idn cadernos

ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO

idn Instituto da Defesa Nacional

nº 12

Estratégia da Informação e Segurança no Ciberespaço

Investigação conjunta IDN-CESEDEN

Dezembro de 2013

Instituto da Defesa Nacional

Os Cadernos do IDN resultam do trabalho de investigação residente e não residente promovido pelo Instituto da Defesa Nacional. Os temas abordados contribuem para o enriquecimento do debate sobre questões nacionais e internacionais.
As perspectivas são da responsabilidade dos autores não reflectindo uma posição institucional do Instituto de Defesa Nacional sobre as mesmas.

Director
Vitor Rodrigues Viana

Coordenador Editorial
Alexandre Carriço

Núcleo de Edições
António Baranita e Cristina Cardoso

Capa
Nuno Fonseca/nfdesign

Propriedade, Edição e Design Gráfico
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Composição, Impressão e Distribuição
Imprensa Nacional – Casa da Moeda, SA
Av. António José de Almeida – 1000-042 Lisboa
Tel.: 217 810 700 E-mail: editorial.apoiocliente@incm.pt www.incm.pt

ISSN 1647-9068
ISBN: 978-972-27-2272-8
Depósito Legal 344513/12
Tiragem 250 exemplares

ÍNDICE

Prólogo

A estruturação em rede das sociedades mais desenvolvidas e a criação do ciberespaço são traços fundamentais do ambiente estratégico do século XXI. O ciberespaço constitui um vetor estratégico privilegiado para o desenvolvimento cultural, social, económico e para a defesa dos valores das modernas sociedades da informação, requerendo por essa razão uma clara perceção do quadro das ameaças e vulnerabilidades a ele associadas.

Dentro deste âmbito, considera-se que o modo pelo qual os diferentes agentes fazem uso da informação conduz, de forma simultânea, ao aparecimento tanto de novas oportunidades como de novas ameaças no ciberespaço, trazendo, deste modo, para a condução política e estratégica dos Estados importantes consequências.

A presente monografia é o resultado da cooperação que, durante os anos de 2012 e 2013, o Instituto da Defesa Nacional (IDN) de Portugal e a Escuela de Altos Estudios de la Defensa (EALEDE) do Centro Superior de Estudios de la Defensa Nacional (CESEDEN) mantiveram em torno de um tema de plena atualidade: a Cibersegurança.

Subordinado ao título genérico "Estratégia da Informação e Segurança no Ciberespaço", aborda-se, de forma umas vezes conjunta e outras descrevendo as particularidades específicas associadas a cada país, alguns aspetos-chave que se podem articular da seguinte forma:

- Ciberespaço: Conceito e Âmbito de Aplicação em Segurança e Defesa;
- Estratégia de Segurança da Informação no Ciberespaço.

No que diz respeito à Segurança no Ciberespaço, desenvolve-se com profundidade:

- A Análise e Gestão do Risco Social;
- A Gestão de Riscos: infraestruturas críticas; ameaças; vulnerabilidades e as boas práticas para a análise e gestão dos riscos;
- Segurança da Informação no Ciberespaço e Capacidade de Resposta a Incidentes Informáticos;
- Ciberdefesa: Capacidades de Ciberdefesa; Ciberexército.

Analisa-se igualmente o "estado da arte" em Portugal e Espanha, para finalmente se chegar a umas conclusões conjuntas.

Este projeto, que define as implicações e a perceção do impacto do ciberespaço na Segurança e Defesa dos Estados, pretende caracterizar o enquadramento concetual e operacional adotado por Portugal e Espanha. Neste contexto, tendo em conta os esforços atualmente em curso nos dois países, procura-se identificar pontos de convergência e refletir sobre a possibilidade de desenvolvimento futuro de iniciativas conjuntas, sobretudo de natureza bilateral, mas também multilateral, no quadro das organizações internacionais, em particular da OTAN e da UE.

O documento é o resultado da aproximação de posições iniciais, superação de diferenças e flexibilização de posturas – um exercício exemplar do valor da negociação – com resultados que conferem um valor acrescentado a ambos os países. No final, conseguiu-se obter um produto moderno, incisivo e prospetivo que, sem dúvida, poderá constituir uma referência para outros países.

Adicionalmente, este projeto serviu também para reafirmar a vontade de cooperação em projetos comuns, que se iniciaram em 2010 e terão a sua continuidade no período 2013-14. Evidenciando-se o êxito conseguido nesta aposta conjunta, é possível constatar que estes projetos se transformaram numa realidade cooperativa exemplar.

Prologo

La estructuración en red de las sociedades más desarrolladas y la construcción del ciberespacio son características fundamentales del entorno estratégico del siglo XXI. El ciberespacio constituye un vetor estratégico privilegiado para el desarrollo cultural, social, económico y la defensa de los valores de las sociedades modernas, de la información y el ciberespacio, imponen una clara percepción del marco de las amenazas y vulnerabilidades.

Dentro de este marco, se considera que el modo en que los diferentes agentes utilizan la información resulta ser, de forma simultánea, generadora tanto de nuevas oportunidades como de nuevas amenazas en el ciberespacio, provocando así importantes consecuencias para la conducción política y estratégica de los Estados

La presente monografía es el fruto de la cooperación que durante los años 2012 y 2013 han mantenido el Instituto da Defesa Nacional (IDN) de Portugal y la escuela de Altos Estudios de la Defensa (EALEDE) del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) entorno a un tema de plena actualidad, la Ciberseguridad, que cuando se iniciaron estos estudios ya se percibió como tema emergente de gran importancia.

Bajo el título genérico "Estrategia de la Información y Seguridad en el Ciberespacio", se afronta, de forma unas veces conjunta y otras describiendo las particularidades específicas en cada país, un repaso en profundidad a algunos temas clave que se pueden articular en:

- Ciberespacio: Concepto y Ámbito de Aplicación en Seguridad y Defensa;
- Estrategia de Seguridad de la Información en el Ciberespacio.

En lo relacionado con la Seguridad en el Ciberespacio, se desarrolla en profundidad:

- El análisis y gestión del riesgo social
- La Gestión de Riesgos: Infraestructuras críticas; amenazas; vulnerabilidades y las buenas prácticas para el análisis y la gestión de riesgos
- Seguridad de la Información en el Ciberespacio y Capacidad de Respuesta ante Incidentes Informáticos
- Ciberdefensa: Capacidades de Ciberdefensa; Ciberejército;

Igualmente se afronta el Estado del Arte en Portugal y España, para llegar por último a unas conclusiones conjuntas.

Este proyecto de definición de las implicaciones y percepción del impacto del ciberespacio en la Seguridad y Defensa de los Estados, pretende caracterizar el marco conceptual y operativo adotado por Portugal y España. En este contexto, teniendo en

cuenta los esfuerzos atualmente en curso en ambos países, se busca identificar los puntos de convergencia y examinar la posibilidad de desarrollo futuro de iniciativas conjuntas, sobre todo de naturaleza bilateral, y también multilateral, en el marco de las organizaciones internacionales, en particular la OTAN y la UE.

El texto, es el resultado de aproximación de posiciones iniciales, superación de diferencias y flexibilización de posturas –un ejercicio ejemplar del valor de la negociación- con resultados que dan valor añadido a ambos países. Se ha obtenido un producto moderno, incisivo y prospetivo, que sin duda será referente para muchos otros países.

Además, este proyecto ha servido para afianzar los proyectos comunes, que se iniciaron en 2010, y que tendrá su continuidad en el periodo 2013-14, evidencia del éxito obtenido en esta apuesta conjunta que se ha transformado en una realidad cooperativa ejemplar.

Direção: Vítor Daniel Rodrigues Viana (Major-General, Diretor do IDN)
Coordenador: Luís Costa Figueiredo (Coronel do Exército, IDN)
Investigadores: Fernando Vicente Freire (Coronel do Exército, IDN)
Paulo Viegas Nunes (Tenente-Coronel do Exército, Estado-Maior do Exército)

Presidente: Fernando Davara (General de Brigada, Ejército de Tierra)
Vogal: Oscar Pastor Acosta (Gerente de Segurança da ISDEF – Ingeniería de Sistemas para la Defensa de España)
Coordenador: Emilio Sánchez de Rojas (Coronel, Ejército de Tierra – CESEDEN)

Parte I – Enquadramento

A estruturação em rede das sociedades mais desenvolvidas e a própria construção do ciberespaço constituem características fundamentais da conjuntura estratégica do século XXI. Neste contexto, pensar o mundo em que vivemos passa por perspetivar uma sociedade em rede, em que a interação entre os homens deixa de ser influenciada por barreiras geográficas e passa a ser condicionada pela disponibilidade e pelo tempo de acesso aos recursos de informação.

Entendendo a evolução tecnológica como um desafio e uma oportunidade de convergência para padrões de crescimento económico e social mais desenvolvidos, importa incentivar a inovação e fomentar a adoção das novas Tecnologias de Informação e Comunicação (TIC) garantindo, de forma sustentada, a convergência nacional para a Sociedade de Informação. Dentro deste contexto, constata-se que a forma como os diferentes atores utilizam a informação pode ser simultaneamente geradora de novas oportunidades e de novas ameaças no ciberespaço, apresentando importantes implicações na condução da política e da estratégia dos Estados.

Exemplos como os da Estónia em 2007 e da Geórgia em 2008 demonstram que cada Estado terá que garantir não só a utilização segura do ciberespaço aos seus cidadãos como a salvaguarda da própria soberania. Neste contexto, importa analisar o risco social e o impacto dos diversos tipos de ciberataques, diferenciando os de motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocar em risco a Segurança e Defesa do Estado. Neste contexto, também se reconhece a existência de um nível nacional e supranacional da segurança cibernética, equacionada e integrada em dois domínios diferentes e complementares: a Cibersegurança e a Ciberdefesa.

Na era da informação criam-se cada vez mais dependências derivadas do funcionamento em rede. Por isso, não será possível assegurar o desenvolvimento e bem-estar social, sem garantir a segurança e proteção das infraestruturas essenciais ao normal funcionamento da vida em sociedade. Este tipo de infraestruturas, conhecidas como infraestruturas críticas nacionais, integra também as redes de informação. Nesse sentido, importa refletir sobre as principais envolventes da utilização da informação, em particular, o desenvolvimento de uma Estratégia da Informação Nacional e o levantamento de um sistema de proteção das infraestruturas de informação capaz de promover a livre utilização e garantir a segurança do ciberespaço.

1. Ciberespaço: Conceito e Âmbito de Aplicação em Segurança e Defesa

Não há dúvida de que o ciberespaço, como um ambiente "virtual onde se agrupam e relacionam utilizadores, linhas de comunicação, *sites*, fóruns, serviços de internet e outras

redes"[1], tornou-se um novo "espaço", que a par dos tradicionais domínios da interação humana como a terra, o mar, o ar e o espaço, é o meio onde se desenvolvem as atividades económicas, produtivas e sociais das nações mais desenvolvidas. "O Ciberespaço toca praticamente tudo e todos. Proporciona uma plataforma para a inovação e prosperidade, e os meios para melhorar o bem-estar geral de todo o mundo"[2].

Por isso, não é de estranhar que os governos manifestem a intenção de defender os ativos e interesses estratégicos dos seus países nesse âmbito. Assim, na "Estratégia Internacional para o Ciberespaço", assinada pelo presidente dos EUA, Barack Obama, podemos ler: "Todos os Estados têm o direito inerente de legítima defesa e de reconhecer que certos atos hostis realizados no ciberespaço podem obrigar a tomar ações no âmbito dos compromissos que temos com nossos aliados militares. Reservamo-nos o direito de usar todos os meios necessários: diplomáticos, informacionais, militares e económicos, adequados e consistentes com o direito internacional aplicável, a fim de defender a nossa nação, os nossos aliados, os nossos parceiros e os nossos interesses"[3].

Segundo o Dicionário da Real Academia Espanhola (DRAE), "ciberespaço" é o "ambiente artificial criado por meios informáticos"[4], enquanto "cibernauta" é a "pessoa que navega por ciberespaços"[5]. Não encontramos na DRAE a definição de "cibersegurança" ou "ciberdefesa", mas podemos encontrar que o prefixo "cyber"[6] é um elemento composto que significa "cibernético" e vem da palavra "cibernética". Esta, por sua vez, faz referência ao "estudo das analogias entre os sistemas de controlo e comunicação dos seres vivos e os das máquinas e, em particular, caracteriza a aplicação dos mecanismos de regulação biológica e tecnológica"[7]. Este termo apresenta uma definição similar no Dicionário Houaiss da Língua Portuguesa[8]. Etimologicamente, o termo vem do francês (*cibernétique*), que por sua vez o adotou do inglês (*cybernetics*), mas tem origem no grego (*κυβερνητικ*), onde ele se refere à "arte de governar um navio". Assim, podemos concluir que a "cibersegurança" se refere à "segurança cibernética", assim como a "ciberdefesa" se refere à "defesa cibernética".

Atendendo ao seu aspeto mais técnico, o ciberespaço pode ser definido como "um conjunto de redes e sistemas de comunicação que estão interligados, entre si de forma direta ou indireta"[9]. O ciberespaço é assim um ambiente em si mesmo, onde se deve

1 Gobierno de España, *Estrategia Española de Seguridad: Una responsabilidad de todos*. 2011.

2 White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. 2011.

3 White House, *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World*. 2011.

4 Real Academia Española, «ciberespacio», *Diccionario de la Lengua Española - Vigésima segunda edición*. oct-2001.

5 Real Academia Española, «cibernauta», *Diccionario de la Lengua Española - Vigésima segunda edición*. oct-2001.

6 Real Academia Española, «ciber-», *Diccionario de la Lengua Española - Vigésima segunda edición*. oct-2001.

7 Real Academia Española, «cibernética», *Diccionario de la lengua española - Vigésima segunda edición*. oct-2001.

8 Dicionário Houaiss da Língua Portuguesa, Instituto Antônio Houaiss de Lexicografia e Banci de Dados da Língua Portuguesa S/C Ltda (Rio de Janeiro), Círculo de Leitores, Lisboa, 2002, pp.922

9 O. Pastor Acosta, J. A. Pérez Rodríguez, D. Arnáiz de la Torre, y P. Taboso Ballesteros, *Seguridad Nacional y Ciberdefensa*, 1a. ed., vol. 6, 7 vols. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2009.

ter em linha de conta tanto a sua componente tecnológica, isto é, as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-los, como os fatores humanos, uma vez que são estes que caracterizam os utilizadores deste ambiente. Para se poder entender adequadamente seu funcionamento e os seus riscos, deve-se prestar especial atenção às pessoas que acedem ao ciberespaço assim como com as suas diferentes culturas e motivações.

No mundo globalizado de hoje, em que se procura o acesso a grandes quantidades de informação em tempo útil, o ciberespaço constitui uma dimensão crítica do funcionamento normal da sociedade moderna, da sua segurança, da sua economia, dos seus negócios, etc. A necessidade de acesso e troca permanente de informação tem inerentemente associada critérios de segurança, uma vez que esta informação deve ser protegida contra acessos ou modificações não autorizados.

Porém, o ciberespaço apresenta uma série de características particulares, que é necessário estudar com cuidado, de forma a podermos identificar a sua relevância nos âmbitos da segurança e defesa. Vejamos de forma sucinta quais são estas características:

Caráter dinâmico: O Ciberespaço tem uma frequência de mudança elevada. Os diferentes sistemas que o integram, mudam e modificam-se constantemente, especialmente as suas interligações. As vulnerabilidades são descobertas quase diariamente e as ameaças emergentes surgem e mudam constantemente.

Custo irrelevante de acesso: Hoje em dia a barreira económica de acesso ao Ciberespaço é muito pequena, estimando-se que atualmente mais de um terço[10] da população mundial tenha acesso à internet.

Enorme potencial de crescimento: Tanto a nível de funcionalidades como de velocidade de troca de informação.

Alta capacidade de processamento: Capacidade elevada de procura, processamento e também de armazenamento de informação.

Caráter assimétrico: Neste novo domínio, com muito poucos recursos podem-se desenvolver ações hostis de grande impacto. A assimetria revela-se tanto ao nível dos recursos como do conhecimento necessário para desenvolver essas ações.

Anonimato: É muito difícil detetar e seguir a origem de um ataque, o que dificulta a capacidade de dissuasão e resposta.

Alta capacidade para produzir efeitos físicos: Refletida na possibilidade de atingir uma ampla gama de indústrias e dispositivos.

Transversalidade: uma ação ou evento ocorrido no ciberespaço pode afetar um ou mais domínios de atividade das modernas sociedades, como sejam a área política, económica, social ou mesmo a segurança e defesa dos Estados.

No âmbito particular da Defesa, a terra, o mar, o ar e o espaço têm constituído os domínios tradicionais de desenvolvimento das operações militares e, por conseguinte,

10 ICT Data and Statistics Division - Telecommunication Development Bureau - International Telecommunication Union, «The World in 2011. ICT Facts and Figures», International Telecommunication Union, Place des Nations 1211 Geneva 20 - Switzerland, nov. 2011.

é neles que se têm centrado os esforços relacionados com a obtenção de capacidades militares. No entanto, o Ciberespaço já foi definido e aceite como o quinto domínio operacional, no qual se levam a cabo operações militares específicas e em relação ao qual as operações militares que se desenvolvem nos outros domínios dependem cada vez mais.

Até um passado recente, a orientação no campo da Defesa em matéria de proteção do ciberespaço, era essencialmente de natureza reativa e estática, focada na defesa dos sistemas de informação e telecomunicações, através da implementação de medidas preventivas, de deteção e de recuperação de diferente natureza (físicas, pessoal, técnicas, etc.). Esta abordagem tem sido tradicionalmente caracterizada como INFOSEC (*INformation SECurity*), assumindo em Espanha a designação de STIC (*Seguridad de las Tecnologías de la Información y las Comunicaciones*)[11] e em Portugal a designação de Segurança da Informação.

A nível internacional, quando nos referimos à segurança da informação e do ciberespaço, os termos frequentemente usados são normalmente expressos em inglês (*information assurance*[12] *cyber security, infosec, computer security, computer networks security, computer networks defence, cyber defence, critical information infrastructure protection*, ...[13]), mas geralmente o seu significado tem diferentes matrizes, dependendo do país de origem e de quem os usa. Neste âmbito, verifica-se que nem sempre é possível encontrar concordância com a tradução direta dos termos anglo-saxónicos que os compõem.

Devido à natureza dinâmica do próprio ciberespaço, as já mencionadas medidas "infosec", apesar de necessárias, já não resultam atualmente numa aproximação suficientemente forte para proporcionar um nível de proteção adequado, no que à segurança da informação se refere. É assim que surge o conceito de Ciberdefesa[14], procurando agrupar o conjunto de medidas e ações que se adaptam a este novo ambiente de informação dinâmico e que são capazes de proporcionar a proteção da informação e os sistemas que agora passam a ser geridos também de acordo com este novo cenário operacional. Além disso, realiza-se um estudo mais amplo dos serviços de segurança a proporcionar no próprio ciberespaço, não apenas focado na proteção da disponibilidade, integridade e confidencialidade, mas também incluindo serviços como autenticação, rastreabilidade e não-repúdio.

O ambiente do moderno campo de batalha é cada vez mais multidimensional e descontínuo, observando-se que as operações militares se foram alargando progressivamente a áreas tradicionalmente não militares. As Forças Armadas da era da informação

11 Centro Criptológico Nacional y José A. Mañas, «Guía de Seguridad de las TIC (CCN-STIC401) Glosario y Abreviaturas». dic-2006.

12 *Information Assurance* pode traduzir-se como *segurança (em sentido lato) da informação*, mas será certamente mais adequado traduzir-se este termo como *garantia da informação*, para podermos diferenciá-lo de *Information Security (INFOSEC)*, que normalmente tem um significado mais restrito quando se utiliza a língua inglesa.

13 Néstor Ganuza, Alberto Hernández, y Daniel Benavente, «NECCS-1: An Introductory Study to Cyber Security in NEC». NATO CCD COE Publications, jun-2011.

14 Ciberdefesa, em inglês "*Cyber Defence*", é definida como "a aplicação das medidas de segurança para proteger os componentes da infraestrutura TIC contra ciberataques, sendo estes ciberataques assumidos como "uma forma de guerra cibernética, que pode ocorrer em combinação com um ataque físico ou não, que se destina a perturbar os sistemas de informação de um adversário".

dependem, cada vez mais, da utilização do ambiente de informação e do próprio ciberespaço para conduzir todo o espectro das operações.

Neste contexto, no âmbito militar e intimamente ligadas ao conceito de ciberdefesa, surgem as Operações no Ciberespaço, ou *Computer Network Operations* (CNO), incluindo no seu âmbito ações de natureza defensiva, de exploração das capacidades dos possíveis adversários ou mesmo de resposta ofensiva. A nível internacional, diferentes nações e organizações têm vindo a adotar este conceito e estão atualmente a envidar esforços para obter as capacidades necessárias à sua implementação.

Assim, na doutrina tradicional dos nossos aliados, como é a do Departamento de Defesa dos Estados Unidos (DoD – *United States Department of Defense*), o Estado-Maior Conjunto indica, dentro da Doutrina de Operações de Informação[15], que as capacidades CNO se compõem de:

- ***Computer Network Defense*** *(CND)*, que inclui as medidas adotadas através da utilização de redes de computadores para proteger, controlar, analisar, detetar e responder a atividades não autorizadas nos sistemas de informação e comunicações. As ações CND não procuram apenas proteger os sistemas amigos de um adversário externo, mas também contemplam a possibilidade de a sua exploração ocorrer a partir do interior da própria organização.
- ***Computer Network Exploitation*** *(CNE)* que integra as capacidades de recolha de informações (intelligence) levadas a cabo através do uso de redes de computadores para recolher dados das redes de comunicações e dos sistemas de informação de um potencial adversário.
- ***Computer Network Attack*** *(CNA)*, que inclui as ações desenvolvidas através da utilização de redes de computadores para interromper, negar, degradar ou destruir a informação tratada pelas redes de comunicações e pelos sistemas de informação (do possível adversário), ou dos próprios sistemas de informação e comunicações amigos.

Perspetivando-se a tendência crescente para o aumento da capacidade disruptiva e destrutiva das ciberameaças, tanto a nível internacional como nacional, os países mais desenvolvidos têm vindo a desenvolver e a reforçar a sua capacidade nacional de ciberdefesa, explorando assim, de forma sinérgica e cooperativa, as capacidades existentes nas suas Forças Armadas. No caso de Portugal e Espanha, a cooperação com as estruturas da OTAN e da UE tem vindo também a ser explorada, de forma a defender os interesses nacionais e a fazer face ao espectro global das ameaças emergentes no ciberespaço.

2. Estratégia de Segurança da Informação no Ciberespaço

O extraordinário desenvolvimento das Tecnologias de Informação e das Comunicações tem convertido o ciberespaço num recurso vital para o funcionamento das moder-

15 Joint Chiefs of Staff, «Joint Publication 3-13 Information Operations». DoD, 13-feb2006.

nas sociedades, porque, por um lado, promove e simplifica a relação entre cidadãos, administração pública e empresas e, por outro, constitui um elemento básico para a prestação de serviços essenciais à comunidade. O crescimento da sua importância aumentou muito o interesse de organismos internacionais pelo seu desenvolvimento integrado, como a Organização para a Cooperação e Desenvolvimento Económico (OCDE), que considera a internet como um "elemento essencial para promover o desenvolvimento económico e bem-estar social, assim como para fortalecer a capacidade das sociedades para melhorar a qualidade de vida dos seus cidadãos"[16].

A importância das redes de comunicações no mundo de hoje é indissociável da necessidade de protegê-las contra incidentes de qualquer natureza que possam afetar o seu funcionamento, uma vez que as consequências da interrupção ou alteração da funcionalidade de redes de comunicações poderia afetar gravemente as funções sociais fundamentais, tal como é reconhecido pela Estratégia de Segurança espanhola[17]: "A Cibersegurança não é um mero aspeto técnico de segurança, mas a pedra angular da nossa sociedade e do sistema económico. Dada a importância crescente dos sistemas informáticos na economia, a estabilidade e prosperidade económica do país dependerá em grande medida da segurança do nosso ciberespaço."

Também Portugal, ao identificar a "Estratégia da Informação e a Segurança do Ciberespaço" como um vetor estratégico estruturante da revisão da sua Estratégia Nacional de Segurança e Defesa, reconhece a importância de proteger e defender o processo de geração de valor associado ao desenvolvimento do potencial estratégico nacional neste domínio.

Como esperado, o aumento exponencial da atividade no ciberespaço trouxe também um aumento da sua utilização maliciosa e dos incidentes de segurança[18]. Em particular, os ataques de natureza intencional têm sofrido um aumento significativo ao longo dos últimos anos, demonstrado, nomeadamente, pela utilização cada vez mais frequente da internet com o propósito de mobilização social ou protesto político e, acima de tudo, pelo surgimento e desenvolvimento de uma autêntica indústria de produção e exploração de código malicioso (vírus, *trojans*, criação e operação de *botnets*[19], etc.), caracterizada por um elevado nível de especialização e cujos benefícios económicos são substancialmente maiores que o tráfico mundial de marijuana, cocaína e heroína[20].

Por esta razão, governos e organizações internacionais têm demonstrado uma preocupação crescente pela segurança do ciberespaço, o que se materializou na publicação,

16 Organisation for Economic Co-Operation and Development, «Shaping Policies for the Future of the Internet Economy», OECD, Seoul, Korea, OECD Ministerial Meeting on the Future of the Internet Economy, mar. 2008.

17 Gobierno de España, *Estrategia Española de Seguridad: Una responsabilidad de todos*. 2011.

18 European Network and Information Security Agency (ENISA), «Inter-X: Resilience of the Internet Interconnection Ecosystem», abr. 2011.

19 Daniel Plohmann, Elmar Gerhards-Padilla, y Felix Leder, «Botnets: Detection, Measurement, Disinfection & Defence», European Network and Information Security Agency (ENISA), mar. 2011.

20 Symantec, «Informe sobre Cibercrimen de Norton», 2011.

por parte de muitas nações, das respetivas Estratégias Nacionais de Cibersegurança. A título de exemplo, mencionamos os documentos elaborados pelos governos dos Estados Unidos[21], Canadá[22], Japão[23], Reino Unido[24], Alemanha[25], França[26], e Holanda[27]. No âmbito multinacional, diferentes organizações como a União Internacional das Telecomunicações[28], a Organização para a Cooperação e Desenvolvimento Económico[29] ou a Organização do Tratado do Atlântico Norte[30] têm redigido documentos que refletem as respetivas posições sobre a segurança das redes de comunicações e do próprio ciberespaço. No que diz respeito à União Europeia, foi recentemente publicada uma Estratégia de Cibersegurança que pretende constituir uma base comum para todos os Estados membros[31]. De acordo com o programa de trabalho da Comissão para 2012[32], foi entretanto publicado pela ENISA um conjunto de normas para garantir a segurança das redes de comunicações da UE como dos próprios Estados membros[33].

No âmbito militar, na sequência da aprovação em 2009 de um Conceito de Operações em Redes de Computadores[34], o Estado Maior da União Europeia (*European Military Staff* – EUMS) desenvolveu também um Conceito de Ciberdefesa que foi entretanto aprovado pelo Conselho da UE[35].

Finalmente, em Espanha, o ministro do Interior anunciou no início de 2012 a intenção do Governo avançar com a elaboração da Estratégia Espanhola de Cibersegurança[36].

---

21 White House, *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World*. 2011.

22 Government of Canada, *Canada's Cyber Security Strategy - For a Stronger and more Prosperous Canada*. 2010.

23 Information Security Policy Council of Japan, *Information Security Strategy for Protecting the Nation*. 2010.

24 UK Office of Cyber Security, *Cyber Security Strategy of the United Kingdom Safety, Security and Resilience in Cyber Space*. 2009.

25 Federal Ministry of Interior, *Cyber Security Strategy for Germany*. 2011.

26 Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *Information systems defence and security - France's strategy*. 2011.

27 Ministry of Security and Justice, *The National Cyber Security Strategy (NCSS)*. 2011.

28 UIT-T, «Seguridad de las telecomunicaciones y las tecnologías de la información - Exposición general de asuntos relacionados con la seguridad de las telecomunicaciones y la aplicación de las Recomendaciones vigentes del UIT-T». 2009.

29 OECD, «OECD Policies for Information Security & Privacy». 2009.

30 Néstor Ganuza, Alberto Hernández, y Daniel Benavente, «NECCS-1: An Introductory Study to Cyber Security in NEC». NATO CCD COE Publications, jun-2011.

31 Disponível em http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

32 Comisión Europea, *COM (2011) 777 final/2 Vol. 2/2. Anexo a la Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones. Programa de Trabajo de la Comisión para 2012*. 2011.

33 Disponível em http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

34 EU Concept for Computer Network Operations in EU-led Military Operations (CNO) [13537/09. dated 22 September 2009]

35 EU Concept for Cyber Defence for EU-led Military Operations [EEAS 01729/12. dated 08 October 2012]

36 Mercedes Oriol Vico, «Apoyo Personal del Ministro del Interior a la Ciberseguridad», *SEGURITECNIA*, pp. 22–24, jun-2012.

Do mesmo modo, o Governo de Portugal, mediante resolução ministrial [37] estabeleceu como prioritária a revisão da Estrutura Nacional de Segurança da Informação e o levantamento de um Centro Nacional de Cibersegurança, tendo para esse efeito já sido apresentada uma primeira proposta de Estratégia Nacional de Cibersegurança[38].

37 Resolução Conselho de Ministros n.º 12 de 2012, *Diário da República*, 1.ª Série, n.º 27, 7 de fevereiro.

38 ENC, (2012). *Proposta de Estratégia Nacional de Cibersegurança*. Disponível em http://www.gns.gov.pt/NR/rdonlyres/ED57762F-3556-4C05-9644-888E35C790BB/0/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf. Consultado em 23 de novembro de 2012.

Parte II – Segurança no Ciberespaço

1. Análise e Gestão de Risco Social

A análise da cartografia tradicional não nos permite verificar que no interior do território nacional existem diversos cabos de telecomunicações e infraestruturas de informação, materializando os milhares de ligações transnacionais que permitem dar suporte à internet (*World Wide Web*). Existe assim uma falta de perceção sobre a natureza e limites do ciberespaço, caracterizado pela indefinição de fronteiras tais como se conhecem na sua expressão física ou geográfica. Esse facto, gera a dificuldade de definir a maneira pela qual um Estado pode exercer a sua soberania sobre uma área ou ambiente que não domina e não controla.

O elevado ritmo da evolução tecnológica tem vindo também a reduzir significativamente o ciclo de vida útil dos produtos associados às novas TIC. O facto de as suas aplicações serem objeto de ampla aceitação por grande parte da sociedade e possuírem um ciclo de vida cada vez mais curto, faz com que muitas empresas acelerem o processo de comercialização, lançando produtos para o mercado (*hardware* e *software*) sem que estejam completamente testados. Esta situação induz novas vulnerabilidades estruturais e funcionais nas redes e nos sistemas que integram as infraestruturas de informação uma vez que estas passam a incluir não só diferentes gerações de equipamentos mas também equipamentos com potenciais problemas de funcionamento.

A preocupação com estas vulnerabilidades assumiu especial importância e evidência na transição do milênio passado, em que um problema informático (*bug* do ano 2000) obrigou à realização de testes exaustivos a todas as infraestruturas que utilizassem processadores. Só a completa compreensão da extensão das interdependências de uma infraestrutura (verticais e/ou horizontais) permite identificar as necessárias medidas corretivas, destinadas a controlar este efeito. O facto de esta interdependência transcender as "fronteiras de soberania" do Estado introduz ainda, como vimos, um fator de complexidade adicional ao problema.

Neste contexto, também é motivo de preocupação o facto de existir uma forte dependência das infraestruturas de informação relativamente do funcionamento de uma grande heterogeneidade de redes de todos os tipos. Se falhar uma destas redes produz-se um "efeito dominó" e em pouco tempo deixam de operar muitos dos sistemas de que dependem infraestrutura críticas, essenciais para a vida da sociedade.

Neste caso, atribui-se um especial destaque às redes de energia e de telecomunicações, das quais dependem física, estrutural e funcionalmente múltiplos organismos e serviços, como as centrais de produção e distribuição de energia elétrica, os serviços de emergência, o sistema bancário e os próprios sistemas de comando e controle das Forças Armadas.

A dimensão do risco está intimamente ligada ao valor/dependência que um ator apresenta face ao recurso (informação) e às consequências negativas que a sua utilização incorreta pode implicar para a sua atividade. Os recursos de informação são considerados

tanto mais críticos quanto maior for o grau de dependência existente sobre eles. As medidas de segurança a adotar, devem ser proporcionais ao impacto negativo previsto para a sua indisponibilidade ou funcionamento incorreto.

De acordo com esta abordagem, como se discutirá adiante, é possível determinar o risco através de métodos qualitativos/quantitativos que permitam realizar a sua avaliação[39] com base no valor da ameaça esperada, na vulnerabilidade avaliada/determinada, no valor da medida de salvaguarda adotada para o minimizar e no valor do impacto previsto para o ataque/ameaça na infraestrutura de informação.

Quando se analisa o risco associado às infraestruturas de informação nacionais, é necessário ter em atenção que este resulta do efeito conjugado de três fatores importantes: dos recursos a proteger (alvos potenciais), da deteção das vulnerabilidades da infraestrutura de informação e das ameaças que, explorando essas vulnerabilidades, podem afetar os recursos que pretendemos proteger.

Avaliado o risco, após a análise realizada, este pode ser gerido de diversas formas, nomeadamente através da sua redução (adoção de contramedidas), manutenção (aceitação do risco) ou transferência para terceiros. A escolha associada a cada uma destas três opções está, naturalmente, intimamente relacionada com o valor que se atribui ao recurso a proteger. Quanto mais crítico for um recurso, maior será a necessidade de assegurar a adoção das contramedidas necessárias para reduzir o risco que se lhe encontra associado. Procura-se assim garantir a disponibilidade do recurso e evitar a possível rutura da infraestrutura crítica, mesmo quando em presença de um ciberataque.

Face a este objetivo, a segurança e a proteção contínua das infraestruturas de informação tem de ser encarada como um processo contínuo e sistémico. Associada à realização de uma contínua análise do risco, todos os países terão também de assegurar permanentemente a sua gestão, conforme se pretende detalhar adiante.

2. Gestão de Riscos

2.1. Ativos Estratégicos: Infraestruturas Críticas

Todos os dias fazemos uso das inovações oferecidas pelas tecnologias móveis, pelas comunicações eletrónicas e pela internet, conforme se encontra refletido nos relatórios de organismos como a CMT (*Comisión del Mercado de las Telecomunicaciones*)[40], que indica que, em abril de 2012, o número de linhas de telefones celulares em operação em Espanha atingiu os 55,2 milhões; existiam 119,6 linhas para cada 100 habitantes; e havia 11,2 milhões de linhas de banda larga, 24,4 por 100 habitantes[41].

---

39 Pode-se quantificar o risco por meio da seguinte expressão: R = (A.V / Ms), onde R é o valor do risco, A o da ameaça, V o da vulnerabilidade, Ms o da medida de salvaguarda e I o do impacto previsto . Ver Jesus Bispo (2002). *A Sociedade de Informação e a Segurança Nacional.* Lisboa: Instituto Português da Conjuntura Estratégica.

40 Disponível em http://www.cmt.es/.

41 Comisión del Mercado de las Telecomunicaciones, «NOTA MENSUAL», CMT, abr. 2012.

As pessoas, os Estados e as empresas estão cada vez mais "digitalmente dependentes", como demonstra o facto de que hoje cerca de 30% do comércio mundial se basear na internet[42]. Deste modo, as TIC (Tecnologias da Informação e Comunicação) e a segurança da informação revelam-se cada vez mais de uma importância fundamental, tanto para proteger a privacidade e construir a confiança nos canais eletrónicos, como para garantir o funcionamento eficaz dos Estados e das organizações.

Por outro lado, as redes de comunicações estão a tornar-se cada vez mais complexas e, em consequência, as suas vulnerabilidades também aumentam com a sua complexidade. As violações de segurança e os ciberataques podem causar danos consideráveis a pessoas e organizações, e o seu elevado grau de interconexão pode propagar muito rapidamente o seu impacto tanto a nível nacional como internacional. Em suma, a cibersegurança deve ser uma preocupação para todos.

As infraestruturas sobre as quais assentam os serviços essenciais, isto é, as funções sociais vitais, como a saúde, os serviços de emergência, a segurança, o bem-estar social e económico da população, não estão imunes a esta tendência. Assim, por exemplo, centros geradores e sistemas de transporte de energia, as refinarias de petróleo ou os sistemas de distribuição de gás, utilizam os Sistemas de Controlo Industrial (ICS – *Industrial Control Systems*)[43] para a gestão e a monitorização dos correspondentes processos. Estes ICS têm passado por uma transformação significativa nos últimos anos, passando de sistemas autónomos de tecnologias proprietárias, a arquiteturas abertas, altamente interligadas com sistemas corporativos e inclusive com a internet[44]. Estas infraestruturas passam a ser consideradas infraestruturas críticas (IC)[45], porquanto a sua perturbação ou destruição pode afetar gravemente um Estado a ponto de este passar a ser incapaz de manter a funcionar os serviços essenciais que elas asseguram[46].

Os antecedentes relacionados com a proteção das IC na Europa[47] remontam ao Livro Verde, de 17 de novembro de 2005, onde se coloca a necessidade de lançar um Programa Europeu para a Proteção de Infraestruturas Críticas[48]. Este documento apresentou as opções para uma resposta da Comissão ao pedido do Conselho para estabelecer um Programa Europeu orientado para a Proteção de Infraestruturas Críticas (PEPIC, em inglês EPCIP – *European Programme for Critical Infrastructure Protection*) e para a criação

42 ENISA, «Protecting Europe's Citizens against Cyber Attacks», 2008.

43 Sistemas e redes de comando e controlo desenhados para apoiar os processos industriais. O maior subgrupo das ICS são os sistemas SCADA (Supervisory Control and Data Acquisition).

44 ENISA, «Protecting Industrial Control Systems. Recommendations for Europe and Member States», Report/Study, dic. 2011.

45 Department of Homeland Security, «Critical Infrastructure». [Online]. Available: http://www.dhs.gov/critical-infrastructure. [Accessed: 14-ago2012].

46 Department of Homeland Security, *Homeland Security Presidential Directive 7*. 2003.

47 Infraestruturas críticas europeias são as infraestruturas críticas situadas em algum Estado membro da União Europeia, cuja perturbação ou destruição afetaria gravemente, pelo menos as desse Estado membro.

48 Comisión Europea, *COM(2006) 786 final Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas*. 2006.

de uma Rede de Informação para a Comunicação de Alertas em Infraestruturas Críticas (CIWIN – *Critical Infrastructure Warning Information Network*).

A 12 de dezembro de 2006, a Comissão aprova a comunicação sobre o PEPIC da qual se estabelece um quadro legislativo para as atividades de proteção das infraestruturas críticas na UE (União Europeia) e, posteriormente, surge a Diretiva 2008/114/CE do Conselho[49], que estabelece um procedimento para a identificação e designação das Infraestruturas Críticas Europeias (ICE), onde se defende uma abordagem comum para avaliar a segurança de tais infraestruturas, a fim de melhorar e, assim, proteger as necessidades da população.

Em Espanha, a transposição da citada diretiva, a Lei 8/2011, pela qual se estabelecem medidas para a proteção das infraestruturas críticas, define 12 setores estratégicos responsáveis por proporcionar os serviços essenciais para o Estado e para os cidadãos[50].

Dentro de cada um destes setores (Administração, Espaço, Indústria Nuclear, Indústria Química, Centros de Investigação, Água, Energia, Saúde, Tecnologias da Informação e Comunicações, Transporte, Alimentação, Sistema Financeiro e Tributário), existem infraestruturas de cujo funcionamento dependem estes serviços essenciais, designadas por Infraestruturas Estratégicas (IE)[51]. As IE que são reconhecidas como indispensáveis para o bom funcionamento dos serviços essenciais são designadas por Infraestruturas Críticas (IC)[52].

Nesta lei, define-se o Sistema de Proteção das Infraestruturas Críticas, composto por uma série de instituições, organismos e empresas, quer dos setores público quer do privado, com responsabilidades atribuídas ao nível da garantia do normal funcionamento dos serviços essenciais ou da segurança dos cidadãos, traduzindo um particular ênfase na necessidade de perspetivar a segurança a partir de uma visão holística.

Com a finalidade de desenvolver, definir e ampliar os aspetos contemplados nesta lei foi publicado o Real Decreto 704/2011[53], através do qual se aprova o Regulamento relativo à proteção das infraestruturas críticas. Como aspetos a rever, podemos citar os diferentes planos de proteção incluídos neste Real Decreto:

- **Planos Estratégicos Setoriais** (PES): constituem os instrumentos de estudo e planeamento que abrangem todo o território nacional e que permitirão conhecer, em cada um dos setores abrangidos, quais são os serviços essenciais prestados à sociedade, o seu desempenho global, as vulnerabilidades do sistema, as potenciais consequências da sua indisponibilidade e as medidas estratégicas necessárias para a manutenção da sua atividade.

49 Consejo de la Unión Europea, *Diretiva 2008/114/CE*. 2008.

50 Jefatura del Estado, *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. 2011.

51 Infraestruturas Estratégicas são instalações, redes, sistemas e equipamentos e as tecnologias da informação sobre as quais reside o funcionamento dos serviços essenciais.

52 Infraestruturas Críticas são infraestruturas estratégicas cujo funcionamento é indispensável e não permite soluções alternativas, pelo que a sua perturbação ou destruição teria um grave impacto sobre os serviços essenciais.

53 Ministerio del Interior, *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*. 2011.

- **Plano de Segurança do Operador** (PSO): são os documentos estratégicos que definem as políticas gerais dos operadores críticos, destinados a garantir a segurança do conjunto de instalações ou sistemas da sua propriedade ou gestão.
- **Planos de Proteção Específicos** (PEP): são documentos operacionais onde se devem definir medidas concretas já tomadas e aquelas que se prevê venham a ser adotadas pelos operadores críticos para garantir a segurança integral (física e lógica) das suas infraestruturas críticas.

Como já foi mencionado anteriormente, as IC não estão imunes ao impacto dos avanços tecnológicos e, portanto, podemos dizer que quase todas têm como denominador comum uma base tecnológica que as sustenta, as TIC. Portanto, quando se fala em proteção das IC, espera-se que a cibersegurança vá ter um peso muito importante:

- Por um lado, temos as TIC que em si mesmas prestam um serviço essencial e que, portanto, constituem as IC do setor estratégico das TIC, ou infraestruturas críticas da informação.
- Por outro, as TIC são necessárias à prestação adequada de serviços essenciais por parte de IC de outros setores estratégicos, como por exemplo, os ICS, os sistemas SCADA, etc.

Quanto ao primeiro aspeto, os antecedentes a nível europeu têm origem na Diretiva COM (2006) 251 da Comissão Europeia[54], na qual se estabelece uma abordagem a três níveis, que inclui medidas específicas para a segurança das redes e da informação, o quadro regulamentar das comunicações eletrónicas e define o combate ao cibercrime como uma prioridade.

Posteriormente, com a Diretiva COM (2009) 149 da Comissão Europeia[55], foram definidos cinco pilares para a segurança das TIC: preparação e prevenção, deteção e resposta, mitigação e recuperação, a cooperação internacional e a definição de critérios para o setor estratégico das TIC.

Surge entretanto também a Diretiva COM (2011) 163 da Comissão Europeia[56], que se pode considerar o detonador para a materialização de uma Estratégia Europeia para a Segurança da Internet (ESIS – *European Strategy for Internet Security*), que tem já como objetivo a proteção das IC do setor estratégico TIC e não só da internet, contrariamente ao que sugere a sua designação. Finalmente, mais recentemente, foi aprovada essa estratégia que propõe, entre outras, as seguintes ações[57]:

- Designar agências em cada Estado-membro.
- Integrar os CERT (*Computer Emergency Response Teams*) governamentais numa rede europeia para fomentar a troca de informações.

---

54 Comisión Europea, *COM(2006) 251 final - Una estrategia para una sociedad de la información segura – «Diálogo, asociación y potenciación»*. 2006.

55 Comisión Europea, *COM(2009) 149 final sobre protección de infraestructuras críticas de información «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»*. 2009.

56 Comisión Europea, *COM(2011) 163 final sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global»*. 2011.

57 Disponível em http://ec.europa.eu/information_society/newsroom/cf/dae/ document.cfm?doc_id=1667.

- Definir medidas orientadas para criar uma cultura de segurança da informação e incentivar a colaboração público/privado.
- Acordo para o estabelecimento de protocolos em caso de incidentes.
- Incentivar o setor privado para melhorar a adoção das boas práticas de segurança e para que se melhore a segurança de produtos e serviços.
- Reforçar e coordenar melhor os esforços de I&D + I na área da segurança da informação.
- Incentivar, a partir da UE, os Estados membros a reforçar os mecanismos apropriados para melhorar a sua cibersegurança.

Como já mencionado anteriormente, a maioria das nações não se encontra alheia a esta tendência, sendo possível identificar muitas estratégias nacionais em matéria de cibersegurança, algumas das quais já foram inclusivamente sujeitas a revisões: Estónia, Finlândia, Eslováquia em 2008, Canadá e Japão em 2010, República Checa, França, Alemanha, Lituânia, Luxemburgo, Holanda e Reino Unido em 2011.

No estudo realizado pela ENISA sobre as estratégias nacionais de segurança cibernética[58], os aspetos comuns a todas elas, relacionados especificamente com as IC, são os seguintes:

- Necessidade de identificar as IC, incluindo os ativos críticos, os serviços e as interdependências entre elas.
- Desenvolver ou melhorar, tanto a prevenção, deteção e a capacidade de resposta como os planos de recuperação e as medidas de proteção das IC.

Por outro lado, merecem uma menção especial as iniciativas levadas a cabo pelos Estados Unidos, que já no ano de 2002 aprovaram o Projeto de Implementação da Lei de Gestão Federal da Segurança da Informação (FISMA – *Federal Information Security Management Act*), que visava a proteção das infraestruturas críticas de informação no âmbito federal[59]. Mais tarde, no Plano de Proteção das Infraestruturas Nacionais (NIPP – *National Infrastructure Protection Plan*), aprovado em 2009, enfatiza-se a necessidade de incluir as ameaças cibernéticas nas análises de risco das IC[60]. Atualmente, o *Cybersecurity Act* de 2012[61], já requer que os operadores realizem a análise de risco cibernético das suas IC.

Como se tem indicado, tanto em Espanha como em Portugal ainda estão a ser desenvolvidos os trabalhos para a publicação da Estratégia Nacional de Cibersegurança, onde se espera que venha a ser atribuída uma ênfase especial à proteção das IC, em linha com o que acontece com as restantes estratégias nacionais já publicadas.

A respeito da proteção das TIC que sustentam as IC de outros setores estratégicos, podemos citar como referências nacionais em Espanha as Diretrizes STIC, do CCN

58 ENISA, «National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace», Report/Study, may 2012.

59 Senate and House of Representatives of the United States of America, *Federal Information Security Management Act of 2002 - Title III of the E-Government Act (Public Law 107-347)*. 2002.

60 Department of Homeland Security, *National Infrastructure Protection Plan - Partnering to enhance protection and resiliency*. 2009.

61 Senate and House of Representatives of the United States of America, *Cybersecurity Act*. 2012.

(Centro Criptológico Nacional)[62], nomeadamente, as pertencentes à série 480, focadas na proteção dos sistemas SCADA:

- CCN-STIC – 480A SCADA - Guia de boas prácticas.
- CCN-STIC – 480B SCADA – Compreender o risco do negócio.
- CCN-STIC – 480C SCADA – Implementar uma arquitetura segura.
- CCN-STIC – 480D SCADA – Estabelecer capacidades de resposta.
- CCN-STIC – 480E SCADA – Melhorar a consciencialização e as competências específicas.
- CCN-STIC – 480F SCADA – Gerir o risco de terceiros.
- CCN-STIC – 480G SCADA – Desenvolvimento estruturado de projetos.
- CCN-STIC – 480H SCADA – Estabelecer uma direção permanente dos processos.

2.2. Ameaças

A ameaça à segurança das TIC pode ser definida como "qualquer circunstância ou evento passível de explorar, intencionalmente ou não, uma vulnerabilidade específica num sistema de TIC, resultando numa perda de confidencialidade, integridade e disponibilidade da informação manipulada ou da integridade ou disponibilidade do Sistema"[63]. Tomando como base esta definição, existem diferentes tipologias de ameaças que, por afetarem os sistemas, podem ser agrupadas em:

- Desastres naturais;
- Ameaças de origem industrial;
- Erros ou falhas não intencionais;
- Ataques deliberados.

Ainda que as ameaças associadas às catástrofes naturais, a origem industrial e a erros ou falhas não intencionais, estejam sempre presentes, é necessário analisar com maior profundidade os ataques deliberados, já que a sua sofisticação, precisão e potencial impacto estão em constante evolução, elevando o nível de risco a que os sistemas estão submetidos. A sua identificação e catalogação correta é a chave para se poderem estabelecer estratégias adequadas de proteção do ciberespaço.

Dependendo da motivação associada aos ataques deliberados, podemos agrupar as ameaças em[64]:

- **Cibercrime**, centradas essencialmente na obtenção de benefícios económicos através de ações ilegais. As ações relacionadas com a fraude bancária, com cartões de crédito ou a realização de transações em diferentes páginas *web*, constituem exemplos de ações comuns relacionadas com este tipo de ameaças.

62 Disponível em https://www.ccn.cni.es/.

63 Centro Criptológico Nacional y José A. Mañas, «Guía de Seguridad de las TIC (CCN-STIC401) Glosario y Abreviaturas». dic-2006.

64 O. Pastor Acosta, J. A. Pérez Rodríguez, D. Arnáiz de la Torre, y P. Taboso Ballesteros, *Seguridad Nacional y Ciberdefensa*, 1a. ed., vol. 6, 7 vols. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2009.

- **Ciberespionagem**, com foco na obtenção de informações, seja para benefício próprio ou para deter um benefício monetário posterior com a sua venda. A informação mais suscetível de identificar-se neste campo pode pertencer, nomeadamente, a um governo ou até a organizações privadas, e ser classificada, sendo esta uma mais valia para os atacantes.
- **Ciberterrorismo**, onde se procura um impacto social e político significativo pela destruição física. Neste contexto, as infraestruturas críticas constituem os alvos de ataque mais prováveis.
- **Ciberguerra**, pode ser definida como uma luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha.

Finalmente, o "*hacktivismo*" ou ciberactivismo, pelo seu impacto crescente também tem vindo a assumir-se como um campo de ação da ciberameaça.

Para se poder analisar as ameaças que podem afetar cada infraestrutura é conveniente determinar quais são as possíveis fontes de ameaças ou atores com mais possibilidade de ataque, assim como a probabilidade de que este ataque ocorra com base nas suas motivações. Estas fontes de ameaça podem ser classificadas da seguinte forma[65]:

- Cibercriminosos;
- Espiões industriais;
- "*Hacktivistas*";
- Terroristas;
- Nações;
- *Hackers*;
- Pessoal interno.

Por outro lado, as motivações, que podem ser independentes da origem da ameaça podem, por sua vez, classificar-se do seguinte modo[66]:

- **Benefícios económicos**. Constituem a motivação mais comum no domínio do ciberespaço. A realização de atos fraudulentos para conseguir dinheiro, o roubo de informações para venda pela melhor oferta ou a execução de ataques (ou fornecer os meios para isso) em troca de um benefício monetário são atos comuns que se enquadram nesta motivação. Cibercriminosos, espiões industriais e o pessoal interno são tradicionalmente os perfis do atacante com essa motivação.
- **Vantagens táticas ou competitivas**. Esta é outra motivação que pode suscitar a atuação de diferentes agentes. Por exemplo, o roubo de informação militar de uma nação no meio de um conflito pode dar uma vantagem tática ao inimigo, ou a obtenção de informações relacionadas com uma organização ou empresa pode dar uma vantagem competitiva a outra entidade. As nações e os espiões industriais são os agentes mais suscetíveis a ter essa motivação.

65 Daniel Benavente y Spanish Defence Staff, «Threat Analysis Methodology. Spanish input for MNE 7 Objetive 3.1 Risks, Vulnerabilities and Threats.» 2012.

66 Idem.

- **Motivações políticas**. Podem levar diferentes organizações a atacar ou realizar ações prejudiciais contra governos ou organizações públicas. Os perfis de ameaça que mais se encaixam nesta motivação são os terroristas e os "hacktivistas". Os conflitos entre diferentes nações também se encaixam, por vezes, dentro deste âmbito.
- **Destruição ou dano**. Os terroristas surgem também associados claramente a essa motivação, pois tendem a procurar a execução de ataques que têm esse efeito. Por outro lado, as nações que entram em conflito também podem vir a inserir-se neste grupo.
- **Fama ou vingança**. A procura de notoriedade e fama está geralmente associada aos *hackers*, que buscam reconhecimento em diferentes comunidades e fóruns, tendo como objetivo saltar as barreiras de segurança, mas não causar nenhum dano, embora possam aceder a informações sensíveis. Pessoal interno de uma organização também pode ser movido por esta motivação, mas estes tendem a perpetrar ações mais relacionadas com vingança.

Um primeiro critério para determinar a classificação dos ciberataques pode passar também por analisar o nível de organização dos mesmos, agrupando-os em[67]:

- **Ataques simples**. Ataques sem coordenação ou com um nível de organização muito reduzido, executados por uma pessoa ou várias mas sem nunca formar uma organização propriamente dita. O seu impacto é médio-baixo.
- **Ataques organizados**. Ataques que são executados e coordenados por um número significativo de pessoas que fazem parte de um grupo organizado. O impacto é normalmente médio, mas depende do tipo de objetivos que buscam.
- **Ameaças Persistentes Avançadas** (APT – *Advanced Persistent Threats*). Estas ameaças são criadas por um grupo de pessoas com um perfil de elevada perícia tecnológica; permanecem ao longo do tempo e o seu desenvolvimento está particularmente focado num alvo específico. Com uma precisão muito elevada, a probabilidade de ocorrência é alta e o seu impacto pode ser bastante forte.
- **Ataques coordenados de grande escala**. Esses ataques são executados e dirigidos por uma organização ou uma nação, e envolvem um elevado número de atores, que podem pertencer ou não à organização. O impacto pode ser elevado ou muito elevado.
- **Ciberataques coordenados com ataques físicos**. O nível de coordenação que requer este tipo de ataque é o mais elevado, e a combinação entre ataques em diferentes dimensões (terra, mar e ar) deve ser executado com grande precisão. O impacto é extremamente elevado.

De acordo com o último relatório sobre o estado das ciberameaças em 2011, do Centro Criptológico Nacional de Espanha[68], as tendências reveladas pelas ameaças mais comuns são:

67 Idem.

68 CCN-CERT, «Ciberamenazas 2011 y Tendencias 2012», mar. 2012.

- Ameaças relacionadas com o campo da ciberespionagem são as mais dinâmicas e, dentro deste âmbito, as APT estão a aumentar o risco progressivamente, prevendo-se que venham a proporcionar um nível de risco bastante elevado. Os ataques direcionados podem ser precedidos de uma APT.
- O *Hacktivismo* tornou-se especialmente importante em 2011, não apenas pelo número de ataques e pela sua frequência de execução, mas também pela sua agressividade e pelo seu elevado nível de divulgação social.
- Ataques contra ferramentas e produtos de autenticação e Autoridades de Certificação (CA – *Certification Authority*[69]), sendo o objetivo final atacar as organizações com um alto valor em propriedade intelectual. A estratégia proposta, baseia-se em atacar entidades que podem proporcionar meios para atacar as primeiras de forma mais eficiente.
- O *malware* continua a evoluir, sendo os "Cavalo de Troia" o tipo de *malware* dominante e a evolução do código malicioso "ZeuS" um problema a considerar. Os *exploits kits* e *botnets* ainda são amplamente utilizados e as técnicas de *spam* e de *phishing* permanecem em níveis bastante elevados.
- Os ataques contra os dispositivos móveis têm aumentado a par do uso de *smartphones*, aumentando especialmente as ameaças relacionadas com o *malware* móvel e a perda de dados.
- Os ataques contra as instituições financeiras e cartões de crédito, relacionadas diretamente com a área do cibercrime, continuam a proliferar, tendo ainda em conta que o chamado "mercado negro" se diversificou nos produtos que oferece.
- Ameaças contra redes sociais continuam a ser especialmente ativas.
- As ameaças de natureza tecnológica, que podem afetar as infraestruturas críticas e podem causar danos muito elevados, também registaram um forte aumento sendo os ciberataques os mais perigosos pela probabilidade de ocorrência e impacto potencial. Foram detetados ataques direcionados contra IC, como o Stuxnet. O risco a que estão sujeitas as IC subsiste como um dos pontos mais preocupantes.

2.3. Vulnerabilidades

Do ponto de vista da segurança da informação, uma vulnerabilidade pode ser definida como "qualquer fraqueza/debilidade de um equipamento/recurso (ativo) ou grupo de ativos que podem ser exploradas por uma ou mais ameaças"[70]. As vulnerabilidades não são só consideradas características inerentes à natureza dos ativos, uma vez que também se

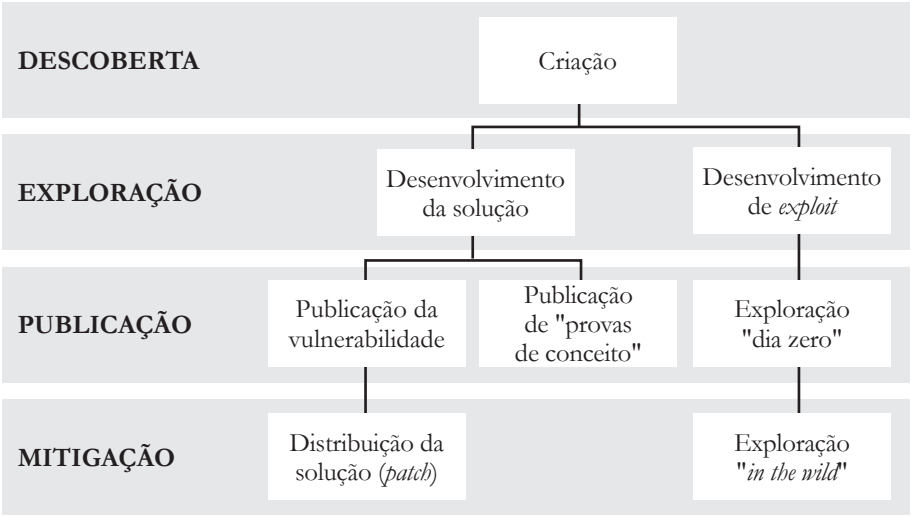
69 Entidade que garante a autenticidade e veracidade dos dados recolhidos num certificado digital expedido. Trata-se de um tipo de instituição notarial que oferece validade a um facto jurídico. O procedimento da Autoridade de Certificação produz-se graças à posse e utilização de uma chave privada que garante a identidade do proprietário do certificado digital. Isto possibilita a assinatura e a validação eletrónica dos certificados emitidos.

70 ISO - International Organization for Standardization, «ISO/IEC 13335-1:2004 - Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management». 2004.

considera uma vulnerabilidade a presença de erros de projeto, implementação, operação ou gestão de um sistema de informação que pode ser explorado e a partir da qual resulta um efeito não desejado ou não esperado que comprometa a política de segurança do sistema[71].

Uma mesma vulnerabilidade afeta de forma diferente o nível global de risco de uma organização. Isto depende de fatores como a facilidade com que ela pode ser explorada ou o próprio ativo ser atingido dentro da organização por um atacante. Também depende do valor do próprio ativo ou se existem contramedidas na organização que evitem a materialização de ameaças sobre essa vulnerabilidade. No momento de gerir as vulnerabilidades, os Sistemas de Gestão da Segurança de Informação (SGSI)[72] e as diferentes metodologias adotadas, introduzem fatores de ponderação e medida das vulnerabilidades no contexto do sistema de TI afetado.

Figura 1 - Ciclo de vida das vulnerabilidades



A partir do momento em que uma vulnerabilidade é criada intencionalmente no sistema e até que seja mitigada, ela passa por diferentes fases, incluindo as fases de descoberta, exploração, publicação e resolução ou mitigação. Na figura 1 representa-se o que pode ser o ciclo de vida das vulnerabilidades, identificando as suas diversas fases e refletindo as atividades desenvolvidas de forma a explorar as oportunidades oferecidas ao longo da sua evolução, ao invés de se colocar o foco na sua eliminação para deixá-la definitivamente resolvida.

71 Internet Engineering Task Force (IETF), «RFC 4949 - Internet Security Glossary, Version 2». ago-2007.

72 Wikipedia contributors, «ISO/IEC 27001», *Wikipedia, la enciclopedia libre*. Wikimedia Foundation, Inc., 07-ago2012.

As fases acima indicadas não são necessariamente sequenciais, uma vez que existem vulnerabilidades que são ativamente exploradas por atacantes sem que o fabricante ou o gestor do sistema esteja ciente do problema. Essas vulnerabilidades são designadas como de "dia zero"[73], sendo extremamente perigosas porque, ao não serem conhecidas dos fabricantes, fazem com que não existam mecanismos de mitigação públicos, como *patches* para um pacote de *software* ou mesmo um conjunto de regras que permita aos elementos de proteção de perímetro da rede prevenir o progresso dos ataques até aos elementos mais vulneráveis do sistema.

Neste sentido, as empresas e organizações de desenvolvimento de *software* informático estabeleceram um sistema de compensações, destinado a retribuir os indivíduos que descubram vulnerabilidades em aplicações e informem de *bugs* (erros) nos seus programas[74]. Os programas de recompensas orientados para a descoberta de vulnerabilidades nas aplicações constituem uma das medidas de segurança cada vez mais implementadas pelas empresas relacionadas com o mundo das tecnologias. Este estímulo positivo, pode levar a reduzir significativamente as vulnerabilidades publicadas das suas aplicações limitando as situações em que a informação dos seus utilizadores esteja exposta a possíveis ataques que violem a sua privacidade e confidencialidade.

Por outro lado, em *fora* mais ou menos clandestinos da internet, pode-se encontrar o lado mais obscuro do mercado das vulnerabilidades, através de "ofertas" de venda de ferramentas de ataque ou *exploits*[75] que afetam os diferentes produtos para serem usadas de forma ilegal. As organizações criminosas oferecem valores semelhantes ou ainda maiores do que aqueles que oferecem as empresas responsáveis pelo código afetado. Estas vulnerabilidades podem ser exploradas em ataques dirigidos contra alvos e organizações concretas ou massivamente contra utilizadores domésticos, para lhes roubar, por exemplo, informação bancária que possam guardar nos seus equipamentos informáticos.

A grande experiência adquirida tem sido capaz de fortalecer as empresas de desenvolvimento de *software* que anteriormente foram afetadas por um grande número de vulnerabilidades. Esta experiência, tem tornado mais difícil a tarefa de explorar e/ou localizar falhas de segurança nas aplicações fazendo com que o utilizador mal intencionado tenha que evoluir e procurar novas frentes de ataque.

---

73 Um ataque de "dia zero", *0day* ou *zero day*, é um ataque contra um sistema de informação que se baseia em encontrar vulnerabilidades desconhecidas nas suas aplicações informáticas. Este tipo de informação circula geralmente entre potenciais atacantes até que finalmente é publicado em foruns de acesso público.

74 Exemplos deste tipo de programas são o *Mozilla Security Bug Bounty Program*, disponível em http://www.mozilla.org/security/bug-bounty.html, que, segundo os seus próprios criadores, "está desenhado para incentivar a investigação de segurança no *software* Mozilla e para recompensar aqueles que nos ajudam a tornar os clientes mais seguros na sua navegação na Internet"; ou o *Google Vulnerability Reward Program*, disponível em http://www.google.com/about/company/rewardprogram.html, que sendo baseado na "estreita colaboração com a comunidade de investigação de segurança convida a investigação de vanguarda externa a ajudar-nos a manter os nossos utilizadores seguros".

75 *Exploit*, que podemos traduzir por "explorar" ou "aproveitar", é uma sequência de comandos cujo fim é o de causar um erro em alguma aplicação, com o objetivo de originar um comportamento não desejado ou imprevisto nos programas informáticos, *hardware* ou componentes eletrónicos.

É por esta razão que as novas tecnologias e as tendências de evolução das vulnerabilidades têm permitido a localização de novos vetores de ataque que violam por completo a privacidade dos utilizadores comuns. Conceitos e plataformas tecnológicas como serviços em nuvem[76], redes sociais[77] e tecnologias móveis têm oferecido ao utilizador mal intencionado uma nova porta para explorar nos seus ataques e, o que é pior, utilizando como alvo sistemas pouco testados.

Se à problemática anterior, se juntar o uso indevido de dispositivos portáteis como telefones celulares e/ou os mais recentes *tablets*[78], onde se mistura a informação pessoal com a informação do trabalho, por mera conveniência, não só se põe em perigo a privacidade dos dados do utilizador, como também a confidencialidade de valiosa informação empresarial.

Um exemplo da utilização centralizada da tecnologia, e da elevada vulnerabilidade daí decorrente, pode ser ilustrada pelo famoso caso do "apagão BlackBerry"[79] onde, devido a uma "falha" nas instalações da empresa comercializadora do telefone BlackBerry[80], os utilizadores deste dispositivo não puderam dispor de ligação à internet durante vários dias, impedindo assim o acesso a aplicações e informações necessárias ao seu trabalho diário.

Por outro lado, porque o utilizador final continua sem estar suficientemente desperto para a segurança e para os riscos decorrentes de não atualização do seu sistema operativo[81] e das aplicações que dispõe instaladas no seu computador, vamos continuar a detetar novas famílias de *malware*, cada dia mais sofisticadas e mais difíceis de detetar e eliminar. Isso é possível em grande medida porque a automação e o desenvolvimento de *malware* por parte do utilizador mal-intencionado se encontra muito avançada, aproveitando a persistência das vulnerabilidades em certos dispositivos, apesar de serem conhecidas e de se encontrarem ao seu dispor atualizações para solucionar definitivamente os problemas existentes.

---

76 Computação na nuvem, do inglês *cloud computing*, é um paradigma que permite oferecer serviços de computação através da internet.

77 Neste caso refere-se às redes sociais no âmbito da internet, isto é, portais *web* que permitem às pessoas conectar-se com os seus amigos, inclusive realizar novas amizades, a fim de partilhar conteúdos, interagir, criar comunidades sobre interesses similares: trabalho, leituras, jogos, amizades, relações interpessoais.

78 *Tablet* é um tipo de *laptop*, maior que um *smartphone*, construído sobre uma tela sensível ao toque, com o qual se interage com os dedos ou com uma caneta (passiva ou ativa), sem necessidade de teclado físico ou rato, que são substituídos por um teclado virtual.

79 Trata-se do incidente que ocorreu a partir aproximadamente das 11:00 (hora espanhola) de segunda-feira, 10 de outubro, em que os utilizadores do BlackBerry na Europa, África e Médio Oriente tiveram problemas de ligação à internet. O problema foi generalizado e atingiu todas as operadoras móveis, pelo modo evidente com que a incidência afetou este tipo de telefones, independentemente da empresa com quem se havia contratado a conexão.

80 BlackBerry é um modelo de *smartphone* desenvolvido pela empresa canadiana Research In Motion (RIM), que integra o serviço de e-mail móvel e inclui aplicações típicas destes dispositivos: livro de endereços, calendário, lista de tarefas, bloco de notas, etc. É principalmente conhecido pelo seu teclado incorporado. Consultar http://es.blackberry.com/.

81 Sistema operativo denomina um conjunto de programas que, num sistema informático, gerem os recursos de *hardware* e providenciam serviços aos programas de aplicação, executando-se em modo privilegiado em relação aos restantes programas.

2.3.1. *Catalogação das Vulnerabilidades*

Desde as origens da informática, muitas organizações e instituições têm procurado modelar e classificar as vulnerabilidades, inicialmente de forma quase exclusivamente focada nas inerentes ao *software*, para logo se expandir o conceito e estendê-lo a todos os aspetos de um Sistema de Informação. Deste modo, a partir de 1978 pode ser encontrada uma classificação inicial dos "erros de proteção" no código do projeto "*Protection Analysis*", promovido pela divisão de investigação do Departamento de Defesa dos EUA (DoD – *United States Department of Defense*)[82]. Este projeto já procurava na década de 70 os mecanismos de identificação automatizados de vulnerabilidades no *software* dos sistemas da época, enquadrando-as dentro de um processo de melhoria da "avaliação da proteção" desses sistemas.

Muitas das categorizações clássicas de vulnerabilidades geram alguns problemas de classificação por utilizarem taxonomias fixas de vulnerabilidades que, pela sua natureza ou variáveis de exploração, não são simplesmente categorizáveis sob um único critério. Certas vulnerabilidades de *software* podem, por exemplo, ser exploradas local ou remotamente, o que depende de certas configurações específicas do ambiente, alcançando um maior ou menor impacto na organização. Estas metodologias baseadas na categorização clássica tendem a ser substituídas por metodologias estruturadas com base na teoria do prototipado, que propõe uma conceção de categorias com classes heterogéneas e não distintas/discretas. Segundo esta visão, será possível identificar alguns membros mais representativos da categoria do que outros. Os membros mais representativos de cada classe são designados por protótipos, daí o nome atribuído a esta teoria.

Devido às dificuldades de identificação e catalogação de vulnerabilidades, normalmente associadas a muitas metodologias clássicas de análise e gestão de riscos, é necessário definir uma série de atributos, dimensões e métricas de forma a servir de suporte e permitir classificar as vulnerabilidades existentes em diversas organizações.

- **Métricas e controlos:** são valores atribuídos a vulnerabilidades com base em vários fatores, tais como o conhecimento ou desconhecimento da existência de vulnerabilidades, o impacto de cada vulnerabilidade na organização, etc. por exemplo, quantas vezes se realiza o procedimento de atualização de *patches*. Se este controlo se cumpre mensalmente existe uma janela de tempo em que o sistema pode ser mais vulnerável do que se o processo for realizado semanalmente.
- **Atributos:** são as características inerentes às vulnerabilidades que possam surgir no desenho ou arquitetura da organização, decorrentes do comportamento ou ações do próprio sistema ou das características gerais que o caracterizam como, por exemplo, o grau de dificuldade que está associado à gestão de uma dada vulnerabilidade.
- **Dimensão:** também se pode catalogar a vulnerabilidade atendendo ao impacto e alcance que esta tem sobre o tipo de objetivo que pode explorar. Neste contexto, podemos ter vulnerabilidades sobre objetos (*hardware* ou *software*), vulnerabilidades

82 R. BisbeyII. y D. Hollingworth, «Protection Analysis: Final Report», University of Southern California Marina del Rey Information Sciences Inst, ISI/SR-78-13, may 1978.

que afetam os fatores humanos ou sociais, vulnerabilidades associadas às condições ambientais, etc.

Existem diferentes metodologias que, de acordo com um número de critérios específicos, catalogam as vulnerabilidades de diferentes maneiras. Embora os conceitos utilizados por cada uma delas sejam distintos, todos perseguem o mesmo objetivo: simplificar, homogeneizar e normalizar a classificação das vulnerabilidades. Estas vulnerabilidades são normalmente tratadas individualmente, pelo que também se estão a realizar estudos[83], onde se perspetiva e analisa o comportamento das vulnerabilidades no seu todo.

O Anexo I apresenta um breve resumo de algumas das metodologias comuns mais utilizadas hoje em dia.

2.4. Metodologias e Boas Práticas para a Análise e a Gestão de Riscos

Para levar a cabo uma adequada análise/avaliação e gestão de risco relativa à segurança da informação, é essencial analisar os ativos que devemos proteger, as ameaças a que estão sujeitos e as vulnerabilidades que lhe são próprias. Além disso, convém seguir uma metodologia, definida e formalmente estabelecida, que guie os nossos passos neste processo, garantindo que consideramos todas as atividades que é necessário realizar e não nos perdermos na análise, ajudando-nos a selecionar medidas de proteção para gerir adequadamente o risco que enfrentamos.

No anexo II apresenta-se um breve resumo[84] das principais metodologias, reconhecidas como tal a nível internacional[85], para a Análise e Gestão de Risco de Segurança da Informação.

3. Segurança da Informação no Ciberespaço e Capacidade de Resposta a Incidentes Informáticos

Importa iniciar esta secção com uma clarificação da terminologia utilizada, uma vez que existem muitas siglas (formadas a partir dos termos em inglês), que são muitas vezes utilizadas como sinónimos ou com um significado muito semelhante à Capacidade de Resposta a Incidentes Informáticos.

Provavelmente, o termo mais utilizado internacionalmente é CERT[86], designando uma Equipa de Resposta a Emergências Informáticas, provavelmente porque foi o

83 Su Zhang, Xinming Ou, Anoop Singhal, e John Homer, «An empirical study of a vulnerability metric aggregation method». NIST - National Institute of Standards and Technology, 2011.

84 Technical Department of ENISA Section Risk Management, «ENISA - Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools». ENISA, 01-jun2006.

85 Filipe Neto Rodeia Macedo, «Models for Assessing Information Security Risk», Dissertação para obtenção do Grau de Mestre em Engenharia Informática e de Computadores, Universidade Técnica de Lisboa, 2009.

86 Embora seja este o significado original de CERT, conforme o mantém a Universidade Carnegie Mellon, convém referir que, para evitar confusão, mais tarde o Departamento de Segurança Nacional dos Estados Unidos passou a utilizar esta mesma sigla no seu US-CERT, modificando porém o sentido da letra "R", que desta feita já não corresponde a "*Response*", mas sim a "*Readiness*". Seguramente, reconhece-se esta designação como mais consistente com a realidade do serviço que presta.

primeiro a aparecer no final dos anos oitenta. A agência DARPA (*Defense Advanced Research Projects Agency*), pertencente ao Departamento de Defesa dos EUA; poucos dias depois do seu lançamento, criou o primeiro Centro de Coordenação de Equipas de Resposta a Emergências Informáticas (CERT/CC – *Computer Emergency Response Team/Coordination Center*[87]), localizado na Carnegie Mellon University[88], em Pittsburgh, Pennsylvania.

Logo depois, com um objetivo similar dentro de seu âmbito, o Departamento de Energia dos EUA constituiu o seu CIAC (*Computer Incident Advisory Capability*), ou seja, uma Capacidade de Aconselhamento face a Incidentes Informáticos.

Depois de um certo tempo, o modelo foi adotado na Europa, mas, neste caso, usando o nome de CSIRT (*Computer Security Incident Response Team* – Equipa de Resposta a Incidentes de Segurança Informática), posto que o termo CERT tinha sido protegido como uma marca registrada pela Universidade Carnegie Mellon.[89]

Desta forma, constata-se o aparecimento de muitas outras siglas para referenciar este mesmo tipo de capacidades, como IRT (*Incident Response Team* – Equipa de Resposta a Incidentes), CIRT (*Computer Incident Response Team* – Equipa de Resposta a Incidentes Informáticos) ou SERT (*Security Emergency Response Team* – Equipa de Resposta a Emergência de Segurança) mas todas de utilização muito menos frequente do que as mencionadas anteriormente.

Na sequência das decisões tomadas na Cimeira de Praga (2002) e Istambul (2004), a OTAN também se comprometeu a implantar uma capacidade semelhante a um CERT, denominando-a como CIRC (*Computer Incident Response Capability*) da OTAN ou NCIRC (*NATO Computer Incident Response Capability* – Capacidade de Resposta a Incidentes Informáticos da OTAN).

Apesar de ser possível concluir que os termos CERT, CSIRT ou CIRC são utilizados para referenciar o mesmo tipo de capacidades cibernéticas, não podemos pensar que estas são sempre as mesmas. Dependendo da comunidade a que devem servir, ou a missão que cumprem, haverá diferentes tipos de CIRC especializados[90], entre os quais podemos citar: académicos, comerciais, para a proteção das infraestruturas críticas de informação (CIIP – *Critical Information Infrastructure Protection*), do setor público, da defesa, nacionais, para as PME (Pequenas e Médias Empresas), etc.

Dependendo do seu caráter específico, cada CERT estruturará o seu funcionamento de diversas formas segundo, nomeadamente, um dos seguintes modelos organizativos[91]:

87 Consultar http://www.cert.org/

88 Consultar http://www.cmu.edu/

89 Em todo caso, a Universidade de Carnegie Mellon permite o uso da marca CERT a todos os CSIRT que partilhem um compromiso com a melhoria da segurança das redes ligadas à internet, devendo estas solicitar-lhes, para esse efeito, a correspondente autorização para utilizar a marca CERT junto ao nome de cada CSIRT.

90 Henk Bronk, Marco Thorbruegge, y Mehis Hakkaja, «Cómo Crear un CSIRT Paso a Paso». ENISA - European Network and Information Security Agency, 22-dic2006.

91 Centro Criptológico Nacional, «Guía de Seguridad de las TIC (CCN-STIC810) Guía de Creación de un CERT / CSIRT». sep-2011.

- ***Independente***

  É um CERT que age como uma organização independente, sendo dotado com os seus próprios responsáveis e recursos. Este é o modelo que, em regra, melhor se adapta aos CERT comerciais, que se constituem invariavelmente como empresas independentes para prestar os seus serviços.

- ***Integrado***

  Neste modelo, o CERT está incorporado na organização a que presta serviços ou que o patrocina, funcionando como um departamento, mais ou menos autónomo, da mesma. Geralmente é dirigido por um responsável das atividades que, além dos trabalhadores próprios do CIRC, tem a possibilidade de recrutar o pessoal técnico necessário para a resolução de um incidente, recorrendo, se for necessário, a outras áreas da organização para solicitar assistência especializada. Este é o modelo mais comum de CIRC.

- ***Campus***

  É o modelo que surge nas universidades e nos ambientes de investigação, daí o seu nome, em que há uma sede/localização central, que se denomina CERT principal ou mãe, e muitos locais subsidiários distribuídos (CERT filhos) dependentes do principal, que são mais pequenos e contam com uma grande autonomia de ação. Este constitui o modelo que melhor se ajusta a empresas e organizações multinacionais, com um alto grau de descentralização.

- ***Voluntário***

  Neste modelo, a capacidade CIRC constitui-se *ad hoc*, sendo formada com base num grupo de especialistas que se juntam voluntariamente para prestar serviço a uma comunidade. As redes WARP (*Warning, Advice, and Reporting Points*)[92] são um exemplo deste modelo.

Dependendo do tipo e modelo organizativo de cada CERT, encontraremos um perfil e número diferente de pessoas que nele trabalham mas, geralmente, todos possuem funcionários com altas qualificações técnicas e uma série de características pessoais, que os tornam aptos para trabalhar neste tipo de ambientes tão exigentes. Em geral, o pessoal de um CERT deverá ser[93]: dedicado, inovador, minucioso, flexível, paciente, analítico, bom comunicador, tolerante ao *stress*, orientado para a resolução de problemas e, sobretudo, íntegro.

Embora, como já foi referido, a composição de cada CERT varie muito de caso para caso, encontramos em geral os seguintes papéis/funções atribuídas[94]:

92 Trata-se de um tipo de comunidades, amplamente divulgadas no Reino Unido, de troca de informação de segurança que se foram desenvolvendo para proporcionar um método eficaz para apoiar a defesa contra ataques a pequenas organizações.

93 Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, y Mark Zajicek, «Handbook for Computer Security Incident Response Teams (CSIRTs)». Carnegie Mellon University, abr-2003.

94 Carnegie Mellon University, «CERT®/CC: Computer Security Incident Response Team FAQ», 01-abr2008. [Online]. Available: http://www.cert.org/csirts/csirt_faq.html. [Accessed: 25-ago2012].

• Gestor ou líder da equipa;
• Subgerentes, supervisores ou líderes de grupo;
• Pessoal responsável por prestar ajuda numa situação de crise;
• Pessoal responsável pela gestão de incidentes;
• Pessoal responsável pela análise de vulnerabilidades;
• Pessoal responsável pela análise de dispositivos/equipamentos;
• Especialistas em diferentes plataformas;
• Formadores;
• Investigadores.

Embora com menos frequência, também se pode encontrar outro tipo de papéis/funções num CIRC:

• Equipe de apoio;
• Redatores técnicos;
• Administradores de rede ou sistemas da infraestrutura proprietária;
• Programadores ou responsáveis pelo desenvolvimento de ferramentas específicas;
• Técnicos de desenvolvimento e manutenção de sistemas *web*;
• Responsável pela comunicação e relação com os *media*;
• Pessoal jurídico;
• Pessoal das Forças e Corpos de Segurança do Estado;
• Auditores ou pessoal responsável pela garantia de qualidade;
• Pessoal da área comercial.

As capacidades CIRC são implementadas com o objetivo de proporcionarem diversos serviços, que variam de acordo com a sua missão, mas que podem ser divididos nos seguintes tipos[95]:

• ***Serviços Reativos***

Serviços que são ativados por um evento ou uma solicitação, como um relatório técnico sobre um servidor comprometido, código malicioso amplamente difundido, vulnerabilidades de *software* ou algo que foi identificado por um sistema de deteção de intrusões ou um registo de eventos. Os serviços reativos constituem a componente central do trabalho de um CIRC. Estes tipos de serviços incluem:

• ***Alertas e Avisos***.

Tratamento de incidentes, como:

- Análise de incidentes;
- Apoio na resposta a incidentes;
- Coordenação da resposta a incidentes;
- Resposta a incidentes no local.

Tratamento de vulnerabilidades, que inclui:

- Análise de vulnerabilidades;
- Resposta a vulnerabilidades;

95 Carnegie Mellon University, Stelvio bv, y PRESECURE Consulting GmbH, «CSIRT Services». Carnegie Mellon University, 26-nov2002.

- Coordenação da resposta a vulnerabilidades.

Tratamento de dispositivos ou artefactos, que inclui:

- Análise de dispositivos ou artefactos;
- Resposta a dispositivos ou artefactos;
- Coordenação da resposta a dispositivos ou artefactos.

• ***Serviços Proactivos***

Estes serviços oferecem assistência e informação para ajudar a preparar, proteger e garantir a segurança dos sistemas protegidos, em antecipação de ataques, problemas ou eventos. A prestação desses serviços está essencialmente orientada para reduzir o número de futuros incidentes. Esses serviços incluem:

- Comunicações e anuncios;
- Observatório de tecnologia;
- Avaliações ou auditorias de segurança;
- Configuração e manutenção de ferramentas, aplicações e infraestruturas de segurança;
- Desenvolvimento de ferramentas de segurança;
- Serviços de deteção de intrusões;
- Difusão de informações relacionadas com a segurança.

• ***Serviços de Gestão da Qualidade da Segurança***

São serviços projetados para melhorar os restantes serviços existentes e a funcionarem de forma independente da gestão de incidentes. Tradicionalmente são fornecidos por outras áreas da organização, exteriores ao CIRC, como o departamento de TIC, a auditoria ou o departamento de treino/formação. O envolvimento do pessoal pertencente ao CIRC nestes serviços vai ajudar a melhorar a segurança geral da organização, identificando os seus riscos, ameaças e debilidades. Em geral, trata-se de serviços proactivos que contribuem indiretamente para reduzir o número de incidentes. Porém, importa referir que estes se diferenciam do grupo anterior, porque os seus objetivos são definidos a mais longo prazo. Estes serviços incluem:

- Análise de risco;
- Continuidade do negócio e recuperação de desastres;
- Consultoria de segurança;
- Sensibilização/consciencialização;
- Educação/formação;
- Avaliação ou certificação de produtos.

4. Ciberdefesa

4.1. Capacidades de Ciberdefesa

Para lidar com a rápida mudança tecnológica e o crescente aumento de ciberataques dirigidos contra as suas redes e sistemas de informação, a OTAN decidiu desenvolver um esforço concertado para enfrentar os novos desafios à segurança global e à evolução

do espectro de ameaças, elegendo a ciberdefesa como uma prioridade estratégica para a Aliança.

O novo Conceito Estratégico da OTAN, aprovado na Cimeira de Lisboa que ocorreu em 18 e 19 de novembro de 2010, reconhece explicitamente que a crescente sofisticação dos ciberataques requer o desenvolvimento urgente de uma capacidade de proteção da Aliança contra este tipo de ataques pois, como se tem vindo a comprovar, dela depende a sua própria segurança.

Em 8 de junho de 2011, os Ministros da Defesa dos países membros, aprovaram a revisão da Política de Ciberdefesa OTAN, estabelecendo desta forma uma visão clara para os esforços a desenvolver no contexto da edificação de uma capacidade de Ciberdefesa cooperativa da Aliança.

No ano de 2011, a Agência C3 da OTAN (*NATO Consultation, Command and Control Agency*, NC3A)[96] lançou a sua Iniciativa Multinacional para o Desenvolvimento da Capacidade de Ciberdefesa (MN CD2 – *Multinational Cyber Defence Capability Development*), como resposta ao desafio de desenvolver novas capacidades de Ciberdefesa em tempos de grandes restrições financeiras, o que exige uma abordagem inteligente e eficiente para alcançar rapidamente as capacidades necessárias, tanto no âmbito da OTAN como em cada uma das Nações Aliadas.

A NC3A entendia que a Ciberdefesa se podia definir como "a aplicação de medidas de segurança para a proteção e resposta a ciberataques lançados contra as infraestruturas TIC, requerendo uma capacidade de preparação, prevenção, deteção, resposta, recuperação e extração de lições aprendidas a partir dos ataques que podem afetar a confidencialidade, integridade e disponibilidade da informação, assim como os recursos e serviços dos sistemas de TIC que a processam".

Dentro da Iniciativa MN CD2, para apoiar o desenvolvimento coordenado e interoperável das Capacidades de Ciberdefesa dos países aliados, o Comando Aliado da Transformação (ACT – *Allied Command for Transformation*) encarregou a NC3A de realizar uma análise, classificação ou taxonomia das Capacidades de Ciberdefesa[97], a fim de dar uma ideia clara dos seus aspetos operativos e dividir o esforço de desenvolvimento ou a obtenção em partes manejáveis que possam ser tratadas de forma independente. A classificação destas capacidades é apresentada de forma resumida no Anexo III.

96 É uma agência da OTAN que partilha a personalidade jurídica da Aliança. Os seus estatutos foram aprovados pelo Conselho do Atlântico Norte e opera sob um sistema de financiamento a 100% dos seus clientes, que são geralmente as agências da própria OTAN. A NC3A é parte da estrutura C3 OTAN, juntamente com o NATO C3 Board e a NCSA (NATO CIS Service Agency). A missão da NC3A é facilitar a consecução dos objetivos da Aliança através da prestação imparcial das capacidades de Consulta, Comando e Controlo, Comunicações, Inteligência, Vigilância e Reconhecimento (C4ISR). Mais recentemente, estas entidades fundiram-se e deram lugar à *NATO Communications and Information Agency* (NCIA).

97 NATO C3 Agency, «Multinational Cyber Defence Capability Development (MN CD2) Initiative - Info Sheet». NC3A, 05-may2011.

4.2. Ciberexército

Cada vez com maior frequência, e num maior número de países, tem surgido a opinião de que o crescimento[98] e a sofisticada[99] evolução das ciberameaças tornam necessário enfrentá-las com medidas mais ativas. Neste contexto, as ações a desenvolver devem procurar não só prevenir, detetar, reagir e recuperar as infraestruturas proprietárias – sem neutralizar a ciberameaça desde a sua origem – mas também implementar os aspetos de exploração e de ataque das Capacidades de Ciberdefesa de um atacante. Surgem assim os conceitos de ciberguerra[100] e ciberexército, bem como o desenvolvimento de regras de empenhamento específicas[101] que permitam não só defender mas também, se necessário, passar ao ataque.

Desta forma, podemos encontrar inúmeras iniciativas em diferentes países, orientadas para a criação e estruturação de um Cibercomando Militar[102] ou o de um Ciberexército, dos quais se salientam: EUA[103], Reino Unido[104], China[105], Rússia[106], Irão[107], Índia[108] Paquistão[109], Coreia do Norte[110], Coreia do Sul[111], Israel[112] e, muitos mais.

O Cibercomando Militar dos Estados Unidos é seguramente aquele que dispõe de um corpo doutrinário mais avançado e conceptualmente elaborado, além de ser o que, com mais transparência, reflete o progresso na implementação das suas capacidades.

---

98 McAfee® Foundstone® Professional Services, «Global Energy Cyberattacks: "Night Dragon"», McAfee Labs™, Santa Clara, CA, White Paper, feb. 2011.

99 Mark Clayton, «Stuxnet malware is "weapon" out to destroy ... Iran's Bushehr nuclear plant?», *The Christian Science Monitor*, 21-sep2010.

100 Richard A. Clarke y Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2010.

101 Donna Miles, «Doctrine to Establish Rules of Engagement Against Cyber Attacks», *American Forces Press Service*, BALTIMORE, 20-oct2011.

102 É muito comum encontrar o termo "*Cyber Command*", em documentos escritos em inglês, referindo-se à capacidade militar responsável pela Defesa do Ciberespaço. No entanto, a tradução direta para cibercomando não tem o mesmo significado em português e espanhol, pelo que no presente documento utilizaremos os termos CiberExército ou Cibercomando Militar, pois consideramos que a sua compreensão se aproxima mais do significado original do termo em inglês.

103 U.S. Department of Defense, «Department of Defense Strategy for Operating in Cyberspace». U.S. Department of Defense, jul-2011.

104 Tom Espiner, «MoD cyber-command will combine with intelligence», *ZDNet UK*, 27-jun2011.

105 Carlos Fernández de Lara, «China confirma existencia de escuadrón de ciberguerra: "Ejército Azul"», *BSecure Magazine*, 30-may2011.

106 K. Giles, «"Information Troops"-A Russian Cyber Command?», in *Cyber Conflict (ICCC), 2011 3rd International Conference on*, 2011, pp. 1-16.

107 Agencia EFE, «Irán establece su primer cibercomando para luchar contra ataques informáticos», *El Nacional*, Caracas, 31-oct2011.

108 Harish Gupta, «As cyber attacks rise, India sets up central command to fight back», *Daily News & Analysis*, New Delhi, 15-may2011.

109 Pakistan News Service, «New war between India and Pakistan : Cyber Warfare», *PakTribune*, 08-feb2011.

110 Sangwon Yoon, «North Korea recruits hackers at school», *Al Jazeera English*, 20-jun2011.

111 Channel NewsAsia, «South Korea to set up cyber command against North Korea», *MediaCorp*, Seoul, 09-jul2009.

112 Reuters, «Israel lanza un "cibercomando" contra ataques informáticos», *El Mundo*, 18-may2011.

Considera-se, portanto, o Exército Cibernético americano como referência base para a descrição das características genéricas que qualquer outra nação deverá ter em atenção quando implementa, implementará, ou pretenderá implementar, dentro das suas possibilidades, os respetivos Ciberexércitos.

A 23 de junho de 2009, o Secretário da Defesa norte-americano determinou ao Chefe do Comando Militar Estratégico dos EUA (USSTRATCOM – *US Strategic Command*) a criação e estabelecimento do Cibercomando Militar dos EUA (USCYBERCOM – *US Cyber Command*), com a missão[113] de planear, coordenar, integrar, sincronizar e realizar atividades para:

- Dirigir as operações e a defesa das redes de informação específicas do Departamento de Defesa.
- Preparar e, quando indicado, realizar todo o espectro de possíveis operações militares no ciberespaço, com o objetivo de facilitar as ações em todas os restantes ambientes operacionais.
- Garantir a liberdade de ação dos EUA e dos seus aliados no ciberespaço e negar a mesma liberdade de atuação aos seus adversários.

O primeiro Comandante-em-Chefe do Exército Cibernético é o General Keith B. Alexander, do Exército dos EUA, que compatibilizará o exercício do seu cargo com o de diretor da Agência de Segurança Nacional (NSA)[114], que já detinha. A Capacidade Operacional Inicial (IOC – *Initial Operational Capability*) foi alcançada em 21 de maio de 2010, tornando-se totalmente operacional (FOC – *Full Operational Capability*) em 3 de novembro de 2010[115].

O USCYBERCOM, de acordo com a visão subjacente à sua criação, será o meio pelo qual se consegue centralizar o comando das operações no ciberespaço, fortalecendo e integrando as capacidades do Departamento de Defesa neste domínio, já que reúne todas as cibercapacidades existentes, criando uma sinergia que não existia até esse momento.

Desta forma, o USCYBERCOM será composto pelos cibercomandos e ciberunidades dos vários serviços (Exército, Armada, Fuzileiros e Força Aérea), ramos que compõem as Forças Armadas dos EUA. Neste contexto, temos especificamente[116]:

---

113 U.S. Department of Defense, «U.S. Cyber Command Fact Sheet». US Department of Defense Office of Public Affairs, 13-oct2010.

114 A National Security Agency, define-se a si mesma como a casa dos criptologistas e criptoanalistas dos EUA. Durante os seus mais de 50 anos, tem sido a fonte que tem providenciado informação e em tempo oportuno aos comandantes militares e altos funcionários do governo dos EUA. Pela sua natureza, como membro chave da comunidade de inteligência dos EUA, a NSA está atualmente a enfrentar o duplo desafio de, por um lado, evitar que os adversários estrangeiros possam ter acesso à informação nacional classificada e, por outro, recolher, processar e disseminar informações sobre comunicações externas, para efeitos de inteligência e contrainteligência, assim como para apoiar as operações militares norte-americanas em curso e a desenvolver. Consultar http://www.nsa.gov/.

115 Office of the Assistant Secretary of Defense (Public Affairs), «Cyber Command Achieves Full Operational Capability», *Defense.gov News Release*, 03-nov2010.

116 U.S. Cyber Command, «U.S. Cybercom Trifold», 19-oct2010.

- ***Cibercomando do Exército*** *(ARCYBER – Army Cyber Command)*
  Inclui a componente cibernética do Exército, denominado 2.º Exército (*Army Cyber Command/2nd Army*), onde se integram as seguintes unidades subordinadas[117]:
  - 9.º Comando de Sinais (Transmissões) do Exército, ou Comando de Operações em Rede do Exército (NETCOM – *Network Enterprise Technology Command/9th Signal Command – Army*);
  - 1.º Comando de Operações de Informação (componente terrestre), (*1st Information Operations Command – Land*);
  - Comando de Inteligência e de Segurança do Exército (US Army Intelligence and Security Command – INSCOM), que ficará sob o controle operacional do Cibercomando do Exército para os efeitos das ações/operações no ciberespaço.

  Cibercomando da Força Aérea *(AFCYBER – Air Force Cyber Command)*
  Inclui a componente cibernética da Força Aérea, denominada 24.ª Força Aérea. Inclui as seguintes unidades subordinadas118:
  - Ala 67 de Guerra em Rede (*67th Network Warfare Wing*);
  - Ala 688 de Operações de Informação (*688th Information Operations Wing*);
  - Ala 689 de Comunicações de Combate (*689th Combat Communications Wing*).
- ***Cibercomando da Marinha*** *(FLTCYBERCOM – Fleet Cyber Command)*
  Inclui a componente cibernética da Marinha, designada por 10.ª Frota. Integra, entre outras, as seguintes unidades subordinadas[119]:
  - Comando Naval de Guerra em Rede (*Naval Network Warfare Command,* NNWC);
  - Comando Naval de Operações de Ciberdefesa (*Navy Cyber Defense Operations Command*, NCDOC);
  - Comando Naval de Operações de Informação (*Naval Information Operation Commands*).
- ***Cibercomando dos Fuzileiros*** (Marines) *(MARFORCYBER – Marine Forces Cyber Command)* (*Marine Corps Cyberspace Command*)
  - Inclui a componente cibernética dos Fuzileiros (*Marines*).

Por outro lado, os EUA desde há muito tempo que têm vindo a rever a sua doutrina militar, nas suas diferentes componentes, para adequá-la aos novos desafios colocados pelas operações militares no ciberespaço, procurando desta forma definir as capacidades que devem ser desenvolvidas para enfrentá-los.

Assim, o Exército dos EUA estabeleceu no seu Plano de Desenvolvimento de Capacidades 2016-2028[120] o Conceito de Operações no Ciberespaço (CyberOps – *Cyberspace*

117 U.S. Army Cyber Command, «Army Cyber Command Organization». [Online]. Available: http://www.arcyber.army.mil/org-arcyber.html. [Accessed: 25-ago2012].

118 U.S. Air Force, «24th Air Force - Fact Sheet», abr-2010. [Online]. Available: http://www.24af.af.mil/library/factsheets/factsheet_print.asp?fsID=15663&page=1. [Accessed: 25-ago2012].

119 United States Navy, «U.S. Fleet Cyber Command / U.S. Tenth Fleet». [Online]. Available: http://www.fcc.navy.mil/. [Accessed: 25-ago2012].

120 U.S. Army, «Cyberspace Operations Concept Capability Plan 2016-2028». U.S. Army Capabilities Integration Center, 22-feb2010.

Operation), assumindo que estas se compõem de: Compreensão da Cibersituação (CyberSA – *Cyber Situational Awareness*), Operações em Redes Cibernéticas (CyNetOps – *Cyber Network Operations*), Ciberguerra (*Cyberwar*) e, finalmente, Apoio Cibernético (CyberSpt – *Cyber Support*).

Sem analisar em detalhe as capacidades de CyNetOps e de CyberSpt, que estão essencialmente relacionadas com os aspetos defensivos das Capacidades de Ciberdefesa, considera-se que vale a pena abordar em maior detalhe as capacidades que se devem incluir no CyberSA, diretamente relacionadas com as capacidades de exploração, e na Ciberguerra, que fundamentalmente encorpam as capacidades de resposta a ciberataques.

• Compreensão da Cibersituação (CyberSA)

Compõe-se do conhecimento imediatamente disponível, tanto dos adversários como dos aliados, bem como de todas as informações relevantes sobre as atividades no ciberespaço ou no espectro eletromagnético. Obtém-se a partir de uma combinação de atividades de informações e operativas desenvolvidas tanto no ciberespaço, como nos restantes domínios operacionais, realizadas quer de forma unilateral, quer através da colaboração com parceiros nos setores público ou privado. A discriminação entre as ameaças naturais e artificiais constitui uma parte fundamental desta análise.

Uma adequada compreensão da Cibersituação permitirá tomar decisões adequadas, a todos os níveis de decisão, através da disponibilização de produtos ajustados a cada público-alvo, que podem variar desde os boletins de sensibilização com uma ampla difusão dirigida aos utilizadores em geral, até aos relatos de problemas específicos, extremamente sensíveis e de natureza classificada.

Uma boa compreensão da situação no ciberespaço (Cibersituação) deve incluir capacidades para:

- A compreensão da situação dos adversários e dos aliados, bem como do comportamento e atividades relevantes desenvolvidas por atores no ciberespaço.
- A avaliação das capacidades cibernéticas amigas.
- A avaliação das capacidades cibernéticas e intenções dos adversários.
- A análise das vulnerabilidades cibernéticas dos adversários e dos aliados.
- A compreensão da informação que flui através das redes para permitir deduzir o seu propósito e criticidade.
- A compreensão dos efeitos e do impacto na missão, resultante da exploração das vulnerabilidades e das lacunas existentes no ciberespaço amigo e adversário.

• Ciberguerra

A Ciberguerra é conduzida com base em Operações no Ciberespaço estendendo a projeção de poder no ciberespaço além dos limites tradicionais da defesa do ambiente da informação a proteger para detetar, deter, negar e derrotar os adversários. As capacidades associadas à ciberguerra têm como objetivo atingir tanto as redes de telecomunicações e computadores, como os processadores e controladores integrados em equipamentos, sistemas e infraestruturas.

A Ciberguerra inclui ações de ataque nas quais se combinam ataques a redes de computadores, com outras capacidades de apoio – por exemplo, ataque eletrónico ou ataque físico – para negar a utilização ou manipular a informação que flui através de uma infraestrutura de comunicações.

Na condução da ciberguerra, combinam-se medidas políticas, a recolha de informações, dados de sensores e processos altamente automatizados para identificar e analisar a atividade maliciosa, enquanto se executam ações de resposta (previamente autorizadas) para eliminar ataques hostis antes que estes possam ter impacto disruptivo ou destrutivo. Além disso, na condução da ciberguerra, são utilizados os princípios doutrinários tradicionais de emprego operacional dos exércitos como a defesa em profundidade. Inclui-se neste contexto a vigilância e o reconhecimento associados às operações de segurança, com o objetivo de garantir o alerta precoce relativo às ações inimigas.

Numa análise mais detalhada às capacidades de ciberguerra, constata-se que estas incluem:

- Aceder, tanto por meios diretos como remotos, a redes, sistemas ou nós identificados como alvos, a fim de garantir o acesso requerido pelas ações de ciberguerra contra alvos de oportunidade.
- Permitir o acesso recorrente, tanto pelos meios diretos como remotos, a redes, sistemas, ou nós identificados como alvos, para garantir o acesso necessário à condução de operações no ciberespaço.
- Aceder a *hardware* e a *software* do adversário, por meio direto ou remoto, com o fim de garantir a eficácia das ações de ciberguerra.
- Aceder, recolher e explorar a informação do adversário identificada como alvo, por meios diretos ou remotos, a fim de detetar, dissuadir, negar e derrotar as ações e a liberdade de ação do adversário.
- Habilitar a capacidade de agregar, gerir, decifrar, traduzir linguisticamente, analisar e informar sobre todos os dados recolhidos nos sistemas de gestão do conhecimento, a fim de apoiar as operações no ciberespaço e nos outros domínios operacionais do campo de batalha.
- Proporcionar capacidades de ciberguerra, tanto remotas como de forma expedicionária, a fim de detetar, dissuadir, negar e derrotar as ações e a liberdade de ação do adversário.
- Proporcionar capacidades, baseadas em sensores, para a deteção automatizada de ataques de rede e de intrusões a fim de detetar, dissuadir, negar e derrotar as ações do adversário, integrar a defesa em profundidade, assegurar a nossa liberdade de ação e dos aliados, assim como negar a liberdade de ação do adversário, no momento e local pretendido.
- Atacar (negar, degradar, interromper, enganar ou destruir) as redes do adversário e a sua infraestrutura crítica de informação, a fim de detetar, dissuadir, negar e derrotar as ações e a liberdade de ação do adversário.
- Proporcionar capacidades baseadas em sensores, de resposta à intrusão ou ataque à rede, de modo a detetar, dissuadir, negar e derrotar ações adversárias,

integrando a defesa em profundidade e assegurando a liberdade de ação das forças amigas, assim como negar a liberdade de ação do adversário, no momento e local pretendido.

- Atacar (negar, degradar, interromper, enganar ou destruir) os processadores e controladores integrados nos equipamentos e sistemas do adversário, com o fim de detetar, dissuadir, negar e derrotar as suas ações, integrando a defesa em profundidade e garantindo a nossa liberdade de ação e aliada, assim como negar a liberdade de ação do adversário no momento e local pretendido.
- Proporcionar conhecimento da situação do adversário e de outras redes específicas, com o fim de aumentar o conhecimento geral da situação por parte do comandante, permitindo tanto a condução de Operações no Ciberespaço, como a integração das restantes ações por parte do comandante.
- Entender o adversário e mapear outras estruturas específicas da rede, a fim de garantir o sucesso das operações no ciberespaço.
- Seguir, localizar e prever as atividades do adversário no ciberespaço, a fim de garantir o sucesso das nossas ações de Ciberguerra e o conhecimento da Cibersituação.
- Atacar os recursos de informação do adversário com o fim de dissuadir, prejudicar ou enganar os adversários, e apoiar a consecução dos objetivos globais definidos pelo comandante da missão.
- Mitigar ou evitar as medidas de Ciberdefesa do adversário, com o fim de aplicar com a maior liberdade de ação possível as nossas próprias capacidades de ciberguerra.
- Atingir com o maior impacto possível a infraestrutura cibernética do adversário, com a finalidade de apoiar eficazmente a condução das nossas ações no ciberespaço, bem como a consecução dos objetivos gerais definidos pelo comandante da missão.

Embora a lista agora apresentada pareça longa e ambiciosa, importa considerar que as capacidades necessárias à condução das operações no ciberespaço não serão todas implementadas ao longo dos vários escalões[121] da estrutura militar. A cada nível estratégico, corresponderão diferentes cibercapacidades. Assim, por exemplo, sem entrarmos numa análise detalhada que está além do âmbito deste estudo, é possível referir que as capacidades que permitem conduzir a Ciberguerra não serão desenvolvidas a nível do escalão Companhia, iniciando-se a sua implementação apenas a partes do nível de Batalhão. Por sua vez, a capacidade para aceder ao *hardware* e ao *software* do adversário, por meios diretos ou remotos, com o fim de garantir o apoio necessário às ações de ciberguerra, só se começa a implementar a nível da Componente Terrestre do Teatro de Operações.

121 Para o Exército dos EUA estes escalões militares são: Companhia, Batalhão, Brigada, Divisão, Corpo de Exército, Componente Terrestre do Teatro de Operações, Cibercomando do Exército e Comando Conjunto de Combate.

Finalmente, também faz sentido referir que a doutrina militar dos EUA estabelece como pressuposto para um adequado levantamento das capacidades citadas anteriormente, a necessidade de se contemplarem no seu desenvolvimento os aspetos relativos à doutrina, à organização, ao treino, ao material, à liderança e educação, ao pessoal e às instalações[122].

O Governo dos EUA, refletindo num plano supranacional, a preocupação crescente da comunidade internacional com a necessidade de proteger a livre utilização do ciberespaço e reduzir/deter o número crescente de ciberataques, publicou pela primeira vez, em maio de 2011, uma Estratégia Internacional de Segurança do Ciberespaço (*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*)[123].

O principal objetivo desta estratégia é o de tornar a internet uma infraestrutura de comunicações e informação aberta, interoperável, segura e fiável, capaz de apoiar o negócio e o comércio internacional, fortalecer a segurança internacional e fomentar a liberdade de expressão e a inovação. Neste âmbito, é identificada uma preocupação especial com o facto de existir uma falta de legislação comum e de ser difícil aos diversos Estados atuarem fora das suas fronteiras de soberania. Por esta razão, será necessário intensificar a cooperação internacional no sentido de definir um enquadramento capaz de impor normas de comportamento responsável e de dar resposta aos futuros desafios e ameaças transnacionais.

Os princípios orientadores identificados por esta estratégia são:

- Economia: promoção de normas internacionais, inovação e mercados abertos para assegurar que o ciberespaço serve as necessidades da economia global;
- Proteção das redes: fomentar a segurança, fiabilidade e resiliência;
- Combate ao cibercrime: alargar a colaboração e o combate ao cibercrime;
- Cooperação militar: preparação para fazer face aos desafios de segurança do século XXI;
- Governação da internet: promoção de estruturas eficazes e inclusivas;
- Desenvolvimento internacional: levantamento sustentado de capacidades, para garantir a segurança e prosperidade.

122 Os EUA utilizam o acrónimo DOTMLPF para se referirem aos vetores de desenvolvimento das capacidades militares, correspondendo este acrónimo a Doutrina, Organização, Treino, Material, Liderança e Formação, Pessoal e Instalações (*facilities*).

123 Disponível em http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Consultado em 22 de dezembro de 2012.

Parte III – A Situação em Portugal e Espanha

O Ciberespaço, constituindo um vetor estruturante da sociedade de informação em que vivemos, exige hoje aos Estados uma visão estratégica clara, assente na formulação de objetivos realistas e na definição de linhas de ação concretas, que permitam salvaguardar os interesses nacionais e fortalecer o seu potencial estratégico.

Neste momento, tanto Portugal como Espanha têm desenvolvido um amplo debate no contexto nacional, especialmente orientado para a definição de uma Estratégia Nacional de Cibersegurança. Todavia, não existindo ainda nos dois países uma Estratégia oficialmente aprovada, só se torna possível introduzir neste estudo alguns elementos que, por terem resultado da reflexão nacional em curso e pela sua relevância para este trabalho de investigação, poderão ser considerados como referências orientadoras.

Com o intuito de identificar possíveis áreas de cooperação e de desenvolvimento de sinergias no futuro, são também caracterizadas, no plano nacional, as principais linhas de ação estratégica identificadas nos esforços em curso nos dois países ibéricos.

1. Visión Estratégica de España

1.1. Estrategia Española de Ciberseguridad

Como ya se ha indicado anteriormente, en España, el Ministro del Interior anunció a principios de 2012 la intención del Gobierno de proceder a la redacción de la Estrategia Española de Ciberseguridad[124]. Esta información ha venido siendo completada por las intervenciones públicas de varios miembros del Centro Criptológico Nacional del Centra Nacional de Inteligencia, las últimas de ellas ya en el año 2013[125], donde se presentaron los principales contenidos y las líneas generales del borrador de la futura Estrategia Española de Ciberseguridad.

Según las citadas intervenciones públicas puede anticiparse que esta futura Estrategia Española de Ciberseguridad se inspirará en cinco principios rectores:

- Liderazgo nacional y coordinación.
- Responsabilidad compartida y cooperación público-privada.
- Cooperación internacional.

124 Mercedes Oriol Vico, «Apoyo Personal del Ministro del Interior a la Ciberseguridad», *SEGURITECNIA*, pp. 22–24, jun-2012.

125 Javier Candau Romero, «La Estrategia Española de Ciberseguridad», presented at the Curso sobre 'Seguridad Nacional y Ciberdefensa: estrategias, capacidades y tecnologías', Escuela Técnica Superior de Ingenieros de Telecomunicación - Universidad Politécnica de Madrid, 2013. Luis Jiménez Múñoz, «Contenido de una Estrategia Nacional de Ciberseguridad», in *Fundación Círculo de Tecnologías para la Defensa y la Seguridad*, Paraninfo de la Universidad Politécnica de Madrid c/ Ramiro de Maeztu, 7 28040 Madrid, 2013.

• Proporcionalidad, racionalización y eficacia.
• La protección de los valores constitucionales.

En el citado borrador de la Estrategia, el Gobierno de España, para lograr sus fines de seguridad en el ciberespacio, fijaría los siguientes objetivos a conseguir:

• **Objetivo Global**: Lograr que España haga un uso seguro de las redes y sistemas de información, fortaleciendo las capacidades de prevención, detección y respuesta a los ciberataques.
• **Objetivo 1**: Garantizar que los sistemas de información y comunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de seguridad y resiliencia.
• **Objetivo 2**: Impulsar la seguridad y resiliencia de las redes y los sistemas de información utilizados por el sector empresarial en general y los operadores de infraestructuras críticas en particular
• **Objetivo 3**: Potenciar las capacidades de prevención y respuesta policial y judicial a las actividades del terrorismo y la delincuencia en el ciberespacio.
• **Objetivo 4**: Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.
• **Objetivo 5**: Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades que necesita España para sustentar todos los objetivos de ciberseguridad anteriores.

Para alcanzar los objetivos señalados, la futura Estrategia Española de Ciberseguridad se articula a través de líneas de acción interdependientes:

1. **Capacidad de prevención, detección y respuesta ante las ciberamenazas**: Incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa, y otros sistemas de interés nacional.
2. **Seguridad de los sistemas de información de las Administraciones Públicas**: Impulsar la implantación del Esquema Nacional de Seguridad[126], reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3. **Seguridad de las redes y los sistemas de información que soportan las infraestructuras críticas**: Impulsar la implantación de la normativa sobre Protec ción de Infraestructuras Críticas[127] y de las capacidades necesarias para la protección de los servicios esenciales.
4. **Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia**: Potenciar las capacidades para investigar y perseguir los ciberdelitos sobre la base de un marco jurídico y operativo eficaz.

126 Ministerio de la Presidencia, *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Eletrónica.* 2010.

127 Jefatura del Estado, *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.* 2011.

5. **Seguridad y resiliencia en el sector privado**: Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6. **Conocimientos, Competencias e I+D+i**: Promover la capacitación de profesionales en ciberseguridad e impulsar una I+D+i que proporcione soluciones eficaces.
7. **Compromiso Internacional**: Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.
8. **Cultura de Ciberseguridad**: Concienciar a los ciudadanos, profesionales y empresas, de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

1.2. Ciberdefensa en España: Regulación y Recursos

En el ámbito de Defensa en España, tradicionalmente la seguridad de la información ha estado enfocada principalmente en la protección de las comunicaciones. El uso cada vez más generalizado de los sistemas de información en combinación con los de comunicaciones y, en definitiva, del Ciberespacio, ha supuesto un cambio importante en las estructuras organizativas, el marco normativo y en el planeamiento de las capacidades y los recursos para su protección.

La aprobación de la Orden Ministerial 76/2002, sobre Política INFOSEC, sentó las bases para la protección de la información clasificada del Ministerio de Defensa en los sistemas de información y comunicaciones, introduciendo el concepto de 'acreditación', como "autorización que se concede a un sistema para el manejo de información clasificada en unas condiciones de seguridad determinadas"[128]. Si bien este concepto que era conocido en el ámbito de la información clasificada OTAN (Organización del Tratado del Atlántico Norte) no existía su regulación a nivel español.

Se designa al Ministro de Defensa como Autoridad de Acreditación del Ministerio, el cual delega sus funciones en Autoridades Delegadas de Acreditación (ADA) en cada uno de los ámbitos del Ministerio: JEMAD (Jefe del Estado Mayor de la Defensa) en el EMAD (Estado Mayor de la Defensa), JEME (Jefe del Estado Mayor del Ejército) en el Ejército de Tierra, AJEMA (Almirante Jefe del Estado Mayor de la Armada) en la Armada, JEMA (Jefe de Estado Mayor del Ejército del Aire) en el Ejército del Aire y Subsecretario de Defensa en el Órgano Central del Ministerio de Defensa. Esta primera norma supuso el inicio del desarrollo de un cuerpo normativo completo sobre seguridad de la información y ciberdefensa en el ámbito del Ministerio de Defensa español.

En el año 2006 se publica la Orden Ministerial 76/2006[129], por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa, en la que se designa al

128 Ministerio de Defensa, *Orden Ministerial 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.* 2002.

129 Ministerio de Defensa, *Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.* 2006.

Secretario de Estado de Defensa como Director de Seguridad de la Información del Ministerio de Defensa. Esta Orden Ministerial establece, además, que se desarrollará un conjunto de normativas de segundo y tercer nivel que aborden de forma específica la seguridad cuando la información del Departamento de Defensa se encuentra en las personas, los sistemas de información y comunicaciones, las instalaciones, las empresas y los documentos.

La Instrucción 41/2010 del Secretario de Estado de Defensa, sobre normas de aplicación de la Política de Seguridad de la Información del Ministerio de Defensa[130], designa a la Dirección General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones del Ministerio de Defensa, y al Director General de Armamento y Material como responsable del área de seguridad de la información en poder de las empresas.

Esta Instrucción establece, además, que en cada uno de los ámbitos del Ministerio (Secretaría de Estado de Defensa, Subsecretaría de Defensa, Secretaría General de Política de Defensa, Estado Mayor de la Defensa, Ejército de Tierra, Armada, Ejército del Aire y Unidad Militar de Emergencias), la Autoridad al cargo de dicho ámbito sea el máximo responsable de la dirección, coordinación, ejecución y supervisión de las medidas de seguridad de la información en su ámbito. Asimismo, dicha Autoridad, deberá nombrar un Jefe de Seguridad de la Información para su ámbito y un Jefe de Seguridad de la Información de cada una de las áreas de las Personas, Documentos, Empresas, Instalaciones y Sistemas de Información y Comunicaciones.

Por otro lado, y de carácter general para la Administración Pública española, la Ley 11/2002[131], reguladora del Centro Nacional de Inteligencia (CNI) designa al CNI responsable de "garantizar la seguridad de las tecnologías de la información" en la Administración. Derivado de esta designación, el CNI, a través del Centro Criptológico Nacional (CCN) desarrolla el conjunto normativo denominado CCN-STIC[132], de aplicación en toda la administración pública española y que trata de recoger las normas, procedimientos y guías de seguridad a aplicar en los sistemas de las tecnologías de la información y comunicaciones que manejan información clasificada.

Dentro de las administraciones públicas, el Real Decreto 3/2010[133], por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, establece la política de seguridad en la utilización de medios electrónicos de la adminis-

130 Juan José Díaz del Río Durán, «La Ciberseguridad en el Ámbito Militar», in *Ciberseguridad: Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, vol. 149, Instituto Español de Estudios Estratégicos, Ed. 2010, pp. 217–256.

131 Cortes Generales, *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.* 2002.

132 La serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional, dada la importancia que tiene el establecimiento de un marco de referencia que sirva de apoyo para que el personal de la Administración Pública española lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad. Consultar https://www.ccn.cni.es/index.php?option=com_content&view=article&id=5&Itemid=8

133 Ministerio de la Presidencia, *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Eletrónica.* 2010.

tración pública española y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

En lo que respecta a la Ciberdefensa Militar española, en paralelo a las iniciativas de la OTAN en este campo, se aprueba en el año 2011 la Visión del JEMAD de la Ciberdefensa Militar y el Concepto de Ciberdefensa Militar[134].

En estos documentos se asigna al JEMAD las responsabilidades de:

- Definir las implicaciones en el uso del Ciberespacio derivadas del Concepto de Estrategia Militar.
- Estudiar y evaluar la amenaza en el Ciberespacio desde el punto de vista militar.
- Promulgar la doctrina conjunta al respecto.
- Definir e impulsar el desarrollo de la capacidad de Ciberdefensa Militar que permita garantizar el uso del Ciberespacio en la conducción de las operaciones militares.
- Asegurar la eficacia operativa de las Fuerzas Armadas en el ámbito de la Ciberdefensa, pudiendo supervisar la preparación de las unidades de la Fuerza y evaluar su disponibilidad operativa.

En el Concepto de Ciberdefensa Militar se establece que para la obtención de la capacidad de Ciberdefensa, es necesario el desarrollo de los siguientes aspectos:

- *Material*: para garantizar la concordancia de los procesos de adquisición de material con la rapidez de los cambios tecnológicos y la adecuación a la normativa de protección de la información, prestando especial atención a las garantías de seguridad de toda la cadena de suministros (del hardware y del software).
- *Infraestructura*: para que las instalaciones y componentes de los sistemas de información y comunicaciones cuenten con las adecuadas medidas de seguridad física y de emisiones electromagnéticas no deseadas (TEMPEST – *Transient Electromagnetic Pulse Surveillance Technology*[135]).
- *Recursos Humanos*: para disponer de personal formado técnicamente y con continuidad adecuada para garantizar la eficacia y la eficiencia de la Ciberdefensa, donde el personal militar podrá ser complementado con personal civil cualificado, que forme parte de equipos multidisciplinares en donde se potencien las sinergias.
- *Adiestramiento*: para que el personal esté adecuadamente concienciado e instruido en la seguridad de la información y en la Ciberdefensa. Para ello, los ejercicios de Ciberdefensa son fundamentales, debiéndose potenciar su realización a nivel nacional y fomentar la participación a nivel internacional. Además, se deberán incluir eventos e incidencias de Ciberdefensa en todo tipo de ejercicios militares.

134 Luis Feliu Ortega, «La Ciberseguridad y la Ciberdefensa», in *El Ciberespacio. Nuevo Escenario de Confrontacion*, Madrid: Ministerio de Defensa, Subdirección General de Publicaciones y Patrimonio Cultural, 2012, pp. 37–69.

135 TEMPEST hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones eletromagnéticas no intencionadas, producidas por equipos elétricos y eletrónicos que, detetadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

- *Doctrina*: puesto que la naturaleza de la Ciberdefensa requiere de una doctrina conjunta y alineada con las de la OTAN y UE, para proporcionar a los mandos las bases tácticas, técnicas y de procedimiento, que les permita ejercer su misión de forma eficaz y eficiente.
- *Organización*: para permitir la implementación de una seguridad dinámica, en contra de la actual estructura de los sistemas TIC orientada hacia la protección estática, y el ejercicio de las actividades de explotación y respuesta. Además, la necesidad de una dirección, planificación y coordinación centralizada requiere adaptar la organización para alcanzar la adecuada eficacia de las capacidades necesarias.
- *Colaboración Público-Privada*[136]: para fomentar acuerdos, nacionales e internacionales[137], entre los sectores público y privado, que permitan el intercambio de información y una adecuada coordinación de las acciones.

Una vez aprobados los documentos de Visión y el Concepto, se inician los trabajos para el desarrollo de un Plan de Acción para la Obtención de la Ciberdefensa Militar, que concrete un calendario con las tareas a realizar y sus responsabilidades e identifique los recursos humanos, materiales y financieros necesarios.

Como punto de partida para este Plan, el EMAD dispone de una Capacidad Inicial de Ciberdefensa[138], constituida principalmente por la Sección de Seguridad de la Información CIS y Oficina de Programa Information Assurance del EMAD, que proporcionan la capacidad de inspección y auditoría de seguridad, asesoramiento en seguridad, ciberejercicios y capacidad inicial de respuesta ante incidentes.

A lo largo del año 2012, estas iniciativas para la Ciberdefensa sufren un impulso importante. Así, en julio se publica la Directiva de Defensa Nacional[139] en la que ya se afirma que "*se participará en el impulso de una gestión integral de la Ciberseguridad, en el marco de los principios que se establezcan al efecto en la Estrategia de Ciberseguridad Nacional.*"

Por otro lado, en ese mismo mes de julio de 2012, el JEMAD aprueba el "Plan de Acción para la obtención de la Capacidad de Ciberdefensa Militar"[140], en el que se identifican las acciones necesarias para la obtención de una capacidad de Ciberdefensa Militar

136 En inglés '*Public–Private Partnership*' (*PPP*, *P3* o *P³*). Un ejemplo de este tipo de colaboración es el *EP3R* (*European Public-Private Partnership for Resilience*), que tiene como objetivo proporcionar un marco de gobierno flexible a nivel europeo, para involucrar a atores relevantes, públicos y privados, en las políticas públicas y toma de decisiones estratégicas para fortalecer la seguridad y la resiliencia en el contexto de la *CIIP* (*Critical Information Infrastructure Protection*). Consultar http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/ index_en.htm

137 European Network and Information Security Agency, *Good Practice Guide – Cooperative Models for Effective Public Private Partnerships*. Luxembourg: Publications Office of the European Union, 2011.

138 Juan José Díaz del Río Durán, «La Ciberseguridad en el Ámbito Militar», in *Ciberseguridad: Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, vol. 149, Instituto Español de Estudios Estratégicos, Ed. 2010, pp. 217–256.

139 Presidencia del Gobierno, *Diretiva de Defensa Nacional 2012: Por una Defensa Necesaria, Por una Defensa Responsable*. 2012.

140 Capitán de navío Francisco Zea Pasquín, «Ciberdefensa militar - Las Fuerzas Armadas se preparan para afrontar con éxito los nuevos retos del siglo XXI en materia de ciberseguridad», *Revista Española de Defensa*, pp. 48-49, mar-2013.

que cumpla con los objetivos especificados en el anteriormente mencionado Concepto de Ciberdefensa Militar. Entre los citados objetivos estarían:

- Garantizar el libre acceso al ciberespacio con el fin de cumplir las misiones asignadas a las Fuerzas Armadas.
- Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de responsabilidad militar.
- Ejercer la respuesta oportuna, legítima y proporcionada ante amenazas.

El Plan de Acción diseña una estrategia de obtención basada en un proceso incremental que, empezando por una primera fase denominada Capacidad de Ciberdefensa Militar Básica, que contempla implementar fundamentalmente las cibercapacidades de Defensa, para garantizar la resistencia ante los posibles ciberataques y la recuperación de la funcionalidad de los sistemas ante los daños producidos por los mismos.

Posteriormente se abordará la obtención de la Capacidad de Ciberdefensa Militar Intermedia, en la que además de fortalecer las capacidades de Defensa, se centrará fundamentalmente en desarrollar las Capacidades de Explotación, para permitir la obtención de información sobre las capacidades de los posibles adversarios, unida a actividades de recopilación, análisis y explotación de la misma.

Finalmente, se abordará la Capacidad de Ciberdefensa Militar Permanente, que permitirá la implementación de la capacidades de Respuesta ante los ciberataques, lo que asegurará la disponibilidad de una Capacidad de Ciberdefensa completa, que incluya los tres aspectos de Defensa, Explotación y Respuesta.

En noviembre de 2012, el Ministro de Defensa ordena la creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas dependiente del JEMAD[141], con el objeto de impulsar la obtención de las Capacidades de Ciberdefensa de la forma más eficiente posible. Esto proporcionará una unidad militar altamente especializada, capaz de desarrollar y alcanzar las capacidades de Ciberdefensa anteriormente descritas.

El 26 de febrero de 2013 se publica, en el Boletín Oficial de Defensa, la Orden Ministerial 10/2013[142], por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Esta Orden Ministerial establece el ámbito de actuación del Mando Conjunto de Ciberdefensa, que estará centrado en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas y en aquellas otras que específicamente se le encomienden.

La misión del Mando Conjunto de Ciberdefensa es el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

---

141 Francisco Zea Pasquín (Capitán de Navío), «La Ciberdefensa en las Fuerzas Armadas: perspetiva conjunta», presented at the Curso sobre 'Seguridad Nacional y Ciberdefensa: estrategias, capacidades y tecnologías', Escuela Técnica Superior de Ingenieros de Telecomunicación - Universidad Politécnica de Madrid, 2013.

142 Ministerio de Defensa. BOD, *Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*. 2013.

Los cometidos del Mando Conjunto de Ciberdefensa son:

- Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.
- Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.
- Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un Entorno degradado debido a incidentes, accidentes o ataques.
- Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad.
- Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
- Dirigir y coordinar, en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional.
- Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.
- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento.

Por último, la citada Orden Ministerial 10/2013 establece que el Comandante Jefe del Mando Conjunto de Ciberdefensa será un Oficial General de los Cuerpos Generales del Ejército de Tierra, de la Armada, del Ejército del Aire, o del Cuerpo de Infantería de Marina, dependiente orgánicamente del Jefe de Estado Mayor de la Defensa. El Mando Conjunto de Ciberdefensa será un órgano perteneciente al Estado Mayor de la Defensa, integrado en la estructura operativa de las Fuerzas Armadas.

2. Visão Estratégica de Portugal

2.1. Estratégia Portuguesa de Cibersegurança

Conforme já antes referido, Portugal não dispõe ainda de uma Estratégia Nacional de Cibersegurança, formalmente definida e oficialmente aprovada. No entanto, existem já diversos trabalhos de reflexão[143] e grupos de trabalho oficialmente mandatados para

143 A título de exemplo, referem-se neste contexto, iniciativas como o Grupo de Estudos sobre Contributos para uma Estratégia Nacional de Informação (GECENI) do Instituto da Defesa Nacional, as intervenções da Autoridade Nacional de Segurança (ANS), do Diretor do Centro de Gestão da Rede Informática do

trabalharem em áreas afins, nomeadamente no âmbito do levantamento de uma Estrutura Nacional de Cibersegurança[144].

Neste contexto, na sequência dos trabalhos conduzidos pela Comissão Instaladora do Centro Nacional de Cibersegurança, o Gabinete Nacional de Segurança (GNS) publicou recentemente uma proposta de Estratégia Nacional de Cibersegurança[145]. Esta, apesar de não ter ainda sido formalmente aprovada, constituiu a principal base de referência para a elaboração deste trabalho.

2.1.1. *Enquadramento Conceptual*

A necessidade de levantar mecanismos de proteção e defesa, destinados a garantir a livre utilização da internet e do ciberespaço, tem conduzido os Estados ao aprofundamento de uma cultura de cibersegurança e à tomada de consciência coletiva, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas de combate a todas as formas de ataque cibernético. Assim, iniciativas recentes de âmbito nacional e internacional (ONU, OTAN, EU, OSCE) têm vindo a propor acordos de cooperação e dispositivos legais que definem normas e princípios destinados a garantir uma internet sustentável e um comportamento aceitável no ciberespaço.

Dentro da lógica da defesa dos seus interesses, quando estão em risco a segurança e o bem-estar social, o Estado terá que desenvolver uma "Política para o Domínio da Informação" que permita garantir, não só a convergência estrutural para os parâmetros tecnológicos da Sociedade de Informação e do Conhecimento, como também a Segurança e a Defesa da sua Infraestrutura de Informação.

Atendendo ao princípio de que a cada forma de coação corresponde uma estratégia distinta[146], a utilização da informação e do ciberespaço como forma de coação faz surgir uma nova estratégia, a Estratégia da Informação Nacional (EIN). Assim, como uma das componentes desta Estratégia e subordinada à Estratégia de Segurança e Defesa do Estado (ENSD), surge a Estratégia Nacional de Segurança da Informação (ENSI).

Constituindo o ciberespaço uma das componentes do ambiente da informação, a sua segurança (Cibersegurança), deve ser perspetivada no âmbito da ENSI[147]. Por outro lado,

---

Governo (CEGER), e os Seminários e Simpósios Internacionais relativos à "Estratégia da Informação Nacional", assim como, os trabalhos de investigação desenvolvidos no âmbito do Mestrado em Guerra de Informação da Academia Militar.

144 Neste contexto, através da Resolução do Conselho de Ministros n.º 42/2012, *Diário da República*, 1.ª série, n.º 74, 13 de abril de 2012, foi nomeada uma Comissão Instaladora do Centro Nacional de Cibersegurança. No âmbito dos trabalhos desta comissão, foi desenvolvido um enquadamento estratégico da futura estrutura de cibersegurança nacional.

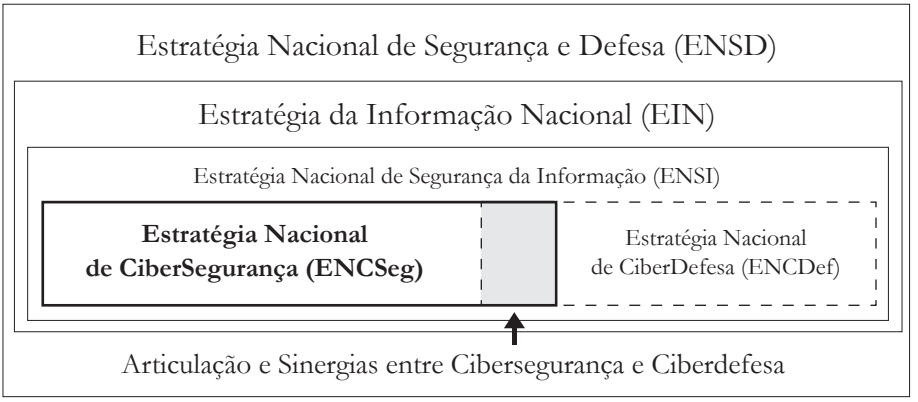
145 Proposta de Estratégia Nacional de Cibersegurança publicada pelo Gabinete Nacional de Segurança. Disponível em http://www.gns.gov.pt/NR/rdonlyres/ED57762F-3556-4C05-9644-888E35C790BB/0/PropostaEstratégiaNacionaldeCiberseguraçaPortuguesa.pdf.

146 Couto, Abel Cabral (1988). *Elementos de Estratégia,* Volume I, IAEM.

147 Nunes, Paulo F. V. (2012). "A Definição de uma Estratégia Nacional de Cibersegurança"*, Nação e Defesa,* n.º 133. Lisboa: Instituto da Defesa Nacional.

importa também referir que, assim como existe uma estreita ligação entre a Segurança e a Defesa Nacional, também a Cibersegurança se revela indissociável da Ciberdefesa do Estado. Na prática, isto significa que não será possível garantir a Cibersegurança sem o levantamento de uma capacidade de Ciberdefesa.

Figura 2 – Enquadramento da Estratégia Nacional de Cibersegurança[148]



Devido ao enquadramento apresentado na figura 2, constata-se que a ENCSeg deverá contribuir tanto para a implementação dos processos de Segurança da Informação associados ao ciberespaço como, de forma articulada e sinérgica, para o levantamento dos mecanismos de Ciberdefesa (zona sombreada da figura 2) que são necessários mobilizar para garantir a própria Cibersegurança do país. A ENCSeg encontra-se assim alinhada não só com a ENSI mas também com a própria EIN.

Neste contexto, parece claro que os benefícios decorrentes da livre utilização do ciberespaço só serão atingidos se formos capazes de proteger e defender as infraestruturas de informação nacionais, garantindo um nível aceitável e sustentável de segurança, fiabilidade e disponibilidade na sua exploração.

2.1.2. *Estratégia Nacional de Cibersegurança: a Visão*

Para Portugal, o ciberespaço impõe novas formas de interação e de relacionamento, levando o país a colocar-se na vanguarda da revolução digital. A definição de uma agenda digital permite disponibilizar benefícios económicos e sociais, estimular a criação de empregos, a sustentabilidade e inclusão social, extrair o máximo benefício das novas tecnologias e melhorar a estrutura de enquadramento nacional.

No entanto, o crescente número de incidentes e ataques maliciosos, que têm como alvo as infraestruturas de informação do governo, instituições públicas e privadas, empresas e cidadãos, tem vindo a demonstrar a necessidade do país levantar uma Estrutura

148 Idem

Nacional de Cibersegurança, capaz de garantir uma eficaz gestão de crises, coordenar a resposta operacional a ciberataques, desenvolver sinergias nacionais e potenciar a cooperação internacional neste domínio.

A necessidade de proteger as áreas que materializam a Soberania Nacional, assegurando a autonomia política e estratégica do país, tem vindo assim a impor a Cibersegurança como uma prioridade nacional. Neste contexto, importa definir uma visão e um enquadramento estratégico, lógico e coerente, que permita alicerçar a Estrutura Nacional de Cibersegurança que se pretende levantar.

A clarificação da finalidade a atingir facilita a dedução dos objetivos da Estratégia Nacional de Cibersegurança, permitindo, a partir daí, perspetivar as linhas de ação estratégica que vão orientar a sua implementação.

2.1.3. *Objetivos e Linhas de Ação Estratégica*

A finalidade a atingir pela Estratégia Nacional de Cibersegurança, constituindo o fundamento da visão estratégica que se pretende estruturar neste domínio, decorre do nível de ambição que for definido pela orientação política.

O principal desafio que o Estado tem que enfrentar é o de estimular uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, ao mesmo tempo que garante a proteção e defesa da sua infraestrutura de informação crítica. Neste âmbito, considera-se que o principal desafio de Portugal se coloca essencialmente ao nível da Garantia da Informação (*Information Assurance*). Este desiderato requer tanto a implementação de processos de Segurança da Informação como de mecanismos de Ciberdefesa.

Com base na finalidade identificada, considera-se que o país deverá procurar atingir os seguintes três objetivos principais:

- Garantir a segurança no ciberespaço;
- Fortalecer a cibersegurança das infraestruturas críticas nacionais;
- Defender os interesses nacionais e a liberdade de ação no ciberespaço.

A visão clara das implicações/necessidades associadas a cada um dos objetivos, permitirá definir uma orientação (geral e específica) traduzida em linhas de ação concretas, destinadas a reforçar o potencial estratégico nacional no ciberespaço. Neste contexto, identificam-se seguidamente linhas de ação estratégica para cada um dos objetivos enunciados.

2.1.3.1. *Garantir a Segurança no Ciberespaço*

As ameaças aos sistemas de informação são dirigidas simultaneamente aos serviços públicos, privados, às empresas e aos cidadãos. Os serviços públicos deverão servir como exemplo para a sociedade e deverão ser capazes de melhorar a proteção dos sistemas de informação e a informação de que são guardiões.

Campanhas de informação e alerta deverão ser implementadas, tendo como alvos principais os cidadãos e as empresas.

Ao mesmo tempo deverá ser elaborada legislação que promova a melhoria da cibersegurança, a luta contra o cibercrime e ainda a promoção da cooperação judicial e internacional.

Para garantir a Segurança do Ciberespaço, foram identificadas as seguintes linhas de ação estratégica:

- Analisar o ambiente de informação e antecipar eventuais ataques de forma a tomar as decisões apropriadas;
- Detetar e bloquear ataques, alertar e apoiar as potenciais vítimas;
- Estimular e potenciar as capacidades científicas, técnicas, industriais e humanas do país de forma a manter a independência nacional neste domínio;
- Adaptar a legislação nacional de forma a incorporar os desenvolvimentos tecnológicos e novas práticas.
- Desenvolver iniciativas de cooperação internacional em áreas ligadas à segurança dos sistemas de informação, ciberdefesa e luta contra o terrorismo de forma a proteger melhor os sistemas de informação nacionais;
- Comunicar e informar de forma a influenciar e a aumentar a compreensão da população portuguesa relativamente à extensão dos desafios relacionados com a segurança dos sistemas de informação.

2.1.3.2. *Fortalecer a Cibersegurança das Infraestruturas Críticas*

A nossa sociedade está cada vez mais dependente dos sistemas de informação e das redes, particularmente da internet, pelo que os ataques a estes sistemas podem ter graves consequências humanas e económicas.

O Estado deve trabalhar para garantir e melhorar a segurança das Infraestruturas Críticas Nacionais, em colaboração estreita com as operadoras de telecomunicações e os detentores dessas infraestruturas.

Para fortalecer a Cibersegurança das Infraestruturas Críticas Nacionais foram identificadas as seguintes linhas de ação estratégica:

- Reforçar a Segurança das TIC nas redes do Governo e da Administração Pública;
- Reforçar a Segurança dos Sistemas de Informação do Estado e dos operadores das infraestruturas críticas para assegurar uma maior resiliência (capacidade de sobrevivência) nacional.

2.1.3.3. *Defender os Interesses Nacionais e a Liberdade de Ação no Ciberespaço*

As autoridades governamentais e os atores relacionados com a gestão de crises deverão ter os meios disponíveis para comunicarem em qualquer situação e com confidencialidade. Para garantir a confidencialidade da informação nestas redes, são necessárias tecnologias de segurança, que teremos que desenvolver nas nossas Universidades e Centros de Investigação.

Para defender os interesses nacionais e a liberdade de ação no ciberespaço, assegurando a proteção da informação e a soberania nacional foram identificadas as seguintes linhas de ação estratégica:

- Reforçar iniciativas nacionais estruturantes da "Sociedade de Informação e do Conhecimento";
- Proteger e defender os mecanismos de Governação Eletrónica do Estado;

• Levantar a Estrutura Nacional de Cibersegurança e Ciberdefesa;
• Estabelecer mecanismos de cooperação nacional e internacional, neste âmbito.

De forma transversal, as atividades desenvolvidas no âmbito da implementação da Estratégia Nacional de Cibersegurança, contribuirão decisivamente para uma utilização mais racional e coerente dos recursos disponíveis, estimulando esforços cooperativos e gerando as sinergias necessárias para reforçar as capacidades nacionais no ciberespaço.

2.2. Ciberdefesa em Portugal: Enquadramento e Iniciativas em Curso

Constituindo a Segurança da Informação no Ciberespaço e a Ciberdefesa vetores relativamente recentes no contexto da Segurança e Defesa Nacional, Portugal tem vindo a definir um quadro de análise a partir do qual procura enquadrar e definir uma Política Nacional de Cibersegurança e de Ciberdefesa.

Neste âmbito, prevê-se que o levantamento desta Política seja equacionado no quadro das iniciativas atualmente em curso no país, nomeadamente, as associadas ao novo Conceito Estratégico de Defesa Nacional[149], ao desenvolvimento de uma Estratégia Nacional de Cibersegurança, ao levantamento de um Centro Nacional de Cibersegurança e de uma Rede Nacional de CSIRT (*Computer Incident Response Teams*). Neste âmbito, têm também vindo a ser tidos em consideração os esforços cooperativos já lançados pelas Organizações Internacionais de que Portugal faz parte integrante (OTAN e UE) e por outros países que, de forma individual ou cooperativa, procuram também estruturar uma capacidade neste domínio.

2.2.1. *Regulação e Recursos*

Ao longo da última década, têm sido desenvolvidas diversas experiências, tanto ao nível nacional como da OTAN[150] e UE[151], suscetíveis de conduzir ao desenvolvimento de políticas, doutrinas e procedimentos destinados a gerir e a integrar as capacidades civis e militares em rede, procurando explorar com maior eficácia o ambiente de informação global em que hoje vivemos

149 Conceito Estratégico de Defesa Nacional (2013). Resolução do Conselho de Ministros n.º 19/2013, *Diário da República*, 1.ª Série, 5 de abril.

150 A política de Ciberdefesa da OTAN prevê a criação de mecanismos políticos e operacionais de resposta a ciberataques, integrando a Ciberdefesa no seu Planeamento de Defesa. Estabelece ainda princípios de cooperação, com os seus parceiros, organizações internacionais, com o setor privado e ainda com as universidades centros de investigação. Paralelamente, esta organização desenvolveu um Plano de Ação de Ciberdefesa que servirá como ferramenta para garantir a aplicação oportuna e eficaz da nova política não só nas suas estruturas mas também para servir de referência ao levantamento de capacidades nacionais em todos os países membros da Aliança.

151 A União Europeia aprovou recentemente o conceito de Ciberdefesa em operações militares (*Cyber Defence Concept in EU Military-led Operations*), procurando articular a cooperação civil-militar neste domínio. Entretanto lançou também um contrato tendo em vista o futuro desenvolvimento de capacidades de Ciberdefesa para a área militar, *A Framework Contract on Developing Cyber Defence Capabilities for the Military (frameCyberCAP)*. Disponível em http://www.eda.europa.eu/procurement/procurement-view/12.cap.op.332---a-framework-contract-on-developing-cyber-defence-capabilities-for-the-military(framecybercap)-.

Em Portugal, foi atribuída ao Gabinete Nacional de Segurança (GNS) a missão de garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal faz parte. De acordo com a sua Lei Orgânica[152], esta entidade exerce também a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas (SCEE). O GNS constitui atualmente o ponto de ligação nacional com a OTAN e com a UE para a área da Cibersegurança e Ciberdefesa cooperativa. Neste âmbito, Portugal celebrou com a OTAN um memorando de entendimento (Memorandum of Understanding-MoU) em 3 de maio de 2011.

O CERT.PT tem-se constituído como um centro de competências nacional ao nível da cibersegurança. Nesse sentido, é um ponto de referência e de contacto que, embora residente na Fundação para a Ciência e Tecnologia (FCT)[153], tem vindo a garantir a interligação nacional à rede europeia de CSIRT e a desenvolver um esforço importante no levantamento de uma rede de CSIRT nacional, federando os diversos centros de competências existentes no país e estimulando a partilha de informação relativa a incidentes de segurança informática. Apesar de na prática assumir um papel relevante na garantia da segurança da informação no ciberespaço nacional, o CERT.PT não possui um mandato expresso do Governo para atuar como entidade responsável pela coordenação nacional no âmbito da cibersegurança do país. No entanto, tal não significa que não exista uma resposta articulada face a incidentes de segurança informática. Estão implementados processos de análise de vulnerabilidades e de gestão do risco das infraestruturas críticas nacionais, por parte das entidades que são por elas responsáveis e que, para esse efeito, desenvolveram mecanismos de proteção específicos, nomeadamente, através do levantamento de CSIRT sectoriais, como é o caso da rede de emergência nacional e das redes das Forças Armadas.

Perspetivando-se de forma consistente a tendência para um aumento das ciberameaças, tanto no âmbito nacional como internacional, o governo português decidiu, através da medida 4 da Resolução do Conselho de Ministros n.º 12/2012[154], rever a Estrutura Nacional de Segurança da Informação (ENSI) e criar um Centro Nacional de Cibersegurança (CNC). Para esse efeito, em abril de 2012, foi nomeada uma Comissão Instaladora do CNC[155] presidida pelo Diretor do GNS.

152 Decreto-Lei n.º 3/2012, *Diário da República*, 1.ª série, n.º 11, 16 de janeiro de 2011.

153 Por Resolução do Conselho de Ministros de 11 de dezembro de 2012, a Fundação para a Computação Científica Nacional (FCCN) será integrada na Fundação para a Ciência e Tecnologia em 2013. A FCCN é a entidade responsável por assegurar a gestão da RCTS – NREN (*National Research and Education Network*). Gere ainda o domínio internet de topo (.pt) e colabora em diversos projetos de investigação nacionais e internacionais. Neste momento, esta instituição tem o estatuto de associação privada sem fins lucrativos de utilidade pública.

154 *Diário da República*, 1.ª série, n.º 27, 7 de fevereiro de 2012.

155 Resolução do Conselho de Ministros n.º 42/2012, *Diário da República*, 1.ª série, n.º 74, 13 de abril de 2012

Portugal tem assim vindo a equacionar o desenvolvimento de uma capacidade nacional de proteção e defesa no ciberespaço, clarificando os aspetos ligados à Cibersegurança dos que, por colocarem em risco a Segurança e Defesa do Estado, se enquadram no domínio da Ciberdefesa, exigindo por essa razão uma participação das Forças Armadas.

2.2.2. *Cibersegurança nas Forças Armadas*

Na Declaração de Praga de 21 de novembro de 2002, foi acordada pelos Chefes de Governo das nações OTAN, a necessidade de fortalecer as capacidades da Aliança na defesa contra ataques informáticos.

De forma a cumprir este objetivo surgiu o PEMGFA/CSI/004, de 14 de fevereiro de 2005, com a Organização e Normas de Segurança nos Sistemas de Informação e Comunicações Conjuntos e o PEMGFA/CSI/301, de 23 de setembro de 2008, que se destina a estabelecer a estrutura orgânica, normas e procedimentos para garantir a Capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas.

Dada a necessidade de cumprir os requisitos de segurança referidos no PEMGFA/CSI/004 de 14 de fevereiro de 2005, foi necessário implementar mecanismos, procedimentos e normativos de gestão de segurança, por forma a detetar, prevenir, deter e recuperar a informação de incidentes que pudessem afetar a confidencialidade, integridade e disponibilidade das Comunicações e dos Sistemas de Informação (CSI) das Forças Armadas (FFAA).

A proteção dos Sistemas de Informação e Comunicações (SIC) militares críticos, requer não apenas a implementação e gestão de medidas de segurança adequadas, mas também uma Capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas (CRISI-FA). A CRISI-FA recorre às estruturas existentes nos Ramos das FFAA e Estado-Maior General das Forças Armadas (EMGFA), utilizando assim, de forma coordenada, as valências existentes em pessoal, material e organização das FFAA que, com a sua estrutura orgânica, normas e procedimentos permite garantir a disponibilidade, a integridade e a confidencialidade nas CSI das FFAA.

Assim sendo, o CRISI tem como missão coordenar a resposta a incidentes de segurança informática nas FFAA e consubstancia-se através de um Grupo de Resposta a Incidentes de Segurança Informática (GRISI), o qual é responsável por receber, analisar e responder a notificações e atividades relacionadas com incidentes de segurança em sistemas informáticos. As atividades do GRISI são dirigidas à área CSI das FFAA.

É da responsabilidades do EMGFA, promover a implementação da política conjunta de segurança da informação, de forma a garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA. O Centro de Coordenação da CRISI (CC-CRISI), constitui o órgão responsável por fazer a ligação à estrutura nacional de Cibersegurança.

2.2.3. *Capacidade de Ciberdefesa: O Papel das Forças Armadas*

As Forças Armadas, à luz da Constituição da República Portuguesa, constituem o corpo social responsável pela defesa do país contra ameaças externas e devem assegurar, em situações de exceção (ex: estado de sítio), o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado. Face à natureza assimétrica

e transversal das ciberameaças, onde se torna difícil clarificar a origem (interna ou externa) e o impacto dos ciberataques, as Forças Armadas devem também assegurar o desenvolvimento de capacidades e assumir competências no domínio da Ciberdefesa do país.

Tendo por base o desenvolvimento e exploração de uma capacidade residente de Guerra de Informação, consubstanciada através de Operações em Redes de Computadores (*Computer Network Operations* – CNO), da condução de Operações de Informação (OI) e da implementação de mecanismos de Garantia da Informação (*Information Assurance* – IA), prevê-se também no âmbito das Forças Armadas o levantamento de uma capacidade efetiva de Ciberdefesa.

Procurando adotar uma aproximação semelhante à que tem vindo a ser seguida pela OTAN e pela União Europeia, pretende-se assim incorporar as lições aprendidas resultantes do emprego operacional das Forças Armadas em missões internacionais, implementar doutrinas e conceitos adaptados ao futuro ambiente operacional e definir um processo de desenvolvimento para a capacidade de Ciberdefesa, assente em arquiteturas de referência. Desta forma, poder-se-á garantir não só a exploração de oportunidades de cooperação nacional e internacional como dar passos seguros no sentido de manter as Forças Armadas ajustadas à envolvente operacional, económica e social em que se inserem.

Com base no conceito de "duplo-uso", considera-se ser verosímil que possa vir a ser equacionada a possibilidade de as Forças Armadas poderem vir a assumir um papel relevante na Ciberdefesa Nacional. Neste contexto, a interligação do futuro Centro de Ciberdefesa (inclui funções de CERT) das Forças Armadas à Rede de CSIRT Nacional poderá potenciar o seu papel tanto no âmbito nacional como no plano internacional. Na materialização deste objetivo, para além das necessárias alterações orgânicas, torna-se necessário equacionar uma adaptação da doutrina vigente e o reforço das capacidades existentes nas Forças Armadas.

3. Linhas de Ação Estratégica Comuns

Atendendo à realidade social, política e económica dos dois países, com base nos elementos recolhidos no âmbito deste estudo, estima-se como possível a identificação de diversas linhas de ação estratégica para a segurança do ciberespaço, tanto em Portugal como em Espanha. Neste contexto, dada a natureza específica das iniciativas e projetos a desenvolver, considera-se importante aprofundar este estudo no sentido de delinear, de forma consistente e assertiva, um plano de possíveis iniciativas conjuntas a desenvolver. O facto de se aguardar para breve a aprovação dos conceitos estratégicos nacionais de cibersegurança dos dois países, reforça esta necessidade e aconselha o desenvolvimento de um futuro projeto de investigação conjunto. O estudo a desenvolver, no contexto deste projeto, permitirá identificar áreas de convergência entre a visão estratégica dos dois países, potenciando as necessárias sinergias e o desenvolvimento de esforços cooperativos de natureza bilateral, como se apresenta na Parte V (Conclusões e Reflexões).

Parte IV – A Situação nas Organizações Internacionais Comuns aos Dois Países

No contexto de alianças e de compromissos internacionais, os Estados têm hoje que articular as suas políticas e estratégias nacionais, de forma a reforçar a defesa de interesses comuns e salvaguardar valores coletivos.

Com o intuito de identificar possíveis áreas de cooperação futuras, desta feita no plano internacional, importa também caracterizar no contexto deste estudo as principais iniciativas e esforços cooperativos na área da segurança e defesa do ciberespaço, nomeadamente os que decorrem no âmbito das organizações de que Portugal e Espanha são parte integrante.

1. Organização do Tratado do Atlântico Norte

A Organização do Tratado do Atlântico Norte (OTAN) dispõe atualmente de um amplo conjunto de capacidades orientadas para a proteção da sua informação e dos seus sistemas, promovendo a sua articulação e coordenação com as capacidades dos diferentes países membros.

Desde 1999 e até à presente data, várias iniciativas têm sido realizadas neste âmbito. Para uma melhor perceção dos passos entretanto dados pela OTAN, vejamos a sequência dessas iniciativas:

- Em 1999, durante a Cimeira de Washington DC, foram aprovadas duas decisões sobre o levantamento de Capacidades de Defesa relacionadas respetivamente com a necessidade de garantir a segurança das comunicações e dos sistemas de informação e com a análise de vulnerabilidades desses sistemas.
- Em 2002, durante a Cimeira de Praga, a segurança da informação constituiu também um ponto central das discussões.
- Em 2004, foi aprovada a criação do NCIRC (*NATO Computer Incident Response Capability*).
- Em 2005, a proteção das infraestruturas críticas foi um dos temas propostos para fazer parte dos programas de defesa contra o terrorismo.
- Em 2006, a Declaração da Cimeira de Riga debruçou-se sobre os desafios de segurança do século XXI.
- Durante o mesmo ano, publicou-se o documento "Orientação Política Global", que incide na necessidade de transformação contínua da OTAN e constitui um guia para o estabelecimento de prioridades relativas às capacidades de planeamento e informações da OTAN.

- Em 2007, estabeleceu-se um acordo ao nível do NC3B (*NATO Consultation, Command and Control Board)* com o objetivo de se constituir um Grupo de Trabalho Executivo a quem foi atribuída a responsabilidade do desenvolvimento da Política de Ciberdefesa, e das recomendações para melhorar a Ciberdefesa, garantindo também desta forma o apoio ao desenvolvimento do "Conceito de Ciberdefesa da OTAN ".
- A política de Ciberdefesa da OTAN foi aprovada em 2008, juntamente com a definição do conceito de Ciberdefesa.
- Durante este mesmo ano, foram constituídos o CCD CoE (*Cooperative Cyber Defence Centre of Excelence*), em Tallinn, e a NCDMA (*NATO Cyber Defence Management Authority*).
- Também em 2008, durante a Cimeira de Bucareste, foi publicado um relatório sobre "O Papel da OTAN na Segurança do Setor Energético"..
- Em 2010, teve lugar a Cimeira de Lisboa[156] onde, para além da aprovação de um novo conceito estratégico e da definição da ciberdefesa como uma capacidade prioritária para a Aliança, foi determinada a revisão da Política de Ciberdefesa da OTAN. Neste contexto, foi identificada a necessidade de se ter em conta os novos desafios e ameaças do ciberespaço e a necessidade da OTAN desenvolver a capacidade para combater ciberataques.
- No ano de 2011, publicou-se a revisão da Política de Ciberdefesa da OTAN, a que se juntou um plano de ação para a sua implementação.
- Em 2012, a OTAN iniciou a revisão da sua Política de Segurança da Informação (*NATO Information Security Policy*) que agora também passou a incluir a Ciberdefesa, o não repudio e a autenticação, que se acrescentaram às características que até aí caracterizavam a segurança da informação (disponibilidade, integridade e confidencialidade).
- Durante o ano de 2012, surgiu também a NCIA (*NATO Communications and Information Agency*) e consolidou-se o desenvolvimento das capacidades do NCIRC.

O desenvolvimento da Política de Ciberdefesa da OTAN, assim como a sua revisão e a criação de um plano de ação para a sua implementação, constituem os elementos fundamentais para o desenvolvimento da ciberdefesa na OTAN. Esta política, baseia-se nos seguintes pontos principais[157]:

- Integração das considerações de ciberdefesa dentro das estruturas da OTAN e processos de planeamento, a fim de ter um núcleo de defesa e gestão de crises.
- Focalização na prevenção, resiliência e defesa dos ativos críticos do Ciberespaço para a OTAN e seus aliados.
- Desenvolvimento de capacidades de Ciberdefesa robustas e centralização da proteção das redes da OTAN.

156 Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, «Lisbon Summit Declaration», *Press Release*, vol. 155, 2010.

157 NATO Public Diplomacy Division, «Defending the networks - The NATO Policy on Cyber Defence». 2011.

- Desenvolvimento de requisitos mínimos para a defesa das redes das infraestruturas de rede das nações consideradas críticas para a OTAN.
- Dar apoio aos aliados para alcançar um nível mínimo em matéria de Ciberdefesa e reduzir as vulnerabilidades das infraestruturas críticas das nações.
- Cooperação com os parceiros, organizações internacionais, setor privado e universidades.

A Política de Ciberdefesa da OTAN deve ser implementada tanto pelas autoridades pertinentes da OTAN como pelas nações aliadas. Após a sua revisão no ano de 2011, o NAC (*North Atlantic Council*) foi designado como a entidade responsável pela vigilância de alto nível relativa à implementação da política de ciberdefesa, além de ser o organismo que deve ser prioritariamente informado sobre os ciberataques ocorridos, assumindo-se como a principal autoridade na tomada de decisões na gestão de crises relacionadas com a ciberdefesa. Deste modo, proporciona-se às nações aliadas o apoio que necessitam na gestão deste tipo de incidentes.

Por outro lado, ao Comité de Política e Planeamento de Defesa foi atribuída a responsabilidade de garantir a vigilância sobre os esforços realizados em Ciberdefesa das Nações Aliadas[158], assim como o aconselhamento ao nível de peritos.

O *NATO Cyberdefence Management Board* (Comité de Gestão da Ciberdefesa OTAN) é a autoridade delegada para levar a cabo as ações necessárias para coordenar a Ciberdefesa, quando se detetar a ocorrência de ciberataques contra a OTAN ou contra as nações. Além disso, este órgão é o principal responsável pelo estabelecimento da Política de Ciberdefesa. Organicamente, atua no âmbito da Divisão de Novas Ameaças à Segurança (ESCD – *Emerging Security Challenges Division*), cuja atividade incide sobre o tratamento dos riscos emergentes e dos novos desafios, abrangendo diferentes dimensões, incluindo elas a Ciberdefesa[159].

Outra iniciativa importante que a OTAN tem levado a cabo é a de desenvolver a capacidade para, face a ciberataques, dar apoio aos países da OTAN. Esta capacidade é proporcionada pelo *NCIRC Technical Centre*, dependente da Agência NCSA (*NATO Communication and Information Services Agency*) que, para esse efeito, deve estar treinado, equipado e organizado de forma adequada para poder realizar este objetivo. Mantém também relações com diferentes CERT para partilhar informação relativa aos incidentes de segurança e para poder tirar proveito da mesma na sua gestão.

Deste organismo também dependem as Equipes de Reação Rápida (RTT – *Rapid Reaction Teams*), levantadas com base numa iniciativa cujo conceito foi definido em 2011, estabelecendo que: "Estes peritos em ciberdefesa são responsáveis por dar apoio aos Estados membros que solicitem ajuda para fazer face a um ataque que afete a nação."

158 NATO, «NATO and cyber defence», 02-ago2012. [Online]. Available: http://www.nato.int/cps/en/natolive/topics_78170.htm. [Accessed: 24-ago2012].

159 Néstor Ganuza, Alberto Hernández, y Daniel Benavente, «NECCS-1: An Introductory Study to Cyber Security in NEC». NATO CCD COE Publications, jun-2011.

esperava-se que estivessem operacionais no final de 2012 e que fossem capazes de garantir esse apoio face a ciberataques[160] já em 2013.

Depois de em 2011 rever a Política de Ciberdefesa, a OTAN, decidiu potenciar o treino e a formação em matéria de Ciberdefesa através do *NATO Cooperative Cyber Defence Centre of Excelence* (NATO CCD COE)[161], onde se prevê que diferentes nações da OTAN congreguem os seus esforços neste domínio. A principal missão do CCDCOE centra-se no reforço da capacidade cooperativa de ciberdefesa, partilhando informação entre OTAN, as suas nações e outras organizações nesta matéria, mediante o desenvolvimento de doutrina e conceitos, educação, Investigação e Desenvolvimento (I&D), análise e consultoria. Neste centro, realizam-se múltiplas atividades ligadas à investigação e treino, tratando áreas relacionadas com o Direito e Política, Conceitos e Estratégia, Ambiente Tático e Proteção da Informação em Infraestruturas Críticas.

Outro dos pontos-chave da revisão da Política de Ciberdefesa da OTAN Cibernética é a promoção da cooperação com outras organizações em matéria de ciberdefesa. Potenciando a complementaridade e evitando a duplicação, essas relações devem concentrar-se na consecução de objetivos comuns e em valores partilhados. Neste contexto, também se chama a atenção para a importância das relações com o setor privado e academia.

Além disso, cabe ainda aqui mencionar, no âmbito da OTAN, o programa de Defesa Contra o Terrorismo, desenvolvido com o objetivo de lutar contra o terrorismo de forma eficiente, contando com a tecnologia mais adequada para proteger os alvos civis e militares.

Face às iniciativas e aos passos entretanto dados pela OTAN neste domínio, constata-se que o NCIRC constitui um elemento-chave da Política de Ciberdefesa Aliada, tal como indica a Declaração dos Chefes de Estado e de Governo, proferida após a Cimeira de Lisboa, de 2010, em que estes se comprometem a acelerar o desenvolvimento e a implementação do NCIRC, até alcançar a sua plena capacidade operacional em 2012[162]. Analisemos pois com um pouco mais detalhe o enquadramento operacional do NCIRC.

O NCIRC foi projetado de forma a ser capaz de disponibilizar uma série de serviços de apoio técnico e jurídico, de resposta a incidentes de segurança informática no âmbito da OTAN, implantando, de forma centralizada, os três grupos de medidas seguintes[163]:

Meios preventivos: que incluem, entre outros, a publicação de boletins de segurança, a distribuição de atualizações de *software* e a disponibilização de equipamentos de análise de vulnerabilidades.

Medidas reativas: que incluem o apoio e a resposta a incidentes ou tentativas de intrusão.

Assessoria jurídica: que incluem a análise forense, a investigação e a atualização normativa.

---

160 NATO - News, «NATO Rapid Reaction Team to fight cyber attack.», 13-mar2012.

161 Consultar http://www.ccdcoe.org/.

162 Lord Jopling, «Information and National Security», NATO Parliamentary Assembly, Bucharest, Committee Report 171 CDS 11 E, 2011.

163 Suleyman Anil, «NCIRC (NATO Computer Incident Response Capability)», in *11th TF-CSIRT Meeting*, Madrid, 2004.

Para esse efeito, a conceção do NCIRC deve garantir os seguintes requisitos:

- Capacidade para coordenar a resposta global da OTAN durante um incidente.
- Fornecer uma base de conhecimento centralizada no apoio aos administradores de sistemas locais.
- Centralizar os serviços *online* e no local.
- Centralizar os acordos de apoio forense e de assessoria jurídica.
- Otimização de recursos.

Servir como ponto de contato da OTAN com outros CERT externos.

Para isso, o NCIRC está estruturado em três camadas ou níveis:

1. *NCIRC CC* (*NATO Computer Incident Response Capability – Coordination Centre*)[164]: Composto pelo NOS (*NATO Office of Security*) e pelo C3 *Staff (Consultation, Command and Control*), assume-se como o nível de coordenação do NCIRC e constitui o ponto central de contato tanto para outros organismos internos da OTAN, como para os parceiros externos, como outros CERT, etc.
2. *NCIRC TC* (*NATO Computer Incident Response Capability – Technical Centre*)[165]: Constituído pelo SOC (*Security Operation Centre*)[166], materializa o nível técnico operacional do NCIRC.
3. Administradores de sistemas e de rede de toda a OTAN, que no seu conjunto, formam o Nível 3 da NCIRC

Finalmente, o catálogo de Serviços da NCIRC inclui os seguintes serviços:

- Gestão de incidentes.
- Informação de vulnerabilidades e ameaças.
- Análise de vulnerabilidades (*online*/no local).
- Serviços de consultoria (tecnológica e forense).
- A recolha de dados e monitorização de informação proveniente de várias fontes: IDS (*Intrusion Detection System*), antivírus, *firewalls*, etc.
- Suporte *online* de atualizações automáticas, *downloads* de *software* e/ou procedimentos operacionais padronizados.
- Análise de incidentes e testes de segurança.

A Ciberdefesa da OTAN é consensualmente reconhecida como área de potencial cooperação civil-militar, sendo por essa razão uma área prioritária para o desenvolvimento de capacidades militares cooperativas sob o conceito de defesa inteligente (*smart defence*).

No processo de levantamento da sua capacidade de ciberdefesa, a OTAN tem também vindo a acompanhar e a prestar especial atenção às múltiplas iniciativas e declarações que têm vindo a ter lugar nesta área nos principais *fora* internacionais, nomeadamente,

164 O Centro de Coordenação Técnico do NCIRC é o primeiro nível da organização.

165 O Centro Técnico do NCIRC constitui o segundo nível. Consultar http://www.ncirc.nato.int/index.htm.

166 O Centro de Operações de Segurança geralmente refere-se à localização física a partir da qual se gere a segurança numa organização e, por extensão, a sua designação também inclui as pessoas e os sistemas de TIC que nele estão incluídos. Muitas vezes não fazem parte de nenhuma CERT, embora possam existir SOC limitados que não constituam uma capacidade CIRC propriamente dita. Também pode ser referenciado pela sua sigla em português/espanhol: COS.

no âmbito da União Europeia, das Nações Unidas, UIT, OCDE e do próprio G8[167]. Por essa razão, procuraremos seguidamente sintetizar as principais iniciativas e contribuições destas organizações internacionais no domínio da cibersegurança e da ciberdefesa.

2. União Europeia

Ao nível da UE, a *Agenda Digital para a Europa (2010-2020)*[168] traçou o objetivo ambicioso de assegurar um "crescimento inteligente" (*smart growth*), estabelecendo como prioridade a exploração das tecnologias digitais de forma a garantir o desenvolvimento económico e benefícios sociais sustentáveis. Salvaguarda-se assim os interesses dos cidadãos e das empresas no contexto da revolução digital, incluindo neste esforço concertado vetores estratégicos estruturantes como o *e-government*, a inclusão social, o *e-health* e a inovação.

O relatório para a implementação da Estratégia de Segurança Europeia, de 2008[169], incluía já as ameaças à cibersegurança entre as principais ameaças e desafios aos interesses e à segurança da UE. Desde então, as iniciativas da UE no âmbito da cibersegurança têm-se vindo a focar essencialmente na harmonização da legislação de combate ao cibercrime e na introdução de instrumentos orientados para o desenvolvimento de políticas de proteção das infraestruturas críticas de informação. A "Agenda Digital", o "Programa de Estocolmo"[170] e a "Estratégia de Segurança Europeia", reafirmam a preocupação da UE com este assunto, sublinhando o facto de, nas áreas da cibersegurança e da luta contra o cibercrime, "a segurança interna e externa dos Estados se encontrar interligada de forma indissociável"[171].

A União Europeia considera o ciberespaço como uma "área de justiça" onde os direitos humanos (incluindo o acesso às novas tecnologias), a liberdade de expressão, o direito à privacidade e a proteção dos dados pessoais devem ser preservados e onde os criminosos, através de um esforço cooperativo de todos os Estados membros, são identificados e processados. Todos os atores, sejam eles indivíduos, Estados ou organizações, deverão ser responsabilizados pelos seus atos e comportamentos no ciberespaço.

---

167 Declaração "Compromisso Renovado para a Liberdade e Democracia", proferida pelo G8 na Cimeira de Deauville, realizada em 26 e 27 de maio de 2011. Disponível em http://www.nepad.org/system/files/deauville_ declaration_final_.pdf.

168 *Digital Agenda for Europe 2010-2020*. Disponível em http://ec.europa.eu/digital-agenda/.

169 Relatório sobre a implementação da Estratégia de Segurança Europeia, *Providing Security in a Changing World*, Bruxelas, 11 de dezembro de 2008, Ref.ª doc. n.º S407/08.

170 *The Stockholm Programme: An Open And Secure Europe Serving And Protecting Citizens*, Bruxelas, 4 de maio de 2010, Refª doc. n.º 2010/C 115/01. Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF.

171 Discurso de Neelie Kroes, Vice-Presidente da Comissão Europeia e responsável pela Agenda Digital, proferido na Reunião de Alto Nível da OCDE sobre a Economia da internet, realizada em Paris, a 28 de junho de 2011. Disponível em http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/479/ &format=HTML&aged=O&language=EN&guiLanguage=en.

No que diz respeito ao combate ao cibercrime, a UE utiliza, como base e referência legal, a Convenção Europeia do Cibercrime, acordada pelos diversos Estados membros a 26 de novembro de 2001 em Budapeste[172]. Neste contexto, as regras da territorialidade e da soberania também se aplicam, devendo todos os Estados membros dispor de legislação e órgãos nacionais próprios, de forma a reforçar a sua cibersegurança e o combate ao cibercrime.

Para reforçar o combate ao cibercrime, o Conselho da União Europeia aprovou entretanto a criação do *European Cybercrime Centre* (EC3)[173] que, a partir do início de 2013, passou a operar na sede da Europol em Haia. Este novo Centro, constitui assim o principal instrumento operacional da UE na luta contra o cibercrime, contribuindo para uma resposta cooperativa mais rápida e eficaz face à ocorrência de ciberataques. Entre outras áreas de intervenção, o EC3 prestará assistência às instituições europeias e aos Estados membros no levantamento de uma capacidade operacional e analítica para apoio à investigação criminal e à cooperação internacional, nomeadamente, quando esta envolva parceiros internacionais.

A *European Network and Information Security Agency* (ENISA), constituindo a agência especializada em assuntos relacionados com a segurança da informação nas redes da UE, tem vindo a assumir-se como um centro de competências técnicas na área da cibersegurança e a desempenhar também um importante papel na coordenação de uma resposta cooperativa dos diversos Estados membros. Neste contexto, dois relatórios[174] publicados recentemente pela ENISA, apontam as grandes discrepâncias registadas nas capacidades operacionais dos *Computer Emergency Response Teams* (CERT) nacionais/governamentais, como o maior obstáculo para a cooperação entre os diferentes Estados membros da UE e um potencial risco para a cibersegurança europeia.

Segundo as conclusões destes relatórios da ENISA, a necessidade de levantamento de uma rede operacional e funcional de CERT nacionais ou governamentais na Europa – até final de 2012 – foi estabelecido em vários documentos oficiais da UE, mas em muitos países as equipas existentes não apresentam "um nível adequado de maturidade". Cerca de metade dos países da UE são apontados como já tendo desenvolvido e estruturado estratégias nacionais de cibersegurança e mais de 80% como empregando entre seis e oito funcionários a tempo inteiro[175]. Uma vez que os constrangimentos

172 Documento disponível em http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ ConventionOtherLg_en.asp. Tradução em português disponível em http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf.

173 Pode-se consultar informação mais detalhada sobre a missão e estrutura do Centro Europeu de Combate ao Cibercrime em https://www.europol.europa.eu/ec3.

174 A ENISA, assumindo o papel de agência de cibersegurança europeia, lançou em 17 de dezembro de 2012 dois novos relatórios: (1) *The Status Report 2012 for CERTs*, que fornece um ponto de situação atual dos CERT nacionais/governamentais da UE, concluindo que o desafio-chave é a diversidade e heterogeneidade registada nas capacidades existentes nos diversos Estados membros; (2) *Updated Recommendations for n/g CERT*, é um relatório que acompanha o primeiro, onde se analisam as restantes lacunas e limitações existentes. Estes relatórios encontram-se disponíveis em http://enisa.europa.eu.

175 Este é, segundo a ENISA, o nível mínimo de recursos humanos necessário. No entanto, em muitos casos,

económicos são comuns a muitos Estados membros, a ENISA aconselha também os CERT a "procurar ativamente fontes alternativas de financiamento", tais como projetos financiados pela UE e projetos de natureza comercial, capazes de envolver a indústria e a sociedade civil.

Relativamente às estruturas e modelos organizacionais existentes, a ENISA refere que no Reino Unido, Holanda, França e Irlanda, os CERT fazem parte dos centros de cibersegurança nacional e que, por essa razão, têm alguma responsabilidade atribuída no âmbito da estratégia de cibersegurança nacional. Na Finlândia, Bulgária e Roménia, os CERT possuem uma certa autonomia mas são supervisionados pelas autoridades reguladoras nacionais de telecomunicações. O GovCERT dinamarquês é gerido pelo Ministério da Defesa, e na Noruega o NorCERT é uma parte da agência norueguesa de segurança nacional, enquanto a Itália e o Chipre não têm um CERT oficial nacional ou governamental a operar com esse estatuto oficial.

Em Portugal, conforme já antes referido, as funções de CERT têm vindo a ser geridas pela Fundação para a Computação Científica Nacional (FCCN), garantindo esta instituição a resposta a incidentes de segurança informática no contexto da comunidade de utilizadores da "Rede de Ciência Tecnologia e Sociedade" (RCTS). De forma supletiva, a FCCN, recentemente integrada na Fundação para a Ciência e Tecnologia (FCT), tem vindo a prestar o serviço de coordenação da resposta a incidentes da rede nacional de CSIRT, com os quais foram celebrados acordos específicos para esse efeito.

No domínio militar, a UE definiu como objetivo o desenvolvimento de uma capacidade autónoma para conduzir operações militares no contexto de uma Política Comum de Segurança e Defesa (*Common Security and Defence Policy* - CSDP) definida com base no Tratado da União Europeia, na Estratégia de Segurança Europeia (*European Security Strategy* - ESS)[176] e no *Headline Goal* (HLG) 2010[177].

Reconhecendo que o exercício do comando e controlo e o emprego das forças militares se encontra cada vez mais dependente de redes de computadores para explorar os benefícios de uma capacidade militar centrada em rede (*Network Enabled Capability* - NEC), a UE definiu em setembro de 2009 um conceito para a condução de Operações em Redes de Computadores (*Computer Network Operations* – CNO)[178].

Em 2011, a atualização do Plano de Desenvolvimento de Capacidades da UE (*Capability Development Plan* - CDP) veio salientar o facto de ser necessário desenvolver uma capacidade efetiva de defesa no ciberespaço. Acompanhando esta evolução doutrinária e as iniciativas entretanto desenvolvidas pela OTAN, o Comité Militar da UE definiu

verifica-se que os recursos têm que ocupar-se de diversas áreas o que constitui uma barreira à sua especialização. Muitos dos CERT nacionais ou governamentais relatam dificuldades na contratação de especialistas em "análise forense digital" e em *reverse engineering*.

176 *European Security Strategy (ESS)*, doc. 15849/03, datado de 5 de dezembro de 2003.

177 *Head Line Goal (HLG) 2010*, doc. 9313/04, datado de 12 de maio de 2004.

178 *EU Concept for Computer Network Operations in EU-led Military Operations (CNO)*, doc. 13537/09, datado de 22 de setembro de 2009.

também o conceito de Ciberdefesa[179], que acabaria por se sobrepor ao conceito de CNO anterior, tendo em conta um contexto mais alargado, definido pelo ciberespaço[180]. O ciberespaço surge assim como o 5.º domínio operacional para a condução de operações militares.

Tendo em vista o desenvolvimento de capacidades militares neste domínio, a Agência Europeia de Defesa (*European Defence Agency* – EDA), responsável pelo CDP, criou em 2011 um Grupo de Projeto na área da Ciberdefesa[181]. Neste âmbito, está a ser concluído um estudo[182] destinado a avaliar a situação atual dos projetos em curso e das capacidades de Ciberdefesa dos vários Estados membros. Foi entretanto também lançado um novo estudo[183] que, partindo dos resultados do anterior, procura definir os requisitos para o levantamento de capacidades militares de Ciberdefesa.

Tendo em vista o desenvolvimento de capacidades militares, agregando diversas iniciativas emergentes dos Estados membros sobre a forma de uma cooperação multilateral sinérgica, a UE definiu o conceito de "agregar e partilhar" (*pooling & sharing*), evitando desta forma duplicações desnecessárias e salvaguardando os interesses da UE. Neste contexto, o Comité Diretivo das Capacidades (*Capabilities Steering Board*) da UE, na sua reunião de 11 de outubro de 2012, manifestou um forte apoio às linhas de orientação estratégica propostas pela EDA.

Na área da Ciberdefesa, as oportunidades de *pooling & sharing* levantadas foram as que se indicam:

- Doutrina e organização: partilha das melhores práticas; partilha de informação relativa às estratégias de ciberdefesa, conceitos, estudos, etc.;
- Interoperabilidade: exploração de sinergias civis/militares e de oportunidades de cooperação com a comunidade civil de cibersegurança;
- Instalações: desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa;
- Liderança e pessoal: campanhas coordenadas de sensibilização na área da ciberdefesa;
- Material e tecnologia: partilha de resultados e esforços de I&D conjuntos em áreas como a análise e estudo de ameaças persistentes e avançadas (*Advanced Persistent Threats*-APT); *pool* de capacidades de ciberdefesa para Quartéis-Generais de nível Operacional e Tático (OHQ/FHQ)
- Treino e exercícios: *pooling* de recursos de treino/educação existentes; partilha de

179 *EU Concept for Cyber Defence for EU-led Military Operations*, doc. EEAS 01729/12, datado de 8 de outobro de 2012.

180 Neste âmbito, constata-se que o termo Ciberdefesa tem vindo a ser utilizado no processo de desenvolvimento de capacidades militares da UE ao passo que o termo Cibersegurança tem vindo a ser utilizado no contexto mais alargado da Estratégia de Segurança Europeia (ESS).

181 Na estrutura da EDA, a Ciberdefesa constitui uma dimensão da área de Gestão do Conhecimento.

182 Estudo 11.CAP.OP.111 da EDA, *Stocktaking study on existing cyber defence capabilities and projects on capabilities in the EU (MilCyberCAP)*.

183 Estudo 12.CAP.OP.332 da EDA, *Framework project on developing Cyber Defence Capabilities for the Military (frameCyberCAP)*.

informação sobre ameaças e incidentes em contexto operacional de missões de ciberdefesa em apoio de missões no âmbito da política de segurança e defesa da UE (missões CSDP).

Em linha com esta orientação, o Comité Diretivo (*Steering Board*) de Ministros da Defesa da UE, de 19 de novembro de 2012, tomou também uma decisão importante para a consolidação da visão estratégica proposta pela EDA, ao reconhecer que a Ciberdefesa constitui uma área prioritária de *pooling & sharing*, onde, devido à sua forte dimensão de duplo-uso, existem grandes condicionamentos políticos capazes de influenciar a Segurança e Defesa da UE.

Também por essa razão, na área das relações exteriores, o interesse pela cibersegurança parece evidente, multiplicando-se os contactos políticos com países com importantes capacidades neste domínio, como sejam os Estados Unidos da América[184], a Índia[185] e a China[186], com os quais a UE estabeleceu estruturas e mecanismos de cooperação especializada.

Tendo sido objeto de uma primeira discussão ao nível dos Diretores da Política de Segurança da UE, em junho de 2012, foi aprovada a 7 de fevereiro de 2013 uma Estratégia Europeia de Cibersegurança[187]. Em termos gerais, constata-se que a cibersegurança constitui uma preocupação para a UE, tanto ao nível estratégico como ao nível técnico, estando em curso diversas iniciativas destinadas a estimular a coordenação de esforços cooperativos e o desenvolvimento de sinergias entre os diversos Estados membros.

No que diz respeito à ciberdefesa, como área privilegiada de cooperação civil-militar, será de esperar que esta venha a ser cada vez mais considerada como área prioritária de desenvolvimento de capacidades militares cooperativas pela UE, adotando os diversos Estados membros para esse efeito os princípios subjacentes ao conceito de *polling and sharing*.

3. Outras Organizações Internacionais

O rápido desenvolvimento das Tecnologias de Informação e Comunicação e o seu impacto social e económico crescente, tornam a evolução do ciberespaço imprevisível.

184 Com os EUA, na sequência da Cimeira UE-EUA de 2010, foi constituído um grupo de trabalho conjunto na área da Cibersegurança e Cibercrime (*Joint Working Group on Cyber Security and Cyber Crime*). A cooperação decorre ao nível da gestão de ciberincidentes, das parcerias público-privadas, das ações de sensibilização e do combate ao cibercrime. Desde novembro de 2011, é conduzido anualmente um exercício de gestão de crises de cibersegurança conjunto EU-USA (*Cyber Atlantic*).

185 Com a Índia, na sequência da Cimeira UE-Índia de 10 de fevereiro de 2012 e em resultado do diálogo político na área das TIC, foi também constituído um grupo de trabalho na área da Cibersegurança (EU--India Cyber Security Working Group). A cooperação decorre ao nível da gestão do risco, de quebras de segurança e do combate a *bootnets*.

186 A Cimeira que teve lugar entre a UE e a China em fevereiro de 2012, também conduziu ao levantamento de uma iniciativa conjunta a EU-China Cyber Task-Force.

187 Disponível em http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

Os instrumentos clássicos de interação e cooperação entre Estados, destinados a reduzir os riscos emergentes no ciberespaço, são difíceis de implementar. Desta forma, para além da OTAN e da UE, têm vindo a surgir iniciativas tanto ao nível nacional como internacional, consubstanciando propostas de enquadramento que definem normas e princípios orientadores tanto do funcionamento sustentável da internet (fiável e seguro) como de um comportamento aceitável no ciberespaço.

3.1. Nações Unidas e a União Internacional de Telecomunicações

A Organização das Nações Unidas (ONU), reconhecendo o papel determinante das Tecnologias de Informação e Comunicação no desenvolvimento socioeconómico da humanidade, tem vindo, ao longo da última década, a dedicar especial atenção às questões relacionadas com a cibersegurança e a ciberdefesa. Como reflexo desta preocupação, com base na necessidade de garantir a disponibilidade e estimular a confiança na utilização das TIC, a Assembleia-Geral da ONU aprovou cinco resoluções especialmente orientadas para a melhoria da cibersegurança da comunidade internacional.

Neste contexto, foram aprovadas resoluções dirigidas respetivamente para a área do combate à utilização criminosa das TIC, A/RES/55/63[188] e A/RES/56/121[189], para a criação de uma cultura de cibersegurança global, A/RES/57/239[190] e A/RES/64/211[191], e para a proteção de infraestruturas críticas de informação a A/RES/58/199[192].

---

188 Aprovada em 4 de dezembro de 2000, esta resolução tem como principal objetivo promover o combate por parte da comunidade internacional à utilização criminosa das TIC. Inspirada na *Declaração do Milénio* das Nações Unidas, disponível em http://www.un.org/millennium/declaration/ares552e.htm, esta reconhece que o livre fluxo de informação pode promover o desenvolvimento económico e social, a educação e a governação democrática. Alerta, por essa razão, para o facto de a crescente utilização criminosa das TIC poder ter um grave impacto em todos os Estados, impedindo assim que os benefícios decorrentes da utilização das novas tecnologias sejam disponibilizados a todos.

189 Esta resolução, aprovada em 19 de dezembro de 2001, cobre muitos dos aspetos já enunciados pela Resolução A/RES/55/63. No entanto, vai um pouco mais longe ao solicitar aos Estados o estabelecimento de medidas de coordenação e cooperação no combate efetivo à utilização criminosa das TIC. Chama a atenção para a necessidade dos diversos países desenvolverem legislação específica, políticas e práticas nacionais de combate ao crime informático.

190 A Resolução A/RES/57/239 tem por foco a criação de uma cultura global de cibersegurança. Aprovada em 20 de dezembro de 2002, afirma a crescente dependência dos governos, empresas, organizações e utilizadores individuais relativamente às TIC, ao mesmo tempo que salienta que os requisitos de cibersegurança devem ser cada vez maiores à medida que os Estados aumentam a sua participação na Sociedade de Informação. Esta resolução torna também claro que os governos e as forças de segurança não serão capazes de lidar sozinhas com os desafios da cibersegurança, necessitando para esse efeito do apoio de todos os utilizadores.

191 Datada de 23 de dezembro de 2003, esta resolução lida com a promoção e criação de uma cultura global de cibersegurança e com a proteção de infraestruturas de informação críticas. Constata a dependência crescente relativamente às tecnologias de informação dos serviços críticos das modernas sociedades como a área energética, transmissão e distribuição, transporte aéreo e marítimo, banca e serviços financeiros, distribuição de alimentos e saúde pública. Assim, esta resolução convida os Estados membros da ONU a desenvolverem estratégias orientadas para a redução dos riscos das infraestruturas críticas de informação, de acordo com a regulamentação e as leis nacionais.

192 Esta resolução cobre as mesmas áreas das quatro resoluções anteriores, mas integra os resultados obtidos das duas fases da Cimeira Mundial designada por *World Summit on the Information Society* (WSIS). A Resolução

A União Internacional das Telecomunicações (UIT), enquanto agência especializada neste domínio, recebeu um mandato da ONU para esta área em 1949, sendo atualmente o principal órgão de coordenação mundial para os governos e setor privado no desenvolvimento de redes, serviços e mecanismos de combate às suas ameaças e vulnerabilidades.

Desde a sua fundação em 1865, a UIT tem vindo a desenvolver um papel importante na área das telecomunicações globais, na segurança da informação e na definição de normas nos diferentes domínios das TIC. Desta forma, a UIT é responsável pela implementação das Resoluções da ONU, de forma a contribuir para a disseminação dos benefícios das novas tecnologias por todas as nações do mundo. Por esta razão, consideramos importante abordar também neste trabalho o mandato da UIT no domínio da cibersegurança e nas áreas com esta relacionadas.

Na área da cibersegurança merece particular destaque, entre outras, a iniciativa *ITU Global Cybersecurity Agenda* (GCA) e o Guia para Elaboração de uma Estratégia de Cibersegurança. A GCA foi lançada em 2007 pelo Secretário-geral da UIT, Hamadoun Touré, como uma *framework* para a cooperação internacional com a finalidade de melhorar a confiança e a segurança na sociedade de informação, encorajando a colaboração com e entre os principais parceiros mundiais e a construção de iniciativas estruturadas sobre as existentes, de forma a evitar a duplicação de esforços.

Uma das questões que assumiu recentemente um maior relevo no seio da UIT, por força da Conferência Mundial das Telecomunicações Internacionais (*World Conference on International Telecommunications - WCIT*), que decorreu no Dubai em dezembro de 2012, foi a alteração do Tratado Internacional de Telecomunicações, que se encontrava em vigor desde 1988. As grandes questões suscitadas nesta conferência, foram as seguintes: "Poderá a Organização das Nações Unidas passar a exercer a regulação global da internet?" e "O princípio da 'internet livre' deverá continuar a fazer parte da filosofia de regulamentação?". No fundo, a estas questões está subjacente a necessidade, sentida pela comunidade internacional, de reformulação do sistema de governação da internet.

Durante os 12 dias de reuniões da WCIT, os representantes dos 193 países presentes, esgrimiram argumentos sobre a melhor forma de equacionar estas questões. As posições defendidas pelos diversos países e empresas revelaram-se por vezes antagónicas. A título de exemplo, verificou-se que, ao longo das discussões, os Estados ditos "ocidentais", a União Europeia e, sobretudo, os EUA não aceitam perder poder. Grandes empresas como a Google, defendem a manutenção do cenário atual. Os países árabes, a Rússia e a China defendem um controlo mais apertado da internet.

Relativamente ao texto final, resultante deste encontro mundial, permanecem os receios manifestados por alguns países europeus de que a nova redação do tratado possa legitimar tentativas de controlo da internet por parte de alguns Estados. De facto, 89

A/RES/64/211 constitui-se assim, como um elemento importante na coordenação internacional dos esforços a desenvolver no domínio da cibersegurança, refletindo o facto de a WSIS ter indicado a UIT como única organização moderadora da Linha de Ação C5, orientada para "gerar confiança e confiabilidade na utilização das TIC".

dos 193 países vinculados à UIT não aprovaram o documento que, de acordo com o calendário estabelecido, vai entrar em vigor a partir de janeiro de 2015.

Portugal e Espanha, como muitos outros países da UE, estão entre os países que não subscreveram o novo Tratado Internacional das Telecomunicações, admitindo-se que os dois, após reflexão interna, o venham a fazer mais tarde.

3.2. Organização para a Cooperação e o Desenvolvimento Económico (OCDE)

Enquanto organização motivada pelo progresso e desenvolvimento económico global, a Organização para a Cooperação e Desenvolvimento Económico (OCDE) tem vindo, desde meados dos anos 1970, a acompanhar a evolução e a analisar o impacto das TIC na economia e na sociedade mundial. Em 1980, a OCDE aprovou as diretivas de salvaguarda da privacidade, o primeiro instrumento político internacional orientado para a definição de uma política focalizada na salvaguarda da segurança e da confiança na utilização das TIC. Desde o início de 1990, a OCDE tem acumulado uma vasta experiência no debate e discussão dos diferentes aspetos ligados tanto à segurança de sistemas de informação e redes como de outras áreas afins, incluindo a autenticação eletrónica, a política de criptografia e a proteção de infraestruturas de informação críticas. Até agora, a abordagem da OCDE para a "segurança no mundo digital" tem sido orientada para o desenvolvimento de *frameworks* de referência para o desenvolvimento de políticas de segurança que permitam que as TIC e a economia da internet adquira um maior dinamismo e facilite o crescimento económico, promovendo assim a inovação e o bem-estar social.

Os principais contributos da OCDE para a área da cibersegurança, refletidos na publicação das diretivas sobre segurança das TIC em 2002, parecem ser a sua capacidade para desenvolver recomendações com base em princípios de alto nível, assentes em políticas flexíveis, capazes de gerar consensos e pontos de convergência, envolvendo neste processo todas as partes interessadas.

As tendências, expressas em documentos mais recentes da OCDE, sugerem pelo menos duas áreas adicionais de estudo. A primeira, está relacionada com o desenvolvimento de políticas de fomento dirigidas ao setor da indústria de cibersegurança, que irá conduzir ao crescimento do emprego qualificado e sustentar a confiança na economia da internet – no sentido de uma "política de cibersegurança industrial". A segunda área emergente é o desenvolvimento de indicadores de cibersegurança mais robustos e internacionalmente comparáveis, para melhorar o processo de tomada de decisão e a coordenação operacional desta área, apoiando assim o desenvolvimento da cibersegurança como um setor económico mais robusto e sustentável.

Neste âmbito, considera-se que o Grupo de Trabalho sobre Segurança da Informação e Privacidade (*Working Party on Information Security and Privacy - WPISP*) merece especial relevo por desenvolver recomendações para a adoção de políticas e definir orientações para manter a confiança da sociedade na economia da internet. Os trabalhos do WPISP, baseiam-se numa análise profunda de áreas como políticas nacionais de cibersegurança, indicadores para a cibersegurança e privacidade, proteção de infraestruturas críticas de informação (CIIP), gestão da identidade digital, *malware*,

Radio-Frequency Identification (RFID), proteção da privacidade e das crianças *online*. O WPISP integra delegados de 34 países membros da OCDE, observadores de outras organizações internacionais, bem como representantes de empresas, sociedade civil e da comunidade técnica da internet.

Enquanto a maior parte das estratégias nacionais tem como objetivo abordar a cibersegurança segundo uma perspetiva ligada à Segurança e Defesa dos Estados, a orientação da OCDE tem sido essencialmente a de concertar iniciativas destinadas a aumentar o nível global de cibersegurança uma vez que só assim será possível aumentar as vantagens competitivas dos Estados na nova economia. Atendendo a esta ideia-força, são já muitos os países que, na articulação das suas estratégias nacionais de cibersegurança, definem como objetivo político fundamental, um reforço das competências e do setor da indústria nacional no domínio da cibersegurança.

A tradução desta evolução interna ao nível estratégico internacional, reflete-se em abordagens holísticas que procuram, de forma integrada, articular num todo mais coerente os aspetos económicos, sociais e até de soberania. No curto prazo, um cenário plausível é o de, a pedido dos seus membros, os *fora* e as organizações internacionais, passarem a construir mandatos cada vez mais específicos, refletindo as suas competências residentes. Esta tendência, permitirá reforçar a sua especialização (*expertise*), no sentido de evitar a duplicação de esforços e permitir maiores sinergias. Em parte, esta situação já se verifica no caso da UE e da OTAN.

3.3. Organizações de Normalização e Gestão da Internet

A internet, estruturada através da interligação de redes de computadores de diferentes países e continentes, tem construído e serve de suporte ao ciberespaço. Este tem vindo a funcionar como um verdadeiro catalisador do desenvolvimento global e a afirmar-se como um recurso essencial para as modernas sociedades, dele dependendo as infraestruturas tecnológicas e os serviços críticos que suportam a vida da maior parte da população mundial.

Pela sua importância para a normalização e gestão técnica da internet, existe um conjunto de organizações internacionais que, pela natureza da sua atividade, poderão vir a orientar o desenvolvimento e a marcar a sua futura utilização. Neste contexto, merecem especial referência a *Internet Corporation for Assigned Names and Numbers* (ICANN), a Internet *Engineering Task Force* (IETF), a *Internet Governance Forum* (IGF) e a *Internet Society* (ISOC).

Estas organizações, na sua maioria privadas e sem fins lucrativos, têm vindo a promover e desenvolver um espaço aberto de reflexão permanente. As suas normas e recomendações são normalmente acatadas pela comunidade de utilizadores da internet, constituindo na prática um importante instrumento de governação e desenvolvimento técnico.

As questões ligadas à cibersegurança e ciberdefesa têm vindo a merecer particular atenção, motivando em muitos casos a constituição de grupos de trabalho especializados.

4. Iniciativas Comuns para a Cooperação Internacional

Atendendo ao conjunto de iniciativas internacionais, já em curso ou a lançar num futuro próximo por organizações a que pertencem Portugal e Espanha, constata-se a existência de uma visão doutrinária cada vez mais convergente, capaz de vir a favorecer uma estratégia comum.

De forma sintética, a tabela 1 identifica as áreas estratégicas comuns de cooperação internacional no Ciberespaço, estruturando-as de acordo com os objetivos estratégicos a atingir e com os elementos associados ao desenvolvimento de capacidades cooperativas na área da cibersegurança e da ciberdefesa. Para cada uma das possíveis linhas de desenvolvimento destas áreas, no âmbito das principais organizações internacionais a que pertencem Portugal e Espanha (OTAN, UE, ONU/ITU e OCDE), procurou-se identificar também as iniciativas em curso e avaliar a sua relevância no domínio estratégico, operacional e económico/industrial.

A tabela apresentada permite assim identificar áreas comuns de cooperação internacional e de potencial convergência estratégica dos dois países, facto que poderá potenciar futuramente o desenvolvimento de sinergias e esforços cooperativos de natureza multilateral.

Tanto para Portugal como para Espanha, a Cibersegurança e a Ciberdefesa surgem como áreas de natural cooperação civil-militar e como áreas prioritárias de desenvolvimento de capacidades cooperativas, nomeadamente, segundo o conceito de *smart defence* no âmbito da OTAN e de *polling and sharing* no contexto da UE.

Tabela 1 – Áreas de Cooperação Internacional Comuns

Áreas Comuns de Cooperação Estratégica Internacional no Ciberespaço	Linhas de Desenvolvimento	OTAN	UE
Documentos Estratégicos de Referência		Conceito Estratégico (2010) Política de Ciberdefesa (2011)	Estratégia de Segurança Europeia (2008) Agenda Digital para a Europa (2010-20) Estratégia de Cibersegurança da UE (2013)
Defesa Coletiva	**Cibersegurança/ Ciberdefesa**	Ciberdefesa (área prioritária)	Cibersegurança e Ciberdefesa (áreas prioritárias)
	Combate ao Terrorismo	Combate ao Terrorismo (área prioritária)	Combate ao Cibercrime em geral (área prioritária)
	Proteção de Infraestruturas Críticas	Segurança Energética (área prioritária)	Proteção das Infraestruturas Críticas de Informação (área prioritária)
	Impacto das novas Tecnologias	Análise das Tecnologias Emergentes (área prioritária)	Desenvolvimento de recursos tecnológicos e industriais de cibersegurança (área prioritária)
Gestão de Crises	**Cooperação Civil-Militar**	Aproximação Civil-Militar (*Comprehensive Approach*)	Aproximação Civil-Militar (*Comprehensive Approach*)
	Compreensão do Ambiente Internacional	Monitorização/Análise do Ambiente Internacional	Estabelecimento de uma política internacional coerente do ciberespaço e promoção dos valores-chave da UE (área prioritária)
	Partilha de Informações *(Intelligence Sharing)*	Melhoria da partilha de Informações	Melhoria da partilha de Informações
Segurança Cooperativa	**Segurança e Defesa**	EU e Rússia	OTAN
	Cibersegurança/ Ciberdefesa	UE	OTAN, USA, China e Índia
Desenvolvimento de Capacidades Cooperativas Área da Cibersegurança/ Ciberdefesa		Iniciativas de *Smart Defence* POC:Information Assurance and Cyber Defence Capability Panel (CaP4 IACD)	Iniciativas de *Polling&Sharing* POC: ENISA e Project Team on Cyber Defence (PT CD), da EDA.
	Doutrina e Organização	➢Política, Plano de Ação e Conceito de Ciberdefesa OTAN, como referência. ➢Partilha de informação e melhores práticas.	➢Conceito de Computer Network Operations e Conceito de Ciberdefesa da UE, como referência. ➢Partilha de informação e melhores práticas;
	Interoperabilidade	➢Sinergias civis/militares e cooperação com a comunidade de cibersegurança civil. Ex: NATO Crypto Interoperability Strategy (cooperação OTAN-EU); NATO PKI; NOLCE File Encryption; NATO Common Criteria CaT.	➢Desenvolvimento, na área da cibersegurança, de uma rede europeia de CERTs (Ex:ENISA). ➢Na área da ciberdefesa, exploração de sinergias civis/militares e cooperação com a comunidade de cibersegurança civil.
	Instalações	➢Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa.	➢Desenvolvimento partilhado de novas áreas para treino e exercícios de ciberdefesa;
	Liderança e Pessoal	➢Campanhas coordenadas de sensibilização e formação na área da ciberdefesa.	➢Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;
	Material e Tecnologia	➢Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. Ex: Multi National Cyber Defence Capability Development (MNCD2); NATO Information Assurance Product Catalogue (NIAPC); ➢*Pool* de capacidades de ciberdefesa para apoio às operações OTAN.	➢Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum. ➢*Pool* de capacidades de ciberdefesa para Quartéis-Generais de nível Operacional e Tático (OHQ/FHQ)
	Treino e Exercícios	➢*Pooling* de recursos de treino/educação; ➢Partilha de informação sobre ameaças e incidentes em contexto operacional de ciberdefesa para apoio de missões OTAN (POC: NCIRC). ➢Exercício NATO Cyber Coalition.	➢*Pooling* de recursos de treino/educação; ➢Partilha de informação sobre ameaças e incidentes em contexto operacional de cibersegurança (POC ENISA) e ciberdefesa (POC EUMS) para apoio de missões de segurança e defesa da UE (missões CSDP). ➢Exercício Cyber Europe.

ONU	OCDE	Relevância Estratégica	Relevância Operacional	Relevância Económica	Área Nova?
Guia para Elaboração da Estratégia Nacional de Cibersegurança (2011) Tratado Internacional das Telecomunicações (2012)	Guidelines Seg SI e Redes (2002) Recomendação Coop Internacional na Lei Proteção Privacidade (2007)	Elevada **= E;** Média = **M**; –Baixa = **B**			**S**-Sim; **N**-Não
Cibersegurança/e-Governance (área prioritária)	Cibersegurança (área estruturante economia global)	**E**	**E**	**E**	**S**
Regulação do Ciberespaço (área prioritária)	Combate ao Cibercrime e Privacidade (área prioritária)	**E**	**E**	**B**	**N**
Contenção de ataques de larga escala (área prioritária)	Proteção SI e Redes (área prioritária)	**E**	**E**	**M**	**S**
e-Governance e normalização (área prioritária)	Monitorização impacto económico das TIC (área prioritária)	**E**	**E**	**E**	**N**
Cooperação política	Cooperação Político-Económica	**E**	**E**	**M**	**S**
Monitorização do ambiente internacional	Monitorização de Mercados e Economia Global	**E**	**E**	**M**	**N**
Troca de informação em *fora* especializados	Troca de informação em *fora* especializados	**E**	**E**	**M**	**N**
Cooperação Internacional	Cooperação Internacional e Desenvolvimento	**E**	**E**	**M**	**N**
Cooperação Internacional	Cooperação Internacional e Desenvolvimento	**E**	**E**	**M**	**S**
Tratados Internacionais POC: Global Cybersecurity Agenda (GCA), da ITU.	Recomendações e Guidelines POC: Working Party On Information Security And Privacy, da OCDE.	**E**	**E**	**E**	**S**
➢ Princípios de regulação e cooperação no ciberespaço. ➢ Partilha de informação e melhores práticas	➢ Recomendações e orientações. ➢ Partilha de informação e melhores práticas	**E**	**E**	**M**	**S**
➢ Adoção de políticas, princípios de normalização e requisitos técnicos	➢ Adoção de políticas, princípios de normalização e requisitos técnicos	**E**	**E**	**E**	**N**
➢ desenvolvimento de centros especializados para cooperação internacional	➢ desenvolvimento de centros especializados para cooperação internacional	**E**	**E**	**B**	**N**
Campanhas coordenadas de sensibilização e formação na área da Cibersegurança;	campanhas de sensibilização na área da cibersegurança;	**E**	**E**	**B**	**N**
Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	Partilha de resultados e esforços de I&D conjuntos em áreas de interesse comum.	**E**	**E**	**E**	**S**
➢ *Pooling* de recursos de treino/educação existentes;	Nada a referir.	**E**	**E**	**B**	**S**

Parte V – Conclusões e Reflexões

As TIC têm-nos conduzido à chamada Sociedade da Informação. Esse facto, tem dado lugar ao aparecimento de novos teatros de operações, como o espaço e o ciberespaço, onde terão lugar os conflitos do futuro.

No ciberespaço, um desses teatros, surgem formas modernas de interação e relacionamento, o que coloca novos desafios aos países que desejam acompanhar as dinâmicas próprias da revolução tecnológica e de um mundo em rede. A definição de uma visão estratégica e a criação de uma agenda digital coerente são ferramentas fundamentais que permitem aos Estados orientar as políticas e promover o desenvolvimento nacional, a fim de obter benefícios económicos e sociais.

A difusão generalizada de aplicações e serviços reais e virtuais baseados nas TIC, associada à proliferação do uso da internet, tem criado uma grande dependência do ciberespaço em todos os setores da sociedade. É hoje consensual que o regular funcionamento das sociedades modernas depende cada vez mais de um uso seguro e fiável do ciberespaço, pois, em virtude dessa dependência, surgem riscos que devem ser considerados e analisados e, se possível, mitigados.

No que diz respeito à Segurança e Defesa, as ameaças têm aumentado de forma alarmante, representando um sério risco para a Segurança Nacional. Dado o crescente número de ciberataques e a natureza cada vez mais disruptiva das ciberameaças, o princípio do "uso livre" da internet pode ficar comprometido, colocando em risco a sua segurança à escala global.

Desta forma, é evidente que a cibersegurança coloca importantes desafios de natureza operacional e estratégica, tanto à comunidade internacional como aos diferentes Estados. As ciberameaças eliminam barreiras geográficas e divisões tradicionais entre o que neste domínio se pode considerar individual e coletivo, publico e privado, nacional e estrangeiro. Perante essa nova realidade, considerando a necessidade de proteger e defender os interesses e a soberania nacional, os países mais desenvolvidos e também mais dependentes de novas tecnologias, têm centrado as suas abordagens na prevenção e resposta a ciberataques, inclusive contra aqueles que, pela sua capacidade disruptiva, podem afetar o funcionamento das infraestruturas críticas e os recursos de informação nacionais.

Ao nível da União Europeia, a maioria dos países tem desenvolvido estratégias nacionais de cibersegurança. Portugal e Espanha também têm vindo nos últimos anos a desenvolver iniciativas para o estabelecimento de capacidades autónomas e de cooperação tanto no domínio da cibersegurança como da ciberdefesa. De uma forma geral, é dada especial atenção à necessidade de explorar sinergias nacionais e de promover a sua articulação permanente com uma estratégia de cooperação internacional, no pressuposto de que é quase impossível lutar contra um problema global com soluções e iniciativas de foco limitado ou local.

No plano nacional, a definição dos objetivos a alcançar e as linhas estratégicas de ação que têm sido desenvolvidas por Portugal e Espanha têm muitos aspetos em comum.

Neste contexto, é possível identificar potenciais áreas de cooperação, considerando-se, por essa razão, importante estender a análise desenvolvida neste projeto de investigação, através do lançamento de um outro projeto – também conjunto, IDN e CESEDEN –, especialmente orientado para a definição de linhas de ação estratégicas conjuntas, capazes de contribuir para um plano de ação destinado a explorar sinergias e fortalecer a cibersegurança e a ciberdefesa de Portugal e Espanha.

Para Portugal e Espanha, assegurar a existência de um ciberespaço seguro e fiável constitui uma prioridade estratégica, em benefício da segurança e da defesa dos interesses nacionais. Para isso, em vez de se adotarem posturas reativas, devem ser promovidas ações proactivas, tendo em vista a garantia da segurança do ciberespaço e a defesa de interesses nacionais e conjuntos. A construção de um futuro digital requer a definição de uma estratégia de segurança nacional orientada para a informação e para o ciberespaço, coordenada com a dos nossos aliados e com as organizações a que pertencemos, capaz de aumentar o impacto das iniciativas (governamentais e privadas) e de afirmar-se como um desafio ao desenvolvimento de sinergias e à assunção de responsabilidades partilhadas por parte de todos os agentes interessados na adoção de uma visão conjunta: Estado, empresas, organizações e cidadãos.

Continuamente surgem novos objetivos, ataques e inimigos, o que obriga não apenas a compreender e enfrentar as ameaças de forma a reduzir as vulnerabilidades, mas também a tomar consciência dos riscos. Para isso devem orientar-se as estratégias de proteção para uma abordagem holística, que entenda a segurança no ciberespaço de forma abrangente (prevenção mais proteção) e que inclua uma adequada gestão dos riscos inerentes (físicos, lógicos e humanos) em todo o ciclo deste processo, desde a prevenção até à solução. Essas estratégias terão de basear-se em análises realistas de gestão do risco, considerando de forma conjunta as ameaças, as vulnerabilidades e o potencial impacto das primeiras sobre as segundas.

Da análise realizada neste estudo, ressalta a existência de uma série de capacidades e debilidades suscetíveis de serem exploradas ou reforçadas, respetivamente, no quadro da cooperação bilateral e multilateral entre os dois países. Nesse sentido, julga-se necessário considerar a possibilidade de analisar, elaborar e desenvolver a curto e médio prazo várias iniciativas, entre as quais se destacam as seguintes:

- Identificar a cibersegurança como um vetor estratégico, da maior importância, para a segurança nacional. Daí resulta a necessidade de aprovar um Plano Nacional de Segurança no Ciberespaço (Plano Nacional de Cibersegurança).
- Centralização da direção da cibersegurança nacional, face à diversificação das competências distribuídas entre os diferentes organismos, em cada um dos dois países, sem prejuízo das responsabilidades particulares.
- Realizar uma revisão ou adequação dos normativos e legislação vigente em ambos os países, fortalecendo-a sem comprometer a privacidade.
- Implementar e manter mecanismos de análise e gestão permanente do risco, incluindo as medidas de resposta aos riscos identificados, e fomentar a colaboração entre o setor público e o privado.

- Desenvolver projetos conjuntos de investigação e desenvolvimento na área de cibersegurança e da ciberdefesa, tanto a nível bilateral como de natureza multilateral. O facto de Portugal e Espanha pertencerem à OTAN e à UE reforça e fortalece a cooperação multilateral estratégica; neste âmbito, no contexto do desenvolvimento de capacidades cooperativas, assume especial interesse a articulação das iniciativas conjuntas quer no âmbito da "Defesa Inteligente" (*Smart Defense*, OTAN), quer no âmbito das iniciativas *Polling & Sharing* da UE.
- Desenvolver mecanismos de troca de informação em matéria de cibersegurança e de ciberdefesa.
- Criação de Equipas Técnicas de Assistência Mútua (Rapid Reaction Teams Ibéricas) em ambos os países, particularmente qualificadas para lidar com incidentes de segurança informática na área das infraestruturas críticas.
- A criação de um "Centro de Certificação de Tecnologias", com a incorporação de conhecimento, e a participação de técnicos dos dois países.
- Estabelecimento de acordos de cooperação e intercâmbio entre as Forças Armadas e de Segurança dos dois países, especialmente no âmbito da doutrina, educação e formação em ciberdefesa e cibersegurança.
- Levar a cabo periodicamente exercícios conjuntos, tanto na área de cibersegurança como da ciberdefesa.
- Criação nos Institutos e Centros de Defesa de ambos os países (CESEDEN e IDN) de um Curso/Seminário sobre "Gestão de Crises e Política de Desenvolvimento Estratégico para a Cibersegurança e Ciberdefesa" de nível político-estratégico. Neste contexto, poderão organizar-se dois cursos de curta duração por ano, um em Portugal e outro em Espanha, ministrados por especialistas de ambos os países.
- Organizar uma ou duas vezes por ano eventos de tipo fórum de debate ou similares sobre temas relacionadas com a cibercriminalidade e a luta contra o ciberterrorismo, com especial ênfase nas forças e corpos de segurança e funcionários judiciais com vista à harmonização dos procedimentos regulamentares e legais.
- Organizar um fórum de debate anual entre os dois países, alternando entre ambos, para refletir e debater sobre as políticas de cibersegurança e proteção de infraestruturas de informação críticas.
- Desenvolver ações e iniciativas conjuntas de sensibilização, com o fim de promover a adoção das melhores práticas, promover a normalização e melhorar a cibersegurança.
- Em definitivo, promover e fomentar uma cultura de segurança no ciberespaço, abrangendo as administrações públicas e o setor privado, organismos e instituições responsáveis pelo ensino e formação e os próprios cidadãos, tanto local, como nacional e internacionalmente.

Anexo I

I.1. VAM – DoD

No ano 2003, a empresa RAND desenvolveu para a DARPA (*Defense Advanced Research Projects Agency)*[193] uma metodologia[194] orientada para a Avaliação e Mitigação de Vulnerabilidades (VAM – *Vulnerability Assessment & Mitigation*). As fases mais críticas desta metodologia são a identificação de vulnerabilidades e a definição de técnicas de segurança para as mitigar.

O método utilizado para a identificação das vulnerabilidades é matricial, isto é, por um lado classifica-se a vulnerabilidade atendendo à natureza dos seus atributos e, por outro, os tipos de objetos sobre os quais se pode explorar essa vulnerabilidade.

Entre os atributos da vulnerabilidade distinguem-se:

- Projeto/arquitetura (centralizada, homogénea, etc.).
- Comportamento geral (detetável, identificável, intercetável, transparente, previsível, etc.).

Segundo a metodologia VAM, os tipos de objeto sobre os quais se pode explorar a vulnerabilidade são:

- Físicos (*hardware*, rede, comunicações, etc.).
- Cibernéticos (*software*, informação, conhecimento, etc.).
- Humanos/sociais (políticas e procedimentos, experiência, etc.).
- Infraestrutura (edifícios, energia, água, ar, ambiente, etc.).

Para a identificação desta taxonomia, um fator muito importante que se destaca na metodologia VAM, é a incorporação da experiência acumulada/passada de utilizadores e de responsáveis pelo desenvolvimento do sistema.

I.2. NIST SP800-30

O NIST (National Institute of Standards and Technology) estabelece no seu guia SP 800-30[195] que os controlos utilizados para determinar as vulnerabilidades não só têm que abarcar a parte relativa aos sistemas de informação, como também refere que estas devem ser avaliadas num ambiente mais amplo, que pode incluir, por exemplo, a estrutura organizacional, a definição de missões associadas ao negócio, as relações com terceiros, etc.

193 A Agência de Investigação de Projetos Avançados de Defesa, é uma agência do Departamento de Defesa dos Estados Unidos, responsável pelo desenvolvimento de novas tecnologias para uso militar. Foi criada em 1958 e foi a partir dela que surgiram os fundamentos da ARPANET, rede de comunicações que deu origem à internet.

194 P. S. Anton, R. H. Anderson, R. Mesic, y M. Scheiern, «The Vulnerability Assessment & Mitigation Methodology», RAND National Defense Research Institute, 2003.

195 Gary Stoneburner, Alice Goguen, y Gary Stoneburner, «NIST Special Publication 800-30 - Risk management guide for information technology systems». National Institute of Standards and Technology, jul-2002.

Utiliza o conceito de condição preliminar ou condição de partida como variável a ter em conta pelas organizações. Trata-se de uma condição inerente à própria organização que pode tornar mais ou menos fácil a exploração das vulnerabilidades, tais como a localização geográfica, o ambiente operacional, a arquitetura da organização ou o processo de negócio.

I.3. ISO/IEC 27005

A norma ISO 27005 (*International Organization for Standardization*) cataloga as vulnerabilidades afetando-as a diferentes áreas gerais[196]:

- Organização;
- Processos e procedimentos;
- Rotinas de gestão;
- Pessoal,
- Ambiente físico;
- Configuração do sistema;
- *Hardware*, *software* e equipamentos de comunicações;
- Dependência de terceiros.

Esta norma enfatiza a identificação das vulnerabilidades que podem ser exploradas por uma ameaça e que podem causar danos aos ativos da organização. Para isso, utiliza uma série de controlos que se não estiverem corretamente implementados poderão constituir, por si próprios, uma nova vulnerabilidade.

I.4. CVSSv2

A Versão 2 do Sistema de Pontuação Comum de Vulnerabilidades (CVSSv2 – Common Vulnerability Scoring System Version 2) é atualmente o sistema de avaliação mais conhecido e utilizado no mundo e, mediante a sua aplicação, são analisadas a maioria das vulnerabilidades exploradas[197].

Devido ao facto de o risco associado a uma vulnerabilidade não se basear apenas na criticidade da mesma, o CVSSv2 foi desenvolvido de modo a cobrir o máximo de cenários possíveis, tendo em conta fatores que vão desde o ambiente em que é possível explorar a vulnerabilidade até à evolução da mesma. Para levar a cabo este estudo, o CVSSv2 baseia-se em três métricas:

- **Métricas básicas:** contêm as características mais gerais e constantes de uma vulnerabilidade, as quais não se encontram associadas nem ao tempo nem ao ambiente. O vetor de ataque, a complexidade da exploração da vulnerabilidade, a disponibilidade, a integridade ou a confidencialidade, são algumas das características medidas nesta métrica.

196 ISO - International Organization for Standardization, «ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management». 2011.

197 Peter Mell, Karen Scarfone, y Sasha Romanosky, «A Complete Guide to the Common Vulnerability Scoring System Version 2.0». National Institute of Standards and Technology, jun-2007.

- **Métricas temporais (opcional):** fatores que interagem diretamente com o tempo, como o estado da vulnerabilidade ou a disponibilidade de um *exploit* que a permita explorar são características que se podem medir nesta métrica.
- **Métricas de ambiente (opcional):** devido ao fato de ser possível localizar a vulnerabilidade em dois cenários diferentes, é necessário ter em linha de conta a possibilidade de esta ser explorada em cada um deles. Por essa razão, é necessário dispor da dita métrica no momento de se especificar o valor que se pretende atribuir a uma vulnerabilidade.

I.5. CWE

A Enumeração Comum de Debilidades (CWE – Common Weakness Enumeration) é uma iniciativa[198], desenvolvida pela MITRE[199], que define um padrão fixo, unificado e mensurável para classificar as vulnerabilidades de *software*. O CWE é baseado num enquadramento genérico e predefinido, através do qual se podem mapear vulnerabilidades CVE face a alguma das vulnerabilidades base estipuladas através do CWE e vice-versa. Portanto, os objetivos fundamentais que o CWE pretende atingir são:

- Definir uma linguagem comum para descrever as vulnerabilidades.
- Servir como padrão de medida das vulnerabilidades para diferentes ferramentas de segurança.
- Fornecer uma linha comum na identificação das vulnerabilidades, sua mitigação e prevenção.

198 MITRE Corporation, «Common Weakness Enumeration — CWE™ A Community-Developed Dictionary of Software Weakness Types», feb. 2012.

199 A instituição MITRE é uma organização sem fins lucrativos constituida para trabalhar em prol do interesse público. Como recurso nacional dos EUA, aplica a experiência obtida em engenharia de sistemas, tecnologias da informação, desenvolvimento de conceitos operacionais e na modernização da empresa para satisfazer as necessidades dos seus patrocinadores. Consultar http://www.mitre.org/.

Anexo II

II.1. MAGERIT

MAGERIT (*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*) é uma metodologia formal desenvolvida para investigar os riscos que suportam os sistemas de informação e para recomendar as medidas apropriadas a tomar para controlar estes riscos[200].

Elaborada em Espanha pelo Conselho de Governação Eletrónica, sob a direção do Ministério das Finanças e da Administração Pública, destina-se a ser aplicada em qualquer entidade da administração pública espanhola (administração geral do Estado, comunidades autónomas e autarquias locais).

A metodologia MAGERIT permite estudar os riscos inerentes à utilização de um sistema de informação e o meio ambiente com ele associado. Propõe a realização de uma análise das implicações dos riscos, o que envolve avaliar o impacto que uma violação de segurança tem na organização, assinalar os riscos existentes, identificar as ameaças ao sistema de informação, e determinar a vulnerabilidade do sistema para evitar tais ameaças, obtendo desta forma resultados concretos para a sua mitigação.

Os resultados da análise dos riscos permitem aos responsáveis pela gestão do risco recomendar as medidas apropriadas a adotar para conhecer, prevenir, impedir, reduzir ou controlar os riscos identificados e assim reduzir ao mínimo o seu impacto potencial ou possíveis danos.

A metodologia MAGERIT procura os seguintes objetivos:

- Educar/consciencializar os responsáveis pelos sistemas de informação para a existência de riscos e para a necessidade de tratá-los em tempo.
- Oferecer um método sistemático para analisar esses riscos.
- Ajudar a descrever e planear as medidas apropriadas a adotar para manter os riscos sob controlo.
- De forma indireta, também prepara a organização para os processos de avaliação, auditoria, certificação ou acreditação, relevantes em cada caso.

A Versão 2 da metodologia MAGERIT, publicada em 2005, e que está atualmente em vigor, está estruturada em três livros:

- **Livro I: Metodologia**[201]. Descreve os passos fundamentais e as tarefas essenciais para levar a cabo um projeto de análise e gestão de riscos: a descrição formal do projeto e a aplicação para o desenvolvimento de sistemas de informação, proporcionado um grande número de ideias práticas, além de fundamentos teóricos e informação complementar.

200 «MAGERIT versión 2 - Portal de Administración eletrónica», 18-ago2011. [Online]. Available: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184. [Accessed: 25-ago2012].

201 Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, y José Antonio Mañas, «MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método». MAP (Ministerio de Administraciones Públicas), 20-jun2006.

- **Livro II: Catálogo de elementos**[202]. Proporciona os elementos e critérios padrão para a modelação do risco e dos sistemas de informação: classes de ativos, dimensões e critérios de avaliação, ameaças e proteções típicas a ter em conta. Também descreve os relatórios que contêm as conclusões e os resultados, de forma a contribuir para a uniformidade dos mesmos.
- **Livro III: Técnicas práticas**[203]. Descreve as técnicas que se utilizam frequentemente para levar a cabo projetos de análise e gestão de riscos como sejam: análise algorítmica e tabular; árvores de ameaças, análise custo-benefício, diagramas de fluxo de dados, técnicas gráficas, planeamento de projetos e análise de Delphi[204].

II.2 Manual Austríaco de Segurança TI

O Manual Austríaco de Segurança das TI (Tecnologias da Informação) foi originalmente desenvolvido para organizações governamentais, mas está atualmente disponível e pode ser aplicado a todo o tipo de empresas ou atividades. É compatível com as normas ISO. A sua última versão é de 22 novembro de 2004.

É composto por duas partes:

- A primeira parte, contém uma descrição detalhada do processo de gestão de segurança das TIC, o qual inclui o desenvolvimento de políticas de segurança, análise de risco, desenho de conceitos de segurança, implementação do plano de segurança e atividades posteriores.
- A segunda parte, é constituída por uma coleção de 230 medidas de segurança de referência.

II.3. CRAMM

CRAMM (*CCTA Risk Analysis and Management Method*) é uma metodologia de análise de riscos desenvolvida em 1987 pela CCTA (*Central Computing and Telecommunications Agency*), do governo do Reino Unido, cujas funções foram atualmente assumidas pela OGC (Office of Goverment Commerce), também pertencente ao governo britânico. Existe uma ferramenta com o mesmo nome (CRAMM) que ajuda a implementar corretamente a metodologia, uma vez que esta é bastante complicada de utilizar sem o apoio desta ferramenta.

Na sua origem, a metodologia CRAMM teve por base as melhores práticas desenvolvidas pelos departamentos e agências governamentais do Reino Unido, razão pela qual é o método de análise de risco preferido pelo governo britânico. Este método, também utilizado em outros países é especialmente dirigido a grandes organizações, tais

202 Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, y José Antonio Mañas, «MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos». MAP (Ministerio de Administraciones Públicas), 20-jun2006.

203 Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, y José Antonio Mañas, «MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas». MAP (Ministerio de Administraciones Públicas), 20-jun2006.

204 O método Delphi é uma metodologia de investigação multidisciplinar para a realização de prognósticos e predições.

como as organizações governamentais ou grandes indústrias. A última versão publicada do CRAMM é a 5.2.

A metodologia CRAMM compreende três etapas[205], cada uma apoiada por questionários, objetivos e diretrizes. As duas primeiras etapas tratam de identificar e analisar os riscos para o sistema de informação. A terceira etapa recomenda como estes riscos devem ser geridos.

As atividades incluídas em cada uma das etapas da metodologia CRAMM são as seguintes:

Fase 1: Estabelecimento de objetivos de segurança.

- Definir o alcance do estudo.
- Identificar e avaliar os ativos físicos que fazem parte do sistema.
- Determinar o valor da informação manuseada, através de entrevistas realizadas aos utilizadores sobre possíveis impactos no negócio que poderiam resultar da indisponibilidade, destruição, divulgação ou modificação desta informação.
- Identificar e avaliar os ativos de *software* que compõem o sistema.

Fase 2: Avaliação dos riscos e dos requisitos de segurança para o sistema proposto.

- Identificar e avaliar o tipo e o nível das ameaças que podem afetar o sistema.
- Analisar o grau de vulnerabilidade do sistema às ameaças identificadas
- Combinar a ameaça e a vulnerabilidade com o valor dos ativos para calcular uma medida de risco.

Fase 3: Identificação e seleção de contramedidas.

- Que devem ser compatíveis com os riscos calculados na etapa anterior.
- A metodologia CRAMM contém uma grande biblioteca de contramedidas tipificadas, com mais de 3000 medidas pormenorizadas, organizadas em mais de 70 agrupamentos lógicos.

II.4. A&K

A metodologia A&K (Afhankelijkheids- en Kwetsbaarheidsanalyse – Dependência e Análise da Vulnerabilidade), embora inicialmente definida pela empresa pública holandesa RCC foi mais tarde completada pelo Ministério do Interior Holandês que, após terminado o seu desenvolvimento em 1996, publicou um manual descritivo do método.

Neste contexto, importa referir que, desde 1994, a análise A&K é o único método utilizado pelo governo holandês para análise de riscos. Além do governo, as empresas holandesas também tendem a usá-lo.

II.5. EBIOS

EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité* – Expressão de Necessidades e Identificação de Objetivos de Segurança) constitui um conjunto exaustivo de diretrizes, utilizado juntamente com uma ferramenta de *software* de código-fonte aberto que facilita sua aplicação, orientado para apoiar a gestão do risco nos sistemas de

205 SIEMENS, «CRAMM - The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures». Siemens Enterprise, 11-oct2005.

informação. Foi originalmente desenvolvido pelo governo francês, apoiado desde 2005 por um grupo de especialistas em gestão do risco, de diferentes origens, que se tem vindo a mostrar muito ativo na manutenção e atualização das diretrizes EBIOS.

Estes especialistas produzem documentos e boas práticas para serem implementadas por utilizadores finais em diferentes contextos. O EBIOS é amplamente utilizado tanto no setor público como no privado, tanto em França como no exterior.

O EBIOS proporciona aos gestores do risco, uma abordagem coerente e de alto nível do mesmo. Ajuda-os a adquirir uma visão global e consistente, útil para apoiar a tomada de decisão dos diretores, nomeadamente em projetos globais (planos de continuidade de negócios, planos diretores de segurança, políticas de segurança, etc.) e também em sistemas mais específicos (locais *web*, redes, mensagens eletrónicas, etc.).

O EBIOS facilita o diálogo, que deve sempre existir, entre os diretores e os gestores de segurança dos projetos. Neste sentido, contribui para a comunicação entre as partes interessadas na segurança e amplia o que se consciencializa para a mesma.

A abordagem proposta pelo EBIOS consiste num ciclo de cinco etapas[206]:

- A primeira etapa encarrega-se da análise do contexto, refletindo as dependências entre os processos globais de negócio dentro do sistema de informação (definição precisa do perímetro, decomposição da informação em fluxos e funções).
- A análise sobre os requisitos de segurança e a análise das ameaças é realizada na segunda e terceira etapas. É realizada de uma forma fortemente dicotómica, proporcionando uma visão objetiva da sua natureza conflituosa e complementar.
- A quarta e quinta fase fornecem um diagnóstico objetivo dos riscos. Para esse efeito, são estabelecidos os objetivos necessários/suficientes de segurança, assim como requisitos mais elevados. Desta forma, comprova-se que a cobertura foi estabelecida e que os riscos residuais são apresentados explicitamente.

Como ferramenta, o EBIOS é muito flexível, sendo capaz de produzir uma ampla gama de produtos/resultados (objetivos de segurança, perfis de proteção, planos de ação, etc.). Podem-se facilmente adicionar padrões de referência à sua base de conhecimento (vulnerabilidades, métodos de ataque, entidades), assim como catálogos das melhores práticas.

II.6. Métodos ISF para a Gestão e Valorização de Riscos

O ISF (*Information Security Forum*)[207] é responsável pelo desenvolvimento de um conjunto de ferramentas e metodologias[208] relacionadas com a gestão e avaliação do risco, entre as quais destacamos:

206 Agence nationale de la sécurité des systèmes d'information, «EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – Méthode de gestion des risques». ANSSI/ACE/BAC, 25-ene2010.

207 O Fórum da Segurança da Informação, é uma organização independente e sem fins lucrativos dedicada a investigar, aclarar e resolver as questões-chave em matéria de segurança da informação e gestão do risco, mediante o desenvolvimento de metodologias, melhores práticas, processos e soluções que satisfaçam as necessidades dos seus membros. Consultar https://www.securityforum.org/.

208 ISF, «Information Security Forum : Tools and methodologies». [Online]. Available: https://www.securityforum.org/whatwedo/publictools/. [Accessed: 18-ago2012].

- **Norma de Boas Práticas de Segurança da Informação**: proporciona um conjunto de princípios e objetivos de alto nível para a proteção da informação, juntamente com as referências às boas práticas associadas. Estas podem ser utilizadas de diferentes maneiras para melhorar o nível de segurança numa organização.

A norma está dividida em cinco partes distintas, em que cada uma das quais cobre um ambiente especifico:

  - Gestão de segurança (ao longo de toda a empresa);
  - Aplicações de negócio críticas;
  - Instalação de computadores;
  - Redes;
  - Desenvolvimento de sistemas.

- **FIRM** (*Fundamental Information Risk Management* – Gestão de Risco da Informação Fundamental): é uma metodologia detalhada para a monitorização e controlo do risco da informação ao nível empresarial. Foi desenvolvido segundo um ponto de vista prático para monitorizar a eficácia da segurança da informação.

Neste sentido, permite controlar sistematicamente o risco da informação entre empresas de várias dimensões. Inclui guias extremamente detalhados que explicam como começar, como dirigir e como conseguir apoio para a sua implementação.

- **O Quadro (Scorecard) de Comando do Risco da Informação**: é uma parte integrada do FIRM. Trata-se de um formulário utilizado para recolher um conjunto de detalhes importantes sobre um recurso de informação específico, como por exemplo o nome do proprietário, a sua criticidade, o nível da ameaça, o potencial impacto no negócio ou a sua vulnerabilidade.
- **Analisador do Estado da Segurança da Informação**: é uma ferramenta também muito detalhada de gestão do risco que analisa ou avalia uma ampla gama de controlos de segurança, que são utilizados pelas organizações para controlar os riscos associados aos seus sistemas TIC.
- **SARA** (*Simple to Apply Risk Analysis* – Análise de Riscos Fácil de Aplicar): é uma metodologia especificada para analisar o risco dos sistemas de informação críticos. Consiste em quatro fases:
  - Planeamento;
  - Identificação de requisitos de segurança;
  - Avaliação de vulnerabilidades e monitorização de requisitos;
  - Relatório.
- **SPRINT** (*Simplified Process for Risk Identification* – Processo Simplificado para a Identificação de Riscos): inicialmente ajuda a estabelecer o nível de risco associado a um sistema, para posteriormente, uma vez os riscos compreendidos completamente, ajudar a determinar como proceder, culminando com a elaboração de um plano de ação para manter os riscos dentro dos limites aceitáveis. O SPRINT pode ajudar a:
  - Identificar tanto as vulnerabilidades dos sistemas existentes como as salvaguardas necessárias para os proteger.

• Definir os requisitos de segurança dos sistemas que estejam em desenvolvimento, assim como os controlos necessários para os atingir.

II.7. ISO/IEC 27005

É uma norma ISO que descreve[209], em termos gerais, todo o processo de gestão de riscos na segurança da informação. Os anexos da norma contêm exemplos de diferentes abordagens sobre a avaliação de riscos na segurança da informação, bem como uma lista de possíveis ameaças, vulnerabilidades e controlos de segurança.

Esta norma pode ser considerada como a mais adotada ao nível internacional, relativamente à gestão de riscos da informação, e estabelece uma estrutura para a definição do processo de gestão de riscos.

II.8. MARION

O método MARION (*Methodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau*) foi desenvolvido pela CLUSIF (*Club de la Sécurité de l'Information Français*)[210] com base numa metodologia de auditoria, o que permite estimar o nível de risco de uma empresa na segurança das suas TIC através da aplicação de questionários. Estes questionários permitem obter indicadores em forma de classificações associadas às várias questões relativas à segurança.

O objetivo da metodologia é o de obter uma visão da organização em relação a um nível de segurança que se considera "certo" e, por outro lado, aferi-lo em comparação com outras organizações que tenham respondido ao mesmo questionário. O nível é calculado com base em 27 indicadores agrupados em seis grupos principais, atribuindo a cada um deles um valor entre 0 e 4. O nível 3 é o nível de segurança que se considera adequado. Para finalizar, realiza-se uma análise de risco mais detalhada para identificar ameaças e vulnerabilidades que devem ser enfrentadas pela organização.

Embora o CLUSIF já não patrocine esta metodologia, por ter sido substituída por uma metodologia mais recente designada por MEHARI (*Méthode Harmonisée d'Analyse de Risques*), que iremos referir abaixo, constata-se que o método MARION ainda é utilizado e tem uma implantação significativa em empresas de língua francesa.

II.9. MEHARI

O MEHARI[211] é um método de análise de risco, projetado pelo CLUSIF francês, que propõe a definição de medidas de redução do risco ajustadas aos objetivos da organização. O MEHARI fornece um modelo de avaliação de risco e processos e componentes modulares. Também melhora a capacidade para descobrir vulnerabilidades através de auditorias

209 Internet Engineering Task Force (IETF), «RFC 4949 - Internet Security Glossary, Version 2». ago-2007.

210 Criado em 1984, é uma organização sem fins lucrativos cujo objetivo é permitir que os profissionais que se ocupam da segurança da informação se reúnam e troquem opiniões, trabalhos e progressos. Com sede em França, está aberto às contribuições e aos membros de todo o mundo.

211 CLUSIF, «MEHARI 2010 Risk Analysis and Treatment Guide». Club de la Sécurité de l'Information Français, ago-2010.

e analisar situações de risco. Inclui fórmulas que facilitam a identificação e caracterização de ameaças e a seleção ótima das ações corretivas.

II.10. OCTAVE

O OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), desenvolvido pela Carnegie Mellon SEI (*Software Engineering Institute*), define uma metodologia de planeamento e avaliação estratégica baseada nos riscos dos Sistemas de Informação.[212] O OCTAVE oferece uma proposta por *motu proprio*, o que significa que as pessoas da organização assumem a responsabilidade de estabelecer a estratégia de segurança da mesma.

O OCTAVE-S (*OCTAVE for Smaller Organizations*) constitui uma variação adaptada à medida das pequenas organizações (menos de 100 pessoas) que possuem meios mais limitados. O OCTAVE-S é dirigido para uma pequena equipa interdisciplinar de pessoas da organização, a qual recolhe e analisa informação para produzir uma estratégia de proteção e planos de mitigação baseados nos riscos operacionais de segurança da organização.

Para utilizar o OCTAVE-S de forma eficaz, a equipa deve ter um profundo conhecimento dos processos de negócio e da segurança da organização, para ser capaz de realizar todas as atividades por si só.

II.11. NIST SP800-30

O SP800-30[213] é um guia para a gestão de riscos nos Sistemas de Tecnologias de Informação, desenvolvido pelo NIST (*National Institute of Standards and Technology*) dentro da sua série 800 de publicações especiais[214].

O SP800-30 proporciona um método detalhado sobre o que se deve ter em conta no âmbito da análise e avaliação dos riscos de segurança das tecnologias da informação. Contém listas detalhadas dos itens que devem ser verificados, gráficos, fluxogramas, fórmulas matemáticas, além de outras referências, principalmente com base em normas e regulamentos norte-americanos.

212 Christopher J. Alberts, Audrey J. Dorofee, James Stevens, y Carol Woody, «OCTAVE® Introduction to the OCTAVE® Approach». Carnegie Mellon Software Engineering Institute, ago-2003.

213 Gary Stoneburner, Alice Goguen, y Gary Stoneburner, «NIST Special Publication 800-30 - Risk management guide for information technology systems». National Institute of Standards and Technology, jul-2002.

214 A série SP-800 é um conjunto de documentos de interesse geral para a comunidade de segurança informática. A série foi criada em 1990 para agrupar, com base numa identificação específica, as publicações centradas na segurança das tecnologias da informação.

Anexo III

Classificação das Capacidades de Ciberdefesa desenvolvida pela NC3A da OTAN

Esta classificação pode servir como um guia para uma análise mais detalhada das capacidades, tecnologias e ferramentas necessárias para implementar uma Ciberdefesa adequada. Decompõe a Ciberdefesa em seis grandes áreas de capacidade, onde cada uma se divide em outras capacidades subjacentes, e assim sucessivamente até se chegar a um nível de detalhe suficiente. As grandes áreas de capacidades identificadas são as seguintes:

1. Deteção de atividade maliciosa

Capacidade que se implementa através da recolha de informação a partir de uma gama alargada de sensores, servindo de base para a análise que realiza a separação dos fluxos de tráfego entre entidades maliciosas, e que permite assim uma avaliação da situação. Isto é conseguido relacionando as entidades maliciosas entre si e estas com as entidades de origem e destino, para além de se ter também em conta o histórico de atividades registadas entre elas. Portanto, esta capacidade é por sua vez composta de:

1.1. Recompilação de dados de sensores: capacidade para recolher num repositório global os dados sobre todas as atividades em curso, através da utilização de sensores e do alinhamento da sintaxe dos dados. Os sensores incluem os sistemas de deteção de intrusão, *scanners* de vulnerabilidade e relatórios de registos de eventos de dispositivos tais como *firewalls*, servidores e *proxies*, entre outros. Além de recolher dados dos sensores, estes dados têm de ser pré-processados para unificar a sintaxe e os pontos de referência.

1.2. Avaliação de Entidades: capacidade para fundir as observações dos sensores em entidades associadas, com propriedades comuns, classificando-as como sendo danosas ou não. No ciberespaço, as entidades podem ser qualquer conjunto de dados relacionados de alguma forma, como por exemplo, os dados associados a um *download* de um *site*, uma chamada de voz sobre IP (VoIP) ou um ataque DDoS. Por sua vez é composto por:

1.2.1. Normalização dos dados de sensores: capacidade para unificar o significado dos dados recolhidos a partir de diferentes sensores, de modo a que expressões diferentes com um mesmo significado se estruturem num mesmo formato, obtendo pontos de referência comuns que facilitem a correlação entre eles.

1.2.2. Correlação de dados de sensores: capacidade para reconhecer vestígios de dados provenientes de diferentes sensores, mas que pertencem a uma mesma entidade, tal como um servidor ou um fluxo de dados específico.

1.2.3. Atribuição de atributos às entidades: capacidade para conferir atributos (como largura de banda consumida ou o tipo de páginas *web* "descarrega-

das") a cada entidade, baseados em dados recolhidos a partir dos sensores que permitam caracterizá-la.

1.2.4. Caracterização de Entidades: capacidade para determinar o tipo de entidade com base nos seus atributos e no conhecimento prévio do seu significado. Uma forma muito simples de caracterização seria, por exemplo, estabelecer que o tráfego para o porto 80 corresponde a um tipo de entidade que chamamos de "transferência da página *web*".

1.3. Avaliação da Situação: capacidade para reconhecer atividades, entendidas como relações entre entidades, seus atores, assim como o seu significado e contexto. Por sua vez, esta compõe-se de:

1.3.1. Correlação de entidades: capacidade para identificar relações entre as entidades que permitam configurar atividades. Essas relações podem ser padrões de tempo que identificam ações sequenciais ou em paralelo.

1.3.2. Localizar a fonte técnica de ataque: capacidade para identificar o servidor a partir do qual o ataque teve origem ou é controlado, o que normalmente vai mais além do que identificar o IP de origem, pois normalmente este terá sofrido um ataque de *spoofing*[215] ou será apenas um nó de um caminho de múltiplos saltos utilizado pelo atacante.

1.3.3. Interpretar a atividade: capacidade para interpretar cada atividade e a sua origem técnica para compreender a extensão e os detalhes da mesma.

1.3.4. Interpretar o contexto: capacidade para identificar relações entre atividades, tanto em sistemas de informação próprios como alheios, através da troca de informação. As atividades já interpretadas são colocadas em contexto mediante a utilização de informação histórica de padrões de atividade, que podem ser comparados com atividades similares registadas em sistemas de TIC alheios, de forma a conferir uma visão global capaz de nos dizer se estamos diante de um ataque genérico ou específico.

1.4. Visualização para apoiar a análise: capacidade para apresentar visualmente atividades, entidades e sensores de modo a facilitar o trabalho dos analistas que têm de lidar com enormes quantidades de dados, e são responsáveis por detetar ações maliciosas.

2. Prevenção, mitigação e eliminação de ataques

Esta capacidade, por sua vez, é constituída por:

2.1. Reconfiguração da topologia dos sistemas: capacidade para modificar a estrutura dos sistemas de informação e comunicações, incluindo os seus serviços, o seu *software* e *hardware*, a sua interligação, assim como a configuração de qualquer um dos seus módulos ou componentes. Por sua vez é composto por:

215 *Spoofing*, no contexto de segurança TIC, refere-se apenas à utilização de técnicas de suplantação de identidade, normalmente com intenção maliciosa. Segundo o elemento identificador que se suplanta falaremos de IP spoofing, ARP spoofing, DNS spoofing, Web spoofing ou email spoofing.

2.1.1. Realojamento dos serviços de informação: capacidade para mover serviços e a sua informação associada para uma infraestrutura TIC alternativa.

2.1.2. Compartimentação de sistemas: capacidade para separar e isolar certas partes de um sistema TIC. Esta capacidade revela-se crucial quando estamos perante um ataque iminente ou em curso, para limitar o impacto e preservar a integridade e a continuidade das operações do resto do sistema.

2.1.3. Desligar componentes e serviços: capacidade para desligar componentes ou serviços a partir de um sistema, como servidores e *interfaces* de rede. Esta pode ser uma medida eficaz para mitigar um ataque, porém pode ter um impacto negativo na operação, razão pela qual a sua aplicação deve sempre ser avaliada previamente.

2.1.4. Revogação de credenciais: capacidade para remover os direitos de acesso a entidades que tinham sido previamente credenciadas, mas cujas credenciais foram comprometidas ou mal utilizadas.

2.1.5. Atualização do *hardware*, *software* e sua configuração: capacidade para modificar o *hardware*, *software* e a sua configuração, de forma a prevenir e mitigar possíveis ataques. Assim, por exemplo, as vulnerabilidades do *software* requerem atualizações periódicas das suas versões, para evitar a sua exploração por parte de possíveis atacantes.

2.2. Controlo do fluxo de tráfego: capacidade para encerrar ou limitar o fluxo de dados a uma determinada largura de banda, ou introduzir-lhe um certo atraso, bem como para alterar o encaminhamento da comunicação, interferir no fluxo de dados ou modificá-lo, com o objetivo de deter ou mitigar um ataque.

2.3. Deceção: capacidade para criar, de forma estática e dinâmica, áreas do sistema TIC onde o ataque se pode desenvolver sem impacto na operação normal do sistema.

2.4. Defesa ativa: capacidade para utilizar técnicas de ataque com o único propósito de deter ou mitigar um ataque em curso. A utilização destas técnicas pode ter a intenção de recuperar o controle sobre seus próprios recursos ou sufocar ataques neutralizando a origem dos mesmos.

2.5. Coordenação da resposta externa: capacidade para coordenar a implementação de medidas com terceiros, nomeadamente com fornecedores nacionais ou internacionais de serviços TIC, para parar ou mitigar os ataques.

3. Análise dinâmica de riscos, ataques e danos

Esta capacidade, por sua vez, é constituída por:

3.1. Análise Dinâmica de Riscos: capacidade para avaliar o risco de forma contínua e automática para poder projetar a situação atual no futuro e prever o possível impacto. Este tipo de análise de risco difere da tradicional, que geralmente se efetua durante a fase de projeto e noutras fases do ciclo de vida do sistema, pelo que deve assumir um caráter automático e contínuo. Faz uso de um ou mais mé-

todos de cálculo, que tomam como entrada determinadas variáveis do ambiente que caracteriza o sistema de informação e comunicações, cujos valores têm que ser possíveis de estimar, tais como:

3.1.1. Valoração de ativos: entendido como o valor dos serviços que proporciona o sistema TIC para a organização em que se insere. Conhecer todos os ativos e determinar a sua importância relativa é fundamental no momento de avaliar o impacto de um ataque e de priorizar as ações tomadas para reduzir o risco suportado pelo sistema.

3.1.2. Avaliação da ameaça: inclui tanto a informação geral sobre as ameaças, que se irá atualizando com produtos de inteligência genéricos, como a informação obtida por meio dos próprios sensores de atividades maliciosas.

3.1.3. Análise de vulnerabilidades: inclui todas as vulnerabilidades detetadas no sistema, descobertas através da utilização de sensores de vulnerabilidades tanto ativos como passivos.

3.1.4. Estrutura do sistema: entendida como uma imagem atualizada e completa do sistema TIC, incluindo os seus dispositivos, conexões, software, a configuração de cada módulo, assim como a informação processada e nele armazenada.

3.2. Avaliação de ataques: capacidade para permitir que um ataque progrida, para analisá-lo e monitorizá-lo, a fim de melhor compreender a intenção e a capacidade do atacante. Por sua vez é composto por:

3.2.1. Análise de ataques em curso: capacidade para analisar as características de um ataque e da sua origem, ao mesmo tempo que este se está a desenvolver, a fim de realizar uma melhor análise da ameaça.

3.2.2. Coordenação da monitorização externa: capacidade para coordenar medidas com terceiros, nomeadamente com colaboradores ou prestadores de serviços, para monitorizar e analisar os ataques em curso.

3.3. Avaliação de danos: capacidade para avaliar os danos causados por um ataque, uma vez que este tenha sido confirmado e detido. O dano pode ocorrer sobre o sistema propriamente dito ou sobre a informação que este armazena e processa. Por sua vez é composto por:

3.3.1. Análise de *malware*[216]: capacidade *para compreend*er o funcionamento do código malicioso.

3.3.2. Identificação dos Sistemas Afetados: capacidade para identificar se um sistema está a funcionar conforme deveria ou se foi afetado por um ataque.

3.3.3. Verificação da integridade da informação: capacidade para verificar se a informação armazenada ou processada no sistema não foi modificada de forma maliciosa.

216 *Malware* provém da fusão das palavras inglesas *malicious software* e faz referência a qualquer tipo de código ou programa cuja intenção seja aceder sem autorização ou causar dano num sistema alheio.

3.3.4. Identificação da informação comprometida: capacidade para identificar qualquer informação cuja confidencialidade tenha sido comprometida, por exemplo, por meio de um *download* sem autorização por parte de um atacante.

3.3.5. Medida da disponibilidade do serviço: capacidade para detetar se os serviços prestados foram afetados por um ataque. Para isso, deve medir-se continuamente a disponibilidade dos serviços, identificando aqueles que são prestados de modo degradado ou que deixaram completamente de se prestar.

3.4. Consciencialização sobre a situação: capacidade para consciencializar de forma visual e rápida os utilizadores e operadores do sistema relativamente à situação do mesmo, incluindo o fornecimento de informação relativa às atividades e componentes do sistema, aos seus objetivos e prioridades, assim como as suas ameaças e vulnerabilidades.

4. Recuperação de ciberataques

Capacidade para recuperar de um ataque, através da restauração ao seu estado original, do sistema, da informação e das suas propriedades de segurança. Esta capacidade por sua vez é constituída por:

4.1. Restauração da integridade do sistema: capacidade para restaurar o sistema para um estado em que tanto a plataforma como os serviços que correm sobre ela garantem o seu funcionamento de acordo com os requisitos de segurança. Isto pode exigir uma reinstalação completa dos mesmos, ou a utilização de uma cópia de segurança cuja integridade foi verificada.

4.2. Restauração da integridade da informação: capacidade para restaurar a informação armazenada ou processada pelo sistema, de forma a que se possa confiar que esta informação se encontra correta e sem modificações não autorizadas. Isto pode exigir a recuperação da informação a partir de uma cópia de segurança/*backup* cuja integridade tenha sido verificada, ou mesmo a eliminação de qualquer peça de informação não confiável.

4.3. Restauração da disponibilidade do serviço: capacidade para tornar os serviços novamente disponíveis após um ataque. Requer a restauração tanto da integridade da informação como do próprio sistema, assim como a reconfiguração do sistema para prevenir novos ataques.

4.4. Registo da informação comprometida: capacidade para manter um registro de toda a informação cuja confidencialidade tenha sido comprometida, a fim de informar corretamente todos os interessados.

5. Tomada de decisão em tempo

Capacidade para decidir sobre as ações a ser implementadas de maneira oportuna. Como os eventos no ciberespaço podem desenvolver-se de forma vertiginosa, isto implicará que em muitos casos a resposta seja automática, para garantir que é suficiente-

mente rápida. Em qualquer caso, será necessário contemplar a tomada de decisão por humanos, para coordenar os resultados de diferentes respostas e selecionar a melhor via a prosseguir no processo de defesa. Esta capacidade, é constituída por sua vez por:

5.1. Identificação de opções: capacidade para identificar as diversas possíveis respostas a um ataque, avaliando as opções e prioritizá-las de acordo com o efeito e o impacto desejados, identificando também as pessoas responsáveis por tomar oportunamente as decisões necessárias para as realizar.

5.2. Coordenação da decisão: capacidade para coordenar uma decisão com as várias partes envolvidas, que podem muitas vezes ser constituídos por diferentes organizações integradas num ambiente de redes e sistemas federados, de modo a que possa ser implementada de maneira adequada.

5.3. Divulgação da decisão: capacidade para comunicar uma decisão a todas as partes envolvidas, incluindo tanto as organizações externas que trabalham com a nossa, como os nossos próprios utilizadores e operadores dos sistemas de TIC.

6. Gestão da informação de ciberdefesa

Capacidade para reunir e partilhar informação de forma a que permita uma troca rápida e confiável da mesma entre diferentes partes. Entre os elementos de informação sobre Ciberdefesa a partilhar encontra-se normalmente uma estimativa da intenção do adversário e da sua capacidade, bem como informação relativa às vulnerabilidades conhecidas, *software* malicioso e às avaliações e certificações dos diferentes produtos de *software* e *hardware*. Esta capacidade, por sua vez é constituída por:

6.1. Recolha e partilha de informação de Ciberdefesa: capacidade para reunir informação proveniente de diferentes fontes e partilhá-la com diversos colaboradores, incluindo a informação recolhida dos próprios incidentes em curso. Isto permitirá uma melhor avaliação de riscos e a implementação de medidas preventivas. A troca de informação deve basear-se num modelo assente na confiança entre as partes e deve ser concebido de forma a permitir uma rápida distribuição da informação, em linha com os requisitos necessários à tomada de decisão em tempo útil.

6.2. Garantia de qualidade da informação de ciberdefesa: capacidade para gestão da fiabilidade da informação de Ciberdefesa recebida, dado que esta pode vir de diferentes fontes, desde fontes abertas na internet a relatórios da comunidade de inteligência.

6.3. Recolha e exploração do histórico de dados: capacidade para registar a informação em bases de dados de curto e longo prazo, de forma a apoiar as ações futuras. O histórico dos dados inclui o tráfego de rede, informação de sensores, etc. Esta informação pode ser utilizada, por exemplo, em conjunto com novos algoritmos de deteção de modo a que, quando aplicada sobre dados referentes ao histórico, se comprove a sua validade, sabendo o que já aconteceu anteriormente.

idn cadernos

ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO

Este trabalho é o resultado da cooperação que, durante os anos de 2012 e 2013, o Instituto da Defesa Nacional (IDN) de Portugal e a Escuela de Altos Estudios de la Defensa (EALEDE) do Centro Superior de Estudios de la Defensa Nacional (CESEDEN) mantiveram em torno de um tema de plena atualidade: a cibersegurança.

O estudo define e analisa as implicações e a perceção do impacto do ciberespaço na segurança e defesa dos Estados, caracterizando o enquadramento concetual e operacional adotado por Portugal e Espanha.

idn Instituto da Defesa Nacional

ISSN 1647-9068