Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas

Tenente-coronel
Rui Manuel Piteira Natário

Major-general
Paulo Fernando Viegas Nunes

1. Introdução

O grande aumento da interligação dos sistemas informáticos ocorrido desde o final da Guerra Fria, particularmente da internet, revolucionou a forma como os governos, as empresas e os indivíduos comunicam e fazem negócios. No entanto, este advento de um mundo hiperligado trouxe também enormes riscos para os sistemas, para os computadores e, mais importante ainda, para o normal funcionamento das infraestruturas críticas (IC) que eles suportam. Embora a definição exacta daquilo que é considerado crítico varie de país para país, há um fio condutor que liga todas as

concepções sobre o assunto: a sua importância para o funcionamento normal da sociedade.

Diversos estudos realizados sobre o assunto realçam a criticidade da protecção dasinfraestruturas de suporte a diversas actividades económicas, industriais e outras. À medida que cresce a ligação dos sistemas de controlo industrial às redes globais, sobem de tom os avisos acerca das crescentes vulnerabilidades que esta ligação acarreta. É hoje razoavelmente consensual afirmar que o impacto de um ataque cibernético sobre uma IC pode ser idêntico, ou mesmo superior, ao de um ataque físico convencional. Ou seja, o ciberespaço assume um papel preponderante, não só como ambiente informacional para a interligação das IC, mas também como origem das maiores ameaças ao seu normal funcionamento.

Assim, a análise das vulnerabilidades das IC, a identificação das ameaças, a avaliação dos impactos e a gestão dos riscos associados, são áreas da maior importância estratégica. Esta responsabilidade é, não só dos governos, mas também das empresas proprietárias e operadoras das IC, sendo assim uma tarefa que exigirá um esforço concertado a vários níveis.

2. Infraestruturas críticas

Embora não exista uma definição formal de "infraestrutura crítica", muitos governos têm tentado definir que partes das suas infraestruturas são verdadeiramente críticas. Existem várias definições de IC e todas elas tentam reflectir a importância que estas instalações e serviços têm para o funcionamento da sociedade moderna.

Todavia, estas definições tendem a ser genéricas uma vez que se destinam a dar uma perspectiva estratégica que, subsequentemente, deve ser analisada caso a caso, sector a sector.

2.1. Definição

Os EUA consideram que as IC são os sistemas e os activos (*assets*), tanto físicos como virtuais, tão vitais ao estado que a incapacidade ou a destruição desses sistemas ou activos terá um impacto debilitante na segurança, economia nacional ou saúde pública (Clarke & Olcott, 2012). O *Department of Homeland Security* (DHS) designou dezoito sectores como sendo críticos e esta classificação engloba tanto as IC ligadas à agricultura como as centrais nucleares, passando pelo sector financeiro. A nível europeu, o Conselho da União Europeia definiu genericamente as IC como sendo os activos e sistemas que são essenciais para a manutenção das funções vitais da sociedade e que, em caso de disrupção ou destruição, afectarão um ou mais estados membros (*Jornal Oficial da União Europeia*, 2008), concentrando-se apenas nos sectores da energia e dos transportes.

Existem muitas outras classificações de IC que reflectem os diferentes critérios

adoptados pelos governos e instituições que as produzem. Nalguns casos, o critério enfatiza a finalidade da IC, noutros é salientado o impacto da sua ausência ou do seu funcionamento deficiente. No Reino Unido, as IC incluem as comunicações, os serviços de emergência, energia e outros, sem que exista uma definição clara do que é uma IC (Cornish, Livingstone, Clemente, & Yorke, 2011), mas considerando que existem certos elementos infraestruturais críticos cuja perda terá um sério impacto na disponibilidade ou integridade de certos serviços, o que levará a sérias consequências económicas ou sociais (Clemente, 2013). Na Alemanha, as IC são as estruturas físicas e organizacionais, de tal modo vitais para o funcionamento da sociedade e economia que a sua falha ou degradação resultará em prolongados cortes nos abastecimentos, disrupção significativa da segurança pública, entre outras consequências dramáticas (BMI, 2009).

A Tabela 1 resume os resultados de um estudo (Brunner & Suter, 2008) sobre quais os sectores considerados como críticos em diversos países. Enquanto alguns são muito rigorosos na definição dos seus sectores críticos, e quais os bens e serviços por eles fornecidos, outros não têm uma lista oficial de sectores considerados críticos (KRITIS, 2004).

SECTORES \ PAÍSES	AUS	AUT	BRA	CAN	EST	FRA	FIN	DEU	HUN	IND	ITA	JPN	KOR	MAL	NLD	NOR	NZL	POL	RUS	SWE	SGP	ESP	CHE	GBR	USA
Banca e Finanças	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Governo Central		•		•	•	•		•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•
Indústria Química e Nuclear				•						•				•	•			•				•	•		•
Serviços de Emergência	•		•	•	•	•			•	•	•		•	•		•	•	•	•				•	•	•
Electricidade/Energia	•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•			•	•	•	•	•
Agricultura/Alimentação	•			•	•	•	•	•	•		•	•			•	•					•	•	•	•	•
Serviços de Saúde	•		•	•	•	•	•		•		•			•	•	•					•	•	•	•	•
Comunicação/Media	•	•				•	•		•		•		•		•	•			•	•	•		•		•
Defesa						•			•	•			•	•		•			•					•	•
Monumentos Nacionais	•																								•
Esgotos/Resíduos	•										•			•	•	•		•					•	•	•
Telecomunicações	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•		•	•
Transportes/Logística	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•
Distribuição de Água	•		•		•	•	•	•	•		•	•		•	•	•				•	•	•	•	•	•

Tabela 1 – Sectores críticos em diversos países. Adaptado de Brunner & Suter (2008)

Estas diferenças podem ser explicadas pela adopção de diferentes abordagens, influenciadas por diversos factores sociais, políticos e económicos. Por outro lado, apesar destas variações, consideramos que a tabela reflecte aquilo que Tabanksy considera serem os três factores que definem uma IC: a sua importância simbólica, a imediata dependência daquilo que produz e, por último, a complexa rede de dependências a que está ligada (Tabansky, 2011). Importa aqui referir que a atribuição de criticidade a sectores como “água” ou “transportes”, demasiado abrangentes e ambíguos, cria dificuldades acrescidas pois é necessário definir prioridades dentro de cada sector (Clemente, 2013).

2.2. Caracterização

Knapp (2011) refere que os termos “rede industrial” e “infraestrutura crítica” são várias vezes utilizados de forma algo confusa. Na sua opinião, uma rede industrial é uma rede que funciona de acordo com algum tipo de sistema de controlo automático que comunica digitalmente pela rede, e uma infraestrutura crítica é uma infraestrutura crítica em rede, que inclui qualquer rede utilizada na operação directa de qualquer sistema do qual dependa uma das infraestruturas definidas como críticas. A incorporação de sistemas informáticos fez com que as infraestruturas tradicionais se tornassem também infraestruturas informacionais. Além disso, foram criadas novas IC que são puramente informacionais: bases de dados que contêm informação vital, tal como registos financeiros ou dados científicos.

Na era da informação, o conceito de “infraestrutura” acaba sempre por, de alguma forma, incorporar um elemento informático o que faz com que, actualmente, a expressão “infraestrutura” seja praticamente indissociável da noção de “infraestrutura de informação” (Tabansky, 2011). Como já vimos, uma infraestrutura é considerada como crítica quando a sua eventual disrupção tem o potencial de afectar seriamente a estabilidade social e a própria soberania do Estado. Apesar de diferentes países terem diferentes concepções de IC, todas têm em comum a existência de um elemento computorizado do qual dependem outros elementos físicos. Assim, as IC incluem habitualmente elementos sensíveis de um ambiente mais vasto que vai além da infraestrutura física para incluir também dados, que podem ser considerados como uma forma de infraestrutura lógica ou “infraestrutura informacional crítica” (Clemente, 2013). Esta infraestrutura informacional é aquilo a que vulgarmente se convencionou chamar ciberespaço.

Contrariamente ao que ocorre com a maior parte dos termos informáticos, não existe uma conceptualização objectiva e universalmente aceite para o ciberespaço, sendo este apenas um termo lato utilizado para descrever o mundo virtual dos computadores e da internet. Embora estas tecnologias sejam importantes para a nossa concepção desta realidade virtual, é evidente que estes elementos constituem apenas uma pequena parte da globalidade das redes políticas, sociais, económicas, culturais e financeiras que constituem aquilo a que vulgarmente se chama ciberespaço (Whittaker, 2004). A génese do termo “*ciberspace*” remonta a 1984 quando foi popularizado na novela *Neuromancer* (Gibson, 1984), onde o autor o definiu como sendo uma alucinação consensual experimentada diariamente por biliões de utilizadores. Nos anos que se seguiram, surgiram na literatura da especialidade diversas análises e teorizações sobre este conceito. Um filósofo considerou que o ciberespaço era definido como sendo o espaço de comunicação aberto pela interligação mundial dos computadores e das memórias dos computadores. Esta definição incluía o conjunto dos sistemas de comunicação electrónicos, na medida em que transmitiam informações provenientes de fontes digitais ou destinadas à digitalização (Lévy, 1999).

Por outro lado, um conceituado especialista na área da defesa considerou que o ciberespaço era um domínio operacional cujo carácter distinto e único era enquadrado pela utilização da electrónica e do espectro electromagnético para criar, guardar, modificar trocar e explorar informação através de sistemas baseados em tecnologia de comunicação de informação interligados e as suas infra-estruturas associadas (Kuehl, 2009).

No entanto, quer a abordagem seja feita a partir uma perspectiva filosófica quer reflicta uma visão mais tecnocrática, todas as modernas definições de ciberespaço reconhecem o seu carácter omnipresente, e colocam-no no âmbito de um ambiente mais vasto, reconhecendo implicitamente as suas profundas ligações ao mundo físico onde estão as pessoas e as infra-estruturas de suporte da sociedade. Ou seja, o ciberespaço é hoje uma parte tão importante da vida moderna que, embora seja muitas vezes considerado com um sector à parte, na prática, está tão ligado aos outros sectores que a distinção deixa de fazer sentido. Assim, a criticidade das IC é avaliada também em função da sua vulnerabilidade à destruição ou interferência por meios informáticos (Tabansky, 2011), pois as modernas infraestruturas estão inteiramente dependentes dos componentes físicos e lógicos do ciberespaço e este é, em si mesmo, considerado como crítico (Clemente, 2013).

Neste contexto, o foco centra-se hoje nas infraestruturas informacionais críticas (IIC) onde a influência do ciberespaço sobre todos os outros sectores se torna evidente. As IIC fortalecem a vasta maioria das infraestruturas físicas e continuam a crescer à medida que estas infraestruturas são ligadas em rede. A natureza complexa das grandes redes distribuídas faz com que seja extremamente difícil avaliar e analisar isoladamente o nível "ciber", mas torna-o fácil de atacar devido à sempre crescente superfície de ataque. A Comissão Europeia (CE) definiu o nível das IIC como sendo o dos sistemas de tecnologias de informação e comunicação (TIC) que são IC por si próprios ou que são essenciais à operação de outras IC (Clemente, 2013). Ou seja, como refere Clemente, podemos estar a atingir um ponto em que a distinção entre "infraestrutura" e "infraestrutura informacional" é irrelevante, porque as duas noções se fundem num sempre crescente círculo de "coisas" críticas (Clemente, 2013). Há ainda a salientar o facto de muitas IC serem propriedade privada. Como se viu na Tabela 1, os sectores críticos são muito variados e, em muitos países, abrangem áreas de negócio que são da esfera da actividade empresarial privada. Esta é uma realidade global que, tanto nos EUA (GAO, 2013) como na CE (ENISA, 2011), acaba por ser uma característica marcante, pois implica que os governos, embora possam decidir da sua criticidade, não podem controlar directamente a gestão de muitas IC.

2.3. Interdependência entre sistemas

Uma infraestrutura é, genericamente, um sistema que combina várias instalações, de forma a permitir diversas actividades ou a disponibilizar determinados serviços. Esta classificação é válida tanto para uma conduta que leva água de nascentes para casas e

campos, como para as vias de comunicação que, incluindo estradas, túneis e pontes, permitem o movimento de pessoas e bens, ou para qualquer outra infraestrutura. Ou seja, uma das propriedades das infraestruturas é que várias esferas de actividade podem estar dependentes do seu correcto funcionamento. Como já vimos, a sociedade moderna depende das IC, mas estas, por sua vez, dependem umas das outras para o seu próprio normal funcionamento. Esta situação de crescente interligação e interdependência foi identificada há vários anos e reportada ao mais alto nível como sendo motivo de grande preocupação, pois a probabilidade um pequeno evento poder desencadear uma cascata de outros eventos com impacto muito alargado é cada vez maior (PC-CIP, 1997). Vivemos assim num ambiente em que não temos apenas relações de dependência, unidireccionais, mas sim relações de interdependência, que são bidireccionais.

Segundo Kelly (2001), as interdependências são de quatro tipos:

– Física: Duas infraestruturas são fisicamente interdependentes quando o estado de uma é dependente da saída material da outra;

– Ciber: Uma infraestrutura tem uma ciber interdependência se o seu estado depende da informação transmitida através da infraestrutura informacional;

– Geográfica: As infraestruturas são geograficamente interdependentes se um evento ambiental local puder causar alterações no estado de todas elas;

– Lógica: Duas infraestruturas são logicamente dependentes se o estado de cada uma depende do estado da outra por meio de um mecanismo que não seja físico, cibernético ou geográfico.

A Figura 1 ilustra a visão de Kelly sobre a complexidade da rede de dependências e interdependências existentes nas IC.

Numa outra perspectiva, o *Idaho National Laboratory* (INL) avançou com uma classificação que, embora com nomenclatura distinta, engloba a classificação anterior adicionando a interdependência de políticas ou procedimentos e a interdependência social ou colectiva (Pederson, Dudenhoeffer, Hartley, & Permann, 2006). A primeira destas ocorre quando uma alteração nos procedimentos aplicados a uma infraestrutura afecta o estado de outra, e a segunda está relacionada com o facto de as infraestruturas terem influência em factores sociais como a opinião pública, medo, confiança do público ou outros factores culturais. Mas, além das diferenças, importa aqui realçar o papel do factor cibernético enquanto elemento estruturante em toda a rede de interdependências.

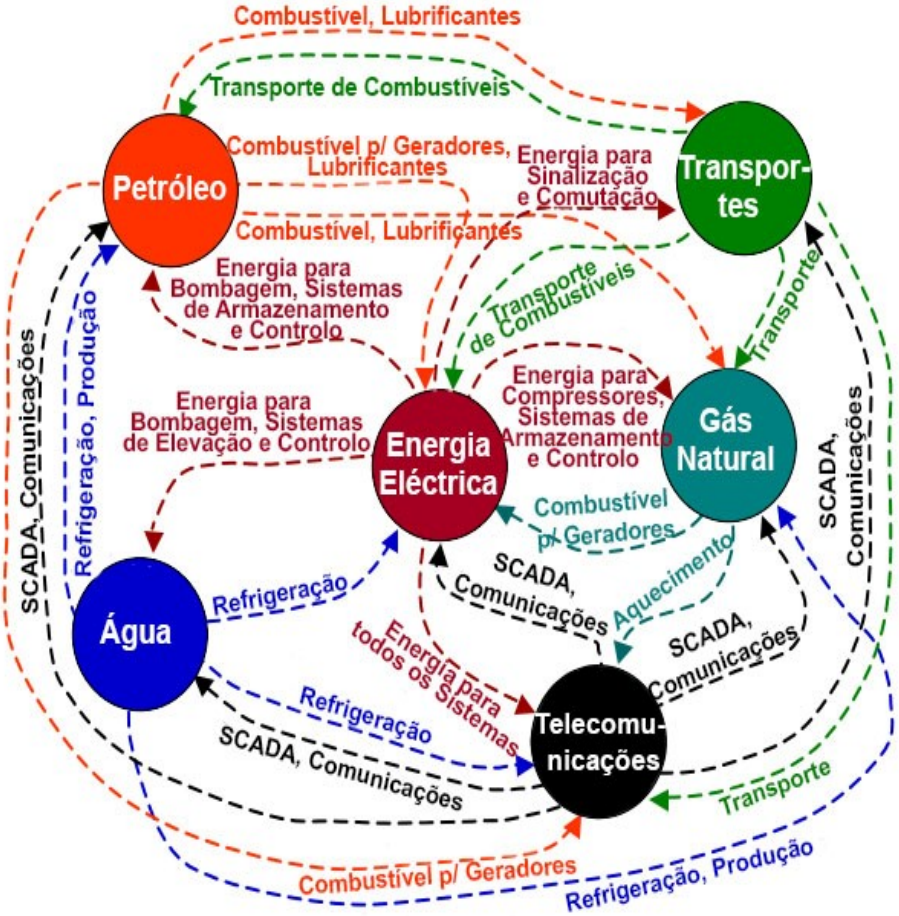

Figura 1 – Exemplos de dependência e interdependência de sistemas. Adaptado de Kelly (2001)

A importância do elemento cibernético neste âmbito foi identificada quando o já citado relatório (PC-CIP, 1997) refere que existe uma dependência colectiva da infraestrutura de informação e comunicações, isto é, essencialmente reconhece a existência de uma crescente e real dimensão "ciber" associada à manutenção e preservação das IC. Desde então, as IC não pararam de acentuar esta interdependência e a infraestrutura informacional está cada vez mais interligada com todas as outras infraestruturas, sejam elas IC ou não. Consequentemente, isolar as infraestruturas críticas das não-críticas é um verdadeiro desafio tendo em conta que o nosso conhecimento das causas de falha das infraestruturas é ainda limitado, especialmente no que diz respeito às suas relações de (inter)dependência (Hämmerli & Renda, 2010).

No passado, a interdependência derivava apenas das relações físicas ou geográficas. Com o desenvolvimento do ciberespaço, que inclui a comunicação de dados e métodos informáticos de comando e controlo automático, surgiram novas relações que, por sua vez, criaram vulnerabilidades adicionais. Estas relações são informáticas (por exemplo,

comando e controlo por meios electrónicos), mas são também lógicas (por exemplo, o mercado financeiro internacional influencia o desempenho de muitas indústrias).

Como já vimos, diversos governos têm vindo a definir quais os sectores das suas infraestruturas que são verdadeiramente críticos, e os actuais sistemas de classificação de IC esforçam-se por ter em conta a complexidade do ciberespaço, do qual dependem muitas das infraestruturas modernas. É precisamente esta ligação entre o "ciber" e todas as áreas da vida moderna que leva a que o governo dos EUA considere, desde 2003, a existência de "Infraestruturas Críticas e Recursos Chave"[1]. Esta expressão é desde então utilizada em vários documentos oficiais para englobar tudo aquilo que o governo dos EUA considera que deve ser prioritariamente preservado (DHS, 2011, 2012). A Figura 2 ilustra esta situação em que a infraestrutura do ciberespaço é a base de todo um complexo edifício de interdependências sobre o qual assenta a vida nas sociedades modernas.

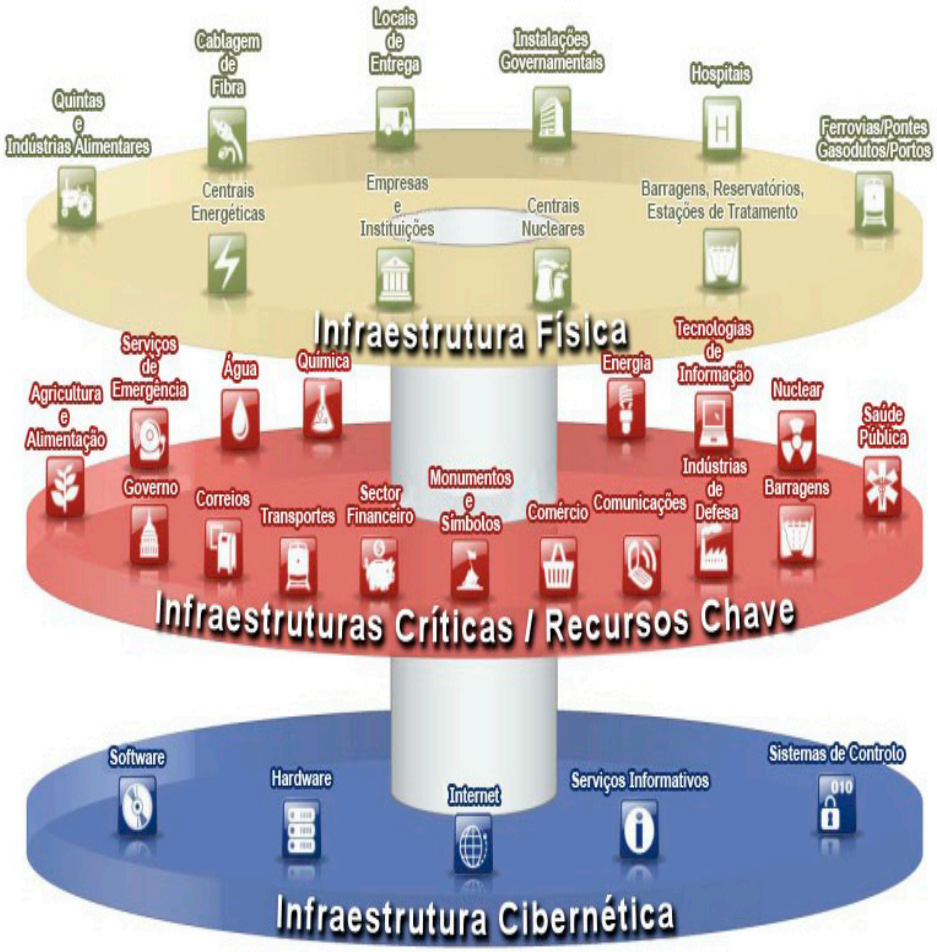

Figura 2 – A infraestrutura cibernética como base de todas as outras. Adaptado de Beggs (2010)

Seja através de ligação directa, proximidade geográfica, ou relações cibernéticas, é inquestionável que as IC não estão isoladas e que as suas interacções criam uma complexa rede de relações, dependências e interdependências que extravasam o âmbito das IC para afectar toda a sociedade (Pederson et al., 2006). Em suma, as relações de interdependência são uma intricada estrutura de múltiplos níveis onde as influências se fazem sentir em todos os sectores da sociedade e do Estado, do domínio público ao privado, e do âmbito regional à escala global.

3. Sistemas SCADA

Os sistemas de controlo industrial[2] são redes e sistemas de comando e controlo concebidos para apoiar processos industriais. Estes sistemas são responsáveis pela monitorização e controlo de uma grande variedade de processos e operações, tais como a distribuição de gás e electricidade, tratamento de água ou transporte ferroviário. O maior subgrupo dos ICS são os sistemas conhecidos por SCADA[3] (ENISA, 2011). Quase todas as IC industriais são geridas remotamente a partir de salas de controlo, utilizando computadores e redes de comunicação. Desde o controlo de processos químicos de fabrico até à sinalização das redes ferroviárias, passando pela gestão da rede elétrica e pelo abastecimento de gás, todos estes processos são controlados por algum tipo de sistema de controlo de supervisão e aquisição de dados, ou seja, tecnologia SCADA (Stouffer, Falco, & Kent, 2008). Os termos “controlo de processos” e “SCADA” eram, até há relativamente pouco tempo, desconhecidos fora do círculo restrito dos profissionais da área. Hoje em dia, são uma das principais preocupações no âmbito da protecção das IC.

3.1. Definição

Vários sectores da indústria, considerados como IC, utilizam algum tipo de sistema de controlo industrial nas suas actividades diárias. Este mundo dos ICS, como ocorre em tantos outros sectores da alta tecnologia, tem o seu próprio léxico para descrever as especificidades da sua actividade. Infelizmente, os termos exactos são muitas vezes mal utilizados e compreendidos. Por exemplo, é vulgar que os ICS sejam referidos como sendo SCADA, o que é simultaneamente pouco rigoroso e enganador (Knapp, 2011). Uma rede industrial é tipicamente constituída por diversas áreas distintas e os sistemas SCADA são apenas uma peça específica de um grande puzzle, separada dos sistemas de controlo propriamente ditos (NCS, 2004). Na realidade, os ICS podem incluir sistemas SCADA, sistemas de controlo distribuído[4], sistemas de controlo de processos[5], terminais remotos[6], ou ainda controladores de lógica programável[7] (NCS, 2004) (Stouffer et al., 2008) (ENISA, 2011). Cada uma destas áreas tem as suas próprias considerações de segurança física e lógica e as suas políticas e preocupações específicas (Knapp, 2011).

Nos sistemas SCADA são os computadores que monitorizam e regulam as operações da maior parte das IC industriais. Estes computadores ajustam automaticamente diferentes

fases dos processos de fabrico, e outras actividades de controlo, com base em dados digitais recolhidos por sensores (Wilson, 2008). Ou seja, são ferramentas de *software* concebidas para construir sistemas de controlo industrial, e utilizadas para a monitorização remota e para o envio de comandos a válvulas e interruptores (NCS, 2004). Os sistemas SCADA são sistemas altamente distribuídos utilizados para controlar activos dispersos geograficamente, por vezes em áreas de milhares de quilómetros, onde a centralização da aquisição de dados e o controlo são críticos para a operação dos sistemas (Shea, 2003). Assim, é frequente que estes sistemas sejam colocados em locais remotos, operem sem intervenção humana, e sejam acedidos apenas esporadicamente por engenheiros ou pessoal técnico, através de ligações de telecomunicações (Wilson, 2008). No entanto, em nome da eficiência, estas ligações estão gradualmente a ser incorporadas nas redes locais empresariais ou mesmo na internet.

3.2. Evolução

Os sistemas SCADA vulgarizaram-se nos anos de 1960, com o crescimento da necessidade de controlar e monitorizar equipamento remoto. A primeira geração destes sistemas tinha uma arquitectura monolítica assente em computadores *mainframe* e funcionava isoladamente. A segunda geração de sistemas SCADA tinha já uma arquitectura distribuída e tirava partido dos desenvolvimentos nas redes locais e na miniaturização. A informação era partilhada em tempo real a partir de estações que cumpriam uma função específica e estes sistemas eram normalmente constituídos por *software*, *hardware* e protocolos proprietários, isto é, específicos de cada firma. A actual terceira geração tem uma arquitectura em rede, semelhante à geração anterior, mas capaz de comunicar tanto através de redes WAN[8] como de redes LAN[9]. Além disso, os novos sistema SCADA utilizam já protocolos e equipamento *standard* (NCS, 2004).

Ou seja, os primeiros ICS eram redes ponto a ponto que ligavam um painel de controlo a um sensor remoto. Estes ICS evoluíram até se tornarem sistemas complexos que suportam a comunicação entre uma central e várias unidades remotas, através de grandes distâncias, por meios de complexas redes em malha (ENISA, 2011). Relativamente ao *software*, há décadas atrás, as grandes companhias proprietárias de muitas IC tinham departamentos internos de engenharia onde eram desenvolvidas aplicações à medida das suas necessidades. No entanto, a evolução da indústria fez com que surgissem cada vez mais e melhores soluções desenvolvidas por firmas externas (Clarke & Olcott, 2012). Isto resultou em menor investimento e custos operacionais e fez com que os ICS se transformassem em arquitecturas abertas, com tecnologias padrão, e altamente ligados a outras redes empresariais e à internet (ENISA, 2011).

Ao longo deste processo evolutivo, a segurança física foi sempre uma preocupação, contrariamente ao que ocorreu com a segurança da informação. Isto ocorreu porque os sistemas estavam isolados fisicamente, sem quaisquer sistemas comuns que quebrassem esse isolamento Assim, antes da banalização da ligação à internet, das aplicações assentes na *web* e dos sistemas empresariais de informação em tempo real, todos os

sistemas industriais eram apenas concebidos para serem fiáveis (Knapp, 2011).

3.3. Vulnerabilidades

Em 1995, o governo dos EUA já reconhecia que as suas IC estavam extremamente dependentes das redes de informação, como a internet, e que eram vulneráveis a ataques originários dessas mesmas redes (SPB, 1995). Os sistemas ICS e as redes de TI empresariais estão hoje completamente interligados, e é vulgar ter sistemas ICS que comunicam através da internet. Assim, tornou-se absolutamente normal fazer administração remota de sistemas de controlo e dos dispositivos de rede a eles associados. Da mesma forma, os engenheiros encarregados das tarefas de controlo podem monitorizar todos os sistemas ICS a partir de diversos pontos fora da rede de controlo, tirando partido das redes globais. A consequência é que os ataques contra os sistemas SCADA podem ter origem em qualquer parte do mundo (ENISA, 2011). Assim, a grande desvantagem derivada da ligação dos sistemas SCADA a redes internas e outras abertas ao exterior, é a sua crescente vulnerabilidade a ataques informáticos.

Em Março de 2007, investigadores no INL levaram a cabo uma experiência chamada *Aurora Generator Test* onde demonstraram a possibilidade de um ciberataque afectar e destruir os sistemas de controlo de geradores vulgarmente utilizados na rede eléctrica (Wilson, 2008). Num vídeo[10] divulgado pelo DHS, um gerador semelhante a muitos outros em utilização nos EUA é forçado a sobreaquecer e parar dramaticamente depois de receber uma série de comandos maliciosos. Embora os investigadores tenham declarado que o teste se destinava apenas a averiguar o potencial impacto de uma falha já corrigida, o vídeo é explícito e deixa no ar a possibilidade da existência de muitas outras vulnerabilidades semelhantes, que podem ser exploradas da mesma forma.

No passado, muitos sistemas ICS eram proprietários e continham arquitecturas e comandos próprios. Os sistemas proprietários são produtos de *software*, customizados, únicos e destinados à instalação em poucos (ou num único) computadores e a sua exclusividade torna-os um alvo menos apetecível para os *hackers*. São menos atractivos porque a descoberta de uma vulnerabilidade leva tempo, e um *hacker* pode considerar que o esforço de vigilância e pesquisa para lançar um ataque a um sistema proprietário não é remunerador (Wilson, 2008). Hoje, os sistemas ICS são maioritariamente assentes em plataformas e sistemas padronizados aplicados a diversos dispositivos, e utilizam *software* COTS[11], o que levou a uma redução dos custos, facilidade de utilização e permitiu ainda a monitorização e controlo remoto a partir de diversas localizações (ENISA, 2011). Esta utilização generalizada de *software* comercial tornou os sistemas SCADA muito mais interessantes para os hackers, pois uma única vulnerabilidade descoberta num produto COTS pode estar integrada em milhares de computadores que tenham instalado esse software (Wilson, 2008).

Mas não foram apenas os protocolos de comunicação proprietários que foram modificados ou substituídos por outros padronizados e abertos. Os próprios sistemas

operativos e as aplicações, utilizados de forma generalizada nos sistemas ICS, migraram de versões proprietárias para versões normais de sistemas operativos (família Windows ou Linux) e aplicações (Microsoft SQL Server, Microsoft Excel, etc). Esta mudança torna estes sistemas vulneráveis ao mesmo tipo de ataques a que estão expostos os sistemas de TI convencionais (ENISA, 2011). Além disso, como os sistemas SCADA não foram originalmente concebidos tendo a segurança como prioridade, em muitos casos, é agora impossível implementar novos controlos de segurança para reduzir as vulnerabilidades já conhecidas (Wilson, 2008). Os antigos sistemas de controlo foram originalmente concebidos como redes isoladas, sem acesso à internet. Portanto, foi necessário adicionar acessos de rede aos sistemas originais de modo a integrá-los na restante estrutura empresarial (Shea, 2003).

No início do séc. XXI, a ligação dos sistemas SCADA à internet aumentou tremendamente e esta mudança levou à exposição de um conjunto de sistemas que nunca foram concebidos para ser ligados a uma rede pública (NCS, 2004). Mas, como os protocolos de comunicação dos ICS nunca foram concebidos para ser seguros, muitos destes protocolos foram originalmente projectados sem autenticação, sem cifra e sem qualquer tipo de garantia da integridade das mensagens, o que expõe a comunicação a uma grande variedade de ataques (ENISA, 2011).

Estes sistemas industriais têm requisitos de funcionamento diferentes daqueles normalmente exigidos a computadores de escritório. Por exemplo, o acompanhamento de um processo químico de fabrico implica uma monitorização continua por parte de um computador integrado numa IC. Na realidade, a maior parte dos sistemas SCADA desempenha tarefas simples como a abertura e fecho de válvulas ou o ligar e desligar de determinados componentes. Nestes casos, não se considera que seja necessário fazer qualquer tipo de actualização a um sistema que está a desempenhar as suas funções de forma adequada. Assim, as actualizações são raras e os sistemas obsoletos que funcionam, ainda que de forma insegura, não são substituídos. Ou seja, apesar de utilizarem *software* COTS, pode ser economicamente inviável suspender o funcionamento de um computador integrado num sistema SCADA para instalar periodicamente todas as novas actualizações de segurança (Wilson, 2008).

Em suma, o ambiente aplicacional de uma IC típica é hoje uma complexa amálgama de aplicações ligadas em rede, criadas por programadores internos e externos, incluindo vendedores de *software* comercial, integradores e criadores que fornecem soluções únicas e proprietárias (Clarke & Olcott, 2012). Ao longo dos últimos anos, têm sido muitos os especialistas que têm denunciado uma variedade de vulnerabilidades de carácter técnico associadas aos sistemas SCADA. Algumas dessas vulnerabilidades impossibilitam a utilização de antivírus nos computadores SCADA e impedem que sejam realizados os mais elementares testes de segurança sem colocar em causa a segurança das próprias instalações e pessoal (Chiesa, 2007). Por outro lado, as ferramentas que podem ser utilizadas com intenções maliciosas estão gratuitamente disponíveis na internet e incluem módulos especialmente concebidos para atacar sistemas SCADA (Chiesa, 2010). Uma das tendências mais preocupantes é o surgimento de aplicações que permitem monitorizar sistemas SCADA a partir de dispositivos de computação pessoal

(Brown, 2011). A pressão empresarial para fazer mais com menos tem levado a um crescimento exponencial do acesso remoto aos sistemas SCADA, considerando-se mais proveitoso que os sistemas sejam monitorizados a partir de casa, em vez de pagar horas extraordinárias a um técnico que trabalhe junto dos sistemas.

Neste contexto, os fabricantes de sistemas SCADA estão cada vez mais a apostar na mobilidade e é hoje possível adquirir *online* uma aplicação "SCADA Mobile" para um *smartphone*, por uma quantia verdadeiramente irrisória. Cumulativamente, o crescente movimento em direcção ao chamado BYOD[12] terá, a breve prazo, um grande impacto na segurança de todos os sistemas de controlo das IC. Não é fantasioso imaginar um cenário em que um técnico, responsável pelo controlo de uma IC, decide levar para o local de trabalho o seu *tablet* PC a partir do qual tem estado, em casa, a monitorizar o funcionamento e os parâmetros do sistema SCADA pelo qual é responsável. No entanto, sem que ele saiba, uma das aplicações que adquiriu recentemente *online* está infectada com um *malware* especificamente concebido para interferir com sistemas idênticos ao que ele próprio opera. Assim, de forma tranquila e segura, um atacante externo tem acesso interno e privilegiado a um sistema do qual depende o funcionamento de toda uma comunidade, ou mesmo de um país. A realidade é que o número de vulnerabilidades técnicas identificadas não pára de crescer (Pollet, 2012) e esse facto está amplamente documentado em diversos documentos oficiais (DHS, 2011) (ICS-CERT, 2013b).

Um outro aspecto que contribui para a vulnerabilidade das IC é o já referido facto de muitas delas serem operadas e geridas por interesses privados. Recentemente, as autoridades dos EUA diagnosticaram uma série de problemas de segurança na rede eléctrica que derivam desta realidade. Por exemplo, algumas companhias preocupam-se apenas em cumprir a lei e não em aplicar segurança efectiva nas suas instalações. Além disso, têm lacunas de segurança nos seus procedimentos e não têm nenhum mecanismo eficaz de partilha de informação sobre cibersegurança (GAO, 2012). Esta preocupação não é nova, já foi reportada em diversos estudos (NERC, 2010) e continua a constar dos mais recentes relatórios oficiais (GAO, 2013). Os resultados de um estudo publicado recentemente pela SANS (Luallen, 2013) são uma amálgama confusa que ilustra a vasta panóplia de problemas de segurança dos sistemas SCADA. Na realidade, embora 50% dos inquiridos afirme ter práticas de actualização dos sistemas, a verdade é que também admitiram a sua incapacidade para monitorizar eficazmente os PLC e as ligações ao equipamento no terreno devido à ausência de segurança nativa nos próprios sistemas de controlo. Ou seja, a maior parte dos inquiridos monitoriza os computadores que executam o *software* de controlo quando deveria estar a monitorizar os próprios controladores embebidos nos sistemas. Infelizmente, a maior parte das organizações não consegue implementar políticas de segurança, como autenticação ou auditoria, nestes controladores uma vez que os mesmos não dispõem de nenhum tipo de controlos de segurança nativos.

A tendência para a diminuição dos custos tem levado a que muitas empresas na área da produção e distribuição de energia tenham reduzido a redundância física dos seus sistemas e estejam dependentes de longas cadeias de abastecimentos de sobressalentes, muitos deles fabricados no estrangeiro. Estas cadeias de abastecimentos criam

dependências externas nos sistemas de suporte e a sua ruptura pode provocar grande impacto. Ou seja, a própria cadeia de abastecimentos é uma vulnerabilidade importante (NERC, 2010). Ainda relacionado com este aspecto, importa referir que, desde 2005, as autoridades dos EUA têm confiscado grandes quantidades de *hardware* proveniente da China, preocupadas com a possibilidade desta tecnologia ser incorporada nas suas IC. Estas preocupações com a cadeia de abastecimentos são agora de tal maneira prioritárias que existem recomendações oficiais para que as companhias evitem a todo o custo a aquisição e instalação de *hardware* chinês, uma vez que há suspeitas relativamente à possibilidade deste ter vulnerabilidades propositadamente embutidas (GIT, 2013) (GAO, 2013).

Em face desta realidade, não admira que alguns especialistas afirmem que os EUA são um dos países mais vulneráveis a ciberataques às suas IC (Baker, Waterman, & Ivanov, 2009), ideia que parece ser comprovada pelo crescente número de incidentes nas IC norte-americanas (ICS-CERT, 2012).

4. Relevância Social

Uma IC é um alvo tentador para um inimigo, seja ele um terrorista ou um estado hostil. Do ponto de vista do ciberespaço, os sistemas SCADA são um dos alvos mais atractivos para funcionários descontentes ou sabotadores que tencionem desencadear um evento em larga escala (Shea, 2003). Por isso mesmo, alguns especialistas acreditam que o papel fundamental desempenhado pelos sistemas SCADA no controlo das IC os torna atractivos para os terroristas (Wilson, 2008). As ameaças cibernéticas à segurança nacional vão muito além dos alvos militares e afectam todas as áreas da sociedade. Tanto *hackers* como governos estrangeiros são cada vez mais capazes de lançar sofisticados ataques de intrusão sobre redes e sistemas que controlam IC civis. Tendo a conta a natureza integrada do ciberespaço, as falhas induzidas por meios informáticos nas redes energéticas, de transporte ou financeiras, podem provocar significativos danos físicos e rupturas económicas.

4.1. Historial de Incidentes

Em Janeiro de 2003, o *worm*[13] *Slammer* conseguiu, durante algumas horas, corromper o sistema de controlo da central nuclear Davis-Besse, no Ohio, tirando partido do facto de este sistema ter múltiplas ligações à internet (Stouffer et al., 2008). Nesse mesmo ano, o *worm Blaster* contribuiu para o efeito cascata do apagão de 14 de Agosto que afectou cerca de 10 milhões de pessoas no Canadá e 45 milhões de pessoas em oito estados dos EUA (Wilson, 2008). Este incidente revelou, não só a fragilidade dos sistemas de controlo industrial, mas também a grande interdependência entre a rede eléctrica e outros sistemas vitais ao funcionamento da sociedade, como as telecomunicações, o fornecimento de água, etc. Em Novembro de 2009, foi iniciada uma série de ciberataques

contra companhias do sector petrolífero e energético à escala global. Estes ataques, lançados a partir da China, envolviam engenharia social, exploração de diversas vulnerabilidades em *software* COTS e a utilização de ferramentas de administração remota para a recolha de informação empresarial classificada sobre financiamentos e projectos para novas explorações petroquímicas (McAfee, 2011).

Em 2010, o mundo foi surpreendido pela descoberta do *Stuxnet*[14], a primeira ciberarma realmente desenvolvida para ser usada contra uma nação estrangeira. Esta arma cibernética, destinada a atingir o programa nuclear iraniano destruindo as centrifugadoras das instalações de enriquecimento de urânio, teve uma grande eficácia, mas abriu uma verdadeira caixa de Pandora. Além das implicações políticas, o *Stuxnet* e os seus sucedâneos catapultaram os sistemas SCADA para os cabeçalhos noticiosos, tornando públicas as suas vulnerabilidade e criando um generalizado clima de insegurança relativamente às IC de todo o mundo. A realidade é que, desde então, o número de ataques contra as IC nos EUA aumentou exponencialmente, tal como se pode comprovar na Figura 3.

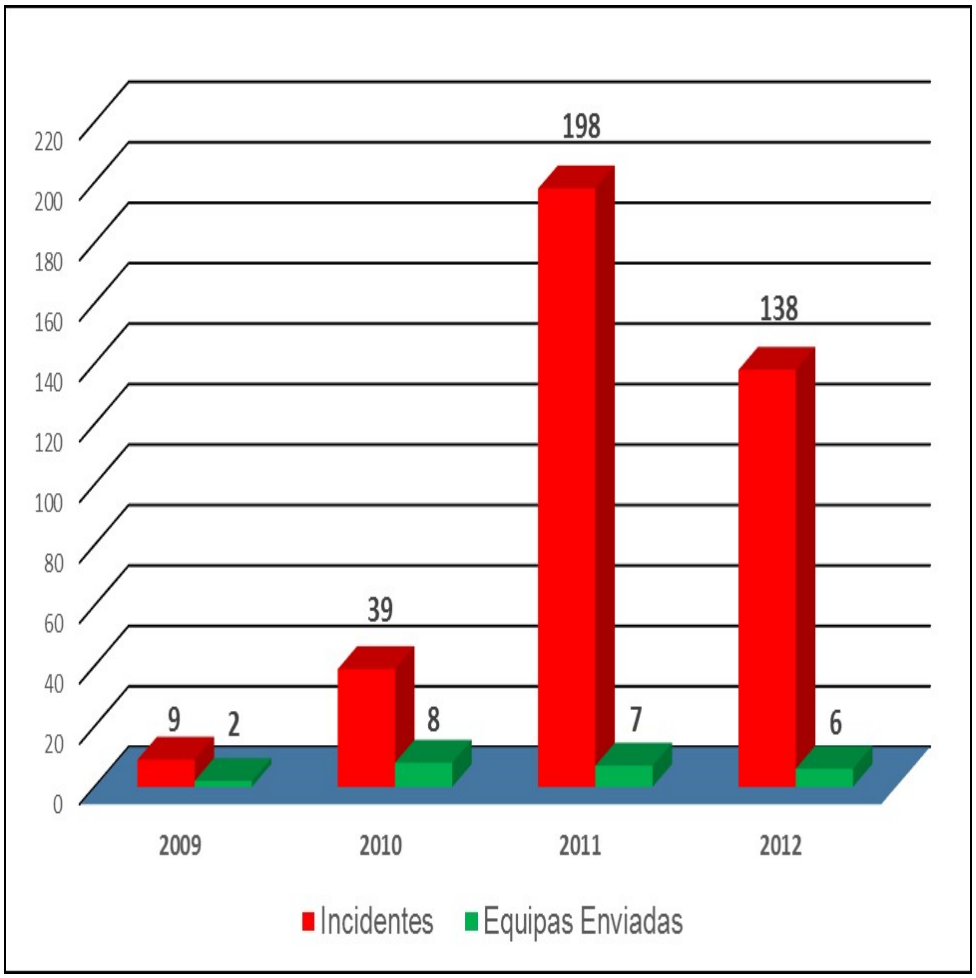

Figura 3 – Evolução do número de incidentes informáticos nas IC dos EUA.

Fonte: ICS-CERT (2012, 2013a)

É importante referir que estes são apenas os incidentes reportados e que muitas organizações optam por nunca dar conhecimento externo daquilo que ocorre nas suas instalações. Além disso, o número extremamente baixo de equipas enviadas ilustra o facto de muitas organizações privadas não solicitarem ajuda para lidar com estes eventos (ICS-CERT, 2013a).

Notícias recentes[15] dão conta de uma intrusão numa base de dados com informação classificada sobre as barragens dos EUA, executada a partir de território chinês. A referida base de dados (*U.S. Army Corps of Engineers' National Inventory of Dams*) tem informação sobre cerca de 8.100 barragens em território dos EUA, e esta intrusão fez subir as preocupações sobre um eventual ataque à infraestrutura da rede eléctrica norte-americana. Estes incidentes demonstraram de forma inequívoca a existência de significativas vulnerabilidades nos sistemas de controlo das IC, facto que continua a ser exaustivamente abordado em diversos relatórios, não só do governo dos EUA (GAO, 2013), mas também de agências europeias (ENISA, 2011) e de grupos de trabalho independentes (Hämmerli & Renda, 2010). Recentemente, o último boletim trimestral da ICS-CERT dá conta da persistente ocorrência de ataques contra diversas IC nos EUA, além da sistemática descoberta de novas vulnerabilidades e ameaças (ICS-CERT, 2013b).

4.2. Ameaças e Impacto

O alerta sobre a dimensão destas ameaças foi oficializado quando, em 1997, o governo norte-americano reconheceu que um comando enviado através de uma rede informática a um computador no controlo de uma IC poderia ser tão devastador quanto uma mochila cheia de explosivos, e o agressor seria mais difícil de identificar (PC-CIP, 1997). Esta preocupação foi sendo sistematicamente transmitida às autoridades norte-americanas, realçando sempre a possibilidade da ocorrência de eventos em cascata resultantes da interdependência das diversas IC (Shea, 2003). Embora considerassem como sendo pouco provável a ocorrência de uma falha catastrófica numa IC, o efeito sinergístico que as diversas IC têm entre si sempre foi motivo de grande preocupação. Por isso mesmo, alguns especialistas lançaram o alerta sobre a possibilidade de acontecimentos em cadeia, nos quais o colapso de uma IC levaria à falha de muitas outras. Este cenário é aquele que provoca maior apreensão entre os especialistas, ou seja, a ocorrência de um ciberataque contra uma IC em combinação com um ataque físico, por exemplo, terrorista. É exactamente no contexto da ameaça terrorista que o DHS (2003) considera que um ataque a uma IC poderá desencadear três tipos de efeitos:

– Efeitos directos na infraestrutura: falha parcial ou disrupção total das funções da IC ou de um recurso chave, e o consequente efeito em cascata, por meio de um ataque directo sobre os seus sistemas;

– Efeitos indirectos na infraestrutura: efeito em cascata e consequências políticas, económicas e sociais que advêm das reacções dos sectores público e privado a um ataque;

– Exploração da infraestrutura: aproveitamento de elementos da infraestrutura atacada para atacar outro alvo.

Uma hipótese, é um convencional ataque bombista ser apoiado por uma interrupção da rede eléctrica ou dos serviços de comunicação. A resultante diminuição da capacidade de resposta dos serviços de emergência fará rapidamente escalar o número de baixas (Shea, 2003), ou seja, o ciberataque aumentará o impacto do ataque físico. Embora a ameaça de um ciberataque, coordenado para amplificar os efeitos de um ataque terrorista convencional, continue a ser uma das grandes preocupações dos especialistas em segurança, não existe consenso sobre a dimensão real do impacto de um ataque directo sobre os sistemas informáticos que controlam as IC (Wilson, 2008). No entanto, o longo historial de incidentes relacionados com as vulnerabilidades das IC já evidenciou o impacto que um ataque premeditado pode ter sobre uma vasta área e grande número de pessoas. Além disso, como já vimos, as IC têm diversas vulnerabilidades, o que as deixa bastante expostas a inúmeras ameaças, tornando-as extremamente falíveis. Entrando em linha de conta com a dependência social das IC, e a grande interdependência entra elas, é lógico considerar que a ligação de todos os sistemas essenciais à vida moderna pode amplificar bastante o impacto de uma calamidade numa IC (GAO, 2012).

Mas o impacto de um ataque sobre os ICS das IC pode variar muito. É normalmente assumido que um ciberataque bem-sucedido causará poucas ou nenhumas baixas, embora possa causar alterações nos serviços. Por exemplo, um ataque contra a rede telefónica pode deixar os utilizadores sem esse serviço durante várias horas enquanto os técnicos reparam os danos provocados. Mas um ataque contra os sistemas de controlo de uma instalação química pode causar danos físicos sobre uma área alargada (Shea, 2003). Esta opinião é partilhada por outros especialistas, que consideram que as consequências de um ataque cibernético contra uma IC podem variar desde a simples, e relativamente inócua, interrupção temporária dos serviços, até actos de sabotagem intencional destinados a provocar elevado número de vítimas, como por exemplo grandes explosões em instalações industriais (Knapp, 2011). Por outro lado, as comunicações são hoje parte integrante da nossa sociedade e não é concebível viver num mundo sem meios de comunicação. Na realidade, as IC fornecem, entre outras coisas, o suporte para a comunicação sem a qual a nossa sociedade não existiria.

Nos últimos anos, as IC tornaram-se dependentes de complexas aplicações de *software* para desempenhar funções sociais vitais que incluem a distribuição de energia, finanças e transportes. Um evento cibernético que afecte uma IC pode, não só afectar a sua área de negócio, mas também afectar a saúde pública, a economia e a segurança nacional (Clarke & Olcott, 2012). Um dos aspectos mais emblemáticos desta nova sociedade é a capacidade para fazer negócios em qualquer fuso horário, a qualquer hora do dia. Como se pode ver na Tabela 1, todos os países consideram que o sector financeiro é uma das suas IC. Na verdade, o sistema financeiro internacional é um gigantesco alvo para

cibercriminosos e ciberterroristas que tentam obter proveitos financeiros, afectando a economia global. Os ataques ao sistema financeiro internacional constituem uma das maiores ameaças do ciberterrorismo, mas acreditamos que é pouco provável que venham a ocorrer, uma vez que o sistema é de facto global. Ou seja, os únicos interessados em lançar ataques desse tipo serão os actores não ligados a nenhum estado em particular, e não será fácil que esses disponham de meios para o fazer. Os estados estão demasiados envolvidos financeiramente para considerarem sequer essa possibilidade. Segundo Wilson, alguns especialistas dos EUA consideraram a possibilidade de lançar ataques contra o sistema bancário chinês (Wilson, 2008). Da mesma forma, os jornais militares chineses especularam que os seus ciberataques poderiam provocar uma interrupção nos mercados financeiros norte-americanos. Mas a verdade é que um ataque deste tipo, lançado sobre *Wall Street*, poderia ter um impacto mais devastador sobre a China do que propriamente sobre os EUA, tal é a interdependência que existe no sistema financeiro internacional (Wilson, 2008).

Esta discussão acerca dos efeitos globais de um ataque sobre o sistema financeiro é indissociável do debate acerca do impacto de um ataque sobre o próprio ciberespaço, uma vez que será esse o veículo utilizado para afectar globalmente os mercados financeiros. Mas, à semelhança do que ocorre com o sector financeiro, nenhum Estado está interessado na destruição ou disrupção do ciberespaço dada a importância que este assumiu em todos os aspectos da nossa sociedade. Na realidade, o ciberespaço e toda a sua infraestrutura de suporte, desde os servidores base[16] do *Domain Name System* (DNS) até aos simples *routers* dos ISP[17] regionais, é uma gigantesca IC.

Num outro contexto, as redes eléctricas nacionais são de duplo uso, no sentido em que alimentam o sector público, incluindo a defesa, e o sector privado. Assim, um ataque sobre um ponto nevrálgico pode desligar um sector da rede eléctrica que alimente simultaneamente hospitais e bases militares (Lukszo, Deconinck, & Weijnen, 2010). Se, por um lado, é verdade que os países rejeitam os ataques contra hospitais, por outro é provável que atinjam alvos militares com armas cibernéticas. Nesse contexto, atacar a rede eléctrica pode ser a melhor forma de debilitar a capacidade militar de uma nação (DHS, 2012) (GAO, 2004, 2012). Ou seja, a existência de diversas vulnerabilidades e a complexa rede de interdependências entre as IC combinam-
-se para criar uma situação em que um ataque contra uma IC pode causar grande impacto sobre quem dela depende. Esta realidade tem sido abordada em diversos estudos conduzidos nos EUA, por exemplo, sob a designação de "alto impacto, baixa frequência"[18]. Num desses estudos (NERC, 2010), é referido que, embora o risco de um ciberataque coordenado contra as IC seja reduzido, o impacto pode ser muito alto, pois o ciclo de aquisição e substituição dos componentes afectados pode levar muitos meses, até anos. Esta é uma consequência das vulnerabilidades atrás elencadas: dependência do sector privado, orientado para lucro, e dependência de uma cadeia de abastecimentos pouco fiável.

Já em 1997, o presidente dos EUA foi informado acerca dos efeitos da desregulação e concorrência em muitas IC industriais. Nesse relatório (PC-CIP, 1997) é explicitamente referido que as organizações incorporaram as TIC para acelerar a entrega dos seus bens

e serviços e evitar todo o tipo de desperdícios, o que levou a que muitas empresas estejam tão orientadas para os seus processos "*just in time*" que a recuperação de uma perturbação, por menor que seja, será extremamente difícil. Ou seja, o impacto pode ser muito elevado e o risco está longe de ser desprezável. Independentemente da natureza e da origem das ameaças, as vulnerabilidades da sociedade moderna são derivadas do facto de esta ser altamente industrializada, utilizando tecnologias complexas e organizadas em sofisticadas estruturas organizacionais. Assim, no decurso da sua evolução tecnológica, a sociedade tornou-se mais sensível à disrupção destas infraestruturas visto que os seus elementos constituintes estão concebidos para funcionar numa lógica de garantia total da cadeia de abastecimento. Esta situação cria um falacioso sentimento de segurança no qual o impacto de um incidente improvável será desproporcionalmente grave. Ou seja, à medida que a robustez dos sistemas aumenta e a susceptibilidade de um país a uma falha na sua cadeia de abastecimento diminui, mais grave será o impacto real de um incidente disruptivo. Este fenómeno é conhecido como o paradoxo da vulnerabilidade (KRITIS, 2004).

5. Risco Social

O primeiro passo para um incremento na segurança dos processos e sistemas de controlo modernos é a compreensão aprofundada dos riscos no contexto da segurança electrónica. Só assim se poderão tomar decisões estratégicas informadas, relativamente aos níveis apropriados de segurança necessários em cada um dos contextos organizacionais. O risco é uma função das ameaças, das vulnerabilidades e dos impactos (NERC, 2010). Nos pontos anteriores foram elencadas diversas vulnerabilidades dos sistemas de controlo associados às IC e outras derivadas das suas relações de interdependência. Além disso, foram, não só analisados alguns dos impactos já provocados por incidentes no passado, mas foi também traçado um panorama geral sobre o impacto previsível de um ataque premeditado sobre uma IC. Ou seja, as ameaças são reais e a prová-lo está o facto de o presidente dos EUA ter recentemente emitido uma directiva[19] e uma ordem executiva[20] exactamente sobre esta temática. Portanto, a questão não é saber se há ou não riscos associados às IC; o problema reside em identificá-los, avaliá-los e mitigá-los.

5.1. Identificação e quantificação

Voltando à definição de risco, este é influenciado pela natureza e magnitude da ameaça, pelas vulnerabilidades a essa ameaça e pelas consequências que daí podem resultar (Chertoff, 2009). A ameaça é o acto em si mesmo, as vulnerabilidades são as partes ou características do sistema que podem ser afectadas por esse acto, e as consequências são o resultado da exploração da vulnerabilidade (NERC, 2010). Todas estas áreas têm que ser tidas em conta para uma verdadeira compreensão dos riscos. Assim, a avaliação do nível de risco associado às IC, utilizando uma abordagem abrangente, tornou-se uma prioridade com vista a permitir um melhor fluxo de informação e melhorar a eficiência

das IC (Hämmerli & Renda, 2010). No entanto, muitas organizações têm grande dificuldade em avaliar correctamente o nível de risco a que estão expostas (Cornish et al., 2011) e estudos recentes mostram que muitas avaliações do risco são mal conduzidas, devido a um desconhecimento dos procedimentos adequados para o efeito e das métricas apropriadas para avaliar qualquer um dos parâmetros importantes (Clemente, 2013). O resultado é que os riscos podem ser exacerbados e afectados por outros factores, uma vez que a sua avaliação não é realizada de modo uniforme: alguns itens de grande importância para uma comunidade local podem ter impacto apenas limitado a uma pequena zona, enquanto outros de menor importância local podem ter impacto a nível nacional (DHS, 2012).

Além disso, há que ter em conta a falta de exactidão das métricas existentes quando aplicadas ao impacto do domínio "ciber" sobre as IC. O espectro de potenciais motivos, meios e oportunidades no ciberespaço está para lá do âmbito de qualquer ferramenta de análise de risco, e a rápida expansão da complexidade do sistema socio-tecnológico torna esta realidade imutável (Clemente, 2013). Os sistemas SCADA eram tradicionalmente encarados como sendo seguros e isolados, logo menos expostos a ciberataques. Consequentemente, as metodologias de avaliação do risco utilizadas eram ajustadas a estes sistemas antigos, sem preocupações de segurança. A recente evolução e integração dos sistemas SCADA nas redes empresariais, conjuntamente com o rápido avanço da tecnologia, alteraram o panorama das ameaças e alargaram as vulnerabilidades o que obriga a uma nova metodologia de avaliação do risco (ITSEAG, 2012).

Assim, apesar de todos os esforços para minimizar a incerteza, o risco pode ter um impacto inesperado devido à complexa teia de interdependências que liga todas as IC e que pode levar a surpreendentes efeitos em cascata (DHS, 2012). Daí a necessidade de desenvolver novas abordagens para avaliar o risco em modernos sistemas SCADA, acautelando as especificidades de cada sector e organização (ITSEAG, 2012). É provável que um sistema de baixo risco necessite menores medidas de protecção do que um sistema de alto risco, mas esta avaliação tem que ser um processo contínuo, à medida que novas vulnerabilidades vão sendo expostas e novas ameaças surgem no horizonte (CPNI, 2012). Embora todos os operadores e proprietários das IC refiram que a segurança é uma prioridade de topo, nem mesmo os países com taxas mais elevadas de implementação de medidas de segurança estão a salvo de ataques (Baker et al., 2009). É exactamente essa a razão que leva as autoridades norte-americanas a colocar no topo da lista de prioridades o desenvolvimento e implementação de novos programas de avaliação do risco (GAO, 2013), e faz com que os europeus sintam a necessidade de uniformizar a taxonomia, as métricas e a gestão do risco de modo a possibilitar uma abordagem uniforme à problemática da protecção das IC (Hämmerli & Renda, 2010) (ENISA, 2011).

5.2. Gestão

Um dos estudos já citados (Cornish et al., 2011) conclui claramente que muitas organizações, por má avaliação do risco, não conseguem investir adequadamente na sua

gestão e mitigação. Além disso, a realidade empresarial e política faz com que a gestão do risco seja muito mais difícil, visto que muitas IC estão fora da alçada geográfica ou jurídica dos governos que delas dependem (Clemente, 2013). Por outro lado, a realidade de contingência financeira leva a que muitas organizações estejam dispostas a aceitar altos níveis de risco numa tentativa de manter as margens de lucro, reduzindo os investimentos em recursos necessários a minimizar as suas vulnerabilidades (Cornish et al., 2011). Estas dificuldades não são novas e haviam sido já identificadas por Shea quando reportou que, em face da incerteza sobre a dimensão real do risco associado aos ataques cibernéticos, as indústrias privadas teriam grande dificuldade em justificar os investimentos necessários para modernizar os sistemas ICS de modo a melhorar os seus níveis de segurança (Shea, 2003).

A situação não melhorou muito nos últimos anos, e continua a não existir uma coordenação global para garantir que a indústria segue as melhores práticas aconselhadas. Além dos aspectos burocráticos relacionados com o facto de muitas IC serem privadas, há também que ter em conta que as ameaças estão em constante evolução. Assim, muitas indústrias escudam-se no facto de a segurança do ciberespaço ser responsabilidade governamental (GAO, 2012), e protelam a aplicação de medidas de segurança. De acordo com o estudo da SANS, que incidiu sobre 700 participantes, 70% dos operadores dos sistemas consideram que os riscos a que os seus sistemas estão expostos são graves ou muito graves, e 33% suspeitam já ter sido alvo de incidentes (Luallen, 2013). É pois urgente que a criação de uma moldura legal e técnica de gestão do risco seja encarada como responsabilidade dos mais altos níveis políticos, tal como já foi sugerido por estudos independentes (Hämmerli & Renda, 2010). É a única forma de resolver a contradição nas posições assumidas por muitas organizações com responsabilidades nesta área: por um lado, demonstram possuir grande consciência dos riscos existentes mas, por outro lado, estão dispostas a aceitar um elevado nível de risco relacionado com segurança cibernética (Cornish et al., 2011).

É impossível proteger completamente um sistema de todas as ameaças. Consequentemente, uma gestão do risco equilibrada tem que ter presente esta realidade e assumir uma abordagem holística com especial atenção para a determinação do equilíbrio entre resiliência, restauração e protecção (NERC, 2010). Sempre foi impossível proteger completamente as IC, mas agora é cada vez mais difícil identificar exactamente aquilo que deve ser protegido. É mais do que apenas infraestrutura; é também informação crítica para o funcionamento da infraestrutura. Nalguns casos, a infraestrutura serve apenas como mero repositório dessa informação valiosa (Clemente, 2013). Os riscos associados às IC, nomeadamente os já referidos HILF, são um tipo de risco que não pode ser transferido, não pode ser completamente segurado e também não pode ser gerido isoladamente por apenas por uma firma. Este tipo de risco tem que ser considerado ao nível do sector em que se insere, particularmente em sectores em que as entidades estão altamente ligadas e interdependentes (NERC, 2010).

O desenvolvimento de novos métodos de avaliação de risco e planos para a sua gestão são a prova de que os governos e as organizações estão conscientes da impossibilidade de proteger completamente as IC. Este facto é assumido frontalmente pelas autoridades

alemãs quando afirmam que, nem o Estado nem os operadores das IC poderão garantir a sua total protecção e a sua completa operacionalidade (BMI, 2009). A consequência, ainda segundo os alemães, é a necessidade de uma mudança de mentalidade de segurança, adoptando aquilo a que chamam uma nova "cultura de risco". Esta nova mentalidade de segurança assenta essencialmente numa partilha de informação sobre os riscos entre todas as entidades interessadas: governo, privados e público em geral. Além disso, preconiza um novo modelo de cooperação entre operadores e responsabilização acrescida pela prevenção e gestão de incidentes. Esta orientação parece ser generalizada e foi também identificada, embora de outra forma, em documentos do governo dos EUA que atribuem à avaliação e gestão do risco um papel preponderante na estratégia da futura protecção das IC (DHS, 2012), dando continuidade a planos já existentes (Chertoff, 2009).

No lado da UE, a situação parece estar um pouco mais atrasada devido à falta de coordenação entre governos e operadores privados (Hämmerli & Renda, 2010), mas ganhou todo um novo impulso em face do surgimento do *Stuxnet*, embora não existam ainda iniciativas específicas para a segurança dos ICS (ENISA, 2011).

5.3. Futuro

Já em 1997, era claramente identificado que a forma mais rápida e eficaz de garantir um melhor nível de segurança contra as ciberameaças seria através de uma estratégia de cooperação e partilha de informação entre os proprietários das IC e as autoridades governamentais (PC-CIP, 1997). No entanto, estudos recentes revelam que existem várias inconsistências, falhas e omissões na forma como muitas organizações gerem as suas vulnerabilidades e ciberdependências, nomeadamente, no que diz respeito à garantia do funcionamento das suas áreas críticas (Cornish et al., 2011). As interligações permitem ganhos de eficiência, mas criam interdependências e, por acréscimo, vulnerabilidades. Aceitar a incerteza inerente a sistemas cibernéticos complexos acarreta riscos políticos, pois implica ausência de controlo. Mas esta realidade é inquestionável e os governos que acreditarem que conseguem controlar todo o ciberespaço estão a assumir uma estratégia de negação da incerteza que tem também grandes riscos associados (Clemente, 2013). A verdade é que existe um distanciamento entre a gestão de topo e os problemas associados ao risco, embora tal facto pareça dever-se apenas a falta de interesse e não a uma negligência deliberada. Mas a prática é que, o aumento do risco é encarado com uma diminuição dos recursos afectos à sua mitigação (Cornish et al., 2011). Neste contexto, parece óbvio que as organizações e os governos só irão reagir em conformidade com a realidade após sentirem o impacto real de um incidente de grandes proporções.

O sector eléctrico tem, a nível mundial, assumido a liderança destas preocupações. Embora seja muito dependente de outras infraestruturas para o seu correcto funcionamento, o sector eléctrico tem sido descrito como o "primeiro entre iguais" uma vez que tem um papel central entre as IC (NERC, 2010). Mas a natureza interligada do mundo das IC não permite que um sector seja analisado de forma isolada e, por isso

mesmo, a grande prioridade do futuro é a melhoria das actividades de gestão e risco de forma transversal a todas as IC (DHS, 2012). Metodologias deste tipo estão, genericamente, a ser adoptadas um pouco por todo o mundo, alinhadas com *standards* internacionais (ITSEAG, 2012) e tentando dar resposta aos desafios apresentados pelo vida moderna. No entanto, esta tarefa é encarada com bastante cepticismo e, num estudo realizado com especialistas de diversos países desenvolvidos, 45% dos inquiridos afirmou que os seus governos não seriam capazes de prevenir convenientemente os ciberataques (Baker et al., 2009). O próprio governo norte-americano revelou recentemente que há falhas na gestão dos riscos associados à cadeia de abastecimentos e que esta, por si só, introduz riscos que as agências federais não conseguiram, até à data, colmatar (GAO, 2013). Talvez os mais cépticos tenham razão quando afirmam que não há um modelo que consiga acompanhar a evolução e sofisticação das ciberameaças às IC, porque as inovações tecnológicas não param de criar novas vulnerabilidades (Baker et al., 2009).

6. Situação Nacional

Em Portugal, as primeiras iniciativas para a protecção das IC tiveram início em 2003, simultaneamente com as primeiras medidas a nível da União Europeia (UE) com vista à elaboração de uma estratégia conjunta para a protecção das Infraestruturas Críticas Europeias (ICE). Nessa altura, considerando que a temática em apreço era de carácter marcadamente multidisciplinar e transversal a todos os sectores estratégicos nacionais, foi criado para esse efeito um grupo de trabalho, coordenado pelo então Conselho Nacional de Planeamento Civil de Emergência (CNPCE).

6.1. Enquadramento Europeu

Em 20 de Outubro de 2004, a Comissão Europeia (CE) adoptou uma Comunicação efectuada ao Conselho e ao Parlamento Europeu, como estratégia global de protecção das IC e propôs a elaboração de um Programa Europeu de Protecção de Infraestruturas Críticas (PEPIC). Em 17 de Novembro de 2005, a CE adoptou um Livro Verde sobre PEPIC, que constituiu um marco importante no reforço do enquadramento comunitário em matéria de protecção das IC. Em Dezembro do mesmo ano, o Conselho Europeu solicitou à CE que apresentasse uma proposta de PEPIC, tendo a Comissão adoptado a Comunicação de 12 de Dezembro de 2006 sobre o assunto. Em Abril de 2007, o Conselho Europeu aprovou um conjunto de conclusões sobre o PEPIC, reafirmando que, em última instância, é a responsabilidade de cada um Estados-membro assegurar a protecção das IC em cada um dos respectivos territórios nacionais.

Esta dinâmica levou a que, em 8 de Dezembro de 2008, tivesse sido publicada a Directiva 2008/114/CE do Conselho Europeu (*Jornal Oficial da União Europeia*, 2008), relativa à identificação e designação das ICE, onde se estabeleceu um procedimento de identificação e designação das mesmas, e uma abordagem comum relativa à avaliação da

necessidade de melhorar a sua protecção. De acordo com esta Directiva, uma ICE é a infraestrutura situada num Estado-membro, cuja perturbação ou destruição tenha um impacto significativo em pelo menos dois Estados-membros, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas. Devido ao elevado número de IC existentes na globalidade do espaço europeu, a CE orientou os seus esforços para a protecção das infraestruturas de dimensão transnacional, deixando a protecção das restantes ao cuidado de cada um dos Estados-membro. Além disso, como já foi referido, a Directiva concentra-se nos sectores da energia e dos transportes, embora perspective já a necessidade de futuramente incluir o sector das TIC.

6.2. Enquadramento legal e institucional

O projecto para a protecção das IC nacionais (Projecto PIC) foi iniciado em 2003, pelo CNPCE, com o objectivo de criar uma definição estratégica das IC a proteger, quer em situação de crise, quer do ponto de vista preventivo, através da definição de políticas mais adequadas para a sua protecção. Este projecto tinha duas fases: a primeira, seria a identificação e classificação das infraestruturas fundamentais para o normal funcionamento do país, e a segunda, consistiria na elaboração de um Programa Nacional para a Protecção de Infraestruturas Críticas (PNPIC), identificando e avaliando as vulnerabilidades das infraestruturas identificadas face às principais ameaças passíveis de as atingir. Na primeira etapa, os diversos sectores estratégicos nacionais foram classificados com base na sua importância relativa, e foram identificadas as respectivas IC. A segunda etapa foi também concluída, mas deveria ser um trabalho em permanente actualização de modo a responder ao constante surgimento de novas ameaças. De referir que, nesta altura, e em face do fatídico atentado ao *World Trade Center*, um dos principais objectivos destes trabalhos era a protecção contra eventuais ataques cinéticos cometidos por terroristas.

A protecção das IC ganhou o devido enquadramento legal quando, em 9 de Maio de 2011, foi publicado o Decreto-Lei nº 62/2011, o qual transpôs para o ordenamento jurídico nacional a supracitada Directiva 2008/114/CE, publicada no final de 2008. Para efeitos deste diploma, considera-se como “infra-estrutura crítica a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções”. E como “infra-estrutura crítica europeia ou «ICE» a infra-estrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da UE, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infra-estruturas”.

O referido diploma define procedimentos relativos à identificação e designação de ICE, estabelece a obrigatoriedade de elaboração de planos de segurança por parte dos

operadores e determina a existência de planos de segurança externos, da responsabilidade das forças de segurança e da protecção civil. Embora vocacionado para as ICE dos sectores da energia e transportes, o Decreto-Lei nº 62/2011 prevê igualmente a aplicação dos mesmos procedimentos às IC nacionais, competindo ao CNPCE a identificação das potenciais ICE de forma permanente, através de um processo faseado, informando a UE e o respectivo proprietário ou operador. Contudo, na sequência da aplicação do Plano de Redução e Melhoria da Administração Central (PREMAC), este organismo foi extinto, por via do Decreto-Lei nº 73/2012, de 26 de Março, que transferiu as suas atribuições para a Autoridade Nacional de Protecção Civil (ANPC), no âmbito do Ministério da Administração Interna. Assim, a ANPC passou a ser o órgão responsável por assegurar o planeamento e coordenação das necessidades nacionais na área do planeamento civil de emergência, além dos acidentes graves e catástrofes.

6.3. Uma possível abordagem

O primeiro passo para a elaboração de um PNPIC terá, obrigatoriamente, que ser a identificação e selecção dos sectores estratégicos mais importantes. Embora Portugal seja um país relativamente pequeno, é completamente impossível proteger todas as áreas importantes e todas as infraestruturas existentes ou mesmo garantir, a cem por cento, a segurança de uma única. Existirão também algumas ameaças e riscos que não poderão ser evitados e cujos resultados serão devastadores. Além disso, a escassez de recursos humanos e materiais obriga a uma criteriosa selecção das infraestruturas que devem ser alvo de atenção prioritária. Apesar destas circunstâncias, será no entanto possível maximizar o nível de segurança das IC que se revistam de maior importância estratégica. Assim, torna-se necessário delinear, dentro daquilo que será economicamente sustentável, um PNPIC com vista a maximizar o nível de segurança de um conjunto de infraestruturas e recursos chave, fundamentais para o bem-estar da população portuguesa e para a segurança do Estado.

À semelhança do que ocorre em muitos outros países, grande parte das IC nacionais são propriedade e/ou operadas pelo sector privado o que obriga o Estado a fomentar um esforço de cooperação para o desenvolvimento de medidas de protecção adequadas. Embora não sendo, nem proprietário, nem operador de muitas IC, o Estado não pode eximir-se das suas responsabilidades e, por isso mesmo, é natural que os operadores privados esperem que sejam os organismos públicos a assumir a liderança deste processo. No entanto, esta postura de expectativa poderá contribuir para negligenciar a tomada de medidas preventivas a nível empresarial. Assim, o Estado deverá apostar na prevenção em detrimento da reacção, assumindo as suas responsabilidades, mas pressionando todas as outras entidades envolvidas, incentivando o sector privado a investir na sua própria protecção. Por outro lado, a situação geográfica particular de Portugal leva que seja necessário dar uma especial atenção à cooperação com Espanha, visto que sectores estratégicos, como a energia e a água, estão intrinsecamente ligados ao nosso vizinho ibérico. Como já vimos, o funcionamento das sociedades modernas deriva das IC não serem um elemento isolado, mas sim parte de um conjunto complexo,

interligado por relações de equilíbrio e interdependência, em que a falta de um único elemento pode colocar em causa todo o sistema. Desta forma, infraestruturas que se encontram dentro do território espanhol poderão desempenhar funções vitais no funcionamento de infraestruturas situadas no território português, e vice-versa.

Um programa nacional de protecção de IC não pode ser focado apenas na defesa contra eventuais ataques físicos de tipo terrorista. Como vimos anteriormente, as principais ameaças hoje são de tipo informático; intangíveis e invisíveis, mas muito reais. Ou seja, é necessário proceder a um levantamento exaustivo da situação dos ICS existentes, com espacial ênfase para os sistemas SCADA. O Estado deverá sensibilizar os operadores privados para esta realidade, divulgando periodicamente as vulnerabilidades detectadas internacionalmente, e mantendo um permanente esforço pedagógico. Assim, o PNPIC deverá dar atenção a um vasto conjunto de ameaças, incluindo os ataques físicos e cibernéticos além dos desastres naturais. Neste contexto, em que as ameaças são muito diversificadas, a gestão de risco assume particular importância. Embora existam diversas metodologias para a gestão do risco, aquela que consta da família de normas ISO 31000 parece ser a mais adequada às necessidades nacionais uma vez que, sendo genérica, pode ser facilmente adaptada e aplicada a qualquer um dos sectores estratégicos a proteger. Esta é uma área em que o Estado deve claramente liderar o processo, criando normas nacionais compiladas, por exemplo, num manual de boas práticas na gestão do risco, à semelhança do que ocorre noutros países.

Embora seja consensual afirmar que existem diversos sectores essenciais ao normal funcionamento de um Estado, a identificação daqueles que são mais importantes, os sectores verdadeiramente estratégicos, e as IC a eles associadas, é um processo sempre polémico e dinâmico. No entanto, a análise dos elementos constantes da Tabela 1 leva à conclusão que há alguns sectores que são considerados como sendo estratégicos na esmagadora maioria dos países considerados no referido estudo. Além disso, as relações de interdependência ilustradas na Figura 1 reforçam esta realidade; o número de sectores verdadeiramente estratégicos é relativamente reduzido. Assim, numa tentativa de focar a atenção naquilo que deve ser preservado a todo o custo, e sem prejuízo da existência de outros sectores essenciais, os sectores estratégicos em Portugal são os seguintes:

6.3.1. Energia

Este sector é particularmente crítico, quer pelo efeito imediato de um ataque às suas infraestruturas, quer pelo efeito que esse ataque provocará nos restantes sectores. Na realidade, este é um sector essencial ao normal funcionamento de todos os outros sectores, uma vez que uma eventual perturbação no fornecimento de energia desencadearia, através das relações de interdependência, a paralisação de IC em diversas áreas de actividade, com consequências imprevisíveis. Neste sector incluem-se as instalações e redes de produção, armazenamento, transmissão e distribuição de energia, nomeadamente de combustíveis, gás e electricidade. Neste contexto, deve ser dada particular atenção à cibersegurança dos centros nevrálgicos de controlo da distribuição e aos ICS das infraestruturas de produção e armazenamento.

6.3.2. Telecomunicações

Contrariamente ao sector energético, a criticidade deste sector não deriva tanto do potencial efeito directo de um ataque às suas infraestruturas, mas antes do efeito catastrófico que a interrupção do seu funcionamento normal desencadeará nos restantes sectores. Por outro lado, é o sector mais exposto às ameaças cibernéticas uma vez que está na base do funcionamento do próprio ciberespaço. Neste sector estão incluídos os sistemas de informação, sistemas de controlo, redes de dados, internet, telecomunicações fixas e móveis e comunicações via rádio e via satélite. É um sector onde deve ser dado particular destaque aos centros de dados e às comunicações de emergência pois a falha neste último serviço pode colocar em causa todo o esforço de coordenação e resposta a uma crise.

6.3.3. Água

Num país em que grande parte do território é sistematicamente assolado por longos períodos de seca, este é um sector verdadeiramente crítico para a saúde pública e para a vida económica, sendo imprescindível proteger a população de roturas de abastecimento e eventuais contaminações. Uma perturbação grave do abastecimento de água acarretaria consequências imediatas no funcionamento de outros sectores, bem como na qualidade de vida dos cidadãos, e um ataque por contaminação causaria milhares de vítimas. Desta forma, torna-se necessário garantir a segurança dos sistemas de armazenagem de água potável e, dentro do possível, garantir a integridade e segurança das infraestruturas necessárias à sua distribuição.

6.3.4. Transportes e Logística

O transporte de passageiros e mercadorias é essencial ao normal funcionamento das sociedades modernas, dada a forte relação de interdependência com todas as áreas de actividade que dele dependem para a distribuição de grande parte dos bens essenciais. Este sector engloba todas as infraestruturas ligados ao transporte e distribuição por via aérea, marítima, fluvial, ferroviária e rodoviária. Sendo completamente impossível proteger todas as redes de transportes, torna-se necessário identificar os seus pontos-chave de modo a minimizar o impacto que um ataque provocará no sistema de transportes e logística. Nesta área destaca-se a segurança dos aeroportos de Lisboa e Porto e dos terminais marítimos de Sines e Leixões. Além disso, são também importantes os centros de controlo de tráfego, onde se destaca o de Santa Maria, nos Açores, responsável pelo controlo de tráfego aéreo em boa parte do oceano Atlântico.

6.3.5. Banca e Finanças

O mundo actual gira em trono de mercados financeiros, cotações bolsistas e negócios de todo o tipo. Este sector engloba as redes de dados financeiros, os meios de pagamento e os valores mobiliários, entre outros elementos necessários ao normal funcionamento de todo o sistema económico mundial. É um sector completamente dependente dos sectores energético e telecomunicações e, além de assentar numa grande variedade de estruturas físicas e recursos humanos, depende essencialmente de serviços disponibilizados a partir

de centros de dados. São exactamente estes centros de dados, inseridos no sector das telecomunicações, um dos alvos prioritários para todo o tipo de actividades ligadas ao cibercrime. Uma perturbação grave do sector financeiro pode levar a uma crise à escala global e, por isso, é particularmente importante preservar a integridade dos dados financeiros e a segurança do funcionamento de todo o sistema.

6.3.6. Governo

Este sector refere-se aos órgãos de soberania a quem compete a execução das funções governativas e administrativas do Estado. Na sua dependência funcionam todos os serviços públicos, em particular os serviços de emergência e protecção civil, aos quais compete uma primeira resposta em situações de crise. Numa situação de emergência, é imprescindível que as instituições públicas assegurem a prestação de socorro às vítimas e a manutenção da ordem pública. Destacam-se, neste âmbito, os órgãos do Governo Central capazes de assegurar o normal funcionamento da sociedade.

7. Conclusões

As economias baseadas no conhecimento estão numa fase de transição para uma situação de total dependência das tecnologias de informação, sem qualquer hipótese de retrocesso para os antigos processos e modos de funcionamento. Na base desta mudança estão as IC que sustentam a nossa defesa nacional, o nosso desenvolvimento económico e a nossa qualidade de vida e que, por isso mesmo, devem ser encaradas à luz da Era da Informação. A velocidade das transformações no ciberespaço está a criar novas fronteiras e a revelar novas vulnerabilidades em diversas áreas de actividade pública e privada. Seja qual for o sector considerado, as organizações dependentes da tecnologia devem estar preparadas para enfrentar um crescimento das ciberameaças criadas pela proliferação e integração das telecomunicações e de sistemas informáticos em todas as IC. Os sistemas de controlo industrial, responsáveis pelo funcionamento das IC, não estão preparados para acompanhar esta mudança e a sua interligação criou uma rede de interdependências que adicionaram uma nova dimensão a todas as vulnerabilidades de que estes sistemas já padeciam.

Na realidade contemporânea, a existência de infraestruturas informatizadas pode ser explorada através da penetração das redes de comunicação, do *software* ou mesmo do *hardware*, de modo a perturbar, paralisar, e até destruir um sistema crítico. Esta ameaça deriva das vulnerabilidades inerentes às propriedades do ciberespaço e, devido a estas mesmas características, a ameaça ciberespacial difere fundamentalmente de todas as outras. Ou seja, às velhas vulnerabilidades somam-se agora as novas ameaças, numa verdadeira panóplia de riscos, muitos deles incomensuráveis. Toda a sociedade depende cada vez mais de um conjunto de infraestruturas, algumas das quais são verdadeiramente críticas para o funcionamento de empresas e governos. Uma ruptura no seu normal funcionamento pode dar origem a graves perturbações sociais e levar até à perda de vidas humanas. Embora a tecnologia hoje existente nos facilite a vida em inúmeros

aspectos, é inquestionável que também nos expõe a um sem número de riscos e ameaças. Isto é, embora a tecnologia nos proteja de algumas ameaças, é imprescindível que seja posta ao serviço da protecção das infraestruturas das quais depende toda a nossa sociedade. À medida que caminhamos para um mundo cada vez mais dependente do todo o tipo de dispositivos electrónicos, é necessários termos todos a consciência do impacto potencialmente catastrófico que um pequeno erro pode ter na população de todo um país.

O crescente número de incidentes relacionados com ataques informáticos contra as IC atesta da sua relevância, enquanto alvos preferenciais para um potencial inimigo do Estado. Embora se continue a considerar que apenas os estados terão capacidade para desenvolver verdadeiras armas cibernéticas, a realidade não é assim tão simples. Tudo era mais evidente quando a guerra era feita apenas com viaturas blindadas, navios e aviões, e a comparação do potencial de combate era um exercício essencialmente aritmético. No ciberespaço tudo é diferente, e tentar aferir as capacidades cibernéticas de um inimigo pode ser apenas um exercício de pura futilidade.

Embora seja do conhecimento público que algumas grandes potências estão a desenvolver capacidades nesta área, as ameaças proveniente de pequenos estados e de grupos terroristas são impossíveis de avaliar com o mínimo grau de rigor. Na realidade, o problema passa, em grande parte, pelo carácter intelectual deste poder. As grandes potências podem investir imensos recursos em pesquisa e desenvolvimento, mas a uma pequena potência basta dispor de um génio talentoso para ser uma ameaça a considerar seriamente. Ou seja, contrariamente ao que ocorria com os meios tradicionais, no ciberespaço, mais recursos não se traduzem necessariamente em mais poder. Isto significa que a aritmética perde o seu valor neste novo contexto. Uma grande potência pode ter ao seu serviço um batalhão de *hackers* talentosos, mas a um grupo terrorista pode bastar ter apenas um *hacker* genial, mais interessado em ganhar dinheiro do que em contribuir para o bem-estar comum, para fazer pender o balanço de poder no ciberespaço para o lado supostamente mais fraco.

Esta situação de assimetria de poder, conjugada com a situação de crescente interdependência de todos os sistemas e tendo por pano de fundo a incerteza acerca da origem das ameaças, leva a que seja impossível avaliar com rigor o risco associado a uma ocorrência catastrófica envolvendo uma IC. No entanto, parece-nos seguro afirmar que a intrincada rede de relações de dependência existentes na sociedade moderna aumenta exponencialmente a superfície de ataque disponível, fragilizando diversos sectores de actividade. Consequentemente, o impacto previsível de uma ocorrência catastrófica numa IC também aumenta, como consequência lógica da rede de interdependências em que todas as IC estão hoje integradas. Ou seja, a tendência para um aumento das vulnerabilidades, acompanhada pela dependência tecnológica e agravada pela incerteza acerca da real dimensão das interdependências, contribuem, simultaneamente, para uma expansão da superfície de ataque e para um aumento no possível impacto de um ataque, logo para um aumento do risco social. Ou, dito de outra forma, o aumento das vulnerabilidades expande a superfície de ataque, a rede de interdependências aumenta o potencial impacto e a dependência tecnológica amplifica o risco social.

O mundo moderno valoriza a interligação em detrimento da segurança o que dificulta imenso a tarefa de todos quantos tentam desenvolver novas abordagens à cibersegurança. Todas as organizações, governamentais ou privadas, que procurem enfrentar estes problemas terão que encontrar novas formas de partilhar informação sensível acerca de ameaças e vulnerabilidades, envolvendo todas as partes interessadas num esforço colectivo com vista à protecção das IC. É necessário que as organizações sejam adaptáveis e capazes de acompanhar o ritmo da mudança, ajustando em permanência as suas metodologias de avaliação do risco, tentando minimizar a dependência da cadeia de abastecimentos.

Há ainda que estabelecer uma clara hierarquia de prioridades, concentrando os investimentos onde eles são mais necessários e orientando esse esforço para sectores onde as dependências garantem algum tipo de redundância. Os desafios são complexos e até agora muitos esforços têm sido toldados pela inércia burocrática inerente a um mundo dominado por interesses que nem sempre estão em linha com os do bem-estar geral. Mas a protecção das IC tem que ser assumida como um verdadeiro desígnio nacional, para o qual devem contribuir todas as entidades privadas em parceria com os governos e organizações internacionais que lidam com ciberameaças.

Idealmente, seria desejável a criação de uma instituição nacional para a protecção das IC, que envolvesse os vários sectores estratégicos. No entanto, a criação desta estrutura dedicada exclusivamente às IC não é condição *sine qua non* para a condução de um programa de protecção eficaz. Seja qual for a instituição responsável, a ANPC ou outra, o verdadeiro problema passará sempre pela sensibilização dos responsáveis políticos e pela atribuição de recursos humanos e materiais a esta tarefa, que requere um trabalho permanente de monitorização e actualização, além da colaboração com Espanha e com as instâncias europeias responsáveis nesta área. Além disso, a protecção das IC portuguesas tem também que ser uma responsabilidade partilhada entre o sector público, o sector privado e os cidadãos, tanto para reduzir ameaças e riscos como para minimizar prejuízos. Assim, caberá ao Estado incentivar o sector privado a adoptar medidas adequadas à protecção das suas IC através de regulamentação adequada, da criação de parcerias que potenciem eventuais sinergias, e do apoio ao desenvolvimento de programas sectoriais, e até mesmo empresariais, de proteção de IC.

Bibliografia

Baker, S., Waterman, S., & Ivanov, G. (2009). *In the Crossfire: Critical infrastructure in the Age of Cyber War*. McAfee, Incorporated.

Beggs, P. (2010). Securing the Nation’s Critical Cyber Infrastructure. *California Information Security Office Meeeting*. Department of Homeland Security.

BMI. (2009). *National Strategy for Critical Infraestructure Protection*. Bundesministerium des Innern.

Brown, J. (2011). Exploiting SCADA Systems. *Swiss Cyber Storm 3*. University of Applied Science Rapperswil.

Brunner, E. M., & Suter, M. (2008). *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*. Center for Security Studies, ETH Zurich.

Chertoff, M. (2009). National Infrastructure Protection Plan. *Department of Homeland Security*.

Chiesa, R. (2007). SCADA (in)Security: Hacking Critical Infrastructures. *24th Chaos Communication Congress*.

Chiesa, R. (2010). SCADA Security: From physical security to cyberwarfare. *Security Canada Expo*.

Clarke, R. A., & Olcott, J. (2012). *Confronting Cyber Risk in Critical Infrastructure: The National and Economic Benefits of Security Development Processes*. Good Harbor Consulting.

Clemente, D. (2013). *Cyber Security and Global Interdependence: What is Critical?.* Chatham House.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2011). *Cyber Security and the UK's Critical National Infrastructure*. Chatham House.

CPNI. (2012). *Process Control and SCADA Security: Guide 1 – Understand the Business Risk*. Centre for the Protection of National Infrastructure.

DHS. (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Department of Homeland Security.

DHS. (2011). *Common Cybersecurity Vulnerabilities in Industrial Control Systems*. Department of Homeland Security.

DHS. (2012). *Office of Infrastructure Protection Strategic Plan: 2012–2016*. Department of Homeland Security.

ENISA. (2011). *Protecting Industrial Control Systems – Recommendations for Europe and Member States*. European Network and Information Security Agency.

GAO. (2004). *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*. U.S. General Accounting Office.

GAO. (2012). *Cybersecurity: Challenges in Securing the Electricity Grid*. U.S. Government Accountability Office.

GAO. (2013). *Cybersecurity: A Better Defined and Implemented National Strategy Is*

Needed to Address Persistent Challenges. U.S. Government Accountability Office.

Gibson, W. (1984). *Neuromancer*. Ace Science Fiction Books.

GIT. (2013). *Emerging Cyber Threats Report 2013*. Georgia Institute of Technology.

Hämmerli, B., & Renda, A. (2010). *Protecting Critical Infrastructure in the EU*. Centre for European Policy Studies.

ICS-CERT. (2012). *Incident Response Summary Report 2009 – 2011*. Industrial Control Systems Cyber Emergency Response Team, Department of Homeland Security.

ICS-CERT. (2013a). *Year in Review – 2012*. Industrial Control Systems Cyber Emergency Response Team, Department of Homeland Security.

ICS-CERT. (2013b). *ICS-CERT Monitor*. Industrial Control Systems Cyber Emergency Response Team, Department of Homeland Security.

ITSEAG. (2012). *Generic SCADA Risk Management Framework for Australian Critical Infrastructure*. IT Security Expert Advisory Group.

Jornal Oficial da União Europeia. (2008). (Vol. L 345/77). CE. Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:PT:PDF

Kelly, T. K. (2001). Infrastructure Interdependencies. *A Workshop on Electricity Security and Survivability*. Carnegie Mellon University.

Knapp, E. D. (2011). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Elsevier Science.

KRITIS, B. (2004). *Critical Infrastructure Protection: Survey of World-Wide Activities*. Bundesamt für Sicherheit in der Informationstechnik.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), (pp. 24–42). Potomac Books, Inc.

Lévy, P. (1999). *Collective Intelligence: Mankind's Emerging World in Cyberspace*. Helix books. Perseus Books.

Luallen, M. E. (2013). *SCADA and Process Control Security Survey*. SANS.

Lukszo, Z., Deconinck, G., & Weijnen, M. P. C. (Eds.). (2010). *Securing Electricity Supply in the Cyber Age*. Topics in Safety, Risk, Reliability and Quality, 15. Springer.

McAfee. (2011). *Global Energy Cyberattacks: "Night Dragon*. McAfee Foundstone.

NCS. (2004). *Supervisory Control and Data Acquisition (SCADA) Systems*. National Communications System.

NERC. (2010). High-Impact, Low-Frequency Event Risk to the North American Bulk Power System. *A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the US Department of Energy's November 2009 Workshop*.

PC-CIP. (1997). *Critical Foundations: Protecting America's Infrastructures*. President's Commission on Critical Infrastructure Protection.

Pederson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of US and International Research*. Idaho National Laboratory.

Pollet, J. (2012). Hacking SCADA Systems – 2011 Year in Review. *Hacker Halted*. EC-Council.

Shea, D. A. (2003). *Critical infrastructure: Control Systems and the Terrorist Threat*. Congressional Research Service.

SPB. (1995, December). White Paper on Information Infrastructure Assurance. Security Policy Board.

Stouffer, K., Falco, J., & Kent, K. (2008). *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*. National Institute of Standards and Technology.

Tabansky, L. (2011). Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs*, *3*.

Whittaker, J. (2004). *The Cyberspace Handbook*. Media Practice. Taylor & Francis Group.

Wilson, C. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service.

---

[1] *Critical Infrastructures and Key Resources (CIKR).*

[2] *Industrial Control Systems* (ICS). De modo a tornar o texto mais perceptível, iremos doravante utilizar as siglas inglesas vulgarmente utilizadas na literatura de referência sobre esta temática.

[3] *Supervisory Control And Data Acquisition.*

[4] *Distributed Control Systems (DCS).*

[5] *Process Control Systems (PCS).*

[6] *Remote Terminal Units (RTU).*

[7] *Programmable Logic Controllers (PLC).*

[8] *Wide Area Network*. O conceito associado a esta sigla é o de uma rede que cobre uma vasta área geográfica, com ligações que muitas vezes vão além das fronteiras nacionais.

[9] *Local Area Network*. Estas são as redes locais que ligam computadores em casa, numa escola ou num escritório.

[10] Meserve, Jeanne, *Staged cyber attack reveals vulnerability in power grid*, Central News Network, 26 de Setembro de 2007, disponível em http://edition.cnn.com/2007/US/09/26/power.at.risk/, consultado em 6 de Junho de 2013.

[11] *Commercial Off The Shelf*. É uma designação para o *software* comercial disponível para o público em geral.

[12] BYOD é uma sigla inglesa para *Bring Your Own Device* (Traga o Seu Próprio Dispositivo). Este fenómeno está directamente relacionado com o surgimento de um número cada vez maior de dispositivos de computação móvel bastante avançados. O BYOD implica que os funcionários possam utilizar os seus próprios dispositivos pessoais (*smartphones*, *tablets* ou *laptops*) no ambiente laboral e com eles possam aceder aos recursos da rede da empresa.

[13] Um *worm* (verme) informático é um programa malicioso que se replica a si próprio de forma a expandir-se para outros sistemas, normalmente através de redes informáticas. Distingue-se dos vírus informáticos na medida em que não necessita "infectar" um outro programa para se multiplicar, sendo completamente independente.

[14] O Stuxnet é um *worm* concebido especificamente para atingir as unidades de enriquecimento de urânio do Irão, em Natanz. O *worm* é incomum visto que, apesar de se propagar através de computadores com sistema operativo Windows, a sua carga útil é direccionada apenas para uma configuração específica de sistemas SCADA, ou seja, exactamente aquilo que o Irão tem nas suas centrifugadoras. Na altura da sua descoberta, o Stuxnet foi considerado o mais avançado malware já estudado e aumentou significativamente o nível da ciberguerra. Actualmente, já é claro que se tratou de um ataque cibernético real sobre as instalações nucleares do Irão com a maioria dos especialistas a acreditar que Israel está por trás disso, com a ajuda dos EUA. O Stuxnet é a primeira arma cibernética de nível militar do mundo conhecida publicamente, capaz de destruir máquinas, e o ataque retardou significativamente o programa iraniano de enriquecimento de urânio ao danificar cerca de 1.000 centrifugadoras.

[15] Gertz, Bill, *The Cyber-Dam Breaks*, The Washington Free Beacon, 1 de Maio de 2013, disponível em http://freebeacon.com/the-cyber-dam-breaks/, consultado em 6 de Maio de 2013.

[16] Estes servidores (*root name servers*) são uma parte crítica da infraestrutura da internet, porque são a base da tradução dos endereços em linguagem humana para endereços IP que são utilizados na comunicação entre máquinas na rede. Embora só existam treze servidores lógicos, desde Junho de 2013, por motivos de redundância, existem 374 servidores físicos dispersos por diversos países.

[17] *Internet Service Providers.* É o nome vulgarmente dado às companhias que disponibilizam acesso à internet.

[18] *High-Impact Low-Frequency (HILF).*

[19] The White House, Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), disponível em: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, consultado em 16 de Julho de 2013.

[20] The White House, Executive Order No. 13636, 78 Fed. Reg. 11737 (Feb. 12, 2013), disponível em: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, consultado em 16 de Julho de 2013.