ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO E A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS:

Contributos para um Modelo Nacional de Análise e Gestão do Risco Social

Rui Manuel Piteira Natário

Dissertação para a obtenção do grau de

Mestre em Guerra de Informação

Lisboa

2014

ACADEMIA MILITAR

DIRECÇÃO DE ENSINO

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO E A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS:

Contributos para um Modelo Nacional de Análise e Gestão do Risco Social

Rui Manuel Piteira Natário

Dissertação de Mestrado em Guerra de Informação

Trabalho realizado sob a supervisão:

TCor TM (Doutor) Paulo Fernando Viegas Nunes

Lisboa

2014

AGRADECIMENTOS

As primeiras palavras de agradecimento são para o meu orientador, Tenente-Coronel de Transmissões Doutor Paulo Viegas Nunes, pelas suas sugestões, apoio e partilha do saber. Todo o seu esforço de orientação foi no sentido de me motivar para manter o rigor científico e me aproximar da excelência académica. Caso eu não o tenha conseguido, não será certamente por responsabilidade sua.

Uma palavra de agradecimento também para a Dr.ª Isabel Pais, da Autoridade Nacional de Protecção Civil, pela extrema simpatia e pela disponibilidade demonstrada na partilha dos seus trabalhos nesta área de estudo.

Uma última palavra para a minha família, e para todos aqueles que de mais perto convivem comigo, pela paciência e pelo incentivo.

RESUMO

As infraestruturas críticas suportam todos os aspectos do nosso quotidiano. São os alicerces da nossa civilização e a vanguarda do nosso futuro. Elas permitem a existência de cada elemento da nossa sociedade e não há maior prioridade que garantir a sua segurança, preservando a sua integridade e garantindo a continuidade do seu funcionamento. Os Estados estão hoje tão dependentes das suas infraestruturas críticas que a sua protecção se tornou um assunto de segurança nacional, e as suas vulnerabilidades uma matéria discutida ao mais alto nível. As infraestruturas críticas são actualmente uma mescla de sistemas, uma verdadeira rede de redes, com retalhos de tecnologia moderna e obsoleta, combinados numa paisagem fragmentada pela partilha entre a propriedade pública e privada. A rápida banalização da Internet e a integração das telecomunicações e dos computadores, ligaram as infraestruturas críticas entre si e criaram uma intrincada e vulnerável rede de interdependências que está exposta a um grande número de ameaças, internas e externas. Assim, apesar de isoladas fisicamente, as infraestruturas críticas estão sujeitas aos potenciais efeitos em cascata resultantes da falha em apenas uma delas. Os sistemas de controlo industrial são extremamente vulneráveis a ataques vindos do ciberespaço e este facto foi já demostrado por diversas vezes numa série de incidentes que causaram grande impacto tanto em várias infraestruturas críticas como na sociedade que delas depende. Esta vulnerabilidade é a génese de um crescente risco social que ameaça a segurança dos próprios Estados. A identificação e gestão dos riscos associados a estas infraestruturas é hoje uma área de estudo de grande importância para assegurar um futuro mais seguro, minimizando o impacto das múltiplas ameaças que pendem sobre o conjunto de instalações industriais e serviços que estão na base do modo de vida das sociedades modernas. Neste sentido, as melhores práticas a nível internacional apontam para a adopção de uma abordagem holística dos riscos e para um aumento da resiliência a todos os possíveis cenários de catástrofe natural ou ataque intencional. Além disso, generalizou-se a adopção de procedimentos apoiados em normas internacionais que sendo de aplicação genérica podem facilmente ser adaptadas às especificidades nacionais de cada Estado. O caminho a seguir por Portugal deve ser este; adoptar as melhores práticas a nível internacional, ajustando-as à realidade nacional.

Palavras-chave: infraestruturas críticas, vulnerabilidades, ciberespaço, ameaças, impacto, segurança nacional, risco social.

ABSTRACT

Critical infrastructures support every aspect of our daily lives. They are the foundations of our civilization and the frontline of our future by allowing the existence of each element of our society. There is no higher priority than ensuring their safety, preserving their integrity and ensuring the continuity of their operations. States are now so dependent on their critical infrastructures that protecting them has become a national security issue, and their vulnerabilities a matter discussed at the highest level. Critical infrastructures are currently a mix of systems, a true network of networks, with scraps of modern and obsolete technology, combined in a fragmented landscape, due to a split between public and private property. The trivialization of the Internet along with the rapid integration of telecommunications and computers, brought critical infrastructures together and created an intricate and vulnerable mesh of interdependencies which is exposed to a large number of threats, both internal and external. Thus, although physically isolated, critical infrastructures are subject to potential cascading effects resulting from the failure of just one of them. Industrial control systems are extremely vulnerable to attacks from cyberspace and this fact has been repeatedly demonstrated in a series of incidents that caused major impact on several critical infrastructures, and on the communities depending on them. This vulnerability is at the genesis of a growing social risk that threatens the States' security itself. Identifying and managing risks associated with these infrastructures is nowadays an area of study of great significance to ensure a safer future, minimizing the impact of multiple threats that hang over the set of industrial facilities sustaining the basis of our way of life. In this sense, the best international practices point to the adoption of an all hazards approach to risk and increased resilience to all possible scenarios of natural disaster or deliberate attack. Furthermore, the widespread adoption of procedures supported by international standards, being generic in its application, can be easily adapted to each State national specificities. This should be the way forward for Portugal; adopt the best international practices, adjusting them to the national reality.

Key-Words: critical infrastructures, vulnerabilities, cyberspace, threats, impact, national security, social risks.

LISTA DE ABREVIATURAS

ANPC – Autoridade Nacional de Protecção Civil

BYOD – Bring Your Own Device

CE – Comissão Europeia

CIKR – Critical Infrastructures and Key Resources

CNPCE - Conselho Nacional de Planeamento Civil de Emergência

COTS – Commercial Off-The-Shelf

DCS – Distributed Control Systems

DHS – Department of Homeland Security

DNS – Domain Name System

EUA – Estados Unidos da América

HILF – High-Impact Low-Frequency

HMI – Human Machine Interface

IC – Infraestruturas Críticas

ICS – Industrial Control Systems

IED – Intelligent Electronic Device

IIC - Infraestrutura Informacional Crítica

ISP – Internet Service Provider

LAN – Local Area Network

MTU – Master Terminal Unit

NADB – National Asset Database

OCDE – Organização para a Cooperação e Desenvolvimento Económico

PCS – Process Control Systems

PEPIC – Plano Europeu de Protecção de Infraestruturas Críticas

PIC – Protecção de Infraestruturas Críticas

PLC – Programmable Logic Controller

PMTL - Protected Measures Target List

PNPIC – Plano Nacional de Protecção de Infraestruturas Críticas

RTU – Remote Terminal Unit

SAC – Sistemas Adaptativos Complexos

SCADA – Supervisory Control And Data Acquisition

TCP/IP - Transmission Control Protocol/Internet Protocol

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

WAN – Wide Area Network

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

INTRODUÇÃO

O interesse em redor das Infraestruturas Críticas (IC) é motivado pelo facto de estas estarem na base do funcionamento da nossa sociedade e serem vulneráveis, tanto ao nível da sua actividade estrutural, como ao nível das interdependências entre si. Além disso, a evolução tecnológica levou ao crescimento das vulnerabilidades cibernéticas pois estas infraestruturas, de forma geral, funcionam apoiadas em sistemas informáticos de diversos tipos. A nível físico e estrutural, estas infraestruturas estão expostas a várias ameaças e podem ser danificadas por incúria, por actos deliberados, ou por fenómenos naturais. Simultaneamente, 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 IC críticas que eles suportam pois estas estão agora expostas a um número crescente de ameaças cibernéticas. 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. 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 originar avultadas perdas económicas, graves perturbações sociais, e levar até à perda de vidas humanas.

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 das infraestruturas 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, avaliação dos impactos e a gestão dos riscos associados, são áreas da maior importância estratégica. 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. 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.

A presente dissertação encontra-se dividida em dez capítulos, que reflectem a abordagem aplicada no estudo. No primeiro capítulo apresenta-se a metodologia de investigação seguida, referindo as principais fontes bibliográficas de suporte da dissertação, e são identificados os objectivos a atingir com o trabalho desenvolvido. É formulada a questão central e as consequentes questões derivadas, de forma a orientar o trabalho de investigação, e levantam-se as hipóteses a ser verificadas. Por último, apresentam-se os conceitos basilares de suporte a todo o trabalho subsequente.

Seguidamente, no segundo capítulo, são elencadas as características comuns a todas as IC, é analisada a evolução dos critérios para a sua identificação, e é introduzido o conceito de Infraestrutura Informacional Crítica (IIC). No terceiro capítulo, estudam-se os sistemas de controlo industrial, com particular destaque para os sistemas de supervisão e aquisição de dados pois estes estão, de alguma forma, presentes na maioria das IC. No quarto capítulo, são analisadas as vulnerabilidades das IC, com especial atenção sobre as vulnerabilidades dos sistemas de controlo industrial dada a sua relevância para a problemática em apreço.

A eventual exploração destas vulnerabilidades é abordada no quinto capítulo, onde se estudam os diversos tipos de ameaças, o seu potencial impacto sobre as IC e a consequente relevância social que resulta desta realidade. O sexto capítulo aborda o risco social que decorre da exploração das vulnerabilidades das IC. Neste capítulo, são analisadas várias definições de risco, metodologias para a sua gestão e são citados alguns exemplos da utilização de normas a nível internacional. Nesta sequência, o sétimo capítulo trata da Protecção de Infraestruturas Críticas (PIC), analisando diferentes definições deste conceito e estudando diferentes abordagens à PIC a nível internacional. O oitavo capítulo traça um panorama geral da situação em Portugal, enquadrando-a no contexto europeu, analisando as

diversas fases da evolução da PIC a nível nacional, e dando uma panorâmica geral sobre as IC existentes no nosso país.

No nono capítulo, sintetizam-se os assuntos abordados mais relevantes, responde-se à questão central, propondo uma série de contributos para o Plano Nacional de Protecção de Infraestruturas Críticas (PNPIC), e identificam-se alguns dos desafios a enfrentar para a implementação deste Plano. No final do trabalho, o décimo capítulo apresenta as conclusões alcançadas e deixa mais algumas ideias para uma possível orientação a seguir por Portugal na salvaguarda das suas infraestruturas críticas.

1. METODOLOGIA DA INVESTIGAÇÃO

Esta dissertação foi elaborada com recurso à consulta de bibliografia nacional e estrangeira sobre o assunto, disponível em fontes abertas acessíveis através da Internet, mas também proveniente de artigos científicos e monografias. A metodologia seguida foi, proceder a uma revisão de literatura incidindo sobre os diversos estudos conduzidos a nível internacional sobre esta temática, bem como sobre as orientações estratégicas seguidas por alguns países. Sendo um trabalho que se debruça sobre conceitos e noções subjectivas, numa primeira fase foi feita uma recolha de informação com vista à sistematização das definições que estão na base de todo o estudo. Ou seja, o estudo seguiu uma metodologia baseada na sistematização de conceitos, pois esta é uma área onde há uma enorme variedade de definições e interpretações díspares entre si. Além disso, recorrendo a contributos do mundo empresarial, produzidos por especialistas em segurança de IC, foram identificadas as principais vulnerabilidades das IC e as maiores ameaças que estas enfrentam.

Com base nesta informação, numa retrospectiva de alguns incidentes relacionados com IC e ainda numa breve análise de dados estatísticos, deduziu-se a relevância social do tema da dissertação. Seguiu-se uma análise a diversas posturas relativamente à gestão do risco existentes em diferentes países. As fontes bibliográficas foram constituídas por estudos de carácter técnico, oriundos do meio académico e da indústria, por trabalhos de âmbito estratégico, produzidos por diversas entidades governamentais em vários países, e ainda por análises efectuadas por organismos independentes. Considerámos também os estudos comparativos levados a cabo por diversas entidades independentes, com o intuito de sintetizar as melhores práticas e compilar as recomendações mais relevantes a nível internacional. Assim, a abordagem metodológica seguida foi fundamentalmente interpretativa, baseada essencialmente na análise documental. Este trabalho serviu como base de referência para atingir o objectivo principal de chegar a conclusões que possibilitassem responder à questão central, contribuindo assim para uma abordagem mais objectiva e pragmática à situação da PIC nacional.

1.1 Objectivos da Investigação

O objecto do estudo será a análise da vulnerabilidade das IC, a sua exposição a ameaças provenientes da sua ligação ao ciberespaço, e a análise e gestão do risco associado à PIC. Nomeadamente, pretendeu-se analisar diversos modelos de PIC existentes em diferentes países que serviram como base de referência para uma abordagem mais objectiva e pragmática à situação nacional. Foram tidos em consideração os estudos realizados por diversas entidades independentes, de modo a sintetizar as melhores práticas e compilar as recomendações mais relevantes a nível internacional. Assim, os objectivos da dissertação foram:

- Caracterizar as Infraestruturas Críticas e as suas vulnerabilidades;
- Avaliar o estado da arte através do estudo comparativo de diferentes modelos e abordagens para a protecção de IC a nível internacional;
- Analisar e avaliar o risco social no ciberespaço;
- Elencar possíveis contributos para a elaboração de um Plano Nacional de Protecção de Infraestruturas Críticas.

Pretendeu-se fazer uma análise comparativa, não só das estratégias relativamente à PIC, mas também à própria metodologia de análise e gestão de risco associada a estas estratégias. A síntese das diferentes abordagens a nível mundial foi o ponto de partida para uma proposta estruturada com base nas melhores práticas e adequada à realidade portuguesa. Tudo isto com o objectivo último de elencar alguns contributos para a elaboração de um Plano Nacional de Protecção de Infraestruturas Críticas (PNPIC).

De salientar que o presente estudo, embora focando ameaças internas e externas ao Estado, não se debruça sobre os riscos associados a ameaças acidentais, provocadas por catástrofes naturais. O foco deste trabalho é contribuir para a definição de um modelo de análise e gestão de risco social no ciberespaço capaz de apoiar o desenvolvimento de um Plano de Protecção de Infraestruturas Críticas para Portugal, atendendo às vulnerabilidades tecnológicas das IC, e à dependência da sociedade relativamente ao ciberespaço e ao seu correcto funcionamento.

1.2 Formulação do Problema

Este trabalho segue uma abordagem em que as ameaças existentes, intencionais ou não, potencializadas através das possibilidades oferecidas pelas novas tecnologias, exploram as vulnerabilidades existentes nas IC e geram assim riscos sociais. A concepção de um PNPIC assenta num esforço de coordenação entre as entidades governamentais e o sector privado, culminando num modelo de gestão de risco social do Estado, em permanente actualização por meio de um ciclo contínuo de análise e gestão do risco. Assim, a questão central da minha dissertação foi:

Atendendo às vulnerabilidades tecnológicas das IC, e à dependência da sociedade relativamente ao ciberespaço e ao seu correcto funcionamento, será possível definir um modelo de análise e gestão de risco social no ciberespaço capaz de apoiar o desenvolvimento de um Plano de Protecção de Infraestruturas Críticas para Portugal?

Consequentemente, surgiram diversas questões derivadas que se elencam em seguida:

1. Como se caracterizam as infraestruturas críticas e os seus sistemas de controlo?
2. Quais as vulnerabilidades destes sistemas e as ameaças cibernéticas que as podem explorar?
3. É possível proteger as infraestruturas críticas contra ataques cibernéticos?
4. Quais as medidas de protecção adequadas às infraestruturas críticas?
5. Qual a melhor metodologia para a análise e gestão do risco?
6. No âmbito da protecção de infraestruturas críticas, quais as melhores práticas a nível internacional e como podem ser aplicadas à realidade portuguesa?

Utilizando as questões anteriormente elencadas como estruturação do trabalho a desenvolver, levantaram-se as seguintes hipóteses de investigação:

1. As infraestruturas críticas e os sistemas de controlo industrial são extremamente vulneráveis e estão expostos a um número crescente de ameaças cibernéticas;
2. Não é possível proteger completamente todas as infraestruturas críticas e a criação de um processo contínuo de análise e gestão do risco é a única solução para mitigar o impacto das ameaças sobre as IC;

3. A criação de um Plano de Protecção de Infraestruturas Críticas tem que se apoiar num modelo de análise e gestão de risco e nas melhores práticas internacionais para permitir uma protecção eficaz das IC;
4. Uma estratégia nacional de protecção de infraestruturas críticas deve apoiar-se na síntese das melhores práticas internacionais, adaptando-as às necessidades específicas de Portugal.

Assim, após a formulação da questão central, efectuou-se uma revisão de literatura, tendo em vista conhecer o estado da arte nesta temática. Posteriormente, foram definidas as questões derivadas e as hipóteses a verificar.

1.3 Limitações e Dificuldades

Uma vez que muitos países tratam a PIC como uma questão de segurança nacional, nem sempre é disponibilizada publicamente informação relevante sobre o assunto, particularmente traduzida para inglês e disponível através de fontes abertas como a Internet. Contudo, no mundo ocidental, existe uma grande quantidade de literatura sobre esta temática, tanto sobre as políticas oficiais dos Estados como sobre as melhores práticas aconselhadas em diversas áreas de actividade industrial e económica. Todavia, muitos governos digladiam-se com os operadores privados numa tentativa de delimitar as áreas de responsabilidade pela protecção destas infraestruturas, o que tornou algo confusa a recolha de informação pois são muitas as perspectivas em presença, e todas elas muitas distintas entre si.

Assim, a definição e caracterização das IC foi feita com base em documentos produzidos por organismos oficiais de diversos Estados, sem esquecer os trabalhos apresentados por investigadores do mundo académico nem outros realizados por entidades independentes ou ligadas à indústria. Este foi o ponto de partida para uma retrospectiva de alguns incidentes relacionados com IC e para a análise de dados estatísticos relativos a estas ocorrências no decurso dos últimos anos. Mas é do conhecimento público que muitas organizações não divulgam a realidade das suas vulnerabilidades, nem dos incidentes que sofrem, devido a questões de concorrência comercial, ou mesmo de segurança nacional. Assim, os estudos comparativos realizados por entidades ligadas a determinados Estados assumem particular relevo pois reúnem muita informação que, de outra forma, não está imediatamente disponível ao público.

1.4 Corpo de Conceitos

O funcionamento da sociedade moderna depende de uma complexa malha de infraestruturas de energia, de comunicações, transportes, alimentação e muitas outras. Mas na realidade não sabemos exactamente o que é uma "infraestrutura". No nosso léxico, em termos genéricos, a palavra "infraestrutura" está associada à noção de conjunto de elementos estruturais que enquadram e suportam um determinado sistema. A palavra "infraestrutura" pode assim estar relacionada com diversos conceitos em diferentes áreas de estudo, mas o senso comum liga-a aos sistemas de saneamento, de fornecimento de energia, e viários de uma cidade ou região.

Ou seja, 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. No dicionário Priberam está definida como “conjunto de instalações, equipamento e serviços, geralmente públicos (redes de esgotos, de água, de electricidade, de gás, de telefone, etc.), que garantem o funcionamento de uma cidade” (Priberam, 2014). Na Infopédia as infraestruturas são definidas como um “conjunto de instalações ou de meios prévios necessários ao funcionamento uma actividade ou conjunto de actividades“ (Infopédia, 2014). Mas estas definições, e outras semelhantes, são vagas e sujeitas a diversas interpretações e, em termos práticos, a definição de infraestrutura depende essencialmente do contexto em que o termo é empregue.

A palavra infraestrutura surgiu no final do séc. XIX no contexto da construção ferroviária para designar a estrutura de suporte dos carris e, em meados do séc. XX, passou a ser empregue para descrever as estruturas fundamentais das modernas organizações e sociedades (Högselius, Hommels, Kaijser, & Vleuten, 2013). Desde então esta designação tem sido utilizada nos mais variados contextos, umas vezes no sentido lato, outras num âmbito mais restrito. Algumas pessoas associaram o conceito de infraestrutura ao que hoje se designa por “indústrias em rede”, responsáveis pelo fornecimento dos meios de transporte, energia, comunicação e água. Outras definições expandiram o conceito para englobar todo o tipo de estruturas básicas, incluindo educação, serviços financeiros e de saúde.

Assim, um dos obstáculos básicos a ultrapassar é o de harmonizar diferentes conceitos relacionados com o termo "infraestrutura". Para os engenheiros civis, por exemplo, as infraestruturas são os elementos construídos, como as condutas e as pontes, descritos em termos de materiais e características de concepção que condicionam as suas reacções a forças físicas. Já para os economistas, uma infraestrutura representa uma entrada para a produção económica, medida em dinheiro e frequentemente quantificada a nível nacional (Chang, 2009). Como iremos ver, estas diferenças fundamentais reflectem diferentes formas de conceptualizar, e até de avaliar, as infraestruturas.

No contexto da PIC, os Estados Unidos da América (EUA), pioneiros na área, definiram em 1997 infraestruturas como sendo "o conjunto de sistemas e redes interdependentes compreendendo indústrias identificáveis, instituições (incluindo pessoas e procedimentos) e capacidades de distribuição que fornecem um fluxo fiável de produtos e serviços essenciais para a defesa e segurança económica dos EUA e para o funcionamento normal do governo a todos os níveis e da sociedade como um todo" (Marsh, 1997). Esta definição, engloba já aquilo que mais tarde foi sistematizado na perspectiva da existência de três níveis de análise das infraestruturas (Bouchon, 2006):

1. A abordagem técnica e de engenharia centra-se nos elementos materiais básicos de uma infraestrutura, requerendo elevados custos públicos ou investimentos privados;
2. A abordagem regulatória analisa a "infoestrutura" dos procedimentos e regras que permitem o bom funcionamento da infraestrutura;
3. Avaliações qualitativas, ou quantitativas, podem ser efectuadas com foco na eficiência dos serviços prestado pela infraestrutura, baseados na existência de fornecedores, utilizadores, fluxo de bens, de pessoas, e de informação.

Este último conceito de "serviços da infraestrutura" é fundamental para estabelecer a ligação entre danos físicos e o impacto social das infraestruturas. Esta noção, que se distingue dos conceitos tradicionais de infraestrutura dos engenheiros e dos economistas, representa um meio-termo que os liga (Chang, 2009).

Num relatório realizado pela Organização de Cooperação e Desenvolvimento Económico (OCDE), concluiu-se que, no contexto das definições oficiais de IC dos países estudados, as definições de "infraestrutura" utilizadas eram genéricas mas todas se referiam a

infraestruturas físicas e a maioria referia também activos intangíveis e redes de comunicações (Gordon & Dion, 2008). Definições mais recentes de IC enfatizam a estrutura subjacente que suporta a sociedade e incluem termos relacionados como "redes" ou "grandes sistemas técnicos" que têm também uma conotação de ligação e integração fundamental para as sociedades modernas (Högselius et al., 2013).

Existem outras definições de infraestrutura mas, de um modo geral, todas elas assentam nos três pressupostos já elencados e que se podem resumir dizendo que uma infraestrutura é a base subjacente de qualquer organização ou sistema e que se pode referir tanto a estrutura física como a redes imateriais, tal como se pode ver na seguinte figura:

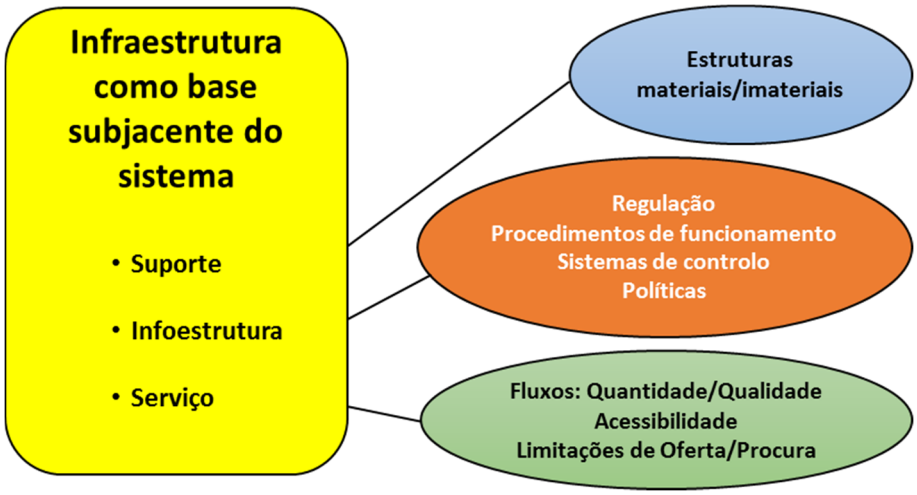


Figura 1 - Os três níveis de análise das infraestruturas. Adaptado de (Bouchon, 2006).

Esta discussão conceptual é de extrema importância pois a ambivalência dos conceitos para as diferentes "partes interessadas"[1] tem sido determinante para a evolução histórica da PIC. Aliás, é a principal razão pela qual os *stakeholders* sistematicamente discordam acerca das interpretações apropriadas e sobre as respostas governamentais adequadas para as vulnerabilidades das infraestruturas (Högselius et al., 2013).

A identificação e priorização dos "activos"[2] de uma dada infraestrutura que são essenciais ao seu funcionamento, ou que representam o maior risco se ameaçados, é essencial para a definição de uma estratégia para a PIC. Todavia, tendo em conta o âmbito e a complexidade do assunto, a identificação rigorosa dos "activos críticos"[3] tem sido uma tarefa extremamente

[1] Em inglês, *stakeholders*. Iremos doravante utilizar este anglicismo pois é de uso corrente no nosso léxico.
[2] Em inglês, *assets*.
[3] Em inglês, *critical assets*.

difícil. De tal modo que, já em 1999, um organismo governamental norte-americano afirmava que muitas agências federais dos EUA, com responsabilidades na PIC, não tinham uma noção clara daquilo que constituía um activo crítico (Moteff & Parfomak, 2004).

Ou seja, no debate sobre prioridades, seleccionando o que é ou não crítico, nem sempre é possível alcançar um consenso semântico que permita uma conceptualização uniforme (Clemente, 2013). Consequentemente, os critérios para avaliar a criticidade de uma infraestrutura tendem a reflectir as preocupações políticas conjunturais e podem ser alteradas à medida que estas evoluem mas, de um modo geral, o adjectivo "crítico" está relacionado com uma função essencial da sociedade, da qual há elevada dependência e, portanto, altamente vulnerável a uma potencial disrupção na infraestrutura (Bouchon, 2006).

O já citado trabalho da OCDE (Gordon & Dion, 2008) revelou que na maior parte dos países a palavra "crítico" refere-se a uma infraestrutura que fornece um suporte essencial para o bem-estar económico e social, para a segurança pública e para o funcionamento das responsabilidades centrais do governo. Na mesma linha, um estudo comparativo conclui que, nos 25 países analisados, um componente ou toda uma infraestrutura são definidos como críticos em função da sua posição estratégica em todo o sistema de infraestruturas e especialmente devido às interdependências entre componentes ou entre a infraestrutura e outras infraestruturas (Brunner & Suter, 2008).

Contrariamente aquilo 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 "ciberespaço"[4] 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

[4] Em inglês, *cyberspace*.

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 informação proveniente de fontes digitais ou destinada à digitalização (Lévy, 1999).

Por outro lado, Daniel Kuehl, 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 infraestruturas 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 infraestruturas de suporte da sociedade.

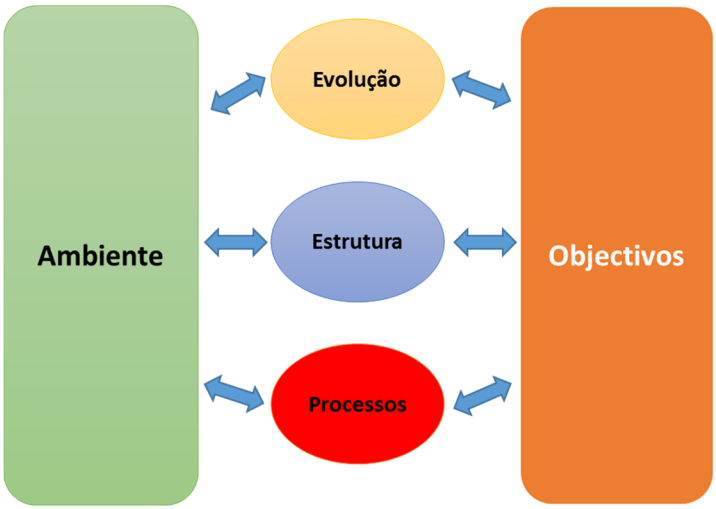


Figura 2 - O paradigma sistémico. Adaptado de (Bouchon, 2006).

A discussão das diversas conceptualizações do significado de "sistema" extravasa largamente o objectivo do presente trabalho, uma vez que quase todas as áreas de conhecimento científico têm a sua própria definição. Assim, no âmbito desta dissertação vamos utilizar uma definição que foi proposta precisamente no contexto das IC, e que tenta sumarizar as noções presentes em muitas das outras áreas. Ou seja, consideramos que um sistema é um conjunto organizado de subsistemas ou componentes e de processos interactivos que é suficientemente coerente para manter um relativo grau de autonomia (Bouchon, 2006). Isto mesmo está representado na Figura 2.

Uma relação de dependência ocorre entre duas infraestruturas quando estas partilham um acoplamento ou ligação através do qual o estado de uma infraestrutura influencia ou é correlacionado com o estado da outra e, nestes casos, a relação é habitualmente unilateral (Rinaldi, Peerenboom, & Kelly, 2001). Dito de outra forma, o termo dependência descreve como um produto ou serviço afecta outro, e no contexto das IC, as ligações são físicas e electrónicas (Gendron, 2010). Actualmente, o governo dos EUA considera que a dependência unilateral ocorre sempre que um activo, sistema, rede, ou conjunto destes, depende de uma entrada, intersecção ou outro requisito de uma outra fonte para funcionar devidamente (DHS, 2013).

As infraestruturas estão frequentemente ligadas em múltiplos pontos através de uma grande variedade de mecanismos, de tal modo que existem relação bidireccionais entre os estados de qualquer par de infraestruturas. Consequentemente, a interdependência é a relação bidireccional entre duas infraestruturas através da qual cada infraestrutura influencia ou é correlacionada com o estado da outra (Rinaldi et al., 2001). O governo norte-americano define interdependência em termos de relações de dependência mútua entre entidades (objectos, indivíduos ou grupos) na qual o grau de interdependência não tem que ser igual nos dois sentidos (DHS, 2013).

2. INFRAESTRUTURAS CRÍTICAS

A expressão “infraestruturas críticas” refere-se, em primeiro lugar a uma aceitação genérica do conceito “infraestrutura”, relacionando-o com os sistemas basilares de uma sociedade considerados nas suas dimensões física e imaterial. Consequentemente, as infraestruturas críticas carecem de uma análise multidisciplinar que abarque todos os aspectos técnicos, legais e funcionais das referidas infraestruturas. Em segundo lugar, uma situação crítica é definida relativamente à possibilidade de ser posta em causa a satisfação dos objectivos definidos pela estratégia nacional, ainda que os critérios de criticidade sejam habitualmente vagos e subjectivos. Além disso, a validade da definição é conjuntural e pode ser limitada no tempo, variando de acordo com as orientações e preocupações políticas do momento. Assim, embora se possa afirmar que todas as IC partilham determinadas características, não existe uma definição formal e universalmente aceite do conceito “infraestrutura crítica”.

2.1 Caracterização das Infraestruturas Críticas

Os critérios de classificação das IC são muito diversificados e aplicados de forma distinta em diversos países, o que leva à existência de várias abordagens para o problema. As mais generalistas e ambíguas caracterizam as IC em função de critérios subjectivos como o seu valor simbólico, enquanto outras, mais objectivas, tentam quantificar a importância que o seu funcionamento tem para a sociedade. Embora não exista uma metodologia única para a identificação e classificação das IC, na nossa opinião existem algumas características que são comuns à esmagadora maioria delas. Nomeadamente, de forma genérica, todas as IC apresentam um elevado grau de complexidade, estão ligadas entre si por diversos tipos de relações de interdependência, são críticas por variadas razões, a sua propriedade não é exclusiva dos governos ou entidades públicas e têm algum tipo de componente informática que as leva a estar ligadas ao ciberespaço.

2.1.1 Sistemas Complexos

Todas as IC têm uma propriedade em comum; são conjuntos complexos de componentes interactivos nos quais a mudança ocorre frequentemente como resultado de processos de

aprendizagem (Rinaldi et al., 2001). Isto é, são Sistemas Adaptativos Complexos[5] (SAC). Nesta perspectiva, útil para a modelação e análise, cada componente da infraestrutura constitui uma pequena parte de uma intrincada rede que forma a infraestrutura global. Outros investigadores, analisando o facto de as IC serem redes de sistemas altamente complexos, definem-nas como "sistemas sócio-técnicos" o que realça duas das suas mais importantes propriedades; o carácter técnico e a importância social (Bagheri & Ghorbani, 2008). São exactamente estas características que estão ilustradas na Figura 3, onde se pode ver como um SAC se insere no ambiente que o rodeia.

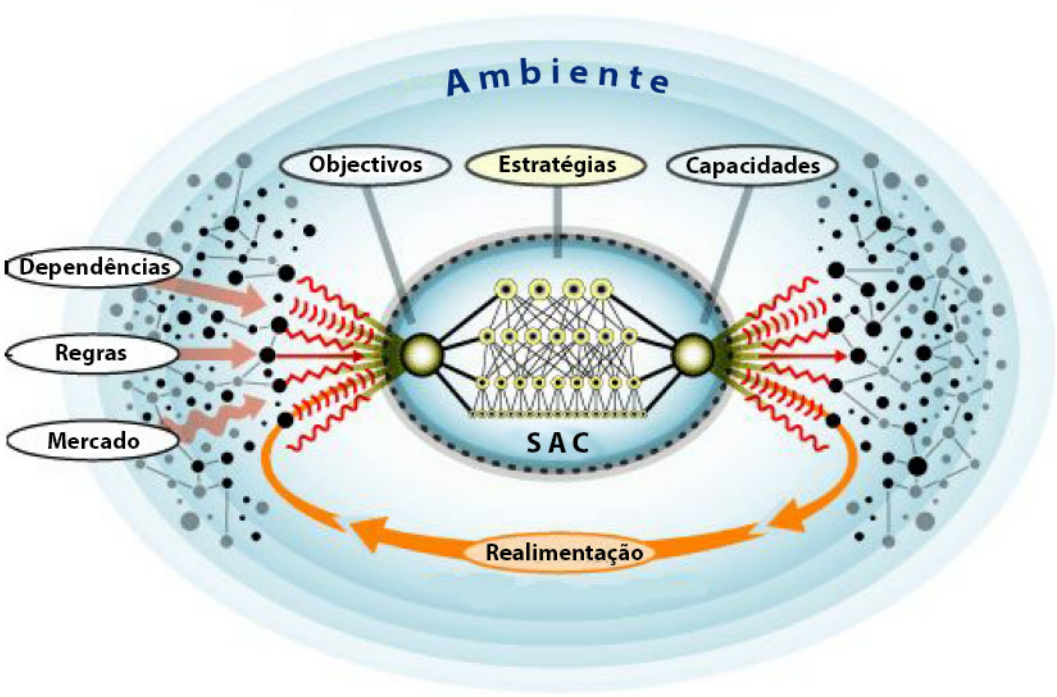


Figura 3 – As IC como Sistemas Adaptativos Complexos. Adaptado de (Bagheri & Ghorbani, 2008).

Em suma, do ponto de vista dos SAC, as infraestruturas são mais que somente a soma dos seus elementos. Tipicamente, à medida que grandes conjuntos de componentes são agregados e interagem entre si, emergem sinergias entre eles (Rinaldi et al., 2001).

2.1.2 Interdependências

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

[5] Em inglês, *Complex Adaptative Systems* (CAS).

uma cascata de outros eventos com impacto muito alargado é cada vez maior (Marsh, 1997). Vivemos assim num ambiente em que não temos apenas relações de dependência, unidireccionais, mas sim relações de interdependência, que são bidireccionais.

A interdependência entre IC pode ser de diferentes tipos, tendo, ao longo dos anos, surgido várias classificações, seguindo na sua formulação diversos critérios. Todavia, continua a existir uma aceitação quase unânime da taxonomia proposta num trabalho pioneiro sobre este assunto (Rinaldi et al., 2001) em que os autores dividem as interdependências em 4 categorias:

- Geográfica: As infraestruturas são geograficamente interdependentes se um evento ambiental local puder causar alterações no estado de todas elas, o que significa que esta interdependência resulta da proximidade geográfica entre elas.
- Física: Duas infraestruturas são fisicamente interdependentes quando o estado de uma é dependente da saída material da outra. Isto é, a interdependência física surge da ligação física entre as entradas e saídas de dois agentes; um bem produzido ou modificado (uma saída) por uma infraestrutura é necessário (como entrada) para que outra infraestrutura possa funcionar.
- 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.
- Ciber: Uma infraestrutura tem uma ciber interdependência se o seu estado depende da informação transmitida através da infraestrutura informacional, ou seja, é uma interdependência devida à transferência, entre infraestruturas, de informação essencial ao seu funcionamento quotidiano.

Numa outra perspectiva, num estudo comparativo sobre diversos modelos existente, o ***Idaho National Laboratory*** avançou com uma classificação mais alargada 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. Um resumo dos

diferentes métodos utilizados para a classificação das interdependências das IC, em função dos critérios utilizados para definir a relação entre as redes de infraestruturas, é apresentado na Tabela 1.

Tabela 1 - Taxonomia das Interdependências. Adaptado de (Ventura, García, & Martí, 2010).

Critério de Definição da Relação	Dependências
Natureza das entidades envolvidas	• Humano – Objecto • Objecto – Humano • Humano - Humano
Direcção da relação	• Unidireccional • Bidireccional
Natureza da relação (o que é partilhado)	• Informação – a ligação é um fluxo de informação • Física – Algo produzido por um elemento é consumido por outro • Geográfica – Entidades partilham a localização • Organizacional/humana/social – Políticas e procedimentos em prática nas organizações
Estado da relação	• Estática – Sem variação em caso de disrupção • Dinâmica – Comportamento varia em função das circunstâncias
Tipo de falha em caso de disrupção	• Em cascata nas entidades associadas • Progressiva • Origem comum

Entre estes 4 tipos de interdependências, as físicas e geográficas parecem ser as mais fáceis de identificar pois bastará analisar a produção, requisitos e localização de cada componente do sistema. As interdependências ciber e lógicas serão mais difíceis de identificar pois as primeiras dependem de uma compreensão dos fluxos de informação entre os sistemas de infraestruturas, e as últimas estão inerentemente dissimuladas entre as muitas relações, recursos e outras interdependências do sistema de infraestruturas (Bagheri & Ghorbani, 2008).

Deste modo, as interdependências físicas e geográficas parecem ser mais relevantes para a modelação espacial e para a simulação, enquanto as interdependências ciber e lógicas serão porventura mais importantes nos domínios operacional e financeiro. Todavia, nunca existiu consenso generalizado sobre a importância relativa destes tipos de interdependência. Em 2007, analisando a importância dos sistemas essenciais à vida, O'Rourke (2007) considerou que estes sistemas eram interdependentes essencialmente devido a factores de proximidade física e interacção operacional. Nesse mesmo ano, outros autores consideraram que a proliferação das Tecnologias de Informação e Comunicação (TIC), a crescente dependência do mercado para a aquisição de bens e serviços (por exemplo, energia eléctrica), e o aumento

dos sistemas de controlo e monitorização automática e fizeram aumentar a prevalência e importância das interdependências ciber e lógicas (Peerenboom & Fisher, 2007), o que está em completa oposição com a análise de O'Rourke.

A Figura 4 ilustra as relações de interdependência entre várias infraestruturas, caracterizadas por múltiplas ligações de diversos tipos que criam uma complexa rede, tornando impossível analisar e compreender o comportamento de uma infraestrutura isoladamente do ambiente em que se insere (Rinaldi et al., 2001).

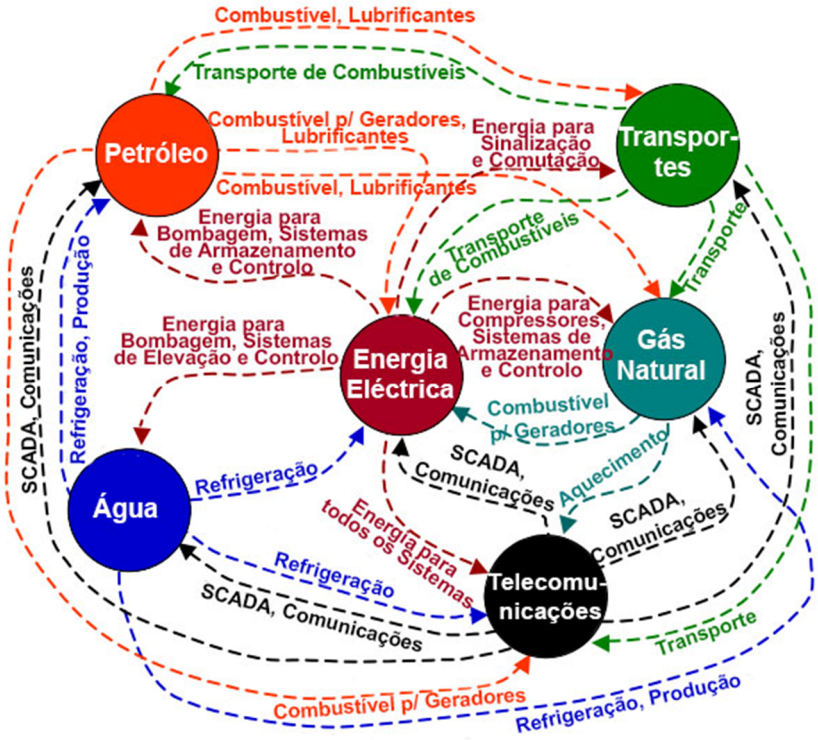


Figura 4 - Exemplos de dependência e interdependência de Sistemas. Adaptado de (Rinaldi et al., 2001).

Estas dificuldades, e os diferentes contextos de análise, levam a que em alguns casos as interdependências sejam encaradas de outra forma. Por exemplo, o governo inglês, no âmbito da resposta a desastres naturais, considera que existem apenas interdependências físicas e geográficas (Office, 2011). Curiosamente, um estudo mais recente, liderado por um grupo de engenheiros civis ingleses, conclui que cerca de 70% das relações de interdependência encontrados são do tipo físico ou organizacional e, portanto, limita a análise ao estudo destas duas, não dando qualquer atenção às dependências ciber ou geográficas (Civil Engineers, 2013).

Os exemplos anteriores ilustram a inexistência de consensos sobre a importância relativa das interdependências, o que dificulta a sua identificação e análise. No entanto, 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.

2.1.3 Criticidade

Uma infraestrutura é considerada como sendo "crítica" sempre que é de grande importância para o funcionamento da sociedade e qualquer falha ou degradação no seu desempenho resulte numa grave perturbação para o sistema global. Face a esta constatação, um critério importante para esta avaliação é a criticidade, como medida relativa da importância de uma dada infraestrutura em termos do impacto da sua disrupção ou falha funcional na garantia do abastecimento, isto é, no fornecimento à sociedade de bens e serviços fundamentais (BMI, 2009).

A criticidade varia também no tempo e no espaço, o que faz com que seja fortemente influenciada pela escala e pelo momento da análise. Em termos geográficos, uma IC pode ser muito importante a nível regional mas não ser relevante à escala nacional, o que implica que a escala da análise afecta a selecção de critérios de criticidade rigorosos, que devem ser adaptados em função dos objectivos a atingir. Em termos temporais, um serviço é mais ou menos crítico em função das horas, dos dias, ou dos meses. Por exemplo, o impacto de uma quebra energética será mais sensível durante o dia, mas este facto poderá ser ainda potenciado pelo factor geográfico. Ou seja, uma falha no abastecimento energético no Inverno terá mais impacto num país frio que num país temperado. Metzger (2004) distingue dois tipos de criticidade distintos, ainda que interligados, relacionando-os com diferentes tipos de infraestrutura:

- Criticidade como um conceito teleológico – uma infraestrutura é inerentemente crítica devido ao seu papel ou função social. Isto significa que em caso de colapso ou dano

na infraestrutura, um objectivo de uma determinada política de segurança já não pode ser alcançado;

- Criticidade como um conceito sistémico – uma infraestrutura é crítica devido ao seu posicionamento estrutural no sistema global de infraestruturas, especialmente porque é um elo de ligação essencial entre outras infraestruturas ou sectores.

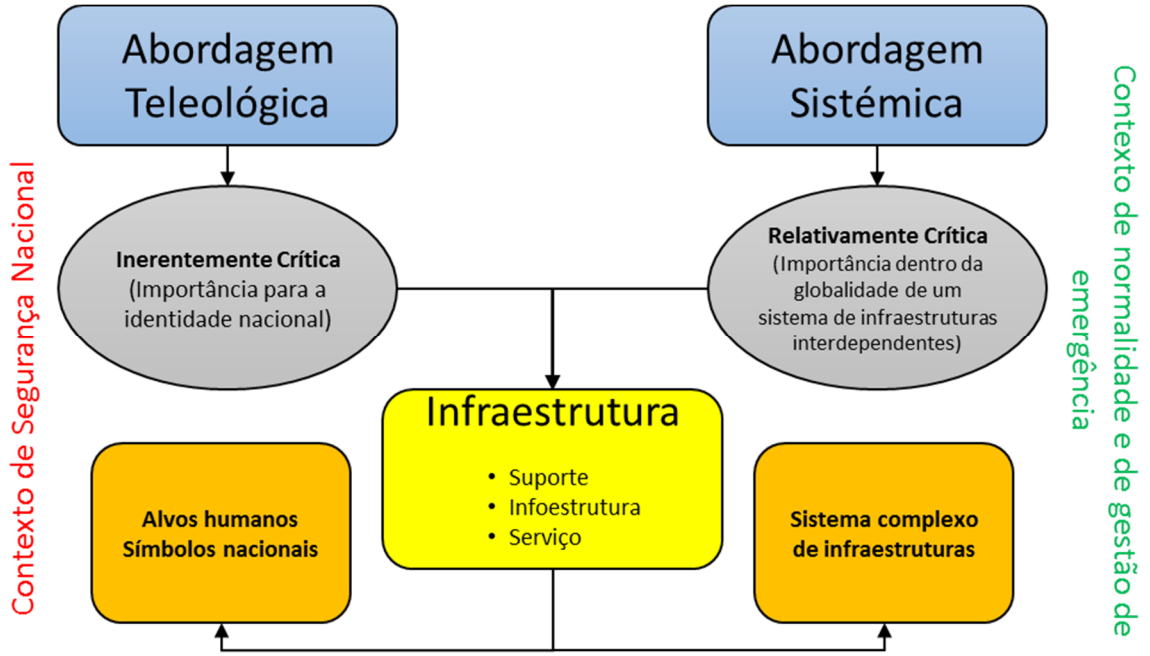


Figura 5 - Duas abordagens à criticidade. Adaptado de (Bouchon, 2006).

Na Figura 5 pode ver-se como estes dois tipos de criticidade podem ser aplicados de igual forma a qualquer tipo de infraestrutura, enquadrando-a em diferentes contextos de análise. Os alemães, expandindo um pouco o conceito anterior, consideram que a criticidade pode ser sistémica, simbólica, ou um misto das duas anteriores (BMI, 2009). Tabansky (2011), referindo-se à realidade israelita, considera serem três os 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. Estas diferenças podem ser explicadas pela adopção de diferentes abordagens, influenciadas por diversos factores sociais, políticos e económicos. Na realidade, boa parte das estratégias para a PIC foram lançadas num contexto de combate ao terrorismo e este facto levanta o problema de saber até que ponto os critérios utilizados são rigorosos e suficientes para avaliar a criticidade das infraestruturas (Bouchon, 2006).

Este é um dos problemas centrais em toda esta discussão; as noções de IC têm, ao longo dos últimos anos, evoluído de um nível de especialidade técnica e científica para integrarem as

agendas políticas, tendo como referência os diferentes contextos socioeconómicos em que se inserem. A tabela que se segue, resume alguns dos diferentes critérios utilizados, por diversos *stakeholders*, para avaliar a criticidade das IC.

Tabela 2 - Diferentes Percepções de Criticidade. Adaptado de (Bouchon, 2006).

Tipo de Actor	Situação de Crise	Critério de Criticidade
Autoridades nacionais e decisores	Incapacidade de garantir os interesses nacionais, a segurança dos cidadãos e a continuação do governo, provocando a perda de confiança no poder e uma crise política	Defesa Nacional, Segurança da Economia Nacional Saúde Pública Moral da Nação
Proprietários de infraestruturas e outros activos	Incapacidade de fornecer um serviço com fiabilidade provocando perdas económicas, perda de competitividade e diminuição da confiança dos clientes	Fiabilidade técnica e de serviço Competitividade Continuidade do negócio
Seguradoras	Incapacidade de garantir o pagamento de seguros em caso de grandes danos, provocando uma disrupção económica da companhia seguradora	Sustentabilidade da seguradora Continuidade do negócio
Outros stakeholders e público em geral	Disrupção de serviços, invalidando a fiabilidade da continuação das actividades do quotidiano e ameaçando os padrões normais de vida e bem-estar económico	Continuidade de serviço em função do grau de dependência

Talvez o melhor exemplo desta subjectividade, e das diferenças de perspectiva, seja o interesse dos EUA nas IC globais espalhadas por todo o mundo. Segundo Clemente (2013), as embaixadas dos EUA, no âmbito do *Critical Foreign Dependencies Initiative*, foram incumbidas de compilar uma lista de IC no país onde estão instaladas. O resultado foi uma lista de 259 locais em todo o mundo incluindo, entre outros, fabricantes de material bélico, indústrias farmacêuticas, centrais hidroeléctricas, fornecedores de serviços de telecomunicações e principais portos. Ou seja, o *Department of Homeland Security* (DHS) tem uma base de dados de IC localizadas fora do território norte-americano mas cuja perda poderá, no seu entender, afectar a saúde pública, os interesses económicos e a segurança nacional dos EUA.

2.1.4 Propriedade Privada

Há ainda a salientar o facto de muitas IC serem propriedade privada. Como já foi referido, há IC em sectores muito variados e que, em muitos países, abrangem áreas de negócio que são da esfera da actividade empresarial privada, chegando mesmo a estimar-se que 90% das IC estejam na posse de privados (KRITIS, 2004). Tendo em conta que a maior parte das IC é operada numa lógica comercial, é inevitável concluir que a sua gestão estratégica só pode ser implementada com uma forte colaboração entre o sector público e o privado, sendo este mesmo facto já reconhecido à escala global (Brunner & Suter, 2008). Esta tendência para a privatização das infraestruturas tem vindo a acentuar-se em vários países (BMI, 2009) e, em resultado desta tendência de transferência para a propriedade privada, também as responsabilidades de segurança, fiabilidade e disponibilidade dessas infraestruturas têm passado gradualmente para o sector privado.

Ou seja, as iniciativas de privatização e liberalização dos mercados tornaram a gestão e protecção das IC mais difícil, senão impossível, de ser alcançada apenas pelos governos (Hämmerli & Renda, 2010). Esta é uma realidade global que, tanto nos EUA (GAO, 2013) como na União Europeia (UE) (ENISA, 2011a), 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.

2.1.5 Dimensão Ciber

A importância do elemento cibernético neste âmbito foi especificamente salientada pela primeira vez em 1997, quando um relatório oficial do governo dos EUA referiu a existência uma dependência colectiva da infraestrutura de informação e comunicações. Isto é, este relatório reconheceu essencialmente a existência de uma crescente e real dimensão "ciber" associada à manutenção e preservação das IC (Marsh, 1997). 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.

Esse mesmo facto foi realçado por outros autores que enfatizaram a existência destas relações de interdependência comunicacional e o consequente surgimento dos chamados "sistemas baseados em cibernética"[6] (Rinaldi et al., 2001). No passado, a interdependência

[6] Em inglês, *cyberbased systems*.

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). Todas estas inovações não seriam possíveis sem o advento das TIC e, consequentemente, importa distinguir entre o conceito de IC no sentido tradicional e no contexto da realidade moderna, na qual este conceito inclui uma dimensão cibernética (Tabansky, 2011).

Ou seja, a sociedade moderna assenta num conjunto de sistemas "ciber-físicos" que são um conjunto de sistemas de sistemas onde existe um forte acoplamento entre os componentes computacionais do sistema, os componentes físicos, os processos e as políticas que regem estes sistemas (Adam, 2010). 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 e que, conjuntamente com as TIC, se tornou um elemento essencial da vida moderna. Embora o ciberespaço seja por vezes considerado como um sector à parte, na prática está tão embebido nos outros sectores que esta distinção não faz sentido.

É precisamente esta ligação entre o “ciber” e todas as áreas da vida moderna que tem sido responsável pelo fracasso de muitos governos na tentativa de definir quais os sectores das suas infraestruturas que são verdadeiramente críticos, uma vez que os actuais sistemas de classificação de IC se debatem com a análise da complexidade do ciberespaço, do qual dependem muitas das infraestruturas modernas. A dimensão e o ritmo de crescimento desta interligação criam problemas sem precedentes, tornando as ligações entre as IC e o ciberespaço uma área de enorme interesse para todas as partes interessadas. As actuais infraestruturas estão inteiramente dependentes dos componentes físicos e lógicos do ciberespaço que, em si mesmo, tem sido considerado como crítico (Clemente, 2013).

A Figura 6 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 das sociedades modernas.

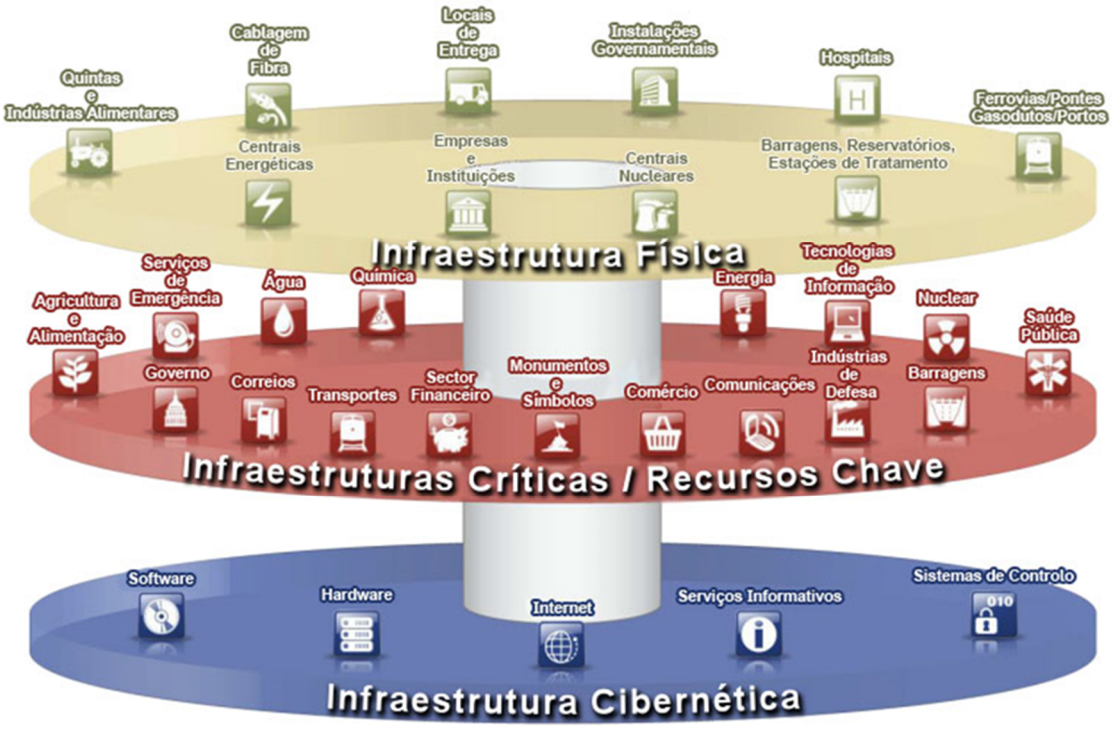


Figura 6 - A infraestrutura cibernética como base de todas as outras. Adaptado de (Beggs, 2010).

2.2 Identificação de Infraestruturas Críticas

Existem muitas 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. 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. Além disso, surge imediatamente a questão acessória de determinar o que deve ser considerado crítico no mundo actual.

2.2.1 Génese e Evolução do Conceito

A vulnerabilidade das IC e as estratégias para a sua protecção assumiram um papel de destaque em Junho de 1995 quando foi criado nos EUA um grupo de trabalho para estudar esta problemática, o *Critical Infrastructure Working Group*. Este grupo tinha como missão genérica identificar as IC, analisar as ameaças sobre elas, avaliar a capacidade de resposta dos organismos governamentais a essas ameaças e propor opções para a criação de uma estrutura a tempo inteiro que desse resposta a todos os problemas de segurança relacionados com as IC norte-americanas. Em resposta às recomendações deste grupo, em 15 de Julho de 1996, o Presidente Clinton criou a *President's Commission on Critical Infrastructure Protection* com o único objectivo de estudar a questão da protecção das IC e as vulnerabilidades norte-americanas a ameaças físicas e cibernéticas.

Esta comissão, sendo presidida por Robert Marsh, recebeu o seu cunho pessoal tendo os resultados do trabalho da comissão ficado para sempre associados ao seu nome[7]. Este relatório (Marsh, 1997), define "infraestrutura crítica" em termos de energia, banca, finanças, transportes, serviços humanos vitais e telecomunicações. Esta foi a primeira publicação oficial a utilizar a expressão "infraestrutura crítica" (Lewis, 2006), tornando-se um dos documentos fundamentais na história da PIC. Ao longo dos anos, foram criados diversos grupos de trabalho que produziram uma variedade de relatórios sobre esta temática. Todavia, estas preocupações só passaram para a primeira linha da agenda política depois dos fatídicos acontecimentos do 11 de Setembro de 2001. Desde então, estes assuntos são discutidos ao mais alto nível e têm sofrido uma enorme evolução durante a última década. Portanto, pode dizer-se que estes acontecimentos nos EUA marcaram definitivamente o arranque do processo de interesse global pela temática da PIC. Todavia, apesar de todos estes factos, e embora todas as definições que surgiram tentem reflectir a importância que estas instalações e serviços têm para o funcionamento da sociedade, nunca foi alcançada uma definição universalmente aceite de "infraestrutura crítica".

Na sequência dos acontecimentos do *World Trade Center*, o DHS lançou a *National Strategy for Homeland Security* na qual, além de identificar as IC, introduz o conceito de "activo essencial"[8] como um subconjunto dos recursos com importância nacional. Este documento,

[7] Em inglês, *Marsh Report*.
[8] Em inglês, *key asset*.

define estes activos essenciais como sendo os alvos individuais cuja destruição não colocará em risco sistemas vitais, mas poderá criar desastres locais ou afectar a moral da Nação. Nesta categoria, incluem-se símbolos, atracções históricas ou instalações pontuais com potencial destrutivo e valor para as comunidades locais (Moteff & Parfomak, 2004). Todavia, no campo legislativo, o *Homeland Security Act* de 2002 introduz já o termo "recurso essencial"[9]. Este termo veio substituir o anterior, em 2003, aquando da publicação da *Homeland Security Presidential Directive 7* que dará origem, em 2006, à primeira versão do *National Infrastructure Protection Plan* (NIPP). Neste documento, surge pela primeira vez a expressão *Critical Infrastructure and Key Resources* (CIKR). Neste plano, os recursos essenciais são definidos como sendo os recursos públicos ou privados que são essenciais ao funcionamento da economia e do governo. Desde então, a expressão CIKR passou a ser utilizada em praticamente todos os documentos oficiais sobre esta temática para designar o conjunto de tudo aquilo que o governo dos EUA considera que deve ser prioritariamente preservado (DHS, 2011a, 2012, 2013).

No contexto das políticas públicas norte-americanas, as definições de "infraestrutura" e "infraestrutura crítica" têm evoluído muitas vezes com alguma ambiguidade, o que tem dado azo a diversas interpretações (Moteff & Parfomak, 2004). Embora existam diversos métodos e critérios com base científica para a análise e identificação das IC, a verdade é que outros factores têm sido muitas vezes preponderantes no processo de selecção daquilo que deve ou não ser protegido. Citamos, a título de exemplo, o caso ocorrido nos EUA durante no processo de criação de um repositório central de CIKR. Paralelamente à elaboração da primeira versão do NIPP, o DHS consolidou e expandiu uma base de dados com a intenção de elaborar um catálogo exaustivo que incluísse um inventário com informação descritiva, respeitante aos activos e sistemas que compunham a listagem nacional de CIKR, a chamada *National Asset Database* (NADB).

Embora a sua verdadeira origem pareça ser incerta (Moteff, 2007), a NADB alegadamente evoluiu a partir de uma pequena lista compilada em 2003 que tinha apenas 160 activos críticos. Mais tarde, nesse mesmo ano, por pressão do Congresso e de diversos Estados, a mesma lista foi expandida para incluir 1.849 activos, recebendo o nome de *Protected Measures Target List* (PMTL) (DHS, 2006). Subsequentemente, foi solicitado às entidades

[9] Em inglês, *key resource*.

estaduais e locais que fornecessem dados sobre IC no âmbito de um processo de análise e auto-avaliação. Como resultado deste trabalho, em Fevereiro de 2004, a PMTL tinha já 28.368 activos, mas não representava devidamente as CIKR norte-americanas (Moteff, 2007). Posteriormente, em Julho de 2004, foi iniciada uma nova ronda de recolha de dados a nível estadual que culminou na compilação de outros 48.701 activos, ou seja, no final de 2005 a NADB tinha um total de 77.069 activos.

No entanto, apesar de todos os esforços desenvolvidos, em Julho de 2006, uma auditoria do DHS concluiu que a NADB tinha falhado os seus objectivos pois continha demasiados activos de baixa prioridade. Nomeadamente, a listagem continha, por exemplo, 4.055 centros comerciais, 1.305 casinos, 539 parques de diversão e outros, onde se incluíam o *Old MacDonald's Petting Zoo*, a *Amish Country Popcorn Factory*, o *Mule Day Parade* e a *Sweetwater Flea Market* (DHS, 2006). O DHS defendeu a sua lista, apesar de esta incluir lojas de donuts, barracas de pipocas e gelatarias, alegando que ainda não tinha sido devidamente priorizada mas que, mesmo assim, representava a panóplia de coisas com que os EUA tinham que se preocupar (Moteff, 2007). Todavia, o Congresso não ficou convencido e, passados alguns meses, suspendeu a utilização da NABD que foi substituída por outras ferramentas (Clemente, 2013). Este caso, parece-nos ser exemplarmente ilustrativo da dificuldade em seleccionar o que é crítico, apesar da existência de critérios e normas orientadoras.

2.2.2 Exemplos Internacionais

Durante os últimos anos, foram desenvolvidos variadíssimos métodos destinados a apoiar a análise do comportamento de uma infraestrutura e os seus pontos de vulnerabilidade. Isto porque a PIC se tornou uma preocupação em muitos países, devido ao potencial efeito que uma disrupção nestes sistemas pode ter na vida dos seus cidadãos. A profusão de critérios e metodologias (Bagheri & Ghorbani, 2008) e as inevitáveis diferenças culturais e geoestratégicas levam à existência de diversas definições de IC. Uma compilação de alguns exemplos da variedade de definições existentes pode ser consultada no Anexo I. 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. Este facto originou o surgimento do conceito que seguidamente se analisa.

2.3 Infraestruturas Informacionais 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 e de propriedade intelectual. 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).

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.

2.3.1 Definição

A expressão “Infraestruturas Informacionais Críticas”[10] refere-se geralmente a sistemas de TIC que são essenciais para as operações das IC nacionais e internacionais (Hämmerli & Renda, 2010). Mas, à semelhança do que ocorre com as IC, também não existe uma definição globalmente aceite para as IIC sendo no entanto vulgar considerar-se que estas são “os serviços de comunicação ou informação cuja disponibilidade, fiabilidade e resiliência são essenciais para o funcionamento da economia, para a segurança e para outros valores essenciais” (Cukier, 2005). Diversos países adoptaram definições ligeiramente diferentes e, num esforço de sintetizar esta diversidade conceptual, a OCDE propôs que as IIC sejam consideradas “as redes e sistemas de informação interligados cuja destruição ou interrupção terá um impacto sério na saúde, segurança e bem-estar económico dos cidadãos, ou no funcionamento eficaz do governo ou da economia” (Gordon & Dion, 2008).

2.3.2 Relevância

O papel das IIC e a sua relevância para a PIC têm vindo a crescer, levando a um incremento da relação entre cibersegurança e PIC e simultaneamente salientando o facto de parte dos problemas globais estarem ainda dependentes de soluções locais (Hämmerli & Renda, 2010). Estudando a situação em vários países, a OCDE conclui que, embora esta não seja igual em todos os países estudados, existe uma forte relação entre as IC e as IIC, o que, em parte, se

[10] Em inglês, *Critical Information Infrastructures* (CII)

deve à existência de diversos critérios para avaliar o que são as IIC e as próprias IC (Mansfield & Carblanc, 2008). Ou seja, 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).

Apesar da profusão de diferenças nos contextos políticos nacionais e internacionais, o mais importante é entender que as IIC fazem parte integrante do funcionamento dos sistemas TIC dos quais a Internet é um componente muito importante devido nomeadamente, à sua difusão e convergência tecnológica global. Por outro lado, além das diferenças, importa aqui realçar o papel do factor cibernético enquanto elo de ligação entre as IC e as IIC, e como elemento estruturante de toda a rede de interdependências. Neste contexto, um dos elementos mais importantes da infraestrutura de informação são os sistemas de controlo e instrumentação industrial que serão analisados no próximo capítulo.

3. SISTEMAS DE CONTROLO INDUSTRIAL

Os termos "rede industrial" e "infraestrutura crítica" são várias vezes utilizados de forma algo confusa. Uma rede industrial é uma rede que funciona de acordo com algum tipo de sistema de controlo automático que comunica digitalmente pela rede. Por seu turno, uma infraestrutura crítica é uma infraestrutura em rede, que inclui qualquer rede utilizada na operação directa de qualquer sistema do qual dependa uma das infraestruturas definidas como críticas (Knapp, 2011).

3.1 Definição

Os sistemas de controlo industrial (em inglês, *Industrial Control Systems* - ICS)[11] 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. Vários sectores da indústria, considerados como IC, utilizam um ou vários tipos de sistemas de controlo industrial nas suas actividades diárias.

Na realidade a expressão "sistemas de controlo industrial" é uma designação genérica que engloba diversos sistemas de controlo onde se podem incluir sistemas de supervisão e aquisição de dados (em inglês, *Supervisory Control And Data Acquisition* – SCADA), sistemas de controlo distribuído (em inglês, *Distributed Control Systems* – DCS) além de uma grande variedade de outras configurações de sistemas de controlo (Stouffer, Falco, & Kent, 2013). Os DCS são utilizados para controlar processos industriais e são normalmente integrados na arquitectura de controlo como sendo um nível de supervisão, monitorizando uma multiplicidade de subsistemas integrados, ou seja, são sistemas de controlo de processos (em inglês, *Process Control Systems* - PCS) (Knapp, 2011).

As funções mais importantes dos ICS são essencialmente as seguintes: Recolha de dados (armazenamento, conversão, datação, etc), monitorização (monitorização de estados instantâneos, de tendências, de desempenho e gestão de alertas), controlo (controlo directo,

[11] De modo a tornar o texto mais perceptível, iremos doravante utilizar as siglas inglesas vulgarmente utilizadas na literatura de referência sobre esta temática.

pontos de controlo, controlo sequencial), planeamento e acompanhamento (funções não críticas, registos), manutenção e mudança (colocar e retirar de serviço, actualizar, manter e desenvolver) (Holmgren, Johansson, & Malmgren, 2010).

3.2 Sistemas SCADA

A área dos ICS, como ocorre em tantos outros sectores que integram componentes de 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. 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. Todavia, é ainda vulgar que os ICS sejam referidos como sendo SCADA, o que é simultaneamente pouco rigoroso e enganador (Knapp, 2011). Na realidade, 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. Cada uma destas áreas tem as suas próprias considerações de segurança física e lógica e as suas políticas e preocupações específicas.

3.2.1 Descrição

Os SCADA são o maior subgrupo dos ICS (ENISA, 2013) e 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 eléctrica 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 et al., 2013). Os 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 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 (Stouffer et al., 2013). 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. Esta dispersão geográfica, leva a que os termos SCADA e DCS sejam utilizados de forma intermutável mas o primeiro é habitualmente reservado para sistemas com grande dispersão geográfica (Lewis, 2006). Basicamente, os sistemas SCADA são utilizados em grandes áreas geográficas, enquanto um DCS está confinado a uma área restrita, como uma estação de tratamento de águas residuais.

No entanto, os SCADA e os DCS são frequentemente ligados em rede, como no caso dos centros de controlo de energia eléctrica e as centrais geradoras. Apesar de as centrais serem geridas por um DCS, este tem que comunicar com um SCADA para coordenar a saída da produção com as necessidades de consumo e distribuição (Stouffer et al., 2013). No moderno ambiente empresarial, os SCADA estão gradualmente a transformar-se em verdadeiros sistemas de informação, ou seja, em activos informacionais no seio das organizações. Assim, os sistemas SCADA têm que ser encarados e geridos da mesma forma que qualquer outro sistema de informação crítico.

3.2.2 Arquitectura

Os sistemas SCADA são compostos por *hardware* e software. Tipicamente, o *hardware* inclui (NCS, 2004; Stouffer et al., 2013):

- Um, ou mais, dispositivos de recolha e tratamento de dados no terreno (em inglês, *Remote Terminal Unit* - RTU);
- Um, ou mais, dispositivos que interagem com os RTU, controlando comutadores e válvulas (em inglês, *Programmable Logic Controller* - PLC);
- Um conjunto de sensores inteligentes (em inglês, *Intelligent Electronic Device* – IED) que fazem a recolha de informação, comunicam com outros dispositivos e realizam processamento e controlo local sem necessidade de contactar o centro de controlo;

- Um servidor central colocado num centro de controlo (em inglês, *Master Terminal Unit* - MTU). Este armazena e processa a informação das entradas e saídas dos RTU, enquanto estes (ou os PLC) controlam os processos locais;
- Um sistema de comunicações que transfere dados entre os dispositivos colocados no terreno, as unidades de controlo e o MTU;
- Um conjunto de software programado para dizer ao sistema o que monitorizar, dentro de que parâmetros, que resposta dar fora dos mesmos e que é utilizado no centro de controlo pelos operadores do sistema (em inglês, *Human Machine Interface* - HMI).

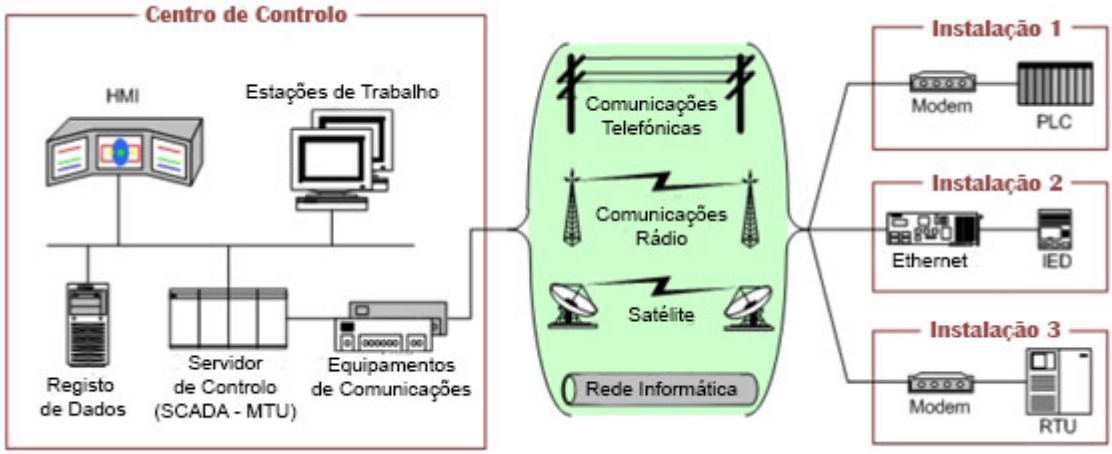


Figura 7 - Arquitectura genérica de um sistema SCADA. Adaptado de (Stouffer et al., 2013).

A Figura 7 ilustra um exemplo genérico de um sistema SCADA, que utiliza todos estes componentes para a gestão de vários locais remotos a partir um único centro de controlo.

3.3 Evolução

Os sistemas SCADA vulgarizaram-se nos anos 60 com o crescimento da necessidade de controlar e monitorizar equipamento remoto e evoluíram paralelamente com o crescimento da tecnologia de computação moderna. A primeira geração destes sistemas tinha uma arquitectura muito simples, monolítica, assente em computadores *mainframe* e que funcionava isoladamente. Quando os primeiros sistemas SCADA foram desenvolvidos, as redes informáticas eram praticamente inexistentes e assim, cada sistema, funcionava de forma independente, sem qualquer tipo de ligação a outros sistemas (NCS, 2004).

A segunda geração de sistemas SCADA tinha já uma arquitectura distribuída e tirava partido dos desenvolvimentos entretanto registados ao nível das redes locais e da miniaturização. A informação era partilhada em tempo real a partir de estações que cumpriam uma função

específica. Estes sistemas eram normalmente constituídos por *software*, *hardware* e protocolos proprietários, isto é, específicos de cada firma. Estas estações eram pequenas, tipicamente do tipo minicomputador, muito menos dispendiosas que as suas antecessoras e estavam ligadas numa rede local (em inglês, *Local Area Network* – LAN)[12] (NCS, 2004).

A actual terceira geração, possui já uma arquitectura em rede, semelhante à geração anterior mas capaz de comunicar tanto através de redes de área (em inglês, *Wide Area Network* – WAN)[13] como de redes LAN. A principal diferença relativamente aos sistemas anteriores é o facto de agora serem utilizados protocolos e equipamento *standard* e não sistemas proprietários (NCS, 2004). Isto é, os actuais sistemas SCADA comunicam através do protocolo utilizado por todos os computadores ligados à Internet (em inglês, *Transmission Control Protocol/Internet Protocol* - TCP/IP)[14] e utilizam *software* comercial (em inglês, *Commercial Off-The-Shelf* – COTS)[15].

Ou seja, os primeiros ICS eram redes ponto a ponto que ligavam um painel de controlo a um sensor remoto. Estes ICS, evoluíram depois 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, 2011a). 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, 2011a). 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

[12] Estas são as redes locais que ligam computadores em casa, numa escola ou num escritório.
[13] Estas são as redes que cobrem uma vasta área geográfica, com ligações que muitas vezes vão além das fronteiras nacionais.
[14] É o protocolo de comunicação padrão entre máquinas na Internet.
[15] É uma designação corrente para o *software* comercial disponível para o público em geral.

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).

3.4 Situação Actual

O crescimento da dependência das IC, e de toda a automação industrial, de sistemas de controlo interligados fisicamente e baseados em cibernética, criou um inesperado conjunto de problemas de segurança para os ICS e, em particular para os sistemas SCADA, que se tornaram os elementos centrais de uma silenciosa revolução industrial, impulsionada pela expansão da informática. Esta penetração dos SCADA, dos DCS, e dos restantes elementos da sua família electrónica, como componentes críticos de todos os aspectos das nossas infraestruturas é tanto inevitável como inexorável. Embora possa constituir uma vantagem económica e permitir uma expansão da capacidade operacional, esta dependência dos omnipresentes ICS representa um novo vector de vulnerabilidade na era da informação digital.

3.4.1 Relevância dos ICS e dos SCADA

Alguns especialistas acreditam, já há alguns anos, que este papel de destaque assumido pelos sistemas SCADA os torna num alvo interessante para os terroristas uma vez que, por motivos que veremos adiante, não estão devidamente protegidos contra ciberataques (Wilson, 2008). De facto, a maioria destes sistemas continua a ser muito vulnerável a ataques informáticos uma vez que as organizações responsáveis pela sua operação continuam a não estar devidamente sensibilizadas para as especificidades da sua segurança. Os ICS são hoje um verdadeiro activo estratégico e o significativo número de incidentes ocorridos na última década originaram uma grande preocupação e discussão entre todos os envolvidos nesta área (ENISA, 2011a).

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 de tecnologia que fornecem soluções únicas e proprietárias. 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. 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 (Clarke & Olcott, 2012).

3.4.2 Comparação entre ICS e TIC

O facto de utilizarem software COTS e estarem ligados à Internet, expõe os ICS genericamente ao mesmo tipo de ameaças que os sistemas de TIC, mas os ICS têm características que os distinguem muito dos outros sistemas de processamento de informação. Segundo a ENISA, existem duas principais diferenças entre os ICS e os sistemas de TIC: os ICS têm prioridades diferentes e implicam riscos com âmbito muito mais alargado e muito maior impacto potencial (ENISA, 2011a).

Os ICS foram concebidos para responder a apertados critérios de desempenho e fiabilidade que não são habituais num ambiente TIC convencional (Stouffer et al., 2013). Genericamente, a prioridade atribuída a cada um dos atributos de segurança é determinada em função da área de negócio. Por isso mesmo, os sistemas que sustentam IC envolvidas na qualidade e segurança de vidas humanas requerem uma perpétua disponibilidade e integridade da informação, requisitos que podem ofuscar a necessidade de proteger os dados de acesso não autorizados, a não ser que isso conflitue com os outros atributos de segurança (DHS, 2009).

Tipicamente, uma rede de informação moderna prioriza os seus objectivos de segurança de acordo com critérios que colocam a segurança da informação em primeiro lugar. Todavia, devido à necessidade de alta disponibilidade e aos requisitos operacionais dos ICS, na maior parte dos sistemas de controlo os objectivos de segurança estão invertidos, como se pode ver na Tabela 3:

Tabela 3 – Objectivos de Segurança nos ICS e nos sistemas TIC. Adaptado de (DHS, 2009).

Objectivo de Segurança	**TIC**	**ICS**
Confidencialidade	Alta Prioridade	Baixa Prioridade
Integridade	Alta Prioridade	Média Prioridade
Disponibilidade	Baixa Prioridade	Muito Alta Prioridade

Por outro lado, muitas diferenças entre os ICS e os sistemas de TIC resultam do facto de a lógica de operação dos ICS ter um impacto directo no mundo físico, ou seja, pode implicar riscos significativos para a saúde e segurança das populações, sérios impactos ambientais, além dos aspectos económicos e financeiros como quebras de produção e impacto negativo na economia nacional (Stouffer et al., 2013). Ou seja, enquanto nos tradicionais sistemas de TIC a principal prioridade é a integridade, nos ICS a disponibilidade é indiscutivelmente o objectivo de segurança mais importante pois estes sistemas são fundamentais para o funcionamento correcto das IC (Dufkova, Budd, Homola, & Marden, 2013).

Como já vimos, inicialmente os ICS tinham pouco em comum com os sistemas TIC visto que eram isolados, todo o *software* era proprietário e o hardware era especializado. À medida que os ICS adoptaram soluções padronizadas, começaram a assemelhar-se a sistemas TIC mas as diferenças persistem e, nalguns casos, tendem mesmo a acentuar-se. No Anexo II podemos ver uma listagem das diferenças mais significativas entre os ICS e os sistemas de TIC, e como estas características influenciam a sua operação e gestão. Na realidade empresarial actual, os objectivos de segurança e eficiência podem, por vezes, conflituar com a segurança na concepção e operação dos ICS. Por exemplo, impor a necessidade de autenticação por palavra passe pode interferir com as acções de emergência dos ICS (Stouffer et al., 2013).

A conjugação destas diferenças cria um ambiente onde é difícil aplicar directamente as tradicionais soluções e procedimentos de segurança. Talvez seja essa a justificação para as dificuldades ocorridas em todo este processo de junção entre as tecnologias de informação e de controlo. Este processo de convergência foi marcado, desde o início, pelo surgimento de tensões entre engenheiros ligados aos sistemas de controlo e os profissionais da informática, dois grupos que sempre trabalharam de forma independente, que têm formação muito diferente e discordam na forma de utilizar as TIC em ambientes de elevada criticidade (Clarke & Olcott, 2012).

A situação actual está bem patente num estudo publicado recentemente pela SANS (Luallen, 2013) cujos resultados 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 PLCs 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.

4. VULNERABILIDADES DAS INFRAESTRUTURAS CRÍTICAS

Já em 1995, o governo dos EUA reconhecia que as suas redes de dados eram vulneráveis, que a sua infraestrutura informacional estava extremamente dependente das redes de informação, como a Internet, e que a mesma estava exposta a ataques originários dessas mesmas redes (SPB, 1995). Actualmente, as IC são entendidas como sendo sistemas de sistemas devido às suas interdependências e é consensual que esta situação é apenas umas das origens das suas vulnerabilidades. Na EU, o Livro Verde da PIC define vulnerabilidade como sendo uma característica da concepção, implementação ou operação de um elemento de uma infraestrutura que o torna susceptível a ser incapacitado por uma ameaça. (Commission, 2005). Do outro lado do Atlântico, o DHS considera que uma vulnerabilidade é uma característica física ou atributo operacional que torna uma entidade aberta a ser explorada ou susceptível a um determinado perigo (DHS, 2010).

4.1 Vulnerabilidades dos ICS

As vulnerabilidades dos sistemas industriais têm vindo a ser realçadas em diversos estudos (Shea, 2003) que chegam mesmo a referir que, apesar das actualizações ocorridas no âmbito dos potenciais problemas informáticos da viragem do milénio, nunca foi dada a devida atenção aos problemas de segurança dos ICS. Infelizmente, a maior parte destes sistemas nunca foi concebida com preocupações de segurança e o resultado é que a generalidade das IC está repleta de vulnerabilidades que carecem de uma atenção constante (GAO, 2004). Em 2010, um grupo de analistas de segurança apresentou os resultados de um trabalho de pesquisa onde, no decurso de testes de penetração efectuados em cerca de 100 centrais produtoras de energia eléctrica nos EUA, foram detectadas mais de 38.000 alertas de segurança e vulnerabilidades (Knapp, 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).

4.1.1 Obsolescência Tecnológica

De acordo com a ENISA, os maiores desafios técnicos no que diz respeito à segurança dos ICS estão relacionados com a obsolescência de diversas tecnologias empregues nestes

sistemas (ENISA, 2011a). Estas tecnologias, foram concebidas partindo de premissas que hoje estão ultrapassadas, tais como o isolamento total dos sistemas ou a sua tremenda especificidade que fazia com que poucos especialistas os entendessem. Uma vez que os requisitos de segurança não foram introduzidos originalmente, é agora extremamente difícil incorporá-los pois, além de muito dispendiosos, podem não ser compatíveis com o antigo *hardware* instalado. Estas vulnerabilidades, são também reconhecidas pelas autoridades norte-americanas que as referem em diversos relatórios oficiais (DHS, 2011b; Stouffer et al., 2013). Em suma, a maior ameaça à segurança dos ICS é a existência de dispositivos não fiáveis, isto é, que foram originalmente criados com falhas de segurança (ENISA, 2011a). Esta situação, é também agravada pelo facto das tecnologias dos ICS terem ciclos de vida muito mais longos que os habituais nas TIC, o que faz com que os sistemas permaneçam vulneráveis por muito mais tempo.

4.1.2 Evolução do Software

Os 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, ainda que de forma insegura, funcionam, não são substituídos.

Há mesmo especialistas que afirmam que, uma vez que os SCADA combinam *hardware* e *software*, não podem ser actualizados como os restantes equipamentos informáticos pois a sua substituição seria extremamente complicada e dispendiosa (Baker, Waterman, & Ivanov, 2009). Em linha com esta visão, há estudos independentes que apontam a existência de *software* desactualizado como sendo a principal vulnerabilidade dos ICS ligados a redes de energia eléctrica (Symantec, 2012). Este assunto, foi recentemente alvo de um estudo da ENISA onde se concluiu que as transformações ocorridos nos sistemas SCADA aumentam as suas vulnerabilidades e que o aumento da segurança poderá ser conseguido através da

correcta e atempada aplicação de actualizações e correcções[16] ao software (ENISA, 2013). Como se pode ver na Figura 8, a "janela de exposição" a uma determinada vulnerabilidade é o tempo entre o momento em que a vulnerabilidade é revelada e o momento em que a correcção é disponibilizada. Numa perspectiva empresarial, considera-se que a "janela de exposição" só é encerrada no momento em que a correcção tiver sido instalada em todos os sistemas (Pauna & Moulinos, 2013).

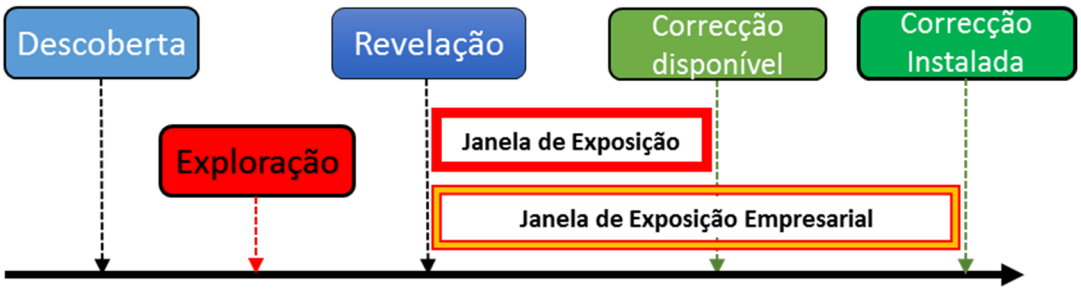


Figura 8 - Janelas de Exposição. Adaptado de (Pauna & Moulinos, 2013).

Embora nos EUA a gestão de correcções e actualizações seja obrigatória para cumprimento de normas federais, os resultados apresentados em 2010 indicam que a "janela de exposição" nas IC analisadas era, em média, de 311 dias, chegando mesmo a existir vulnerabilidades com 1.100 dias e que ainda não tinham sido corrigidas (Knapp, 2011).

Os sistemas de controlo são, por concepção, difíceis de actualizar. Como as suas principais prioridades são a disponibilidade e a fiabilidade (DHS, 2009), mesmo que as actualizações e correcções estejam disponíveis, só são aplicadas aquando de paragens planeadas para manutenção dos sistemas, o que pode ocorrer a intervalos de vários anos. 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).

Assim, parece garantido que continuarão sempre a existir vulnerabilidades por corrigir mas considera-se que seria uma grande melhoria se a "janela de exposição" média fosse reduzida de 311 dias para uma semana, ou mesmo para um mês (Knapp, 2011). Na EU, não existe nenhuma obrigatoriedade comunitária de cumprimento de quaisquer regras de gestão de correcções o que leva a que existam múltiplas posturas face a este problema. Neste âmbito,

[16] Em inglês, *patches*.

importa referir que a recomendação da ENISA vai no sentido de impor normas neste domínio (Pauna & Moulinos, 2013).

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 computadores (ou num único) 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 assentam maioritariamente em plataformas e sistemas padronizados aplicados a diversos dispositivos, e utilizam *software* COTS, o que levou a uma redução dos custos, à sua facilidade de utilização e permitiu ainda a sua monitorização e controlo remoto a partir de diversas localizações (ENISA, 2011a).

Os próprios sistemas operativos e as aplicações, utilizados de forma generalizada nos sistemas ICS, migraram de versões proprietárias para versões *standard* 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 TIC convencionais (ENISA, 2011a). A 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).

Além disso, existe também um grande risco de incompatibilidades entre o *software* COTS e os antigos sistemas operativos e aplicações existentes nos ICS, visto que este *software* foi concebido para funcionar em ambientes muito especializados, com características também elas muito específicas (Stouffer et al., 2013). Ou seja, contrariamente aquilo que se possa pensar, a mudança para o *software* COTS não veio colmatar as lacunas de actualização de *software*. Na realidade, muitos operadores de ICS não estão autorizados a actualizar o seu *software*, sob pena de perderam a sua certificação e arriscarem a integridade dos seus sistemas de controlo, o que colocaria em risco a disponibilidade e a operacionalidade dos serviços por si prestados (Symantec, 2012).

4.1.3 Ligação ao Exterior

Não foram apenas as aplicações proprietárias que foram modificadas ou substituídas por outras padronizados e abertas. Os antigos sistemas de controlo foram originalmente concebidos como redes isoladas, sem acesso à Internet. Por essa razão, 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 projectados para ser ligados a uma rede pública (NCS, 2004). Mas, conforme vimos, os protocolos de comunicação dos ICS nunca foram concebidos para ser seguros. Na realidade, muitos destes protocolos foram originalmente implementados 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, 2011a).

Os sistemas ICS e as redes de TI empresariais estão hoje completamente interligados sendo vulgar ter sistemas ICS que comunicam através da Internet, o que torna 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, 2011a). Ou seja, a existência das antigas vulnerabilidades é exacerbada pela crescente ligação de sistemas antigos a redes modernas. Se é verdade que os benefícios da ligação à Internet têm sido notáveis, a vulgarização desta interligação representa uma enorme vulnerabilidade para as IC e para as operações que estas executam (GAO, 2004). Em 2008, num inquérito realizado durante uma conferência sobre segurança de IC, 60% dos participantes revelaram que as suas redes industriais estavam já ligadas, e 98% assumiram que essa interligação aumentava os seus riscos de segurança (Nicholson, 2008).

As implementações originais dos ICS eram susceptíveis de ser atacadas apenas por ameaças locais porque a maior parte dos seus componentes estava em áreas com segurança física e esses componentes não estavam ligados a outros sistemas ou redes de TIC. No entanto, a tendência para a integração dos ICS nas TIC reduziu significativamente esse isolamento do mundo exterior, expondo todas as vulnerabilidades dos ICS e criando a necessidade de

proteger estes sistemas de ameaças externas e remotas (Stouffer et al., 2013). 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.

4.1.4 Elemento Humano

As vulnerabilidades são frequentemente causadas também devido à má divulgação e aplicação de procedimentos de segurança, o que pode permitir que funcionários com acesso a informação sensível dos sistemas explorem vulnerabilidades de forma intencional (Stouffer et al., 2013). Todavia, há também que ter em conta os erros humanos involuntários, provocados por uma falta de interesse ou compreensão dos aspectos da segurança dos ICS (ENISA, 2011a). A mentalidade apática, assumindo que a segurança não é sua responsabilidade, e a noção de que não há riscos de ataque, já tinham sido diagnosticados no supracitado inquérito (Nicholson, 2008) como estando entre as principais causas para a falta de segurança registada nas IC.

Outra das tendências preocupantes é o surgimento de aplicações que permitem monitorizar sistemas SCADA a partir de dispositivos de computação pessoal tipo ***tablets*** ou ***smartphones***. 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, sendo hoje possível adquirir ***online*** uma aplicação "SCADA Mobile" para um ***smartphone***, por uma quantia verdadeiramente irrisória.

Embora as empresas encarem esta tendência com entusiasmo, pois permite-lhes poupar dinheiro, a verdade é que cria todo um novo problema de segurança. Se, por exemplo, um funcionário puder aceder a todos os recursos da sua empresa através de um ***smartphone*** que está infectado com um ***software*** malicioso, este acesso pode resultar num roubo de informação sensível (Cisco, 2014). Assim, o imenso número de dispositivos móveis abre uma nova área de potencial ataque, constituindo uma oportunidade que os atacantes não irão desvalorizar, até porque nalguns países são já a principal forma de aceder à Internet (GIT, 2013).

Cumulativamente, a crescente adopção do chamado BYOD[17] 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. Ou seja, a rápida adopção do BYOD, a utilização de múltiplos dispositivos por utilizador, e todas as outras novidades que surgem constantemente, criam uma rede ciberespacial inteligente mas que tem imensas vulnerabilidades, tantas quantas as que cada utilizador tem no seu perfil de exploração das modernas TIC.

4.2 Interdependência de Sistemas

As nossas infraestruturas não são monólitos isolados; são compostas por elementos agregados formados por diversas partes com autonomia local limitada. Muitas estão inseridas em diversos níveis de hierarquia e múltiplos níveis de redundâncias intencionais e a sua segurança é constrangida por prioridades comerciais e operacionais. Ou seja, embora não planeadas, neste sistema de sistemas existem ligações e interdependências que podem potenciar o impacto de uma falha numa infraestrutura (Ventura et al., 2010).

Assim, uma das propriedades a acautelar na segurança das infraestruturas, deve atender ao facto de várias esferas de actividade poderem estar dependentes do seu correcto funcionamento e de estas poderem também depender de sistemas que estão sob o controlo de diversas entidades, introduzindo novas vulnerabilidades no seu funcionamento (GAO, 2004). O papel das interdependências na gestão das vulnerabilidades das IC, tem sido confirmado por diversas fontes. Alguns autores realçam as vulnerabilidades resultantes da imprevisibilidade das interacções entre infraestruturas e o possível efeito em cascata

[17] BYOD é uma sigla inglesa para *Bring Your Own Device* (Traga o Seu Próprio Dispositivo). Este fenómeno tem uma crescente popularidade um pouco por todo o mundo e 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 (*smartphones*, *tablets* ou *laptops*) no ambiente laboral e com eles possam aceder aos recursos da rede da empresa.

resultante das suas interdependências (Bloomfield, Chozos, & Nobles, 2009). Outros, relembram que as actuais redes de energia e telecomunicações nunca foram concebidas para trabalhar de forma interligada e que, embora os sistemas físicos individuais tenham sido concebidos de forma consistente, as gigantescas redes transnacionais actuais nunca foram projectadas como sistemas integrados (Lukszo, Deconinck, & Weijnen, 2010). Nesta realidade, isolar as IC 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).

4.3 Componente Ciber

O ciberespaço é hoje uma parte tão importante da vida moderna que, embora seja muitas vezes considerado como 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). A vulnerabilidade do elemento ciber foi inicialmente identificada pelo já citado relatório norte-americano (Marsh, 1997), que inclusivamente referia os resultados de um exercício militar decorrido no Verão de 1997, no qual foram expostas diversas vulnerabilidades dos sistemas dos EUA ao potencial ataque de um inimigo com armas cibernéticas.

Nos anos seguintes, estas vulnerabilidades foram-se agravando e esse facto foi sendo identificado em diversos relatórios oficiais nos quais se alertava explicitamente para o facto de os ICS serem particularmente sensíveis a eventuais ataques cibernéticos mas os aspectos da sua cibersegurança não serem encarados como prioritários (Shea, 2003). A dependência da Internet foi também apontada como sendo um novo foco de vulnerabilidade das IC, que podem agora ser atacadas por meio das redes globais às quais estão ligadas, sendo esses ataques quase que exclusivamente cibernéticos (GAO, 2004). Além disso, como os componentes dos sistemas SCADA são seleccionados em função do seu preço, a sua segurança tem sido sistematicamente sacrificada com o objectivo de reduzir custos de aquisição e de consumo energético. O resultado deste tipo de decisões, conduz

inevitavelmente a uma situação em que a maioria dos sistemas SCADA está desprotegida e é vulnerável a ciberataques (Lewis, 2006).

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 derivada da difusão da Internet, adopção de dispositivos móveis, etc. Desta forma, não há como evitar as implicações emergentes da intersecção do ciberespaço com as IC (Clemente, 2013).

4.4 Sector Privado

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, apresentam 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). No já citado inquérito (Nicholson, 2008), os resultados mostraram claramente que o principal entrave à segurança das IC era a limitação de custos.

Esta tendência de diminuição dos custos, tem levado a que muitas empresas na área da produção e distribuição de energia tenham reduzido perigosamente a redundância física dos seus sistemas e estejam cada vez mais 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 ter um 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 (GAO, 2013; GIT, 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 et al., 2009), ideia que parece ser comprovada pelo crescente número de incidentes nas IC norte-americanas (ICS-CERT, 2014). De acordo com o recente inquérito da SANS (Luallen, 2013), os operadores dos ICS estão cientes desta conjuntura. Dos 700 participantes, 70% respondeu que os riscos para os seus sistemas são médios ou elevados, e cerca de 30% afirmou suspeitar já ter sido vítima de algum tipo de incidente de segurança.

5. RELEVÂNCIA SOCIAL

Não é apenas a interligação dos sistemas SCADA ao exterior que é motivo de preocupação, pois mesmo os ICS isolados fisicamente têm sido alvos de ataques planeados especificamente contra eles. De modo geral, as IC são alvo de diversos ataques e as poucas notícias que surgem na comunicação social são apenas a ponta de um iceberg que esconde uma diversidade de acções criminosas e terroristas. As IC desempenham um papel preponderante na garantia do bem-estar dos cidadãos, disponibilizando bens e serviços básicos como energia, água e transportes. Contudo, a segurança das IC não é importante apenas para os cidadãos, é também essencial para a sociedade a nível nacional e global, pois uma perturbação no seu funcionamento pode afectar os próprios Estados, influenciar a confiança da opinião pública, e contribuir decisivamente para a Defesa Nacional. Na realidade, as IC fornecem, entre outras coisas, o suporte para a comunicação e interacção económica e social, sem as quais a nossa sociedade não existiria.

5.1 Ameaças

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 para 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 em 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.

5.1.1 Definição de Ameaça

Uma ameaça é tipicamente encarada em função da intenção e da capacidade efectiva para a concretizar (Peerenboom & Fisher, 2007). O Livro Verde do PEPIC considera que uma ameaça é definida como sendo “qualquer indicação, circunstância ou evento com potencial

para perturbar ou destruir uma IC ou um dos seus elementos. (…) Pode também ser definida como a intenção ou capacidade de um adversário para desencadear acções prejudiciais aos activos críticos" (Commission, 2005). Numa outra perspectiva, os norte-americanos consideram que uma ameaça é "uma ocorrência natural ou artificial, individual, colectiva, ou acção que tem ou indica ter o potencial para prejudicar a vida humana, informação, operação, o ambiente e/ou propriedade" (DHS, 2010). Em suma, no âmbito de definição de risco, como veremos mais à frente, uma ameaça é normalmente entendida como a possível exploração de uma vulnerabilidade (NERC, 2010). Por outro lado, neste âmbito da PIC, o documento primordial já várias vezes citado (Marsh, 1997), identificou a existência de dois tipos de ameaças; as físicas e as cibernéticas.

5.1.2 Ameaças Físicas

Há muitos anos que é conhecido o interesse de diversos grupos terroristas nas vulnerabilidades das infraestruturas públicas e privadas dos países ocidentais, tal como ficou demonstrado aquando da descoberta, no Afeganistão, de um computador com dados estruturais das barragens dos EUA (Shea, 2003). Notícias mais recentes[18] 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. Esta intrusão, fez subir as preocupações sobre um eventual ataque à infraestrutura da rede eléctrica norte-americana.

Desde os ataques terroristas de Setembro de 2001 que aumentaram os avisos relativamente à possível ocorrência de ataques terroristas contra as IC, explorando umas das suas múltiplas vulnerabilidades informáticas mas também provocando a sua falha por meios cinéticos (GAO, 2004). As IC estão expostas a um vasto leque de ameaças físicas; ataques terroristas, falhas técnicas, acidentes com materiais perigosos, criminalidade, vandalismo, e desastres climáticos como cheias, furacões, incêndios ou sismos. Todavia, embora as ameaças contra as IC sejam muito variadas, neste trabalho vamos dar especial atenção às ameaças cibernéticas. Na realidade, enquanto as ameaças físicas, como os desastres naturais, ocorrem

[18] 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

aleatoriamente e com intervalos muito grandes, as ameaças cibernéticas ocorrem presentemente a um ritmo quase diário e com crescente intensidade.

5.1.3 Ameaças Cibernéticas

Em Julho de 2002, o *U.S. Naval War College* realizou um exercício de simulação chamado *Digital Pearl Harbor* envolvendo profissionais das TIC e das diversas áreas de negócio que controlavam parte das IC norte-americanas. O objectivo era desenvolver um cenário para responder a eventos de ciberterrorismo constatando-se que, no final, 79% dos participantes afirmaram ser plausível a ocorrência de um ciberataque com impacto estratégico nos anos seguintes (Caldwell & Hunter, 2002). No entanto, importa também registar o facto de os mais cépticos concluírem que o resultado do exercício mostrava a baixa probabilidade de ocorrência de um cenário desse tipo nos EUA (Wilson, 2008).

A evolução posterior dos acontecimentos veio no entanto dar razão aos primeiros, à medida que os ciberataques se foram intensificando e revelando o seu carácter "epidémico", no sentido em que um sistema afectado pode rapidamente afectar toda a rede a que está ligado (Lewis, 2006). As definições vagas na área da cibersegurança deixam em aberto a possibilidade da existência de diversas interpretações dos factos e das ameaças potenciais. Ou seja, como se resume na Figura 9, existem diferentes percepções relativamente a quem ameaça e ao que está a ser ameaçado.

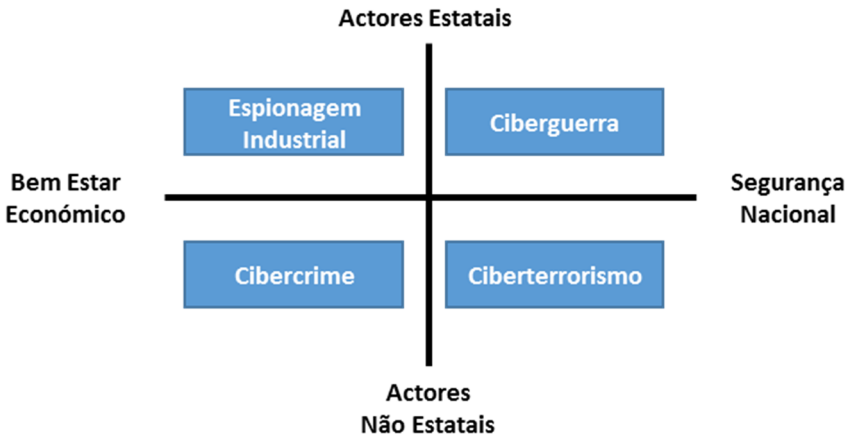


Figura 9 - Percepção do impacto e natureza das ameaças. Adaptado de (CSS, 2009a).

Em 2009, foi realizado um inquérito (Baker et al., 2009) no qual participaram cerca de 600 profissionais das TIC e responsáveis pela segurança das IC de diversos sectores em 14 países, que responderam a uma série de questões sobre os seus procedimentos de segurança e sobre a situação das suas infraestruturas. Embora em caso de ciberataque a atribuição seja

sempre um tremendo desafio, a maior parte dos proprietários e operadores das infraestruturas acreditava que governos estrangeiros estavam já envolvidos em ataques a IC no seu país. Além disso, reconheceram a existência de um número crescente de ataques motivados por simples vandalismo, e de outros com intuitos de extorsão financeira, efectuados por cibercriminosos.

A interdependência cibernética entre organizações é hoje um lugar-comum, e, como já vimos, estas relações são a origem de boa parte das vulnerabilidades das IC. Não há dúvida que as ciberameaças proliferam, tentado explorar todas estas dependências e vulnerabilidades (Cornish, Livingstone, Clemente, & Yorke, 2011). Estas ameaças, contra os sistemas que sustentam as IC, estão a evoluir e crescer, podendo ser intencionais e acidentais. As primeiras, podem ser causadas por grupos criminosos, funcionários descontentes, espionagem ou terroristas, e as últimas podem ser provocadas por procedimentos de manutenção ou alterações do *software* que inadvertidamente provocam uma disrupção dos sistemas (GAO, 2012). A ameaça global dos ataques cibernéticos continua a ganhar relevância, de tal maneira que o *World Economic Forum* lhe deu destaque nos seus últimos dois relatórios (WEF, 2013, 2014).

5.1.4 Outras Ameaças

O processo de identificação de ameaças é inevitavelmente condicionado pela percepção dos decisores que têm que investir recursos para mitigar a ameaça. Esta subjectividade reflecte-se muitas vezes na recusa em assumir a necessidade de investir mais em segurança, aceitando os riscos inerentes. Os executivos geralmente acreditam que empenham os recursos adequados para proteger os seus sistemas. Num estudo já citado, apenas um terço dos executivos inquiridos assumiu a total ou parcial inadequação dos recursos que estava a atribuir à segurança global dos seus sistemas (Baker et al., 2009)

Numa outra perspectiva, além das ameaças tecnológicas, há que considerar também o papel preponderante do elemento humano. Segundo Lewis, as falhas humanas são a vulnerabilidade mais frequente num típico sistema SCADA (Lewis, 2006). A ameaça dos funcionários descontentes é a principal fonte de crimes informáticos. Um funcionário não necessita grandes conhecimentos técnicos, uma que vez que o seu conhecimento interno do sistema permite-lhe ter acesso privilegiado e provocar grandes danos ao mesmo (GAO, 2004). No contexto das IC, os funcionários descontentes, que estão na posse de informação

sobre ICS, são uma ameaça maior que as tentativas externas para violar os procedimentos de segurança (Shea, 2003). Num inquérito conduzido em 2003, 77% dos inquiridos considerou que os funcionários descontentes eram a principal ameaça aos seus sistemas (GAO, 2004). Em suma, a PIC tem obrigatoriamente que ter em linha de conta todas as ameaças; naturais e artificiais, intencionais e acidentais, internas e externas.

5.2 Impacto

A nível europeu considera-se que os impactos são a soma total dos diferentes efeitos de um incidente, tendo em conta um conjunto de aspectos qualitativos e quantitativos como o âmbito, a gravidade, a população afectada, o impacto económico, o ambiente, o efeito politico, as interdependências, os efeitos psicológicos e a duração temporal (Commission, 2005). O alerta sobre a dimensão das ameaças às IC foi oficializado quando, em 1997, o governo norte-americano reconheceu que um comando enviado através de uma rede informática a um computador responsável por assegurar o controlo de uma IC poderia ser tão devastador quanto uma mochila cheia de explosivos, e o agressor seria mais difícil de identificar (Marsh, 1997). Esta preocupação foi sendo sistematicamente transmitida às autoridades norte-americanas, realçando-se sempre nestes casos 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 sinergético e as múltiplas dependências que as diversas IC têm entre si, sempre foi motivo de grande preocupação.

Por isso mesmo, alguns especialistas lançaram o alerta sobre a possibilidade real e iminente de acontecimentos em cadeia puderem conduzir a uma situação em que o colapso de uma IC levaria à falha de muitas outras. Este cenário, é aquele que suscita maior apreensão entre os especialistas, ou seja, a ocorrência de um ciberataque, lançado contra uma IC em combinação com um ataque físico, por exemplo, terrorista. Foi precisamente no contexto da ameaça terrorista que as autoridades norte-americanas consideraram que um ataque a uma IC poderia desencadear três tipos de efeitos (DHS, 2003):

- 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 verosímil a considerar é ocorrência de um ataque bombista convencional 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 afectando um 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 também amplificar bastante o impacto de uma calamidade numa IC (GAO, 2012).

No entanto, importa reconhecer que 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 degradação ou mesmo interrupção total dos serviços básicos que suportam o quotidiano das modernas sociedades. 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. Noutro tipo de situações mais complicadas, um ataque contra os sistemas de controlo de uma instalação química pode causar danos físicos sobre uma área alargada (Shea, 2003). A percepção da existência de uma gama alargada de impactos, 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 um 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.

Nos últimos anos, conforme já foi possível constatar, 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 perturbar, não só a sua área de negócio, mas também 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. 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 ataques desta natureza, 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 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[19] do DNS até aos simples *routers* dos ISP[20] regionais, são 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 et al., 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). Em Março de 2007, investigadores norte-americanos levaram a cabo uma experiência chamada *Aurora Generator Test* onde demonstraram a possibilidade de um ciberataque afectar e destruir os sistemas de controlo dos geradores normalmente utilizados na rede eléctrica (Wilson, 2008). Num vídeo 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.

Já em 1997, o presidente dos EUA foi informado acerca dos efeitos da desregulação e concorrência em muitas IC industriais. Nesse relatório (Marsh, 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, possa vir a ser 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

[19] 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 13 servidores lógicos, desde Junho de 2013, por motivos de redundância, existem 374 servidores físicos dispersos por diversos países.

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

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).

Esta realidade tem sido abordada em diversos estudos conduzidos nos EUA, por exemplo, sob a designação de "alto impacto, baixa frequência" (em inglês, *High-Impact Low-Frequency* – HILF). 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. A nível europeu, esta vulnerabilidade ficou bem patente no apagão italiano de 28 de Setembro de 2003 quando, na sequência de uma tempestade nos Alpes, uma linha eléctrica foi cortada acabando por mergulhar a maior parte da península italiana no caos. O apagão que se seguiu bloqueou milhares de pessoas dentro de carruagens de metro, interrompeu o tráfego devido à ausência de semáforos, cortou o abastecimento de água e parou linhas de produção industriais causando avultados prejuízos. Um outro exemplo emblemático do impacto provocado por efeitos em cascata foi o ocorrido na rede eléctrica europeia em 2006. Uma quebra registada numa linha de alta voltagem na Alemanha resultou em graves interrupções de serviço em França e Itália, além de afectar outros países como Portugal e Espanha, propagando-se até Marrocos ao afectar o funcionamento de um cabo submarino (Högselius et al., 2013). Embora não tenham sido provocados por ataques cibernéticos, estes e outros incidentes ilustram claramente o impacto do efeito em cascata resultante das omnipresentes interdependências.

Em 2010, o mundo foi surpreendido pela descoberta do Stuxnet[21], a primeira ciberarma realmente desenvolvida para ser usada contra uma nação estrangeira. Esta arma cibernética,

[21] O Stuxnet é um *worm* concebido especificamente para atingir as unidades de enriquecimento de urânio do Irão, em Natanz. 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

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 10.

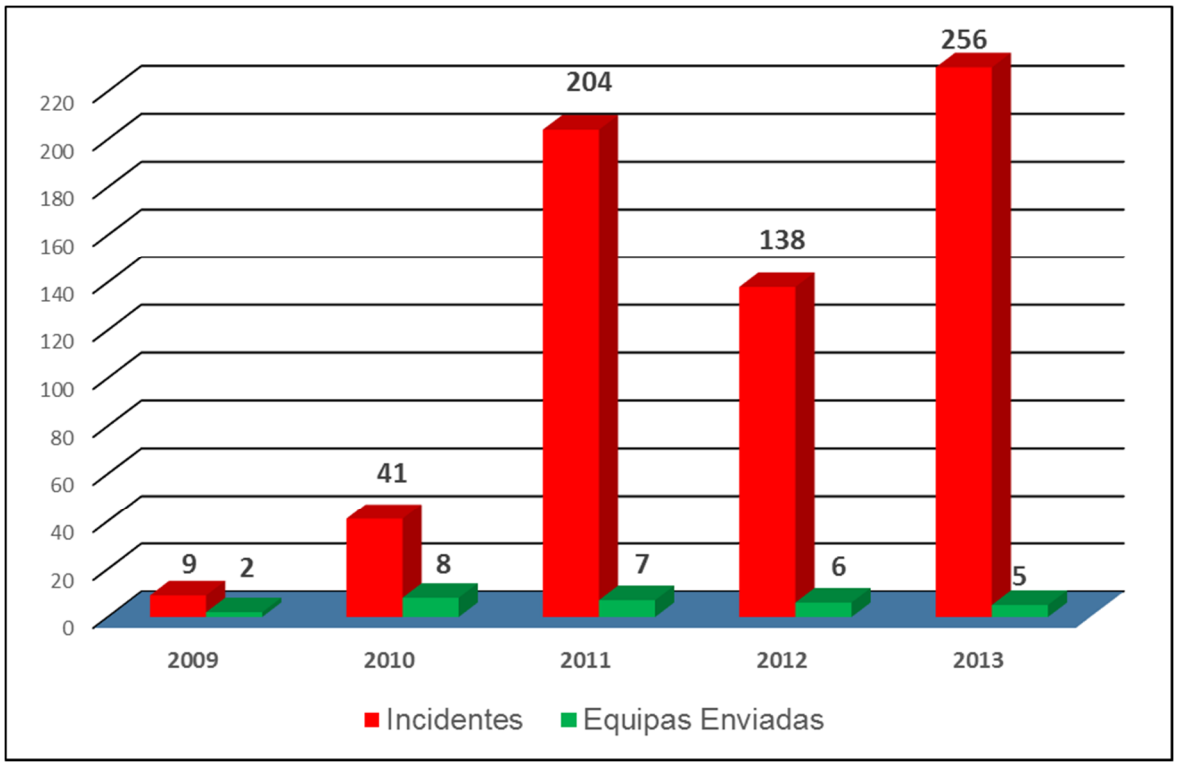


Figura 10 - Evolução do número de incidentes informáticos nas IC dos EUA. Fonte: (ICS-CERT, 2012, 2013, 2014)

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, 2014).

informáticos na medida em que não necessita "infectar" um outro programa para se multiplicar, sendo completamente independente. O Stuxnet 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 foi 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.

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 (Marinos & Sfakianakis, 2013) e de grupos de trabalho independentes (Hämmerli & Renda, 2010). No Anexo III pode ser consultada uma breve listagem de alguns incidentes cibernéticos ocorridos nos últimos anos.

6. RISCO SOCIAL

O primeiro passo para um incremento na segurança dos processos e sistemas de controlo modernos é a compreensão aprofundada dos riscos existentes actualmente no âmbito da segurança electrónica. Só assim se poderão tomar decisões estratégicas informadas relativamente aos níveis apropriados de segurança necessários em cada um dos contextos organizacionais. Evoluímos de uma situação em que os riscos deixaram de ser localizados e passaram a ser globais, o que levou a que as ameaças deixassem de ser encaradas de forma isolada para passarem a ser geridas de um modo integrado, pois é esta a única forma de responder eficazmente ao aumento das vulnerabilidades. Uma vez que aquilo que está em jogo no caso das IC é a potencial perda de vidas humanas, considera-se que o risco associado a estas infraestruturas é um risco social. Nos capítulos 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. Portanto, a questão não é saber se há ou não riscos associados às IC; o problema reside em identificá-los, avaliá-los e geri-los de forma realista e eficaz. A gestão do risco consiste normalmente em evitá-lo, controlá-lo, transferi-lo ou, simplesmente aceitá-lo.

6.1 Definição de Risco

Há semelhança do que ocorre com outros termos, o conceito de "risco" tem sido alvo de uma considerável flexibilidade interpretativa. Diversos estudos quantitativos definem estritamente risco como sendo a probabilidade de um evento indesejável, multiplicada pelo seu impacto. (Högselius et al., 2013). Num contexto muito mais lato, o conceito de "risco de desastre"[22] pode ser definido como sendo o potencial para efeitos adversos da ocorrência de um evento perigoso específico, que é derivado da combinação de ameaças físicas, exposição e vulnerabilidades (Hazards, Science, & Academies, 2012). Esta definição engloba quatro componentes; ameaça, exposição, vulnerabilidade e consequência mas, como veremos em seguida, o mesmo conceito pode ser enunciado de forma mais simplificada.

[22] Em inglês, *disaster risk.*

Na realidade, é vulgar considerar-se que os riscos incluem apenas três componentes; ameaça, vulnerabilidade e consequência. Ou seja, o risco é uma função da probabilidade de uma dada ameaça explorar uma potencial vulnerabilidade e do impacto resultante de uma exploração bem-sucedida dessa vulnerabilidade (Stouffer et al., 2013). 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. Nesta visão, o risco é a combinação de duas probabilidades; a probabilidade de existir uma ameaça capaz de localizar e explorar a vulnerabilidade e a probabilidade de a ameaça conseguir consumar a sua tentativa de exploração (GAO, 2004). Ou seja, o risco é o potencial para um resultado indesejado resultante de um incidente, evento ou ocorrência, conforme determinado pela sua probabilidade e as consequências a ele associadas (DHS, 2010).

A nível europeu, o Livro Verde do PEPIC define risco apenas como a possibilidade de perdas, danos ou ferimentos, sendo o nível de risco uma função de dois factores: o primeiro é o valor atribuído ao activo pelo seu proprietário ou operador e o impacto da sua perda ou modificação, e o segundo é a probabilidade de uma vulnerabilidade específica ser explorada por uma determinada ameaça (Commission, 2005). Apesar da existência de visões estritas e latas do conceito de risco, este conceito e o de "risco social" têm-se tornado muito abrangentes pois as sociedades modernas estão cada vez mais a responder aos riscos tecnológicos resultantes do acelerado processo de modernização que afecta a própria estrutura social (Högselius et al., 2013).

A norma ISO 31000[23] define o risco como sendo "o efeito da incerteza nos objectivos". Nesta definição, a incerteza inclui eventos de ocorrência incerta, e incertezas causadas pela ambiguidade ou falta de informação. Além disso, contempla ainda os impactos negativos e positivos nos objectivos a atingir. A adopção desta norma implica que os gestores de risco têm que aplicar metodologias de tratamento do risco que lidem convenientemente com a incerteza na obtenção dos objectivos, sejam estes quais forem. Mas, no âmbito das IC, não deixa de se considerar a possibilidade de ocorrência dos riscos e, por isso mesmo, é também habitualmente aceite a definição de risco da norma ISO 27005[24], que define os riscos como derivando do potencial para que uma determinada ameaça explore vulnerabilidades de um

[23] ISO 31000: 2009/ISO Guide 73 (Risk Management – Vocabulary).
[24] ISO/IEC 27005:2011 (Information technology - Security techniques - Information security risk management)

activo ou grupo de activos, causando danos à organização. Esta definição, mais simples mas também mais abrangente, é compatível com a maioria das outras definições, boas práticas e normas existentes na literatura, sendo frequentemente referida em documentos da ENISA (Marinos & Sfakianakis, 2013).

6.2 Identificação dos Riscos

As definições de risco atrás enunciadas implicam que a identificação do risco tem obrigatoriamente que ser precedida por uma identificação de ameaças e vulnerabilidades. Todavia, como já vimos, as vulnerabilidades das IC são extremamente complexas e evolutivas. Assim, é muito difícil, senão mesmo impossível, realizar uma análise rigorosa que permita identificar completamente todas as potenciais ameaças que pairam sobre as IC. Da mesma forma, a teia de interdependências tem um comportamento imprevisível o que dificulta imenso a tarefa de identificar com clareza todos os eventuais impactos de um incidente nos serviços fornecidos por uma IC. A identificação do risco é também condicionada por requisitos legais que impõem níveis mínimos de funcionamento e o cumprimento de regras de segurança. As falhas podem surgir de diversas formas e ser provocadas por uma miríade de causas. Na maior parte dos casos, são intencionalmente provocadas por vândalos, criminosos ou terroristas, acidentalmente provocadas por desastres naturais ou erros humanos ou ainda devido a erros de decisão dos engenheiros, dos gestores ou dos reguladores. Com a sociedade focada na ameaça terrorista, nunca é de mais recordar que a maior parte dos incidentes de grande impacto foi provocada por desastres naturais ou por erros humanos. Quando há responsabilidade humana, os problemas ocorrem frequentemente devido a elementos internos (Cukier, 2005).

Uma ferramenta útil para a identificação de riscos é a análise de registos históricos relativos a incidentes do passado. Mas embora estes registos possam ser importantes, a sua utilidade é limitada pois existem condicionalismos para a sua utilização. Por um lado, de pouco servirá analisar os efeitos de um fenómeno natural ocorrido há mais de cinquenta anos uma vez que o mundo nessa altura era radicalmente diferente daquilo que é hoje. As mudanças climáticas em curso nos nossos dias levantam questões importantes acerca da validade da interpretação de dados históricos, nomeadamente no que diz respeito à intensidade de furações e cheias (Hazards et al., 2012). Por outro lado, os dados históricos têm um interesse muito limitado no contexto dos riscos informáticos pois o ritmo da mudança é de tal ordem acelerado que quase diariamente são conhecidas novas vulnerabilidades e, consequentemente, surgem

novas ameaças. Neste contexto, a identificação dos riscos actuais, e daqueles que podem surgir no futuro, deverá ser conseguida à custa de processos de cenarização e de exercícios de simulação.

6.3 Avaliação dos Riscos

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. Assim, a avaliação do risco é o processo de identificação dos riscos para os indivíduos, para o funcionamento e para os activos de uma organização, através da determinação da probabilidade de uma vulnerabilidade identificada poder ser explorada e da avaliação do impacto daí resultante. Esta estimativa do risco, inclui uma avaliação dos controlos de segurança que podem mitigar cada ameaça assim como dos custos associados à sua implementação, comparando os encargos da segurança com as perdas associadas a um incidente (Stouffer et al., 2013). 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).

Existe um número significativo de metodologias para a avaliação do risco em IC e, de uma forma geral, o método utilizado é linear: classificação das ameaças, identificação das vulnerabilidades e avaliação do impacto. Esta é uma abordagem já consolidada para a avaliação de risco e constitui a base de quase todas as metodologias existentes (Giannopoulos, Filippini, & Schimmer, 2012). No entanto, muitas organizações têm grande dificuldade em avaliar correctamente o nível de risco a que estão expostas (Cornish et al., 2011). 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).

A avaliação do risco é subjectiva pois nem todos os *stakeholders* concordam relativamente à probabilidade de ocorrência um ataque cibernético, nem quanto ao impacto provocado por este. Assim, além da percepção da criticidade temos também a subjectividade do risco. Contrastando com o facto de não existir uma definição universalmente aceite para "risco", parece existir uma banalização da avaliação do risco em função de um "valor esperado". Esta prática é agravada pelo facto de, na sociedade actual, o valor das coisas ser gradualmente substituído pelo preço das mesmas (Pais, Sá, Lopes, & Oliveira, 2012). Além disso, avaliar o risco em função da probabilidade de ocorrência de incidentes tem outras limitações que se prendem com a nossa percepção, muitas vezes distorcida, de perigosidade.

Estes factores psicológicos e emocionais, que definem a percepção do risco, têm um profundo impacto no comportamento das comunidades (Hazards et al., 2012). Por exemplo, no que toca ao risco sísmico, existe no público em geral e nas próprias autoridades, a noção de que um evento sísmico de consequências sérias só voltará a ocorrer num horizonte temporal para lá das nossas vidas (Pais et al., 2012). Segundo Bouchon (2006), surgiram diversos mal-entendidos quando se transferiram as noções associadas ao risco da área das ciências exactas para as ciências sociais, pois com esta transição surgiu a necessidade de incluir factores como as condições políticas, económicas e sociais na sua análise. Todavia, é hoje geralmente aceite que o risco tem que ser encarado numa perspectiva social, pois depende da forma como é percepcionado pela sociedade. Assim, é necessário distinguir entre "risco real" e "risco percepcionado" porque, embora possam ser muito diferentes, são ambos igualmente importantes para a avaliação do risco.

Isto leva a que as decisões estratégicas para lidar com o risco sejam tomadas em função dos papéis e responsabilidades dos decisores, das influências que sofrem e das opções políticas que dispõem. Nas mesmas condições, expostas a ameaças semelhantes, comunidades diferentes podem desenvolver estratégias e políticas diametralmente opostas para a redução do risco (Hazards et al., 2012). Existe uma grande diferenciação entre as diferentes metodologias de avaliação do risco consoante o âmbito em que são utilizadas, a audiência a que se destinam (decisores políticos, investigadores académicos, etc) e o seu domínio de aplicabilidade (a nível de activos, de infraestrutura ou do sistema global de infraestruturas.). Estes atributos não são mutuamente exclusivos no sentido em que o domínio de aplicabilidade define também a audiência a quem se destina a metodologia. Por exemplo, uma metodologia de avaliação de risco aplicável a grandes sistemas transnacionais será

dirigida a decisores políticos e não a operadores locais (Giannopoulos et al., 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. A amplitude do 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 até agora 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, alargando e expondo as suas vulnerabilidades o que, na opinião das autoridades australianas, obriga ao desenvolvimento de uma nova metodologia de avaliação do risco específicamente para estes sistemas (ITSEAG, 2012). Ou seja, não existe um consenso sobre o risco em sistemas ciber-físicos o que leva a que este seja estimado de forma ad-hoc, sector a sector, sem que existam soluções coerentes para quantificar e gerir o risco. Por exemplo, será que a rede eléctrica, distribuída e com grande dispersão de clientes, está mais ou menos exposta ao risco que uma indústria química local, com uma pequena população na vizinhança? Em muitos casos, as metodologias de avaliação de risco aplicadas às IC são adaptações de outras que foram desenvolvidas para aferir riscos dentro do ambiente confinado de uma organização. Consequentemente, estas metodologias talhadas para as necessidades destas organizações são tendenciosas, pois só consideram parte das ameaças relevantes (Giannopoulos et al., 2012).

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. Assim, e considerando o espectro total de ameaças sobre as IC, a única alternativa que nos parece ser viável é a de ser adoptada uma abordagem abrangente da análise do risco, tal como se pode ver na Figura 11.

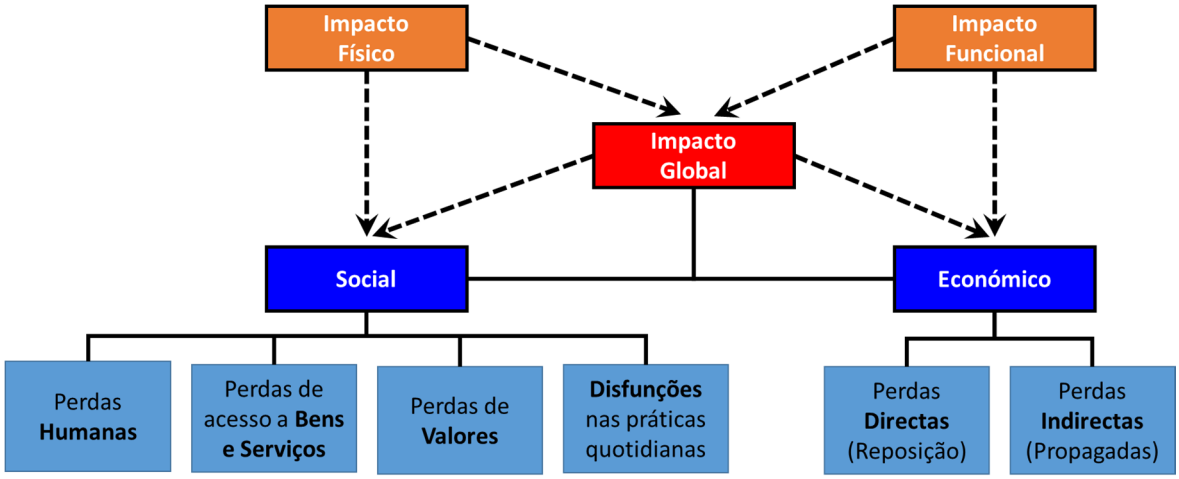


Figura 11 - Perspectiva Holística da Análise de Risco. Adaptado de (Pais & Sá, 2009).

É provável que um sistema de baixo risco necessite menores medidas de protecção 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. 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 própria prática da gestão do risco, de modo a possibilitar uma abordagem uniforme à problemática da protecção das IC (ENISA, 2011a). As metodologias de avaliação de risco a nível europeu não têm o mesmo nível de maturidade, em termos de eficácia e abrangência, que as suas congéneres dos EUA, o que não é surpreendente se tivermos em consideração a dispersão das IC europeias por diferentes países com diferentes culturas e posturas relativamente às questões de segurança (Giannopoulos et al., 2012).

6.4 Gestão do Risco

O risco de uma falha cibernética, seja devida a um problema de software, a uma acção maliciosa, a uma avaria mecânica, ou até mesmo a um fenómeno atmosférico, é um problema sério para a actual sociedade. Sendo hoje universalmente aceite que é impossível anular completamente o risco, a solução passa então por encontrar formas apropriadas de geri-lo.

6.4.1 Definição

Em termos genéricos, a gestão do risco consiste em medir e avaliar o grau de risco existente na operação normal de qualquer processo (Bagheri & Ghorbani, 2008). Ou seja, é um processo de identificação, análise, priorização e mitigação de potenciais danos para a estrutura, funcionamento ou objectivos de uma organização (Cornish et al., 2011). Na prática, a gestão do risco é um processo contínuo que identifica as ameaças que potencialmente poderão afectar uma comunidade, avalia os seus impactos, desenvolve e implementa estratégias de gestão, reavalia e revê essas estratégias e desenvolve e ajusta as políticas de gestão dos riscos (Hazards et al., 2012).Ou seja, tal como definido na norma ISO 31000, são as actividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco.

Existem diversas metodologias de gestão do risco que maioritariamente se integram no conjunto de técnicas que induzem a organização dos sistemas e, baseadas nessa informação, identificam vulnerabilidades e ameaças (Bagheri & Ghorbani, 2008). Estas técnicas não estão restritas ao campo das IC, na realidade na sua maioria foram adoptadas de outras áreas de estudo e adaptadas para a PIC. De entre todas as definições de gestão de risco existentes parece-nos que uma das que melhor resume todos os conceitos fundamentais é a utilizada pelas autoridades britânicas que consideram que a gestão do risco é um processo de identificação, compreensão, gestão, controlo, monitorização e comunicação do risco (Office, 2011). Mas ainda mais abrangente, é a definição utilizada pelas oficialmente autoridades norte-americanas que definem a gestão do risco como sendo o processo de identificação, análise, avaliação, comunicação de risco com vista a aceitá-lo, evitá-lo, transferi-lo ou controlá-lo num nível aceitável considerando os custos e benefícios das acções tomadas (DHS, 2010).

6.4.2 Objectivos

De forma genérica, todas as técnicas de gestão de risco são baseadas na definição restritiva que considera apenas a probabilidade de um evento ocorrer e a multiplica pela medida das suas consequências. Esta é a abordagem preferida por muitos decisores pois é baseada nas mesmas premissas teóricas que suportam outros tipos de análise económica e pode ser aplicada a situações com grande grau de incerteza (Yohe, 2010). Nos últimos anos o âmbito das disrupções e crises tem sido alargado e, devido à crescente interligação e

interdependência das infraestruturas, os seus impactos têm aumentado. Internacionalmente, os governos têm respondido a este novo ambiente de risco adoptando gradualmente abordagens do tipo "todos os riscos"[25] para as políticas e práticas relativas às IC. Estas abordagens focam-se na gestão da incerteza do ambiente de risco através da criação de resiliência contra os riscos conhecidos e os imprevistos.

Ou seja, em vez de se focar na probabilidade de ocorrência de ameaças específicas, uma abordagem de resiliência *all-hazards* centra-se nas prováveis consequências da falha de uma activo específico, rede, ou outra componente da infraestrutura, e tenta mitigá-las. Uma abordagem deste tipo engloba ainda a noção que planear para um tipo de risco ou desastre pode também pode também aumentar a resiliência face a outro tipo de evento. Na realidade, diferentes eventos podem ter impactos semelhantes nas infraestruturas. Por exemplo, tanto os fogos florestais como as inundações podem provocar quebras no fornecimento de energia eléctrica (Office, 2011). Em suma, o objectivo de avaliar os riscos de forma abrangente (abordagem *all-hazards*) é garantir os níveis adequados de protecção para todas as IC, a minimização dos pontos de falha e a existência de procedimentos de recuperação rápida (Gendron, 2010).

No que diz respeito aos desastres naturais, como já vimos, os registos históricos são de utilidade muito limitada neste contexto. O impacto provocado por desastres do passado não pode servir como referência para o futuro. Por um lado, a sociedade e os seus sistemas de suporte são cada vez mais interdependentes. Por outro lado, as mudanças no ambiente físico, provocadas pelas alterações climatéricas em curso, sugerem que a probabilidade e os impactos futuros podem subir (Hazards et al., 2012). Assim, a resposta às mudanças climáticas requer uma abordagem à gestão de risco na qual a adaptação e a mitigação sejam vistas como parte de um processo iterativo que explicitamente entre em linha de conta com as mudanças ao longo do tempo e as tenha em consideração para efectuar as necessárias correcções (Yohe, 2010). A ideia que as sinergias originadas por uma abordagem comum a todas as ameaças irá fornecer o nível de segurança necessário é questionável, mas atractivo, em face dos finitos orçamentos para segurança e da consciência de que a prevenção de ataques pode nem ser possível em face da miríade de ameaças (Gendron, 2010).

[25] Em inglês, *all-hazards*.

A consequência, segundo as autoridades alemãs, 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 (BMI, 2009). 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. 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, 2011a).

Existem quatro estratégias normalmente utilizadas para a gestão de risco: prevenir, transferir, controlar e aceitar (DHS, 2010). No âmbito das IC, como já vimos, é impossível eliminar totalmente os riscos, e muito difícil transferi-los. Ou seja, restam apenas a redução dos riscos minimizando tanto quanto possível as vulnerabilidades, e a aceitação do risco residual. Assim, a escolha das estratégias de gestão de risco requer uma regular reavaliação dos novos dados e modelos dos riscos e das mudanças nas características socioeconómicas e demográficas de uma sociedade. Embora o risco residual seja omnipresente, as estratégias de gestão de risco podem contribuir para o desenvolvimento da resiliência a desastres, disrupções e crises. Ou seja, podemos concluir que as bases para a construção da resiliência a desastres de qualquer tipo são a compreensão, a gestão e a redução dos riscos (Hazards et al., 2012).

6.4.3 Aceitação do Risco

É hoje consensual afirmar que a eliminação total do risco não passa de uma utopia. Esta unanimidade deriva em boa medida daquilo a que já chamaram o "paradoxo das IIC", mas que é também aplicável às IC. Isto é, seja qual for o nível de segurança e protecção que se aplique, as vulnerabilidades e o risco de falha não são completamente eliminados. As formas tradicionais de resolver estes problemas — através de tecnologia, mercados ou regulação — não funcionam. A tecnologia é insuficiente, os mercados não funcionam e os governos têm sido relutantes em agir (Cukier, 2005). Ou seja, tal como reconhecido num relatório

elaborado pelas autoridades suíças, a protecção total de todas as IC, contra todas as ameaças e riscos, é impossível, não só por razões técnicas mas também por motivos financeiros (CSS, 2008). 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).

Atingir um nível aceitável de risco é um processo que consiste em reduzir a probabilidade de ocorrência de incidentes através da mitigação, ou eliminação, de vulnerabilidades e dos potenciais impactos da sua exploração. Consequentemente, a priorização de vulnerabilidades deve ser baseada no custo e benefício de modo a introduzir essa variável no modelo de negócio, com vista a possibilitar a implementação de controlos de segurança (Stouffer et al., 2013). Na prática, 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 pelas autoridades norte-americanas num relatório dando conta 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). Se o risco não pode ser completamente eliminado a consequência directa é a necessidade de acções de gestão para lidar com o risco residual. A existência de riscos diversificados, tecnológicos, naturais, acidentais, intencionais, implica forçosamente que a única abordagem possível seja do tipo ***all-hazards***. No entanto, um facto permanece inquestionável; é impossível proteger completamente um sistema de todas as ameaças. Assim, uma boa gestão destes riscos deve seguir uma abordagem holística, com foco específico na determinação do balanço apropriado entre resiliência, recuperação e protecção (NERC, 2010). Embora todas estas componentes sejam importantes, no contexto actual, a resiliência tem estado no centro das atenções das organizações, e dos próprios Estados, destacando-se a sua importância no processo global de gestão do risco.

6.5 Resiliência

Nos últimos anos o conceito de resiliência assumiu um papel fulcral no domínio da protecção civil, sendo aplicado em diferentes sectores como prevenção de emergências, resposta a

desastres, cibersegurança e PIC. A utilização generalizada do conceito tem originado diferentes interpretações e, baseadas nestas últimas, diferentes estratégias têm enfatizado diferentes aspectos da resiliência e fornecido definições distintas consoante o contexto em que o conceito é aplicado.

6.5.1 Definição

Segundo Bouchon (2006), a expressão "resiliência" refere-se normalmente à capacidade de recuperar de um choque, dano ou perturbação, ou seja, é a capacidade de ser flexível. No entanto, ainda segundo o mesmo autor, a palavra é utilizada de forma distinta em diferentes áreas:

- Na física e na engenharia, a resiliência é definida como sendo a propriedade física de um material que pode regressar à sua forma ou posição original depois de ser sujeito a uma deformação que não excede a sua capacidade elástica;
- Em psicologia é utilizada para descrever a capacidade das pessoas para lidar com o *stress* e com catástrofes;
- No mundo dos negócios, a resiliência é a capacidade de uma organização, recurso ou estrutura para suportar o impacto de uma interrupção do negócio e recuperar e recomeçar as suas operações.

A ênfase nas consequências e na recuperação sugerem que a melhoria da resiliência não é apenas um problema técnico, mas que tem também uma dimensão social (Chang, 2009). Assim, como os serviços básicos têm influência directa no bem-estar económico, segurança e tecido social das comunidades, a resposta inicial e a recuperação rápida estão intimamente ligados à resiliência comunitária. Além disso, o conceito de resiliência, tal como o de infraestrutura, é evolutivo. Na sua enunciação actual, a resiliência comunitária é um atributo primordial que reflecte o grau de preparação de uma comunidade e a capacidade para responder e recuperar de uma catástrofe (O'Rourke, 2007). Ou seja, este conceito refere-se geralmente à capacidade de uma comunidade continuar a funcionar durante e depois de um evento de grande impacto.

No contexto das IC vamos utilizar neste trabalho o conceito de resiliência enunciado pelas autoridades do Reino Unido, e que foi também adoptado pela Austrália. Na formulação britânica, a resiliência é a "capacidade dos activos e das redes para anteciparem, absorverem, adaptarem e recuperarem durante uma disrupção" (Office, 2013) e é conseguida através da combinação dos componentes da Figura 12.

Figura 12 - Componentes da Resiliência. Adaptado de (Office, 2013)

Neste conceito, a Resistência refere-se à protecção física directa, a Fiabilidade à capacidade da infraestrutura de continuar a operar sob diversas condições, a Redundância à adaptabilidade de um activo ou rede, e a Resposta e Recuperação à capacidade da organização para responder e recuperar de uma disrupção (Office, 2013). A Figura 13 resume as principais características da resiliência de um sistema.

Figura 13 - Características da Resiliência dos Sistemas. Adaptado de (Bouchon, 2006)

Em suma, a resiliência de um sistema pode ser definida como a "capacidade para se adaptar a condições mutáveis e se preparar para, suportar e rapidamente recuperar de uma disrupção" (DHS, 2010).

6.5.2 Resiliência e Gestão do Risco

Em face da definição de resiliência apresentada no ponto anterior, é obvio que o conceito está relacionado com a gestão de risco mas vai para além deste processo na medida em que assume a existência de eventos inesperados cujos riscos não podem ser mitigados através da clássica análise probabilística do risco (CSS, 2011). Uma gestão de risco eficaz é a chave para o desenvolvimento da resiliência, especialmente quando desenvolvida a nível empresarial, de modo a desenvolver uma cultura organizacional onde a resiliência e a continuidade de negócio sejam integradas nas operações. Isto cria a chamada "resiliência organizacional" que não é mais que a "capacidade de uma organização antecipar, planear e responder a incertezas e disrupções nas operações normais do seu funcionamento" (Office, 2011).

É neste contexto que, segundo outro relatório (CSS, 2011) elaborado pelas autoridades suíças, se consideram as seguintes três perspectivas para analisar a resiliência:

- Como um objectivo da gestão de risco – Nesta opção, a resiliência é o objectivo primordial das políticas de protecção e a gestão do risco é o método para atingir esse fim. Ou seja, a resiliência substitui ou complementa o conceito de protecção como objectivo das actividades de gestão de risco;
- Como parte da gestão de risco – Neste caso, as actividades de fortalecimento da resiliência são necessárias para lidar com o risco residual, isto é, com os riscos que não foram identificados ou foram subestimados e, portanto, não englobados nas medidas de protecção e prevenção;
- Como alternativa à gestão de risco – Esta postura é um desafio aos tradicionais métodos de gestão de risco e promove a resiliência como uma nova forma de lidar com o risco em ambientes complexos. Argumentando que a análise probabilística do risco não é adequada para sistemas socioeconómicos confrontados com riscos dinâmicos e não-lineares. Assim, em vez de prevenir riscos e proteger a manutenção do estado actual, os sistemas que seguem esta orientação desenvolvem a sua resiliência através do aumento das suas capacidades adaptativas.

O exemplo mais notável de adopção desta última opção é o do governo australiano, mas é verdadeiramente excepcional a nível mundial e tem importantes implicações a nível das políticas a ser desenvolvidas (CSS, 2011). A abordagem australiana ao risco nas IC vai para

além da gestão do risco e da continuidade de negócio (que em grande medida se limitam a responder a riscos previsíveis) para responder a riscos imprevistos e imponderáveis (Attorney-General, 2010). Um dos aspectos mais importantes desta postura é o trabalho entre sectores e o desenvolvimento da resiliência organizacional, como se pode ver na figura seguinte:

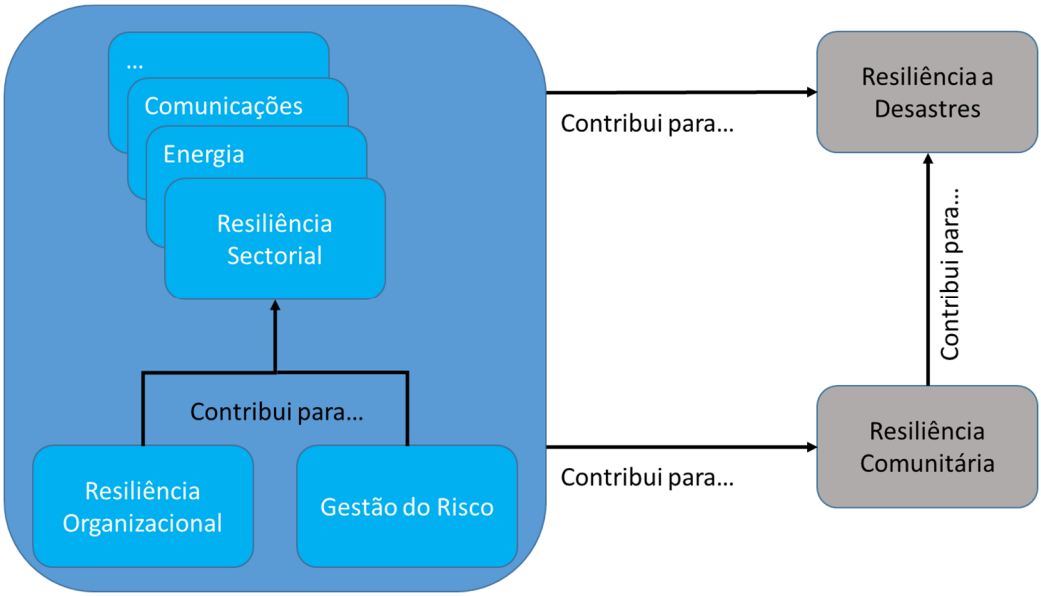


Figura 14 - Relação entre diversos tipos de resiliência. Adaptado de (Attorney-General, 2010)

Por outro lado, se a resiliência for definida com um objectivo da gestão do risco, não há necessidade de alterações substanciais nas estratégias de gestão de riscos já existentes.

Figura 15 - Ciclo de resiliência para proprietários de infraestruturas. Adaptado de (Office, 2011).

No entanto, se a resiliência for integrada no âmbito dos esforços de gestão do risco, as metodologias têm que ser adaptadas, o que significa que a segunda perspectiva sobre a

resiliência tem também um impacto significativo sobre as práticas da gestão do risco (CSS, 2011). A maior parte dos países optam pela segunda abordagem, integrando resiliência como parte da gestão do risco, tal como fazem os britânicos que seguem o ciclo ilustrado na Figura 15. Embora a resiliência pareça estar na ordem do dia, num levantamento exaustivo feito a uma extensa lista de metodologias de gestão do risco, um dos organismos da Comissão Europeia (*Joint Research Centre/Institute for the Protection and Security of the Citizen*) concluiu que a resiliência é o elemento ausente, ou é apenas referido de forma implícita (Giannopoulos et al., 2012).

6.6 Exemplos Internacionais

Importa referir que os aspectos atrás elencados são de utilização generalizada a nível mundial e, por isso mesmo, seguem-se alguns exemplos da sua utilização por diversos países.

6.6.1 Abordagem Holística

As autoridades australianas dão especial ênfase à aplicação de uma abordagem ***all-hazards*** na sua gestão do risco em sistemas SCADA por considerarem ser a mais adequada para a análise da exposição aos riscos provenientes de uma grande variedade de potenciais vulnerabilidades de segurança (ITSEAG, 2012). Como já vimos antes, o governo britânico também considera a abordagem mais abrangente como sendo a que deve ser aplicada no planeamento e preparação da resposta a desastres (Office, 2011, 2013). Além disso, há ainda a salientar um aspecto que nos parece ser de capital importância; o governo britânico considera ser absolutamente desnecessária a duplicação de normas para responder a riscos específicos. Ou seja, a abordagem ***all-hazards*** para a criação de resiliência é a mais apropriada uma vez que, normalmente, diversos riscos ocorrem simultaneamente ou consecutivamente (Office, 2011). Os alemães, tendo em conta que as IC podem estar expostas a variadas ameaças que devem ser analisadas e incluídas na análise de risco, consideram que a escolha de opções para a acção a tomar deve ser apoiada numa abordagem ***all-hazards*** (BMI, 2009).

No Canadá, considera-se que avaliar os riscos de forma integrada, com uma abordagem do tipo ***all-hazards***, pode ser eficaz na redução da vulnerabilidade de pessoas, propriedade, ambiente e economia (Gendron, 2010). Isto é, a gestão de risco com uma abordagem holística ajuda na preparação para uma variedade de eventualidades, desde acidentes naturais a ameaças intencionais (PSC, 2014). Esta postura é também vertida no planeamento

transfronteiriço que o Canadá faz com os EUA no sentido de responder aos riscos e interdependências das suas IC (PSC/DHS, 2010). No lado norte-americano, os mais recentes planos governamentais para esta área são inequívocos na elevação da resiliência a objectivo primário do planeamento de protecção de segurança das IC, enfatizando a necessidade de responder a todos os riscos (DHS, 2013). Em suma, tal como referido num relatório da OCDE, as posturas internacionais face a esta questão tendem a assumir uma abordagem abrangente do risco, considerando um vasto leque de ameaças contra as IC (Gordon & Dion, 2008).

6.6.2 Utilização de Normas Internacionais

Apesar de terem desenvolvido as suas próprias normas e metodologias, no contexto da resiliência a desastres, as autoridades norte-americanas começam gradualmente a reconhecer a vantagem da utilização de normas internacionais para a gestão do risco, nomeadamente, a família ISO 31000, uma vez que permitem a aplicação de uma terminologia uniforme e padronizada a nível internacional (Tsai, 2013). Os australianos, no âmbito da gestão do risco em sistemas SCADA, optam por uma metodologia compatível com as principais normas internacionais como as ISO 31000[26], ISO 27005[27] e ISO 27001[28] (ITSEAG, 2012), tal como se pode verificar na Figura 16.

Além disso, o governo australiano apoia frontalmente a utilização do conjunto de normas ISO 31000 por proprietários e operadores de IC (Attorney-General, 2010). O Canadá alinha também nesta postura e o seu guia de gestão de risco para IC é adaptado da norma ISO 31000 (PSC, 2010). A nível europeu, os alemães usavam como referência para a gestão do risco a norma AS/NZS 4360:2004, antecessora da norma ISO 31000:2009 (BMI, 2008) e os suecos utilizam as normas das séries 27000 e 31000 (MSB, 2010). Os britânicos utilizavam a sua norma BS 25999[29], mas está já em curso a transição para as normas ISO 22301[30] e ISO 22313[31] (Office, 2011). Por último, importa referir que os espanhóis adoptam os guias britânicos para a gestão do risco em sistemas SCADA e em ambiente empresarial, traduzindo e adaptando os seus manuais por meio de um acordo de parceria entre Estados (CCN, 2010a,

[26] ISO 31000:2009, Risk management – Principles and guidelines
[27] ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management
[28] ISO 27001:2013, Information technology— Security techniques — Information security management systems — Requirements
[29] BS 25999, Business Continuity Management
[30] ISO 22301:2012, Societal Security — Business continuity management systems — Requirements
[31] ISO 22313:2012. Societal Security — Business continuity management systems — Guidance

2010b) o que ilustra a superfluidade de produzir novos estudos e documentação sobre um assunto que, embora continue em permanente evolução, já foi amplamente estudado.

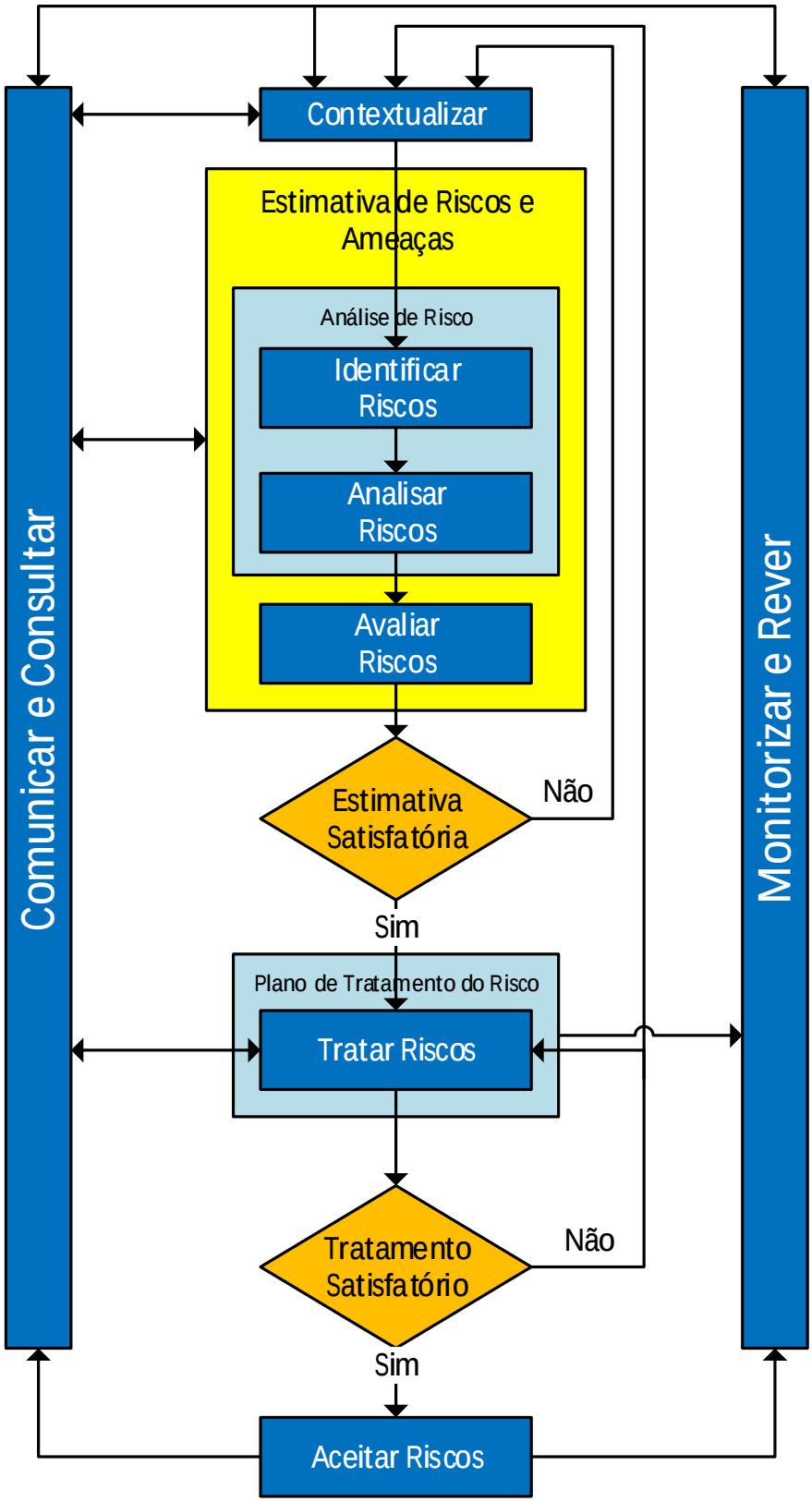


Figura 16 – Gestão de Risco ISO 31000 e ISO 27005. Adaptado de (ITSEAG, 2012).

6.6.3 Ciclo PDCA

A ENISA considera que os métodos de gestão de risco para organizações englobam a capacidade para avaliar riscos associados a alvos específicos — sistemas de informação, aplicações informáticas ou infraestruturas — e depois agir no sentido de mitigar e gerir estes riscos. Para atingir este objectivo, é recomendado que as organizações utilizem um processo iterativo como o ciclo PDCA[32] (ENISA, 2011b). O governo australiano preconiza também a utilização do ciclo PDCA como parte integrante da sua política global de gestão de risco em sistemas SCADA (ITSEAG, 2012), tal como se pode ver na Figura 17.

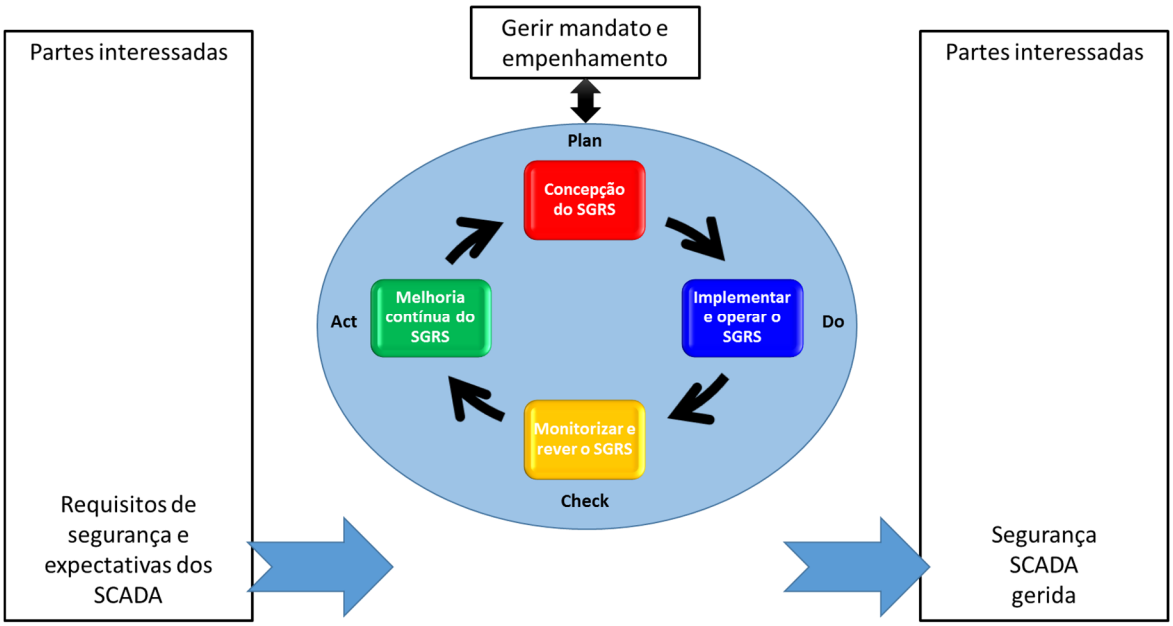


Figura 17 - Ciclo PDCA aplicado ao Sistema de Gestão de Riscos de Segurança (SGRS) em SCADA. Adaptado de (ITSEAG, 2012)

Por último, uma referência às autoridades suecas que, mencionando a utilização do ciclo PDCA em diversas normas internacionais, utilizam-no como referência para as suas actividades rotineiras com o objectivo de melhorar a segurança nos seus ICS (MSB, 2010). Em suma, a utilização de procedimentos padronizados e normalizados a nível internacional parece ser uma prática seguida por países tradicionalmente preocupados com a segurança dos seus sistemas, mas também é uma postura seguida pelas autoridades europeias.

[32] O ciclo PDCA (do inglês *Plan, Do, Check, Act*) é um método iterativo de gestão no qual os quatro passos se repetem ciclicamente visando o controlo e melhoria contínua de processos e produtos. É também conhecido como ciclo de Deming.

6.7 Desafios

Como já foi referido, as dificuldades sentidas pelas empresas em justificar o investimento em segurança não são novas, e a situação não melhorou muito nos últimos anos, continuado 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. 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).

Uma das principais dificuldades que persiste é a utilização de terminologia técnica relativa à gestão que risco que dificulta a sua compreensão tanto por decisores políticos e pelo público em geral. Se a capacidade de gerir o risco é um dos objectivos do aumento da resiliência, o vocabulário do risco tem que ser adaptado de modo a que todos os *stakeholders* possam entender os riscos e as suas potenciais consequências (Tsai, 2013). Esta mesma necessidade foi já sentida a nível europeu na medida em foi detectada a urgência em estabelecer taxonomias e métricas comuns levando possivelmente ao surgimento de uma moldura geral de gestão de risco para as IC e para todo o ciclo da PIC (Hämmerli & Renda, 2010).

Sempre foi impossível proteger completamente um sistema de todas as ameaças, mas agora é cada vez mais difícil identificar exactamente aquilo que deve ser protegido nas IC. É mais 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 mitigado e também não pode ser gerido isoladamente apenas por uma

entidade ou organização. 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).

A avaliação do risco é frequentemente efectuada com recurso a métricas pouco rigorosas para aferir vulnerabilidades, ameaças e potenciais impactos, facto que constitui um problema para todos os países que dependem de redes interdependentes e complexas, ou seja, praticamente todos os países à escala global (Clemente, 2013). 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. Um exemplo é o da Austrália onde, como já foi referido, se assume a necessidade de uma nova metodologia de avaliação de risco para SCADA (ITSEAG, 2012), preocupação que é corroborada a nível europeu (Dufkova et al., 2013). 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).

7. PROTECÇÃO DE INFRAESTRUTURAS CRÍTICAS

Como já vimos, em termos genéricos, 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. Neste contexto, a protecção das IC assenta na definição dos riscos e depende em grande medida da própria definição de IC, da sua catalogação e finalmente da selecção das medidas destinadas a mitigar os riscos identificados. Ou seja, a PIC começa pela identificação dos sectores prioritários das IC a proteger, e continua com a aplicação técnicas de gestão de risco de forma sectorial ou individual.

7.1 Definição

O termo "protecção de infraestruturas críticas" refere-se genericamente a todas as actividades, incluindo pessoas, meios físicos e sistemas de comunicações, que são indispensáveis à manutenção da segurança pública, urbana e nacional, e da estabilidade económica. Os métodos de PIC devem fazer face a uma vasta panóplia de ameaças contra as IC, desde as que são provocadas intencionalmente por pessoas, a acidentes naturais imprevisíveis, passando ainda por uma série de eventos imponderáveis. Ou seja, a PIC trata de proteger activos considerados inestimáveis para a sociedade. A nível europeu, o já citado Livro Verde define a PIC como sendo a "capacidade de preparar para, proteger contra, mitigar, responder a, e recuperar da ruptura ou destruição de uma IC" (Commission, 2005).

Nos EUA existem diversas definições mas, de um modo geral, todas elas enfatizam o facto da PIC se centrar na gestão global dos riscos para as infraestruturas, reduzindo as vulnerabilidades, afastando as ameaças, e minimizando o impacto ou consequências dos eventos nefastos que ocorram. Neste contexto, a protecção engloba um vasto conjunto de actividades que passam por fortalecer as instalações físicas contra diversos tipos de riscos, criar resiliência e redundância nos variados sistemas utilizados nas operação diárias, implementar medidas de cibersegurança e desenvolver planeamento de continuidade de negócio incluindo treinos e exercícios. Em suma, a PIC pode ser definida como a aplicação de processos de gestão de risco e continuidade do negócio, com o objectivo de reduzir vulnerabilidades nas IC através da diminuição da frequência, duração e âmbito das rupturas e facilitar a preparação, resposta e recuperação.

7.2 Sectores Críticos a Nível Internacional

A noção de criticidade é motivo de debate aceso, a nível académico, empresarial e político. Assim, reconhecer que a criticidade é uma questão de percepção (Bouchon, 2006) implica:

- A necessidade de identificar e compreender as diferentes percepções de criticidade dos *stakeholders*;
- A definição do nível de criticidade aceitável para cada tipo de *stakeholder*, em função do contexto político;
- A definição de uma estratégia de PIC, equilibrando os interesses dos diferentes *stakeholders*.

Existe no seio dos decisores políticos um permanente debate acerca das implicações de ter uma lista de IC ambígua ou em permanente mutação. A ambiguidade acerca daquilo que é uma IC pode levar a uma utilização ineficiente dos recursos disponíveis para a sua segurança, protegendo demasiadas infraestruturas, defendendo as instalações erradas ou aplicando medidas desajustadas. Por outro lado, limitar arbitrariamente o número de IC apenas devido a restrições orçamentais pode ser a causa da exposição de uma vulnerabilidade particularmente perigosa (Moteff & Parfomak, 2004).

Tabela 4 - Sectores críticos em diversos países. Adaptado de (Brunner & Suter, 2008)

	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	•		•		•	•	•	•	•		•	•		•	•	•				•	•	•	•	•	•

Na identificação de sectores críticos, todos os países têm seguido o exemplo do Relatório Marsh (Marsh, 1997) que foi a primeira publicação oficial a relacionar IC com sectores

empresariais ou indústrias específicas. A escolha do "sector" como unidade de análise é uma abordagem pragmática que segue vagamente as áreas de interesse dos negócios e indústrias existentes (Brunner & Suter, 2008). Isto significa que, ainda hoje, é válida a definição de sector assumida no Relatório Marsh que considerava um sector como sendo "um grupo de indústrias ou infraestruturas que desempenham uma função similar dentro de uma sociedade" (Marsh, 1997). Enquanto alguns países são muito rigorosos na definição dos seus sectores críticos e de quais os bens e serviços por eles fornecidos, outros não têm uma lista oficial de sectores considerados críticos (KRITIS, 2004). A Tabela 4 resume os resultados de um estudo (Brunner & Suter, 2008) sobre quais os sectores considerados como críticos a nível internacional.

Os resultados mostram que a cobertura sectorial dos diversos programas de PIC tende a ser muito abrangente, ilustrando os dois tipos de criticidade referidos no Capítulo 2 e realçando a aplicação de diferentes critérios para aferir essa mesma criticidade. Embora alguns países tenham desde então ajustado as suas políticas de PIC para acompanhar a permanente evolução das ameaças, no que toca à selecção de sectores os critérios mantêm-se essencialmente os mesmos. Ou seja, as alterações são por vezes meramente semânticas e trata-se apenas de refinar a delimitação de subsectores, nomeadamente, no caso de sectores demasiados abrangentes como "Água" ou "Alimentação". Além disso, um estudo da OCDE (Gordon & Dion, 2008) realça o facto de a maior parte dos governos, na adopção de uma perspectiva abrangente dos sectores críticos, incluírem os sectores responsáveis por partes substanciais do seu PIB e do emprego. Por último, vale a pena salientar o facto de a Tabela 4 conter diversos sectores considerados como de infraestrutura no sentido tradicional, tal como os transportes e comunicações, mas também muitos outros que, à partida, não seriam de infraestrutura como a área financeira ou o governo.

7.3 A PIC a Nível Internacional

Há cerca de uma década, surgiram nos dois lados do Atlântico os primeiros documentos oficiais a assumir a impossibilidade da protecção total das IC. Na Alemanha, no contexto de uma análise à escala mundial, concluía-se que existem apenas duas verdades universais relativas à PIC: é impossível a qualquer país atingir segurança a 100% nas IC, e não existe uma forma ideal de resolver este problema (KRITIS, 2004). Nos EUA considerava-se que era impossível defender os sistemas de computadores de todos os ataques e preconizava-se uma resposta baseada na aplicação de contramedidas identificadas através da análise de

risco, contendo três conceitos: protecção, detecção e reacção (GAO, 2004). A protecção trata das políticas, procedimentos e controlos técnicos para a defesa contra ataques. A detecção monitoriza as potenciais falhas nas medidas de protecção que possam resultar em quebras de segurança. Por último, a reacção, envolvendo frequentemente intervenção humana, reage às falhas detectadas tentando evitar que sejam causados danos.

Para a análise sumária daquilo que globalmente se tem feito à escala mundial, vamos recorrer ao trabalho que tem vindo a ser realizado pelas autoridades suíças pois resumem em relatórios anuais as melhores práticas e o ponto de situação da PIC a nível mundial. Em 2008, verificava-se já que a PIC era encarada como uma parte essencial da segurança nacional em numerosos países onde estavam a ser implementadas diversas medidas políticas e administrativas para melhorar a segurança das IC (CSS, 2008). Nesta altura, eram identificadas à escala global as seguintes tendências: Aumento da resiliência e abordagem *all-hazards*, centralização da responsabilidade e crescente atenção sobre a dimensão cibernética. Volvido um ano, o relatório indicava que a PIC continuava a ser um assunto de grande importância, embora as tendências fossem já um pouco diferentes: Continuação do interesse na dimensão cibernética, expansão da cooperação internacional e novo impulso na resolução dos desafios das parcerias entre entidades públicas e operadores privados (CSS, 2009b).

Como resultado desta evolução, no ano seguinte o relatório concluía que os objectivos da PIC variavam em função da sua especificidade e propósito. Ou seja, eram utilizados termos demasiado generalistas como “prevenção”, “mitigação de vulnerabilidades” e “protecção de interesses vitais” o que criava uma confusão entre aquilo que seriam os objectivos da PIC e os seus princípios enformadores (CSS, 2010). Nesse contexto, o relatório propõe uma hierarquia que nos parece absolutamente ajustada pois permite distinguir os diversos níveis a que a PIC é tratada, sistematizando e diferenciando os conceitos basilares que deverão estar na génese da construção da definição de uma estratégia nacional relativa a esta problemática. Estes níveis, estão ilustrados na Figura 18 onde se pode ver que, num patamar superior, estão os princípios que devem orientar a definição das estratégias de segurança nacional. Imediatamente abaixo, estão as políticas enformadoras da PIC que definirão quais as IC a proteger. Por último, estão os planos sectoriais que deverão ser obrigatoriamente coordenados com os operadores privados.

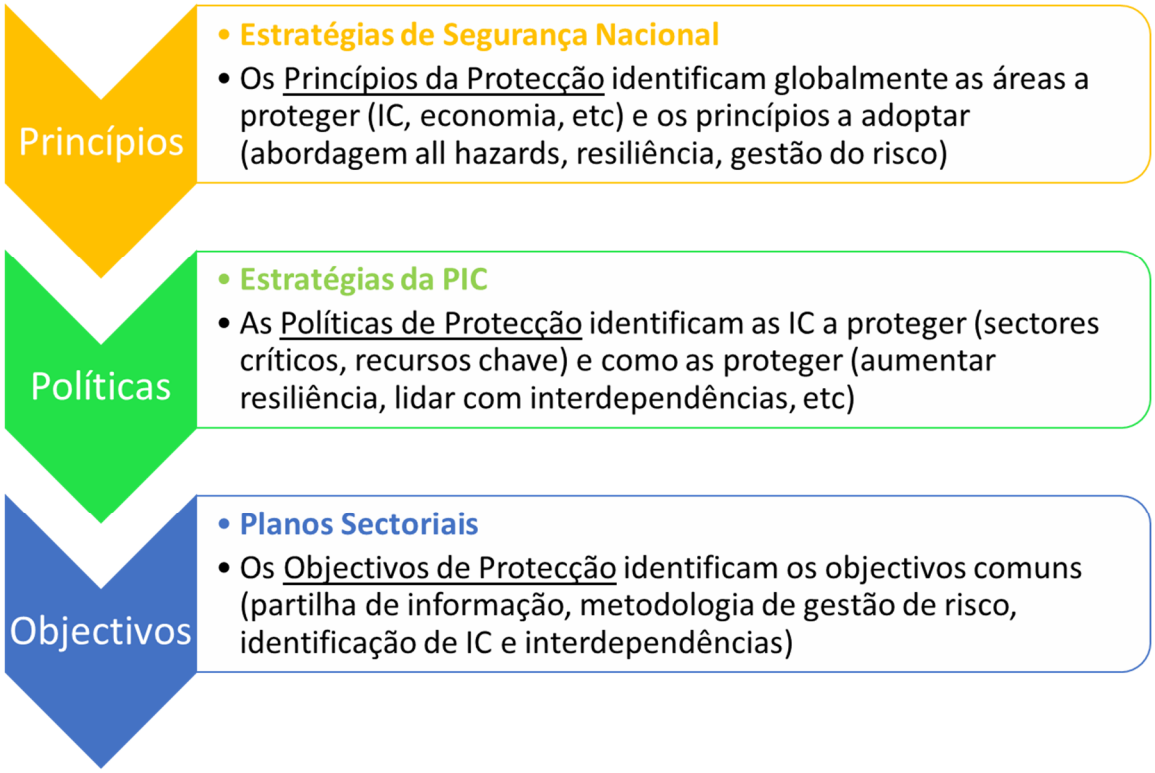


Figura 18 - Três níveis de Estratégia para a PIC. Adaptado de (CSS, 2010)

As dificuldades para operacionalizar a PIC são grandes pois os sistemas ciber-físicos podem ser extremamente complexos. Estes sistemas podem ter que satisfazer simultaneamente requisitos de fiabilidade, segurança em tempo real e protecção mas os operadores e os engenheiros são, na maior parte dos casos, especialistas apenas numa destas áreas. Estas limitações podem também levar a divergências nos objectivos de concepção dos sistemas. A fiabilidade pode exigir muita redundância, mas torna a coordenação de múltiplas réplicas em tempo real muito mais difícil. Uma boa protecção pode exigir frequentes autenticações e verificações de segurança o que, por sua vez, pode degradar a facilidade de utilização e o desempenho em tempo real (Adam, 2010). Por outro lado, como já foi referido, as IC confundem-se com as IIC e logo a PIC também se torna PIIC. Mas continuam a existir áreas de conhecimento associadas a sistemas de controlo industrial que são distintas daquelas que tratam da infraestrutura cibernética. E não se trata apenas de conhecimento técnico, mas também de conhecimento empresarial uma vez que é fundamental entender o funcionamento económico de um sector industrial para conseguir melhorar a sua cibersegurança (Dufkova et al., 2013).

Assim, parece ser óbvia a existência de 4 perspectivas diferentes para a PIC: uma perspectiva de segurança das TIC, uma perspectiva económica, uma perspectiva de cumprimento da lei

e uma perspectiva de segurança nacional (Brunner & Suter, 2008). Estas perspectivas competem entre si pela distribuição de recursos técnicos e sociais utilizados na PIC e é fácil entender que os diferentes *stakeholders*, desde entidades governamentais à comunidade tecnológica, passando pelas companhias de seguros, tenham interesses divergentes. Além disso, as forças policiais enfatizam a sua visão do risco na perspectiva do cibercrime, enquanto as companhias privadas tendem a encarar o risco em termos de custo económico (Brunner & Suter, 2008). Apesar de todas as dificuldades, das diferentes perspectivas em análise e dos diferentes interesses em conflito, um facto permanece inquestionável: a PIC tornou-se uma preocupação de tal ordem importante que até velhos inimigos e rivais se juntam para debater interesses comuns nesta área. Falamos dos trabalhos bilaterais entre os EUA e a Rússia com vista ao estabelecimento de acordos sobre conflitos no ciberespaço, concretamente ataques sobre IC em caso de conflito (Rauscher & Korotkov, 2011).

8. SITUAÇÃO NACIONAL

Em 1992, o Tratado de Maastricht impunha o desenvolvimento de redes transeuropeias como potenciadoras do desenvolvimento e coesão social e o conceito de Infraestrutura Crítica Europeia (ICE), que está hoje na ordem do dia, confirma o sucesso deste esforço colectivo. Por um lado, o conceito sublinha o facto de as infraestruturas serem de facto omnipresentes e críticas para o funcionamento da sociedade actual. Mas, por outro lado, esta noção ilustra uma das desvantagens desta transição das infraestruturas europeias: exactamente devido a serem (inter)dependentes de serviços baratos e estáveis, as sociedades estão vulneráveis a rupturas no funcionamento das suas infraestruturas críticas. Em 2004, acompanhando a evolução dos acontecimentos a nível internacional, as autoridades europeias deram início a uma série de estudos sobre a PIC. Simultaneamente, foram desenvolvidos em Portugal os primeiros esforços nesta área, que resultaram num levantamento e classificação das IC nacionais.

8.1 Contexto Europeu

Na UE, o estudo da PIC iniciou-se quando, em resposta a uma solicitação do Conselho Europeu junto da Comissão Europeia (CE) no sentido de se elaborar uma estratégia comum sobre o tema em questão, em 20 de Outubro de 2004, a 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 o já citado Livro Verde sobre PEPIC (Commission, 2005), 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, optando claramente por uma abordagem *all-hazards*, mas assumindo que o terrorismo continuava a ter prioridade sobre todos as outras ameaças

Na sequência dos apagões de 2003 e 2006, mencionados no capítulo 5, os decisores políticos europeus interiorizaram definitivamente a noção que a Europa estava em risco e era necessária uma abordagem abrangente que tivesse em conta os ataques terroristas, os desastres naturais e as falhas técnicas. Além disso, as características transnacionais do espaço europeu, que implicam que a ruptura numa infraestrutura de um estado membro pode

afectar outros estados, levam à necessidade de criar um nível mínimo de protecção comum (Högselius et al., 2013). Assim, em 2006 foi produzido algum trabalho de reflexão neste domínio, tendo a Comissão adoptado a Comunicação de 12 de Dezembro de 2006 sobre o assunto[33]. 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 dos Estados-membros assegurar a protecção das IC em cada um dos respectivos territórios nacionais.

Esta dinâmica levou a que, em 08 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, assim como 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, a Directiva concentra-se apenas nos sectores da energia e dos transportes, embora perspective já a necessidade de futuramente incluir o sector das TIC.

No âmbito OTAN, muitas iniciativas e trabalhos têm vindo a ser desenvolvidos, sobretudo desde o 11 de Setembro de 2001, especialmente a nível dos Comités Sectoriais com responsabilidades no Planeamento Civil de Emergência. Estes trabalhos são apenas com o objectivo de orientar e apoiar os países membros da aliança na área da PIC, sendo coordenados pelo *Ad-hoc Working Group on Critical Infrastructure Protection*. Portugal é membro desde grupo de trabalho desde 2004, tendo sido inicialmente representado pelo

[33] COM(2006) 786 final, Communication from the Commission on a European Programme for Critical Infrastructure Protection, disponível em http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm, consultado em 13 de Outubro de 2014

agora extinto Conselho Nacional de Planeamento Civil de Emergência (CNPCE) (Pais, Sá, & Gomes, 2007).

8.2 Evolução da PIC em Portugal

Em Portugal, as primeiras iniciativas para a protecção das IC tiveram início em 2003, simultaneamente com as primeiras medidas a nível da União Europeia com vista à elaboração de uma estratégia conjunta para a protecção das ICE. Nessa altura, considerando que a temática em apreço era de carácter marcadamente multidisciplinar e transversal a todos os sectores estratégicos nacionais, foi atribuída essa responsabilidade ao CNPCE. Assim, o projecto para a protecção das IC nacionais (Projecto PIC) foi inicialmente coordenado e desenvolvido 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 (Pais et al., 2007)

Este projecto foi desenvolvido por um grupo de trabalho, formalmente constituído em 2004, e inicialmente previa-se que decorresse em duas fases (Pais et al., 2007). Mais tarde, foi ajustado e, actualmente, considera-se que os trabalhos se desenvolveram em 3 fases distintas mas que, nas suas fases intermédias, englobam as anteriores duas fases, alargando o seu âmbito (Mendes & Pais, 2012). Tentando resumir esta evolução, podemos afirmar que a primeira fase foi a identificação e classificação das infraestruturas fundamentais para o normal funcionamento do país, a segunda consiste na análise desses resultados e avaliação do risco associado a essas infraestruturas, e a última fase será a elaboração e implementação de um Programa Nacional para a Protecção de Infraestruturas Críticas (PNPIC) (Mendes & Pais, 2012; Pais et al., 2007; Pais & Sá, 2009). Importa 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 (Pais et al., 2007).

A protecção das IC ganhou o devido enquadramento legal quando, em 9 de Maio de 2011, foi publicado o Decreto-Lei 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 União Europeia, 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 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 União Europeia 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 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.

Em 2013, o Despacho nº 13692/2013 do MDN, de 28 de Outubro, que enquadra a ciberdefesa no Conceito Estratégico de Defesa Nacional refere o potencial devastador dos ataques cibernéticos e reconhece que essas acções representam uma ameaça crescente sobre as IC, cujos efeitos e impactos podem provocar o colapso da estrutura tecnológica que suporta a organização social e económica do País. Recentemente, o Decreto-Lei 69/204 de 9 de Maio de 2014, que criou o Centro Nacional de Cibersegurança (CNCseg), refere claramente as responsabilidades deste organismo relativamente a incidentes ou ciberataques que ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais. Por último, importa salientar que o Decreto-Lei n.º 138/2014, de 15 de Setembro, estabelece o regime extraordinário para salvaguarda de activos estratégicos em sectores fundamentais para o interesse nacional. O artigo 2º do referido Decreto-Lei define activos estratégicos

como sendo “as principais infraestruturas e activos afectos à defesa e segurança nacional ou à prestação de serviços essenciais nas áreas da energia, transportes e comunicações”.

8.3 Infraestruturas Nacionais

Os dados que se seguem resumem o essencial da realidade apresentada pelos principais operadores nacionais num seminário organizado pela KPMG, e pela revista Segurança e Defesa, em 2012. No sector energético, a REN (Redes Energéticas Nacionais) tem a seu cargo o transporte de electricidade em muito alta tensão (MAT) e a gestão técnica global do sistema eléctrico nacional. As redes energéticas nacionais consistem em 8.371 km de linhas aéreas para transporte em MAT, assentes em 17.845 apoios, 78 subestações críticas e algumas muito críticas. A REN é também responsável pelo transporte de gás natural em alta pressão e pela gestão técnica global do sistema nacional de gás natural, garantindo a recepção, armazenamento e regaseificação de gás natural liquefeito, bem como o armazenamento subterrâneo de gás natural. Para esse efeito, a REN conta com 1.300 km de gasoduto para transporte em alta pressão, 195 estações de gás, três cavernas de armazenamento e um terminal de recepção, descarga e recarga de navios metaneiros.

A um nível inferior, na distribuição eléctrica há que considerar as centenas de subestações de alta e média tensão, além de toda a rede de baixa tensão para os clientes domésticos. Existem também 35 centrais hidroeléctricas, oito centrais termoeléctricas, torres eólicas, 4.000 km de fibra óptica e 25 torres repetidoras de transmissão em micro-ondas (usadas para redundância). Um aspecto muito importante na realidade nacional é a existência de um mercado enérgico liberalizado que permite a existência de pequenos operadores privados de produção e distribuição energética. Assim, tal como ocorre na energia eléctrica, a distribuição de gás natural a consumidores domésticos é também efectuada por diversos operadores nacionais e locais. Por último, importa referir a existência de duas refinarias, uma das quais instalada no complexo de Sines que, como veremos adiante, é de importância vital a nível nacional.

Relativamente aos transportes terrestres, existem mais de 3.000 km de rodovia tendo a Brisa responsabilidade por 1.674 km distribuídos por 24 auto-estradas por onde passa 80% do PIB nacional, monitorizados por 630 videocâmaras e ligados por 700 km de fibra óptica. No lado rodoviário, a REFER é a empresa responsável pela gestão da infraestrutura o que engloba a gestão da capacidade, a conservação e manutenção da infraestrutura ferroviária e a gestão

dos respectivos sistemas de comando e controlo da circulação, tudo isto feito a partir de três centros de controlo. Existem 2.794 km de linhas e ramais ferroviários em exploração, dos quais 1.629 km são electrificados e onde 1.137 km de rede principal têm sinalização mecânica e 1.649 km têm sinalização electrónica. A rede ferroviária nacional inclui também 1.049 passagens de níveis, 2.128 pontes, 90 túneis, 564 estações e 28 subestações eléctricas, e uma rede nacional em fibra óptica redundante e três centros de dados. Relativamente ao abastecimento de água, só a EPAL (que abastece 2,9 milhões de pessoas em 34 municípios) conta com 2 fábricas de água, 24 postos de cloragem, 42 reservatórios, 41 estações elevatórias e 1.430 km de rede de distribuição.

Como já foi referido, na primeira fase do Projecto PIC as infraestruturas nacionais foram classificadas de acordo com critérios que reflectem a sua importância relativa para o País e foram também catalogadas e georreferenciadas numa base de dados. O critério adoptado para esta classificação foi de natureza funcional, de acordo com aquilo que está preconizado a nível europeu, considerando-se infraestrutura crítica aquela que, caso sofra uma disfunção, pode pôr em causa o funcionamento do país e o bem-estar da sua população (Mendes & Pais, 2012). O trabalho da segunda fase tem em conta a existência dos diversos tipos de ameaças que impendem sobre as IC, de natureza intencional ou acidental. Na verdade, no domínio genérico das ameaças, o PNPIC segue as melhores práticas a nível internacional, preconizando um abordagem holística do tipo ***all-hazards*** relativamente às potenciais ameaças a considerar. Ou seja, não se limita a estudar apenas uma ameaça, tendo em conta as potenciais ameaças mais plausíveis em território nacional, a saber: o sismo, o ataque cibernético as acções de tipo terrorista (Pais & Sá, 2009). No entanto, considera-se que a ameaça com maior potencial para provocar graves perturbações, danos e disfunções será do tipo sísmico (Pais, Sá, Lopes, & Oliveira, 2011).

Os resultados obtidos no decurso da primeira fase do PNPIC permitiram identificar alguns factos e conclusões que ilustram uma realidade nacional preocupante (Pais et al., 2007). Nomeadamente, foram identificadas cerca de 12.000 infraestruturas, das quais se destacam os seguintes aspectos:

- Mais de 65% das IC nacionais pode ser seriamente afectada por uma ocorrência sísmica;
- Mais de 300 sugerem um elevado potencial para acções mal-intencionadas;

- Algumas infraestruturas encontram-se em zonas de elevado risco de incêndio florestal ou em leitos de cheia;

Além disso, cerca de 2,5% infraestruturas inventariadas até ao momento foram classificadas como críticas (Mendes & Pais, 2012) o que significa que em Portugal existem cerca de 300 IC devidamente inventariadas e referenciadas. Destas, cerca de metade pertencem aos sectores da energia e transportes, embora o sector das comunicações e tecnologias da informação represente também uma importante parcela das nossas IC. É ainda importante salientar a relevância nacional do complexo de industrial Sines visto ser uma área de importância económica fulcral, onde estão situadas cerca de 10% das IC nacionais (Pais et al., 2012). Por último, há que referir que no conjunto total das IC nacionais se inclui uma pequena minoria que pode cumprir os critérios para ser ICE o que impõe a necessidade uma grande coordenação com Espanha (Mendes & Pais, 2012). Embora a ANPC saliente o facto de ter contactos com as autoridades espanholas, constatamos com surpresa que o *website* do *Centro Nacional para la Protección de las Infraestructuras Críticas* não refere nenhuma instituição portuguesa na sua lista de ligações internacionais[34].

Neste momento, o Projecto PIC deveria estar já no terreno, todavia a sua implementação tarda a ocorrer pois a segunda fase está em permanente actualização, de modo a responder ao constante surgimento de novas vulnerabilidades e ameaças. Os estudos e projectos existentes parecem incidir maioritariamente sobre riscos sísmicos, descurando as ameaças ligadas ao ciberespaço. Embora seja verdade que mais de 60% das infraestruturas críticas nacionais se encontra em zonas de perigosidade sísmica elevada (Mendes & Pais, 2012), parece-nos essencial dar uma atenção às vulnerabilidades e ameaças ligadas aos sistemas ICS. Ou seja, tem sido dado particular relevo aos riscos sísmicos e outros de natureza ambiental (Pais et al., 2012) mas parece-nos ser evidente a existência de um *deficit* de análise versando as ameaças cibernéticas sobre as IC nacionais.

A nível do tecido empresarial português, em Março de 2010, um estudo efectuado pela KPMG (Gomes & Alberto, 2010) a 70 empresas nacionais revelou que 90% acreditam vir a sofrer um impacto significativo no seu negócio na eventualidade de uma interrupção até 24

[34] http://www.cnpic-es.es/Enlaces_Internacionales/Enlaces_Internacionales/index.html, consultado em 17 de Outubro de 2014.

horas. Apesar disto, apenas 47% afirmaram estar preparadas e ter a necessária resiliência para responder a riscos e falhas. Entre os possíveis riscos, 96% apontaram as falhas no sistema de informação, 83% referiram o absentismo de funcionários e 76% receia a falta de telecomunicações. Isto significa que as empresas nacionais têm já a clara consciência das consequências da ausência de planeamento de resposta adequada a incidentes, temendo potenciais impactos como perdas financeiras, danos de reputação e imagem e quebra de compromissos com clientes e fornecedores.

9. PROPOSTAS

Muito já foi escrito sobre a frase "aquele que tudo defende, nada defende", normalmente atribuída a Frederico, o Grande, soberano da Prússia. Parece-nos que, do ponto de vista estritamente militar, ele estaria absolutamente correcto uma vez que é impossível a qualquer comandante defender a totalidade de um teatro de operações, ou de uma extensa frente, com um número limitado de tropas. Ou seja, exigir que tudo seja preservado resulta na anulação desse mesmo objectivo na medida em que a dispersão de forças levará a que sejam dizimadas. Analogamente, consideramos que a tentativa de defender todas as infraestruturas resultará inevitavelmente numa má gestão de recursos que poderá ter efeitos desastrosos. É neste âmbito que propomos uma abordagem para um PNPIC, assente nas melhores práticas internacionais elencadas nos capítulos anteriores. Esta proposta tem em conta a especificidade da situação nacional, hierarquizando as IC e limitando o número de sectores a defender, numa tentativa de gerir racionalmente os recursos disponíveis.

9.1 Uma Proposta para o PNPIC

O primeiro passo para a elaboração de um PNPIC terá, obrigatoriamente, que ser a identificação e selecção dos sectores estratégicos mais importantes. Como vimos anteriormente, este passo foi já concluído mas talvez fosse oportuno proceder à sua revisão à luz de outros critérios, quiçá mais actualizados e tendo em conta a evolução das melhores práticas a nível internacional. 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 sempre 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. 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.

Por outro lado, a situação geográfica particular de Portugal leva a 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. Embora a nossa realidade seja distinta da espanhola, uma vez que, por exemplo, não temos energia nuclear, isso não impede que tenhamos esse aspecto em consideração até porque um incidente nesse sector poderá ser catastrófico também para o nosso país. 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. Em concreto, nos sectores da água e da electricidade, a ligação com Espanha é absolutamente estratégica e deve ser um ponto fulcral das nossas preocupações.

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 especial 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. O já citado ***deficit*** de estudos sobre vulnerabilidades dos ICS e SCADA talvez possa vir a ser colmatado pelo recém-criado CNCseg. Além disso, sem querer discutir a tese que sustenta que a ameaça sísmica é a que tem mais potencial destrutivo (Pais et al., 2011), parece-nos que esta não será eventualmente a mais provável.

No mundo moderno, julgamos ser pertinente afirmar que há mais probabilidades de uma IC ser alvo de um ataque cibernético que sofrer os efeitos de uma catástrofe natural, sísmica ou de outra natureza. Por isso mesmo, enfatizamos a necessidade de estudar o risco para as IC nacionais de ameaças relacionadas com o ciberespaço. 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. Além disso, como já foi também salientado, é uma norma de aplicação generalizada a nível internacional o que nos permitirá recolher experiências de países mais avançados nesta área.

No Anexo IV propõe-se uma possível metodologia conceptual, envolvendo os diversos ***stakeholders*** num ciclo de análise e gestão do risco social em IC. O referido modelo tem em conta a existência de vulnerabilidades nas IC, e a possibilidade da sua exploração por diversos tipos de ameaças. Esta análise dos riscos levará a uma segunda etapa, na qual será fundamental a colaboração entre as entidades privadas e públicas na identificação dos riscos com vista à definição de um PNPIC assente num modelo de gestão do risco. Como já foi referido, no caso das IC não é possível transferir ou eliminar completamente os riscos e há inclusivamente que considerar também a possibilidade da inacção, ou seja, nada fazer e esperar pelo melhor. Contudo, esta não nos pareçe ser uma solução aceitável. Portanto, há que tentar prevenir os riscos conhecidos, e aceitá-los, desenvolvendo a resiliência e mitigando os possíveis impactos de quaisquer incidentes.

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. Como vimos no Capítulo 2, nos EUA a evolução do estudo desta temática levou

ao surgimento de conceitos como "infraestrutura crítica", "activo essencial" e "recurso essencial". Todavia, no lado europeu não existe uma distinção formal entre estes conceitos, o que parece indicar que o conceito de infraestrutura crítica é entendido num sentido mais lato, abrangendo os outros dois conceitos. No entanto, consideramos que seria proveitoso hierarquizar as infraestruturas de modo a permitir uma redução da subjectividade da aplicação na noção de criticidade sem anular a abrangência do conceito de infraestrutura crítica. Nesta hierarquização dos sectores (ou das IC) poderão ser tidos em conta factores sociais, económicos, ambientais, estratégicos e de segurança do Estado, tal como se pode ver na Figura 19.

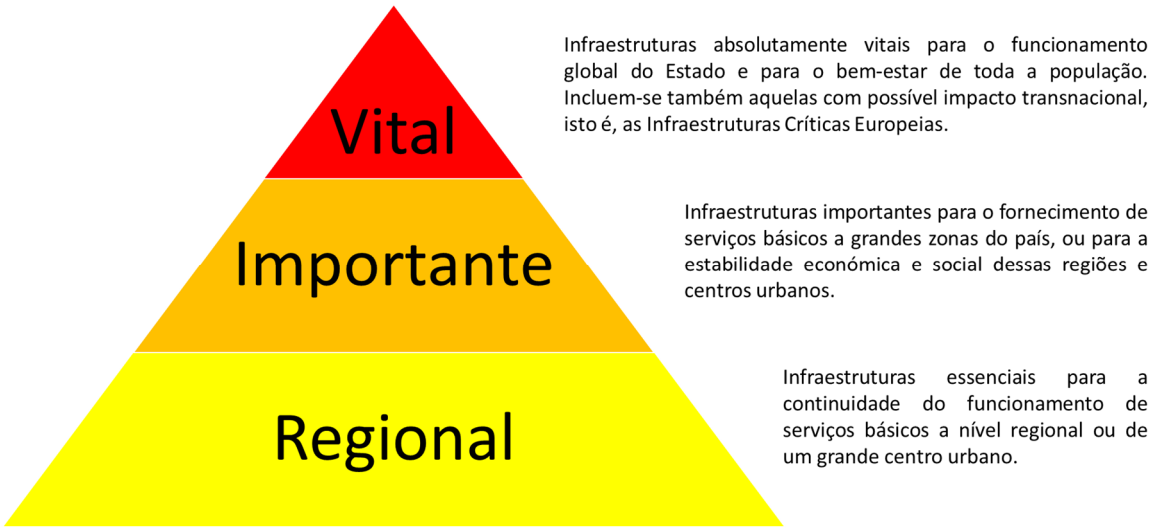


Figura 19 – Possível Hierarquia de Infraestruturas Críticas

No entanto, a análise dos elementos constantes da Tabela 4 leva à conclusão de que há alguns sectores que são considerados como sendo estratégicos na esmagadora maioria dos países considerados no referido estudo. Neste âmbito, as relações de interdependência ilustradas na Figura 4 reforçam esta realidade; o número de sectores verdadeiramente estratégicos é relativamente reduzido.

9.2 Sectores Críticos

Sem ter qualquer tipo de intenção de desvalorizar o trabalho efectuado pela CNPCE (e pela ANPC), a análise dos números obtidos recorda-nos inevitavelmente o ocorrido com a NADB nos EUA. Ou seja, identificar 29 Sectores Estratégicos Nacionais (Pais et al., 2007) parece-nos exagerado porque se considerarmos que tudo é crítico, isso significa que nada é verdadeiramente crítico, e praticamente tudo acaba por ter o mesmo grau de importância ou criticidade. Assim, numa tentativa de focar a atenção naquilo que deve ser preservado a todo o custo, sem prejuízo da existência de outros sectores essenciais, na nossa opinião os sectores

estratégicos em Portugal são os que se elencam no parágrafo seguinte, sem que a ordem pela qual são apresentados corresponda necessariamente a uma hierarquização da sua importância ou criticidade. Nomeadamente, entendemos que os sectores críticos em Portugal devem ser a Energia, as Comunicações, a Banca e Finanças, o Governo, a Água, e os Transportes e Logística.

9.2.1 Energia

Neste sector incluem-se as instalações e redes de produção, armazenamento e distribuição de energia, nomeadamente, de electricidade, derivados do petróleo e gás natural. Assim, este sector tem vários tipos de infraestrutura e de redes que suportam diversos tipos de modelo de negócio. A sociedade moderna tornou-se dependente do fornecimento estável e fiável de electricidade na medida em que este fluxo energético é um recurso essencial para a segurança nacional, saúde e bem-estar, comunicações, finanças, transportes, alimentação e fornecimento de água, aquecimento, refrigeração e iluminação, negócios e até para o entretenimento e diversão. Resumindo, todos os aspectos da vida moderna dependem, de uma forma ou de outra, de energia eléctrica. Ou seja, a sociedade tem uma dependência estrutural do sector energético.

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 poderá desencadear, através das relações de interdependência, a paralisação de IC em diversas áreas de actividade, com consequências imprevisíveis. Sem electricidade, as nossas indústrias interromperão a sua laboração normal, o trânsito rodoviário urbano será bloqueado pela ausência de semáforos, os nossos lares e locais de trabalho ficarão na escuridão e os nossos computadores deixarão de funcionar e de estar ligados à Internet. A utilização generalizada de sistemas SCADA, e outros, para o controlo de sistemas no sector da energia constitui uma vulnerabilidade que potencialmente poderá ser explorada por meios cibernéticos, causando sérios danos e perturbações. Neste contexto, deve ser dada particular atenção à cibersegurança dos centros nevrálgicos de controlo da produção, e aos ICS das infraestruturas de produção e armazenamento.

9.2.2 Comunicações

As redes de comunicações sofreram uma verdadeira revolução na sequência dos avanços tecnológicos das últimas duas décadas, que levaram ao surgimento de uma infraestrutura de telecomunicações que suporta a interligação de um incomensurável número de sistemas informáticos domésticos, empresarias e governamentais. Tirando partido da velocidade e eficiência das comunicações digitais, todas as IC estão presentemente ligadas a diversas redes, com especial relevo para a Internet, o que faz com estejam também ligadas entre si. Esta interligação suporta praticamente tudo aquilo que ocorre no nosso quotidiano, desde movimentos financeiros a distribuição energética, sendo essencial para os serviços da economia, para a competitividade industrial e para a entrega atempada e distribuição de matérias-primas e produtos acabados. Além disso, as redes de comunicação são também fundamentais para o funcionamento de serviços de emergência, são a espinha dorsal dos modernos sistemas militares de comando e controlo, e estão gradualmente a tornar-se incontornáveis no nosso sistema educativo. Isto é, a sociedade tem uma dependência funcional do sector das comunicações.

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 e também todos os processos e pessoas que os suportam. Todos estes elementos estão profundamente interligados entre si o que faz com que uma perturbação num deles possa ter impacto imediato num, ou mais, dos outros. A Internet tem uma dependência vital das redes de telecomunicações e estas dependem de um vasto conjunto de outras infraestruturas. 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. 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.

O funcionamento da sociedade actual assenta em grande medida na informação e na capacidade das organizações para comunicarem de forma rápida e eficaz entre si. Graças à Internet a outras tecnologias de informação, é hoje possível aceder a informação importante

que permite o desenvolvimento de todo o tipo de actividades económicas, políticas e sociais. Muitas empresas são hoje multinacionais que operam à escala global, com prazos extremamente rigorosos e que implicam um permanente esforço de coordenação. Esta realidade só é possível graças à possibilidade de trocar informação em tempo real com fornecedores, clientes e parceiros. Consequentemente, uma falha nas telecomunicações pode ter impacto imediato e acarretar prejuízos avultados. A interdependência da energia e das comunicações e particularmente perigosa, o que torna estes dois sectores num verdadeiro centro de gravidade do risco social.

9.2.3 Banca e Finanças

Este sector engloba as redes de dados financeiros, as instituições de investimento e crédito, os mercados bolsistas e de venda de produtos mobiliários, os sistemas de apoio aos meios de pagamento, e todos os elementos de alguma forma envolvidos nas transacções financeiras necessárias ao normal funcionamento de todo o sistema económico mundial. Na realidade, o mundo actual gira em trono de mercados financeiros, cotações bolsistas e negócios de todo o tipo que movimentam diariamente somas astronómicas, desde os pequenos levantamentos das contas de débito pessoais às grandes transacções entre empresas e Estados.

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.

9.2.4 Governo

Este sector refere-se aos órgãos de soberania, centrais, regionais ou locais, 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, além das forças armadas e de segurança. A criticidade deste sector advém do facto de, numa situação de emergência, ser imprescindível que as instituições públicas assegurem a prestação de socorro

às vítimas, garantam a segurança da propriedade e das populações, mantenham a ordem pública e assumam a coordenação de todos os esforços de resposta e recuperação. Destacam-se neste âmbito os órgãos do Governo Central capazes de assegurar o normal funcionamento das instituições e da sociedade, constituindo-se como referência de estabilidade e continuidade, além de fonte de informação segura e actualizada.

9.2.5 Transportes e Logística

Este sector engloba todas as infraestruturas ligados ao transporte e distribuição por via aérea, marítima, fluvial, ferroviária e rodoviária. 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 é responsável pelo funcionamento das cadeias de abastecimento que sustentam muitos outros sectores e permitem o funcionamento da economia. Embora muitas das vulnerabilidades desde sector sejam ainda essencialmente físicas, relacionadas com a utilização de pontes, viadutos e túneis, existem também muitas vulnerabilidades cibernéticas. A crescente utilização de sistemas de informação para a optimização de trajectos e horários, de sistemas SCADA para controlo de tráfego e sinalização, e de sistemas GPS para rastreio e posicionamento, leva a um aumento da exposição a ataques cibernéticos sobre este sector.

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.

9.2.6 Água

Este sector inclui as fontes, os reservatórios, os sistemas de transporte, de filtragem e purificação de água potável para consumo público, e de água utilizada para arrefecimento e outras aplicações industriais e agrícolas. Além disso, devem ser também tidos em consideração os sistemas de tratamento de águas residuais, pluviais e de abastecimento para combate a fogos. 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 também a integridade e segurança das infraestruturas necessárias à sua distribuição. Paradoxalmente, as alterações climatéricas tornam cada vez mais frequentes os episódios de chuva intensa que sobrecarregam os sistemas de drenagem urbana e causam estragos avultados. Em qualquer uma destas situações, seca ou inundação, não deve ser descurada a atenção a atribuir aos sistemas de esgotos. Em caso de seca, a escassez das fontes de abastecimento pode originar uma maior concentração de poluentes e, em caso de inundação, podem surgir rupturas nos sistemas de tratamento de águas residuais e até de efluentes tóxicos.

9.3 Outras Considerações

Torna-se cada vez mais difícil identificar os pontos e ligações onde a protecção deve ser prioritariamente aplicada. Como resultado desta situação, existe uma crescente dificuldade na identificação daquilo que deve protegido, e os sectores críticos são identificados de forma demasiado genérica, englobando quase todos os aspectos da vida mundana.

9.3.1 Subsectores

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). Neste sentido, podemos, a título de exemplo, considerar os subsectores constantes da Tabela 5. Todavia, esta subdivisão, embora tenda a reduzir a ambiguidade da sectorização genérica, leva a uma imediata multiplicação das áreas a proteger o que nos remete para a citação do início do capítulo. É essa a razão que nos leva a insistir naquilo que nos parece ser um meio-termo; considerar a existência de um número relativamente reduzido de sectores críticos e hierarquizar as IC dentro de cada um deles. Parece-nos ser esta a única forma de acautelar a utilização criteriosa dos meios disponíveis, prevenindo uma eventual dispersão de recursos.

Tabela 5 - Exemplos de possíveis subsectores críticos

Sector	Subsector
Energia	• Electricidade • Gás Natural • Petroquímica
Comunicações	• Telecomunicações • Sistemas de Informação
Transportes e Logística	• Transporte Marítimo • Transporte Aéreo • Transporte Ferroviário • Transporte Ferroviário • Logística
Banca e Finanças	• Bancos • Bolsas • Seguradoras
Governo	• Administração Pública • Parlamento • Poder Judicial • Serviços de Emergência • Forças de Segurança
Água	• Abastecimento Público • Tratamento de Esgotos

Neste sentido, embora se considerem menos sectores, estes continuam a ser emblemáticos dos critérios de criticidade atrás identificados. A criticidade como um conceito sistémico é perfeitamente ilustrada pela escolha dos sectores da energia e das comunicações pois estes são, sem dúvida, casos particulares de inserção fulcral na rede de interdependências. Além disso, a criticidade como conceito teleológico é sobejamente representada pela escolha do sector governamental no sentido em que este sector tem, além de tudo o mais, um papel funcional e simbólico a desempenhar.

9.3.2 Desafios

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 (Marsh, 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 à gestão do 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 nível 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 desempenha 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 muno, alinhadas com ***standards*** internacionais e tentando dar resposta aos desafios apresentados pela 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).

10. CONCLUSÕES

As infraestruturas críticas podem hoje ser encaradas como bens a ser protegidos pelos Estados no âmbito da luta contra o terrorismo, ou como vantagens competitivas no sector privado. Isto é, podem ser analisadas apenas como sistemas de carácter técnico e económico, ou como activos de importância estratégica e de relevância para a formulação da política de Defesa Nacional. As economias baseadas no conhecimento estão em 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 segurança colectiva, o nosso desenvolvimento económico, 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. Isto é, a transversalidade das interdependências numa sociedade em rede potencia o impacto das ameaças, aumentando o risco social.

As tradicionais categorizações das infraestruturas não são adequadas nem à complexidade nem à velocidade de mudança do moderno ecossistema social em que vivemos, e os países industrializados dependem de activos sobre os quais têm pouco ou nenhum controlo. Assim, existe uma incontornável necessidade de criar mecanismos reguladores que estabeleçam parcerias entre as instituições governamentais e os operadores privados. Durante décadas, a generalidade da população do mundo ocidental considerou a disponibilidade e acessibilidade dos seus serviços básicos como algo naturalmente assegurado. É hoje dado como absolutamente garantido o acesso à energia, às telecomunicações, aos transportes, etc. Todavia, esta percepção foi alterada por uma série de incidentes que expuseram um grande número de vulnerabilidades, criando um sentimento de consciência política da criticidade dos sistemas e serviços fornecidos pelas IC.

De um modo geral, todas as organizações estão a tirar partido das tecnologias de informação para acelerar a sua entrega de produtos e serviços, aumentado a eficiência dos seus processos

e eliminando os seus excessos de armazenagem. Muitas empresas estão hoje tão dependentes de abastecimentos coordenados com as suas operações, que até a mais pequena perturbação pode ter um impacto significativo na sua cadeia de produção. 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. O governo partilha com o sector privado a utilização das infraestruturas de comunicação, e tanto os acidentes naturais como os ataques maliciosos afectam de igual modo todas as áreas da vida moderna. Assim, não faz sentido falar de ameaças ao sector público ou sector privado, mas sim de ameaças globais que devem ser encaradas numa óptica de parceira entre as instituições governamentais e os operadores privados. Ou seja, a tarefa de proteger as IC deverá ser uma responsabilidade partilhada entre todos os ***stakeholders***, pois só através de uma efectiva colaboração entre todos se conseguirá colocar em prática uma estratégia de PIC.

A gestão do risco no sentido tradicional não responde nem à complexidade nem ao ritmo da mudança do mundo moderno. Relativamente às IC, esta situação é agravada pelas características enunciadas nos capítulos anteriores, nomeadamente as interdependências, o carácter transnacional e a propriedade privada. Todos estes factores concorrem para dificultar, ou mesmo impossibilitar, a delimitação de um perímetro defensivo. Aliás, este conceito perde a sua validade num mundo em que a conectividade se sobrepõe à segurança e onde é frequente que as avaliações de risco sejam efectuadas com métodos desajustados. 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. 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.

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. 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. Daí a necessidade de aceitar o risco residual como um facto insofismável e incorporar o aumento da resiliência como parte da gestão do risco pois parece ser essa a metodologia mais eficaz para fazer face aos desafios de segurança das IC.

O crescente número de incidentes relacionados com ataques informáticos lançados 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. Neste novo domínio operacional, 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 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. 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. Todavia, para que isso aconteça, é necessária a adopção de terminologia comum e de metodologias assentes nos mesmos princípios de modo a permitir um fluxo de informação que seja facilmente perceptível por todos os ***stakeholders***. O incremento da partilha de informação entre operadores e governo, e entre sectores, será de grande utilidade no esforço comum para a identificação de vulnerabilidades e criação de medidas de prevenção comuns. Até aqui, os proprietários e operadores estiveram fechados na sua própria realidade, centrados unicamente nas ameaças às suas organizações e processos. Por seu lado, os governos têm estado apenas preocupados com as ameaças à segurança nacional que estejam para além dos interesses privados. A realidade actual, em que um inimigo pode, a

partir dos antípodas, atacar remotamente qualquer alvo dentro de um Estado, impõe a criação de um modelo de partilha de responsabilidades e informação a todos os níveis.

A nível nacional, há 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. Neste contexto, assume particular relevância a recente criação do CNCseg uma vez que que terá como função controlar, prevenir e responder aos ciberataques às IC nacionais. Pensamos que seria aconselhável que este organismo envidasse esforços no sentido de colmatar a lacuna que parece existir no que toca à análise do risco nos ICS nacionais. Ou seja, tem sido dado particular relevo aos riscos sísmicos, e outros de natureza ambiental, mas parece-nos existir um ***deficit*** de análise relativamente às ameaças cibernéticas sobre as IC nacionais que poderá, e deverá, ser uma preocupação imediata.

Caso esta entidade entre em pleno funcionamento, poderemos atingir a situação ideal de ter uma instituição nacional dedicada à protecção das IC, envolvendo os vários sectores estratégicos. No entanto, a criação de uma 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, o GNS, o CNCseg, 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.

Urge aprofundar o estudo das interdependências entre as IC nacionais, e as relações com as ICE e operacionalizar um PNPIC capaz de responder aos desafios actuais e futuros. Para tal, 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 protecção de IC.

Resumindo, podemos concluir o seguinte:

- A sociedade em rede cria novas vulnerabilidades derivadas das interdependências estruturais e funcionais entre sectores considerados como sendo críticos para o funcionamento da própria sociedade. No entanto, estas interligações não têm apenas aspectos nefastos e poderão também ser potenciadas numa perspectiva de redundância entre infraestruturas, aumentado a resiliência global do sistema;
- Todavia, a redundância funciona apenas a nível sectorial interno, entre infraestruturas semelhantes, que podem ser utilizadas como sistemas de apoio mútuo em caso de falha parcial da rede, ou do serviço. Relativamente às interdependências entre sectores distintos, a rede de ligações não minimiza o impacto de uma falha. Pelo contrário, tudo indica que contribuirá para o amplificar;
- Além disso, a redundância dentro de um mesmo sector pode ser afectada por lógicas concorrenciais e prioridades empresariais. No contexto actual, onde o sector privado domina a maioria das IC nacionais, caberá às entidades públicas assegurar que, em caso de necessidade, prevalecem os superiores interesses do Estado em detrimento de quaisquer outros;
- Por outro lado, uma rede é tão fraca quanto o seu ponto mais frágil. No caso nacional, a integração europeia e a participação na OTAN, obrigam-nos a acompanhar o nível de exigência dos nossos parceiros internacionais. Para tal, não bastará proceder à adopção de normativos comunitários, ou à criação legislativa de novos organismos governamentais. É necessário colocar no terreno um PNPIC de médio prazo que dê resposta às crescentes ameaças que pairam sobre as nossas IC, e permita coordenar os esforços de todos os ***stakeholders*** nacionais;
- Embora pareça óbvio afirmar que o sector energético e o das comunicações se destacam em termos de criticidade, a verdade é que a sua inclusão na rede de interdependências os coloca em pé de igualdade com os restantes sectores propostos como sendo os mais críticos. Ou seja, actualmente, nenhum sector funciona de forma autónoma e o risco social é transversal a todas as IC;

- Da mesma forma, não nos parece lógico hierarquizar as vulnerabilidades das IC. Mesmo aquelas que, à partida, poderão ser encaradas como menos significativas, poderão causar um impacto devastador na sociedade, se forem maliciosamente exploradas. Este é outro aspecto da transversalidade do risco social; uma pequena vulnerabilidade num determinado sector pode potencialmente causar a ruptura total de um outro sector, devido aos efeitos em cascata que inevitavelmente surgirão na rede global de infraestruturas, afectando significativamente o funcionamento da sociedade.

Neste contexto, a resposta institucional deve ser integrada e articular as áreas do combate à cibercriminalidade, da ciberdefesa e da ciberseguranaça. Só com o envolvimento global de todos os organismos do Estado, de todos os ***stakeholders*** do sector privado, e de especialistas do mundo académico, se conseguirá um reforço real e efectivo do Sistema Nacional de Gestão de Crises.

ANEXO I - Exemplos de Definições de Infraestrutura Crítica

Austrália	The Australian, State and Territory governments define critical infrastructure as: those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security (Attorney-General, 2010)
Canada	Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence (PSC, 2009).
Alemanha	Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences (BMI, 2009).
Inglaterra	The UK's national infrastructure is defined by the Government as: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends". 2 2 Within the national infrastructure, there are certain critical elements, the loss or compromise of which would have a major impact on the availability or integrity of essential services leading to severe economic or social consequences or to loss of life in the UK. These critical elements make up the critical national infrastructure (CNI) (Office, 2013).
Estados Unidos	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would

	have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (DHS, 2013).
Japão	Defined as "the basis of people's social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others. If its function is suspended, deteriorated or become unavailable, it could have significant impacts on people's social lives and economic activities." in the "The Second Action Plan on Information Security Measures for Critical Infrastructures" (ISPC, 2013).
União Europeia	• Infra-estrutura crítica - elemento (asset), sistema ou parte deste situado nos Estados-Membros 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 num Estado-Membro, dada a impossibilidade de continuar a assegurar essas funções; • Infra-estrutura Crítica Europeia - infra-estrutura crítica situada nos Estados-Membros cuja perturbação ou destruição teria um impacto significativo em pelo menos dois Estados-Membros. O significado do impacto deve ser avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infra-estruturas (European Council Directive 2008/114/CE.).
Espanha	• Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. • Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (Ley 8/2011, Boletín Oficial del Estado, Núm. 102, 29 de abril de 2011, Sec. I. Pág. 43370)

ANEXO II - Resumo das diferenças entre os ICS e os sistemas TIC

Adaptado de (DHS, 2009; Holmgren et al., 2010; Stouffer et al., 2013)

Category	Information Technology System	Industrial Control System
Performance Requirements	• Non-real-time • Response must be consistent • High throughput is demanded • High delay and jitter may be acceptable	• Real-time • Response is time critical • Modest throughput is acceptable • High delay and/or jitter is not acceptable
Availability Requirements	• Responses such as rebooting are acceptable • Availability deficiencies can often be tolerated depending on the system's operational requirements	• Responses such as rebooting may not be acceptable because of industrial process availability requirements • Disturbances must be planed and scheduled days/weeks in advance
Risk Management Requirements	• Data confidentiality and integrity are paramount • Fault tolerance is less important (momentary downtime is not a major risk) • Major risk impact is delay of business operations	• Human safety is paramount, followed by protection of the process • Fault tolerance is essential, even momentary downtime may not be acceptable • Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Architecture Security Focus	• Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. • Central server may require extra security	• Primary goal is to protect terminal equipment (such as IEDs or PLCs) • Protection of central server is also important
Security Solutions	• Security solutions are designed around typical IT systems	• Security tools must be tested to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	• Less critical emergency interaction • Access to system resources can be limited and controlled desired degree	• Response to human and other emergency interaction is critical • Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation and Change Management	• Systems are designed to use standard operating systems • Upgrades are straightforward and performed with help of automated deployment tools	• Specific and proprietary operating systems, often without built in security capabilities • Software changes must be made step by step, usually by software vendors because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	• Systems are specified with enough resources to support the addition of third-party applications such as security solutions	• Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities

Communications	• Standard communications protocols • Primarily wired networks with some localized wireless capabilities • Typical IT networking practices	• Many proprietary and standard communication protocols • Several types of communications media used including dedicated wire and wireless (radio and satellite) • Networks are complex and sometimes require the expertise of control engineers
Support	• Allow for diversified support styles	• Service support is usually via a single vendor
Component Lifetime	• Components and systems have a short lifetime(3-5 years)	• Components and systems have a long lifetime(15-20 years)
Access to Components	• Components are usually local and easy to access	• Components can be isolated, remotely located, and difficult to access

ANEXO III - Historial de Incidentes Cibernéticos em ICS e SCADA

Este anexo contém uma síntese de alguns dos mais relevantes incidentes cibernéticos documentados, seguindo, tanto quanto possível, uma linha cronológica. A informação contida neste anexo foi recolhida das seguintes fontes: (Symantec, 2012), (Stouffer et al., 2013), (Wueest, 2014), (GAO, 2004), (Lukszo et al., 2010), (Nordwood & Catwell, 2009), (McAfee, 2011), (Wilson, 2008).

1982

- Explosão no gasoduto Trans-Siberiano - Um *trojan* inserido no software do sistema causou uma explosão de grandes dimensões.

1994

- Ataque à Barragem Roosevelt - Um *hacker* acedeu remotamente a um dos servidores que controla parte do sistema da barragem.

1997

- Comunicações de Tráfego Aéreo – Um adolescente desligou parcialmente a rede telefónica pública em Worcester, Massachusetts, o que provocou uma quebra nas comunicações telefónicas da torre de controlo, segurança do aeroporto, bombeiros e companhias aéreas.

2000

- Descarga de Esgotos - um funcionário descontente, acede ilegalmente ao sistema de controlo de esgotos de Maroochy Shire em Queensland, na Austrália e liberta milhões de litros de esgotos não tratados nos canais da cidade.
- Gasoduto russo - Hackers assumem controlo de um importante gasoduto de gás natural da Gazprom.

2001

- Centro de distribuição eléctrica – Ataque contra o sistema SCADA que controla o fluxo de electricidade na Califórnia.

2003

- Worm SQL Slammer – Explorando uma vulnerabilidade para a qual estava disponível uma correcção desde Julho de 2002, este worm, apenas 10 minutos depois de ter sido lançado na Internet, infectou mais de 90% dos computadores vulneráveis em todo o mundo. Entre estes, estavam os computadores do sistema SCADA da central nuclear Davis-Besse, no Ohio.

- Worm Blaster – Quando foi lançado, infectou mais de 120.000 computadores nas primeiras 36 horas contribuiu decisivamente para aumentar o impacto do apagão que, no dia 14 de Agosto, afectou mais de 50 milhões de pessoas na costa Leste dos EUA e Canadá.

2006

- Semáforos – Dois funcionários públicos acederam ilegalmente ao sistema de controlo de tráfego de Los Angeles e desligaram os semáforos numa série de cruzamentos, exactamente antes da ocorrência de um protesto laboral.
- Tratamento de água - Um intruso estrangeiro penetrou no sistema de controlo de uma estação de filtragem de água em Harrisburg, Pennsylvania, afectando o normal funcionamento da estação de tratamento de água.

2009

- Night Dragon – Foram lançados, de forma sistemática e coordenada, uma série de ciberataques contra empresas do sector petrolífero e energético.

2010

- Central de Natanz – A central de centrifugação de urânio do Irão é atacada pelo Stuxnet, um *software* altamente especializado e concebido especialmente para afectar um determinado tipo de sistemas SCADA.

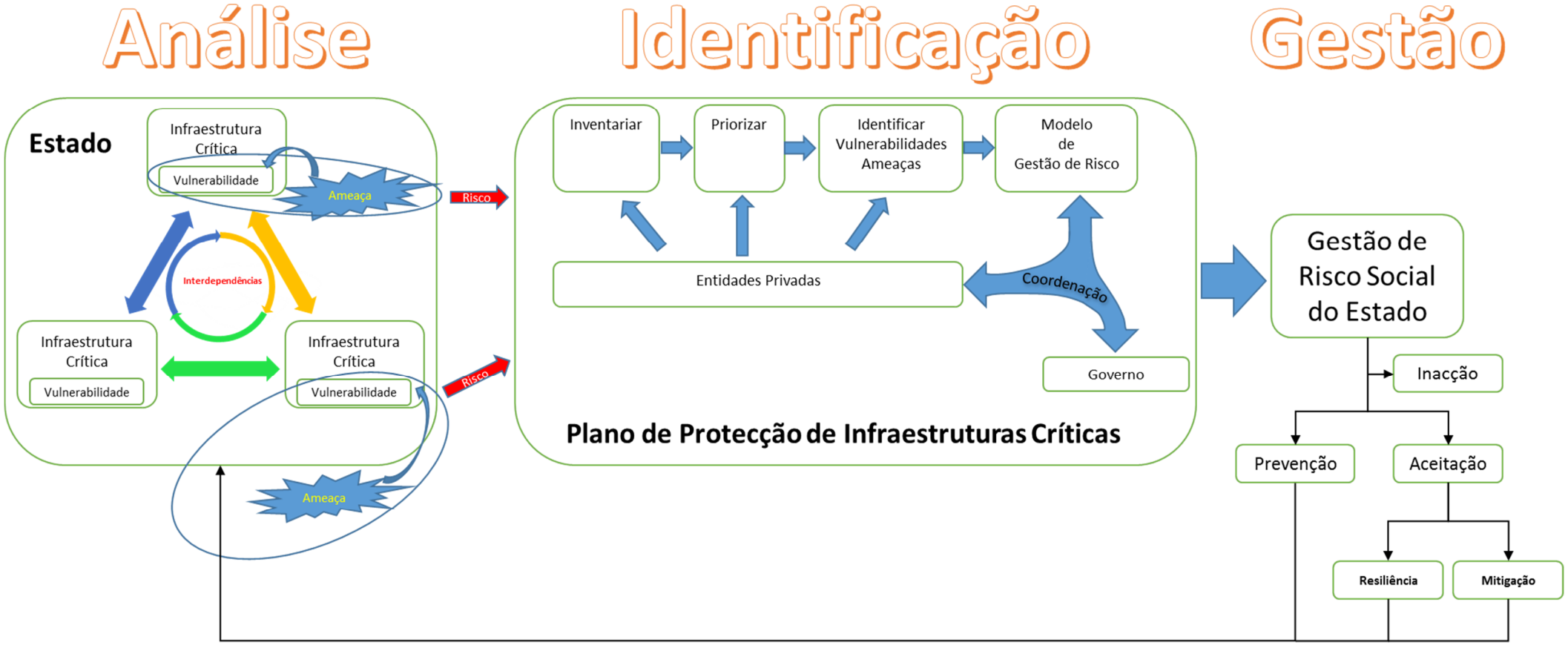
2012

- Aramco – Um ciberataque extremamente destrutivo atingiu cerca de 30.000 computadores numa das maiores empresas produtoras de petróleo na Arábia Saudita.

2013

- Rede eléctrica alemã – uma companhia de gás alemã enviou inadvertidamente um sinal para testar uma nova extensão da sua rede mas o sinal atingiu a rede de controlo e monitorização austríaca que respondeu, originando mais respostas do lado alemão até que parte do sistema teve que ser isolada e desligada para interromper este ciclo.

ANEXO IV – Ciclo de Análise e Gestão do Risco em Infraestruturas Críticas



BIBLIOGRAFIA

Adam, N. (2010). *Workshop on Future Directions in Cyber-Physical Systems Security*. *Report on workshop organized by Department of Homeland Security (DHS)*. Department of Homeland Security.

Attorney-General. (2010). *Critical Infrastructure Resilience Strategy*. Australian Government.

Bagheri, E., & Ghorbani, A. A. (2008). The State of the Art in Critical Infrastructure Protection: a Framework for Convergence. *International Journal of Critical Infrastructures*, *4*(3), 215–244.

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.

Bloomfield, R., Chozos, N., & Nobles, P. (2009). *Infrastructure interdependency analysis: Requirements, capabilities and strategy*. Adelard.

BMI. (2008). *Protecting Critical Infrastructures – Risk and Crisis Management: A guide for companies and government authorities*. Bundesministerium des Innern.

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

Bouchon, S. (2006). *The Vulnerability of Interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art*. Joint Research Centre/Institute for the Protection and Security of the Citizen.

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.

Caldwell, F., & Hunter, R. (2002). *Digital Pearl Harbor': Defending Your Critical Infrastructure*. Gartner, Inc.

CCN. (2010a). *Seguridad en el Control de Procesos y SCADA: Guía 1 - Comprender el Riesgo del Negocio*. Centro Criptológico Nacional.

CCN. (2010b). *Seguridad en el Control de Procesos y SCADA: Guía 5 - Gestionar el riesgo de terceros*. Centro Criptológico Nacional.

Chang, S. E. (2009). Infrastructure Resilience to Disasters. *The Bridge*, *39*(4), 36–42.

Cisco. (2014). *Annual Security Report*. Cisco Systems, Inc.

Civil Engineers, T. I. of. (2013). *Infrastructure Interdependencies Timelines*.

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.

Commission, E. (2005). *Green Paper on a European Programme for Critical Infrastructure Protection – COM(2005) 576 final*. European Commission.

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

CSS. (2008). *Focal Report 1: Critical Infrastructure Protection*. Center for Security Studies.

CSS. (2009a). *Focal Report 3: Critical Infrastructure Protection: Cybersecurity – Recent Strategies and Policies: An Analysis*. Center for Security Studies.

CSS. (2009b). *Focal Report 2: Critical Infrastructure Protection*. Center for Security Studies.

CSS. (2010). *Focal Report 4: Critical Infrastructure Protection: Protection Goals*. Center for Security Studies.

CSS. (2011). *Focal Report 7: Critical Infrastructure Protection: Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use*. Center for Security Studies.

Cukier, K. (2005). Critical Information Infrastructure Protection, Ensuring (And Insuring?) Critical Information Infrastructure Protection. *A Report of the 2005 Rueschlikon Conference on Information Policy*.

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

DHS. (2006). *Progress in Developing the National Asset Database*. Department of Homeland Security.

DHS. (2009). *Recomended Pratice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies*. Department of Homeland Security.

DHS. (2010). *DHS Risk Lexicon*. Department of Homeland Security.

DHS. (2011a). *Strategic National Risk Assessment*. Department of Homeland Security.

DHS. (2011b). *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.

DHS. (2013). *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*. Department of Homeland Security.

Dufkova, A., Budd, J., Homola, J., & Marden, M. (2013). *Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS*. ENISA.

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

ENISA. (2011b). *ENISA ad hoc Working Group on National Risk Management Preparedness*. European Network and Information Security Agency.

ENISA. (2013). *Can we learn from SCADA security incidents?* 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.

Gendron, A. (2010). *Critical Energy Infrastructure Protection in Canada*. Centre for Operational Research & Analysis.

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art*. Joint Research Centre/Institute for the Protection and Security of the Citizen.

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

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

Gomes, R., & Alberto, C. (2010). *Continuidade de Negócio: Assegurar a resiliência na adversidade*. KPMG Advisory.

Gordon, K., & Dion, M. (2008). *Protection of "Critical Infrastructure"and the Role of Investment Policies Relating to National Security*. *Investment Division, Directorate for Financial and Enterprise Affairs, Organisation for Economic Cooperation and Development, Paris* (Vol. 75116). OECD.

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

Hazards, C. on Increasing National Resilience to, Science, & Academies, P. P. T. N. (2012). *Disaster Resilience: A National Imperative*. The National Academies Press.

Högselius, P., Hommels, A., Kaijser, A., & Vleuten, E. van der (Eds.). (2013). *The Making of Europe's Critical Infrastructure: Common Connections and Shared Vulnerabilities*. Palgrave Macmillan.

Holmgren, Å. J., Johansson, E., & Malmgren, R. (2010). *Guide to Increased Security in Industrial Control Systems*. Myndigheten för Samhällsskydd och Beredskap.

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

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

ICS-CERT. (2014). *Year in Review - 2013*. Industrial Control Systems Cyber Emergency Response Team, Department of Homeland Security.

Infopédia. (2014). Infraestrutura. Porto Editora. Consultado em 5 de Julho de 2014, disponível em http://www.infopedia.pt/dicionarios/lingua-portuguesa/infraestrutura

ISPC. (2013). *Cibersecurity Strategy*. Information Security Policy Council.

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.

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.

Lewis, T. G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Wiley.

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.

Mansfield, N., & Carblanc, A. (2008). *Development of Policies for Protection of Critical Information Infrastructures*. OECD.

Marinos, L., & Sfakianakis, A. (2013). *ENISA Threat Landscape: Responding to the Evolving Threat Environment*. European Network and Information Security Agency (ENISA).

Marsh, R. T. (1997). *Critical Foundations: Protecting America's Infrastructures*. President's Commission on Critical Infrastructure Protection.

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

Mendes, C., & Pais, I. (2012). Protecção de Infraestruturas Críticas: Reduzir Vulnerabilidades, Aumentar a Resiliência. *PROCIV*, (51), 6–7.

Metzger, J. (2004). An Overview of Critical Infrastructure Protection (CIP): A Critical Appraisal of a Concept. *Critical Infrastructure Protection and Civil Emergency*.

Moteff, J. (2007). *Critical Infrastructure: The National Asset Database*. Congressional Research Service.

Moteff, J., & Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification*. CRS report for Congress. Congressional Research Service, Library of Congress.

MSB. (2010). *A first step towards a national risk assessment: National risk identification*. Myndigheten för Samhällsskydd och Beredskap.

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*.

Nicholson, R. (2008). *Critical Infrastructure Cybersecurity: Survey Findings and Analysis*. Energy Insights.

Nordwood, K. T., & Catwell, S. P. (Eds.). (2009). *Cybersecurity, Cyberanalysis and Warning*. Nova Science Publishers.

O'Rourke, T. D. (2007). Critical Infrastructure, Interdependencies, and Resilience. *The Bridge*, *37*(1), 22–30.

Office, C. (2011). *Keeping the Country Running: Natural Hazards and Infrastructure*. UK Government.

Office, C. (2013). *A Summary of the 2013 Sector Resilience Plans*. UK Government.

Pais, I., & Sá, F. M. de. (2009). Paradigmas da Protecção de Infra-estruturas Críticas e o Estado da Arte em Portugal. *Planeamento Civil de Emergência*, (21), 36–42.

Pais, I., Sá, F. M. de, & Gomes, H. (2007). Protecção de Infra-estruturas Críticas – A Cooperação Público-Privada. In C. G. Soares, A. P. Teixeira, & P. Antão (Eds.), *Riscos Públicos e Industriais* (pp. 65–84). Edições Salamandra, Lisboa.

Pais, I., Sá, F. M. de, Lopes, M., & Oliveira, C. S. (2011). Infraestruturas Criticas: Propostas Para a Redução do Risco Sísmico. *Planeamento Civil de Emergência*, (23), 16–21.

Pais, I., Sá, F. M. de, Lopes, M., & Oliveira, C. S. (2012). Redução do Risco Sísmico e Tsunamis em Infraestruturas Críticas Industriais. O Caso do Complexo de Sines. In C. G. Soares, A. P. Teixeira, & C. Jacinto (Eds.), *Riscos, Segurança e Sustentabilidade* (Vol. 1, pp. 133–147). Edições Salamandra, Lisboa.

Pauna, A., & Moulinos, K. (2013). *Window of exposure… a real problem for SCADA systems?* European Network and Information Security Agency.

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

Peerenboom, J. P., & Fisher, R. E. (2007). Analyzing Cross-Sector Interdependencies. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences* (p. 112). IEEE Computer Society.

Priberam. (2014). Infraestrutura. Priberam Informática. Consultado em 5 de Julho de 2014, disponível em http://www.priberam.pt/dlpo/infraestrutura

PSC. (2009). *National Strategy for Critical Infrastructure*. Public Safety Canada.

PSC. (2010). *Risk Management Guide for Critical Infrastructure Sectors*. Public Safety Canada.

PSC. (2014). *2014-2017 Action Plan for Critical Infrastructure*. Public Safety Canada.

PSC/DHS. (2010). *Canada-United States Action Plan for Critical Infrastructure*. Public Safety Canada and Department of Homeland Security.

Rauscher, K. F., & Korotkov, A. (2011). *The Russia-U.S. Bilateral on Critical Infrastructure Protection - Working Towards Rules for Governing Cyber Conflict-Rendering the Geneva and Hague Conventions in Cyberspace* (No. Issue 1). EastWest Institute.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25.

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. (2013). *Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology.

Symantec. (2012). *Towards Smart Grids and Smart Metering: How to Protect Critical Infrastructure, Mitigate Fraud and Guarantee Privacy*. Symantec Corporation.

Tabansky, L. (2011). Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs*, *3*(2).

Tsai, P. (2013). *Launching a National Conversation on Disaster Resilience in America: Workshop Summary*. The National Academies Press.

Ventura, C. E., García, H. J., & Martí, J. M. (2010). Understanding Interdependencies among Critical Infrastructures. *9th US National and 10th Canadian Conference on Earthquake Engineering, Toronto, Ontario, Canada*.

WEF. (2013). *Global Risks 2013 (Eight Edition)*. World Economic Forum.

WEF. (2014). *Global Risks 2014 (Ninth Edition)*. World Economic Forum.

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.

Wueest, C. (2014). *Targeted Attacks Against the Energy Sector*. Symantec Corporation.

Yohe, G. (2010). Risk Assessment and Risk Management for Infrastructure Planning and Investment. *The Bridge*, *40*(3), 14–22.