A posição da NATO permite apenas uma resposta adequada e proporcional aos actos de agressão.

Numa segunda parte, fizemos uma contextualização histórica do Stuxnet e apresentámos diversos momentos chave nos acontecimentos ocorridos após a sua descoberta. Este ponto foi fundamental para a introdução do tema da CUSB (Caneta USB), como meio de transporte do *malware*, e, mais tarde, argumentar sobre a sua utilização como meio de criar um laço fraco e despertar o poder da curiosidade.

Na terceira parte, introduzimos os principais conceitos e teorias sociológicas das redes. Esta temática permitiu enquadrar teoricamente os factos ocorridos entre as redes que foram interligadas pela CUSB que transportou o Stuxnet para o Irão, mais concretamente para a central nuclear de Natanz.

Por fim, na quarta e última parte, apresentámos o conceito de inevitabilidade digital. Este conceito surgiu da observação empírica dos factos relativos ao ataque do Stuxnet às instalações nucleares de Natanz e do enquadramento proporcionado pela teoria social de Castells, a *network society*, pela teoria da força dos laços fracos, de Granovetter e pela introdução, através de Loewenstein, de um poderoso factor condicionante de comportamento social: a curiosidade.

Através da apresentação deste conceito, foi possível entender muitos dos conceitos introduzidos na segunda parte, tais como *timeless time* e *space of flows*, densidade da rede, redes egocêntricas, laços fortes e fracos, direcção, intensidade, conteúdo ou recursos, nós e interligações.

Através deste conceito, é possível entender como a convergência das redes e os laços fracos estão a criar um mundo interligado, onde o fluxo de informação é, cada vez mais, contínuo e imparável, determinando a possibilidade crescente de ciberguerra. A tendência para a convergência das redes numa única rede global é facilmente identificável através da crescente necessidade de endereços IP (identificadores únicos atribuídos aos dispositivos ligados através do Internet Protocol). É suficiente olhar para a história da Internet e entender que esta surgiu da convergência de outras redes, a militar e a académica (Ramos, (in press)a, pp.4-5). É ainda possível entender como a importância dos laços fracos é fundamental na convergência gradual das redes na rede global e na conceptualização da inevitabilidade digital.

A inevitabilidade digital, contudo, não pretende ser um conceito determinista ou fatalista. Levinson refere que:

“The reversal of determinism began with the arrival of life itself. Unlike inorganic reactions, the results of which are almost as predictable as two plus two equals four, living processes are animated by dollops of unpredictability. On the individual level, this unpredictability can of course lead to death as well as success; for life as a whole, this noise in determinism serves as a source of novelty via mutation, and is thus one of the cutting edges of evolution. When that evolution gave rise to human intelligence, determinism suffered another reversal, as profound as that which attended the emergence of open-programmed life. To imagine is to disperse to infinity the prospect of a single, unavoidable result. To embody those imaginings into tangible technology is to greatly constrict that field of possibilities—for physical things are less easily wrought than ideas—but even a handful of new technologies, even just two, breaks the spell of a single, inevitable outcome.” (Levinson, 2004, pp.201-202).

De acordo com Levinson, a existência de actores humanos neste conceito confere-lhe uma perspectiva indeterminada. Como já tivemos oportunidade de referir antes,

“se existe vida munida de inteligência, o resultado da produção dessa vida é tão imprevisível quanto ela mesmo. A simples existência de inteligência pressupõe níveis de imaginação ilimitados, levando a resultados ainda em maior número. No entanto, ainda que abordássemos a questão do ponto de vista meramente tecnológico, a simples existência de apenas duas tecnologias em interacção, *per se*, já evitaria a determinação de apenas uma possibilidade de resultado.” (Ramos, (in press)b, p.13).

A simples aplicação deste conceito, por exemplo, à área do *copyright*, permite clarificar porque é que a luta contra a pirataria de conteúdos é uma luta inglória. Não se trata de determinar o futuro, mas sim, enquadrar os acontecimentos, já no presente, para compreender a razão da sua existência

Referências

- Boase, J. e Wellman, B., 2001. A Plague of Viruses: Biological, Computer and Marketing. *Current Sociology*, 49 (6), pp. 1-21. Disponível em: <http://homes.chass.utoronto.ca/~wellman/publications/viruspaper/version.PDF> [Acedido: 30 Dezembro 2013].
- Borland, J., 2010. A Four-Day Dive Into Stuxnet's Heart. *Wired*, [online] 27 Dezembro. Disponível em: <http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-heart/> [Acedido: 5 Janeiro 2014].
- Boylan, M., 2013. Can there be a Just Cyber War?. *Journal of Applied Ethics and Philosophy*, 5, pp. 10-17. Disponível: http://ethics.let.hokudai.ac.jp/ja/files/JAEP5_2013.pdf#page=13 [Acedido: 01 Janeiro 2014].
- Castells, M., 2009. *Communication Power*. Oxford: Oxford University Press.
- Castells, M., 2010. *The Rise of the Network Society*. 2ª ed. Chichester: Wiley-Blackwell.
- Castells, M., 2011. A Network Theory of Power. *International Journal of Communication*, 5, pp. 773-787. Disponível em: <http://ijoc.org/index.php/ijoc/article/view/1136> [Acedido: 19 Novembro 2013].
- Contractor, N., Monge, P. e Leonardi, P., 2011. Multidimensional Networks and the Dynamics of Sociomateriality: Bringing Technology Inside the Network. *International Journal of Communication*, 5 p. 682–720. Disponível em: <http://ijoc.org/index.php/ijoc/article/view/1131> [Acedido: 19th November 2013].

- Dijk, J., 2006. *The Network Society: Social Aspects of New Media*. 2ª ed. Thousand Oaks: Sage Publications.
- Foucault, M., 1979. *Discipline and Punish*. Traduzido do Francês por A. Sheridan. New York: Vintage Books.
- Gordon, C. ed., 1980. *Power/Knowledge: Selected Interviews and other Writings, 1972-1977 by Michel Foucault*. Traduzido do Francês por C. Gordon. New York: Pantheon Books.
- Granovetter, M., 1973. The Strength of Weak Ties. *American Journal of Sociology*, 78 (6), pp. 1360-1380. Disponível em: <http://sociology.stanford.edu/people/mgranovetter/documents/granstrengthweakties.pdf> [Acedido: 24 December 2013].
- Haythornthwaite, C., 1996. Social network analysis: An approach and technique for the study of information exchange. *Library & Information Science Research*, 18 (4), pp. 323-342. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0740818896900031> [Acedido: 26 Dezembro 2013].
- Howard, M., e Paret, P., 1984. *On War [Vom Krieg]*. Indexed ed. New Jersey: Princeton University Press.
- Karimi, N., 2010. Iran's nuclear agency trying to stop computer worm. *NBCNEWS*, [online] Disponível em: http://www.msnbc.msn.com/id/39357629/ns/technology_and_science-tech_and_gadgets/t/iran-nuclear-agency-trying-stop-computer-worm/#.UQFu86VrvfC [Acedido: 6 Janeiro 2013].
- Kaspersky, E., 2011. The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight. *Nota Bene*, [blog] 2 Novembro, Disponível em: <http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/> [Acedido: 5 Janeiro 2014].
- Langner, R., 2013. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. [report] Hamburg: Langner Group.
- Levinson, P., 2004. *Digital McLuhan: A Guide to the Information Millennium*. New York: Routledge.
- Loewenstein, G., 1994. The Psychology of Curiosity: A Review and Reinterpretation. *Psychological Bulletin*, 116 (1), pp. 75-98. Disponível: doi:10.1037/0033-2909.116.1.75. [Acedido: 2 Janeiro 2014].
- Mushkat, R., 1987. Who May Wage War? An Examination of an Old/New Question. *American University International Law Review*, 2 (1), pp. 97-151.
- Ramos, H., (in press)a. Ciberguerra: Apropriação da Tecnologia Hoje, Hegemonia das Nações Amanhã. *Observatorio (OBS*)*. (Em revisão para publicação).
- Ramos, H., (in press)b. Novos Media na Ciberguerra: A Apropriação da Tecnologia na Disseminação do Stuxnet. *Observatorio (OBS*)*. (Em revisão para publicação).
- Rasmussen, A., 2012. Secretary General's Annual Report 2011, *North Atlantic Treaty Organization*, [online] Disponível em: http://www.nato.int/cps/en/natolive/opinions_82646.htm?selectedLocale=en [Acedido: 5 Janeiro 2013].

Symantec, 2010. *Security Response/W32.Stuxnet*. [online] Mountain View: Symantec. Disponível em: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 [Acedido: 7 Janeiro 2013].

TED, 2011. *Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon*. [video online] Disponível em: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html [Acedido: 4 Junho 2013].

Ulasen, S., 2010. *News / VirusBlokAda*. [online] Disponível em: <http://anti-virus.by/en/tempo.shtml> [Acedido: 5 Janeiro 2014].