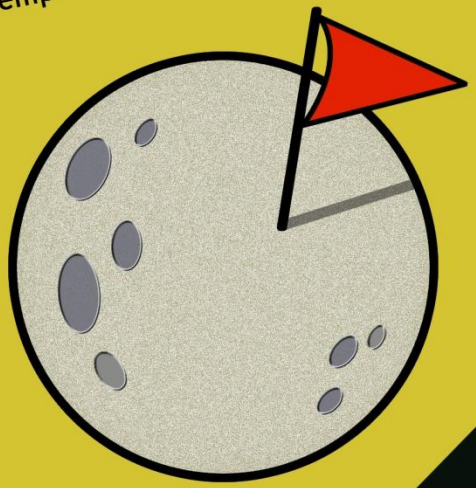
CYBERLAW by CIJIC

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

DIREITO: A PENSAR TECNOLOGICAMENTE

DIREITO: A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO UNIVERSIDADE DE LISBOA

cyber espaço
novas fronteiras

cyber ataques
algumas estratégias de mitigação

cyber segurança
preocupação global

outros
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


CYBERLAW
by CIJIC

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM DOTMLPI-I

INFORMATION SECURITY INCIDENTS RESPONSE: AN DOTMLPF-I APPROACH

PAULO J. BAPTISTA DAS NEVES [1]

e

FERNANDO JORGE RIBEIRO CORREIA [2]

[1] Capitão-Tenente Marinha – DITIC. Correio Eletrónico: baptista.neves@marinha.pt
[2] Capitão-de-Fragata Escola Naval, CINAV. Correio Eletrónico: ribeiro.correia@marinha.pt

SUMÁRIO: 1. INTRODUÇÃO; 2. A METODOLOGIA DOTMLPI-I; 3. CAPACIDADE DE RESPOSTA A INCIDENTES DE SEGURANÇA E O DOTMLPI-I; 4.CONCLUSÃO; 5.REFERÊNCIAS

RESUMO

O conceito de ciberespaço resulta da interligação das redes de comunicações e de diferentes sistemas de informação à escala global. A abstração deste espaço de comunicações apresenta evidentes vantagens para a sociedade de informação em que vivemos. A sua utilização maciça por indivíduos e organizações fez com que ele se tornasse crítico para as empresas e para o próprio estado, pois a exploração das vulnerabilidades dos diferentes sistemas que o utilizam podem afetar as infraestruturas que prestam serviços críticos à sociedade. Para assegurar a qualidade da informação que nele circula é necessário que existam mecanismos de monitorização permanentes, com capacidade de prevenção e resposta aos incidentes que coloquem em causa a segurança da informação.

Existem já vários modelos e normativos para a organização desta capacidade de resposta a incidentes de segurança da informação. Neste artigo iremos apresentar a metodologia utilizada pela OTAN para a edificação de capacidades operacionais, aplicando-a à identificação dos elementos críticos a considerar na edificação de uma capacidade de resposta a incidentes de segurança da informação no ciberespaço.

Palavras-Chave: Ciberespaço, Cibersegurança, Resposta a Incidentes, DOTMLPI-I.

ABSTRACT

The concept of Cyberspace results from - on a global scale - the interconnection of communication networks and different information systems. This immense communication space produces clear benefits for the information society in which we live. Its massive use by individuals and organizations made him critical for companies and for the state itself, since exploiting vulnerabilities of different systems that they use may affect the infrastructures that deliver critical services to society. There has to be permanent monitoring mechanisms - capable in prevention and response to incidents that may undermine the security of information - to ensure the quality of the information that flows.

There are already several models and standards for organizing the capacity to respond to information security incidents. In this article we will present the methodology used by NATO to the edification of operational capabilities and apply it to the identification of critical elements to consider when building one capacity to respond to information security incidents in cyberspace.

Keywords: Cyberspace, Cyber Security, Incident Response, DOTMLPF-I.

1.INTRODUÇÃO

Para uma sociedade de informação como aquela em que vivemos, com comunicações omnipresentes quer a nível pessoal quer ao nível das instituições, o ciberespaço[3] apresenta evidentes vantagens, tornando realidade a sensação de ubiquidade. André Matias e Rogério Bravo no seu artigo sobre o ciberespaço "Geopolítica, geoestratégia e ciberespaço: Notas introdutórias" 0 mencionam que os vetores espaço, tempo e caminho percorrido para se movimentar de um ponto para o outro, praticamente desaparece.

A vantagem de poder chegar instantaneamente a todo o lado, a independência dos fusos horários, levou a que também os Estados e as Empresas utilizem o Ciberespaço como base para as suas infraestruturas de comunicações, não só entre si, mas também como rede de suporte ao comando e controlo das suas infraestruturas, muitas das quais disponibilizam serviços críticos à sociedade.

O Ciberespaço é assim uma realidade complexa onde interagem diferentes dimensões da sociedade e onde o valor maior reside na qualidade da informação que nele circula, seja na comunicação entre pessoas, entre organizações ou mesmo nas comunicações de comando e controlo de sistemas críticos. Este é um espaço virtual cujos acontecimentos se repercutem no mundo físico, tornando-se assim um problema global.

Sendo então a segurança do Ciberespaço vital para a garantia da qualidade da informação, que como vimos poderá ter impacto ao nível dos serviços básicos para o funcionamento da sociedade ou mesmo da soberania do país, estando este sujeito a ameaças que tanto poderão ter origem em atos de protesto social, ou relacionadas com objetivos de natureza criminosa ou mesmo de guerra, compete primariamente aos governos dos países a organização para a segurança e defesa deste espaço. A segurança da informação e a proteção das infraestruturas críticas são da responsabilidade do Estado que "terá de garantir não só a utilização segura do ciberespaço aos seus cidadãos como a salvaguarda da própria soberania" [3].

[3] "Um domínio global e virtual criado pela interligação de todas as redes de Comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas" 0.

De modo a desenvolver as capacidades de Cibersegurança, o estado português, seguindo as recomendações da União Europeia onde cada estado membro deve implementar uma capacidade de resposta a incidentes de segurança cibernética [4], através do decreto-lei 69/2014 de 9 de maio, decidiu criar o Centro Nacional de Cibersegurança (CNCS). O Centro está na dependência direta da Autoridade Nacional de Segurança com "*a missão de contribuir para que Portugal use o ciberespaço de uma forma segura e as suas competências não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço, nomeadamente no que respeita a infraestruturas críticas e integridade das redes e serviços, sendo exercidas em coordenação com estas entidades"* [5].

Em 2015 o governo de Portugal definiu a estratégia nacional de Segurança do Ciberespaço, onde são apresentados como objetivos estratégicos a promoção de "*uma utilização consciente, livre, segura e eficiente do ciberespaço*", a proteção "*dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos", o fortalecimento da "segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais" e a afirmação do "ciberespaço como um domínio de desenvolvimento económico e de inovação*" [6].

A Cibersegurança materializa-se numa verdadeira capacidade de antecipar e responder a incidentes de natureza cibernética que afetem a qualidade da informação que circula no ciberespaço nacional. Existem vários normativos como a ISO/IEC 27035, o guia de boas práticas da ENISA ou o NIST SP 800-61, que apontam metodologias para a edificação de uma capacidade de resposta a incidentes de segurança da informação, neste artigo propomos a utilização da metodologia DOTMLPI-I para a identificação dos elementos críticos a considerar na edificação desta capacidade. Começaremos por apresentar a metodologia DOTMLPI-I e o modo como as Forças Armadas a utilizam para a edificação de capacidades operacionais. No ponto seguinte iremos aplicar esta metodologia para a identificação dos elementos críticos a ter em consideração para a identificação da uma capacidade operacional de resposta a incidentes de segurança da informação. Finalmente apresentaremos as conclusões resultantes da utilização desta metodologia a este tema da Cibersegurança.

2.A METODOLOGIA DOTMLPI-I

O acrónimo DOTMLPI (Doutrina, Organização, Treino, Material, Liderança, Pessoal e Infraestruturas) refere-se aos componentes básicos da edificação de uma capacidade operacional, desenvolvido pelo Departamento da Defesa dos EUA (*Department of Defense – DoD*). É uma abordagem à implementação de capacidades operacionais, de modo a identificar lacunas na sua operacionalização[7]. A este modelo básico, o *DoD* viria a adicionar uma outra componente, as Políticas, com o objetivo de adicionar a esta abordagem a procura de procedimentos comuns entre os diversos utilizadores na utilização da nova capacidade. Este novo modelo é conhecido por DOTMLPI-P [8]. A OTAN adotou este modelo básico de implementação de novas capacidades fazendo apenas uma alteração, a troca do conceito de Políticas por um outro que lhe é bastante caro, a Interoperabilidade, nascendo assim o acrónimo DOTMLPI-I [9].

Antes de abordar cada um dos diferentes domínios que compõem esta metodologia DOTMLPI-I e a sua relevância para a edificação de uma capacidade operacional, seguindo uma perspetiva militar, importa definir este conceito de capacidade. De acordo com a definição da OTAN, uma capacidade operacional é a possibilidade de um comandante militar conseguir executar um conjunto específico de ações, identificando os efeitos necessários para atingir determinado objetivo [10]. Desta definição resulta que uma capacidade operacional é complexa e que não se resume a questões de material ou de procedimentos, no fundo é necessária uma abordagem holística como a que permite a DOTMLPI-I, para o sucesso do seu desenvolvimento e implementação.

DOUTRINA

Numa perspetiva militar a Doutrina aparece ligada ao modo como são conduzidas as operações de combate, sejam manobras, campanhas ou outras, ou seja, os princípios fundamentais que permitem a utilização coordenada de uma ou mais forças militares para atingirem um objetivo comum. A Doutrina baseia-se em princípios comuns, construídos sobre as lições aprendidas durante as operações militares, através de treinos e exercícios. Considerando a sua caraterística imperativa para as Forças militares em campanha, esta está sempre sujeita às políticas comuns acordadas entre

as partes, aos tratados e a restrições de natureza legal, devendo ser sempre seguida, exceto se, de forma muito excecional, o comandante em exercício assim o entender.

ORGANIZAÇÃO

A Organização diz respeito ao modo como os indivíduos se constituem como equipas, e estas em unidades operacionais, executando as funções que lhes são determinadas, de forma a contribuírem para o sucesso da missão. Estas unidades operacionais são suportadas numa estrutura que permite que funcionem de forma coordenada. Esta estrutura tem configurações diversas, de natureza diferenciada e multidisciplinar, conforme se destine às operações propriamente ditas ou a ações de suporte e manutenção. Do desempenho desta estrutura depende em grande parte o sucesso das missões como tal as ações de Treino assumem particular importância.

TREINO

Como descrito no parágrafo anterior, o Treino das equipas é fundamental, sejam unidades individuais, de grupo ou mesmo alianças internacionais, de natureza operacional ou de suporte às várias estruturas que participam nas operações. Só o treino permite aos diversos intervenientes num teatro de operações a resposta pronta e capaz às necessidades estratégicas, operacionais e táticas do comando. Uma das formas de executar as ações de treino é através de exercícios que *incorporem os aspetos apropriados do ambiente operacional no cenário de treino, permitindo à audiência de treino a aprendizagem dos conceitos necessários às diversas capacidades, observando a execução do exercício* [8]. As lições aprendidas através do treino permitem a revisão ou mesmo o desenvolvimento de novos conceitos, com impacto direto no aperfeiçoamento das capacidades operacionais.

MATERIAL

O Material refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais. Esta dimensão abrange desde os equipamentos, à tecnologia, às armas, ou as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão. Os problemas que surgem nesta área podem ter soluções de natureza material, adquirindo o artigo necessário para a sua resolução. Por outro lado também podem ser problemas que não sejam resolúveis através de qualquer aquisição, ou seja, terão de ter uma solução não-material, implicando assim soluções

que envolvam alterações nas outras dimensões, como por exemplo na doutrina, na organização ou no treino [11].

LIDERANÇA

Nesta metodologia a Liderança surge diretamente ligada à Formação, preocupando-se essencialmente com a preparação das chefias para uma abordagem profissional da operação, ou seja ao desenvolvimento da competência profissional para comandar. É fundamental que o líder seja capaz de compreender o objetivo que lhe é apresentado e que conduza a ação para que este seja alcançado com sucesso. Tem de ter a capacidade de dirigir e motivar os membros da equipa, com profissionalismo, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo, as suas capacidades com vista ao sucesso da missão. Como refere *Cecília Bergamini*, *todas as organizações podem contar com bons líderes desde que lhes dispensem o treino adequado e promovam um ambiente favorável onde possam agir com eficácia* [12].

PESSOAL

No referente ao Pessoal o mais importante é garantir que este possui as qualificações necessárias para o desempenho da missão, quer considerando as necessidades em tempo de paz, quer em tempo de crise. O fator humano e a componente social são determinantes, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e disponibilizarem-lhes a formação adequada. Por outro lado é preciso considerar que para algumas missões, o pessoal pode não ter as competências necessárias, sendo por isso necessário envolver pessoal externo ou parceiros civis, como sejam as empresas do setor tecnológico ou outras, para que se possa cumprir a missão. Quando identificadas lacunas na formação do pessoal, ou o surgimento da necessidade de novas competências relevantes para a missão, deve ser feita a ponderação de alteração do plano de formação previsto para os diferentes papéis que os elementos desempenham no seio da equipa ou a contratualização do serviço a entidades externas. Finalmente há que considerar um quadro de pessoal que garanta a disponibilidade dos recursos humanos necessários quer em tempo de paz quer em tempo de crise.

INFRAESTRUTURAS

As Infraestruturas são tudo o que se refere com a disponibilização de instalações adequadas à preparação e condução das operações. Também aqui é importante garantir que as Infraestruturas existentes permitem responder de forma satisfatória aos requisitos de manutenção em tempo de paz e aos requisitos operacionais em tempo de crise. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, oficinas, armazéns, centros de dados, estradas, distribuição de energia elétrica e água, entre outras.

INTEROPERABILIDADE

A estas sete dimensões básicas do modelo, o DoD dos EUA acrescentou as Políticas, mas a OTAN optou por estabelecer um conceito mais abrangente, a Interoperabilidade. Na verdade a diferença é quase inexistente e podemos mesmo considerar que os objetivos são idênticos. No fundo o que esta dimensão extra do modelo pretende é colocar em destaque a importância de existir uma abordagem comum entre as várias entidades ou equipas que participam nas operações. O estabelecimento desta abordagem comum implica que se utilize um conjunto de conceitos partilhados entre as partes, que todos entendam como válidos. Isto pode ser conseguido através de políticas que definam procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo. A OTAN define-a como “a capacidade de agir em conjunto de forma coerente, efetiva e eficazmente para atingir os objetivos táticos, operacionais e estratégicos da Aliança” [13]. De acordo com a missão, existe a necessidade de conduzir as operações num ambiente alargado de parcerias com os nossos aliados por isso a Interoperabilidade assume um papel de destaque na edificação de uma capacidade operacional.

3.CAPACIDADE DE RESPOSTA A INCIDENTES DE SEGURANÇA E O DOTMLPI-I

No ponto anterior foram apresentadas as várias dimensões do modelo DOTMLPI-I, fazendo uma análise básica de cada um dos seus componentes numa vertente de militar. Segue-se uma análise das mesmas dimensões, mas tendo agora por base os conceitos relacionados com a implementação específica de uma capacidade operacional de resposta incidentes no âmbito da Cibersegurança.

DOUTRINA

A existência da Doutrina é fundamental na edificação de uma capacidade de Cibersegurança. Através dela são definidos os objetivos e o âmbito em que se inserem as ações a realizar, contextualizando a existência da capacidade em causa, no panorama global das outras instituições e organizações com responsabilidades idênticas e que têm necessariamente de interagir entre si. Dependendo do contexto em que a capacidade se insere, os documentos doutrinários são tipicamente as leis nacionais que regulam as atividades no Ciberespaço, as Estratégias Nacionais para a Cibersegurança, que definem os objetivos do Estado ou das Organizações e o seu âmbito de atuação no Ciberespaço, bem como os documentos doutrinários que definem as políticas de utilização do mesmo e o modo como interagir com os diferentes atores neste domínio. A ausência destas políticas provoca ambiguidades e reduzem a eficácia de uma efetiva capacidade de Cibersegurança. Ao nível nacional, Estratégia Nacional para a Cibersegurança do Ciberespaço apresenta-se como um importante documento doutrinário, não só pela definição dos objetivos estratégicos do país, mas vai mais longe ao apontar de forma inequívoca as orientações para a sua concretização.[4] Apresenta-se ainda como exemplo de documentos doutrinários a Lei do Cibercrime [14], que regula a utilização da informática e criminaliza as atividades ilícitas de natureza cibernética (em complemento a outros crimes já tipificados no Código do Penal), a publicação do Estado Maior General das Forças Armadas PEMGFA/CSI/301 que estabelece a estrutura orgânica, as normas e os procedimentos para garantir a Capacidade de Resposta a Incidentes de Segurança Informática das

[4]A estratégia nacional de segurança no ciberespaço apresenta como principais eixos de intervenção a "Estrutura de segurança do ciberespaço", o "Combate ao cibercrime", a "Proteção do ciberespaço e das infraestruturas", a "Educação, sensibilização e prevenção", a "Investigação e desenvolvimento" e a "Cooperação" [6].

Forças Armadas ou a sua equivalente PCA 16 sobre a Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha.

ORGANIZAÇÃO

A Organização de uma capacidade de Cibersegurança, no seu sentido mais lato, não difere da organização de outras capacidades. Importa definir uma estrutura organizacional que suporte as diferentes atividades que se pretendem implementar e as respetivas relações e dependências hierárquicas e funcionais. Tipicamente existe um nível superior de decisão e coordenação geral, que poderá agregar as atividades que mais se afastam da sua natureza funcional em órgãos de apoio, como por exemplo a assessoria jurídica ou financeira e a gestão do pessoal. No caso de uma capacidade de Cibersegurança é natural que as diferentes valências técnicas e funcionais se organizem em departamentos com objetivos comuns. Como exemplo apresentamos a necessidade de existência de um departamento de operações no ciberespaço que inclua a gestão de incidentes, um departamento para a definição de políticas e normalização, com uma área de auditoria, que deverá ser independente de todas as outras, com a função de validar o cumprimento das normas, um departamento para a gestão da configuração e apoio técnico aos sistemas e às comunicações com um serviço de *helpdesk.*

TREINO

O Treino é um domínio essencial do modelo para a manutenção e desenvolvimento de uma capacidade. No caso particular do nosso objeto de estudo, a capacidade de respostas a incidentes de segurança é apresentada com objetivos de treino muito concretos, os quais importa que as equipas e a própria organização atinjam, pois são determinantes para garantir esta capacidade. A capacidade de resposta a incidentes de segurança depende fortemente de equipas com a formação adequada e com processos de atuação perfeitamente interiorizados, pois em algumas situações de elevado risco, a garantia da qualidade da informação depende de uma ação pronta e eficiente. A OTAN organiza anualmente exercícios de natureza cibernética para treino das suas estruturas. Nos exercícios denominados *Cybercoalition*, a OTAN define como objetivos principais de treino a Capacidade de Decisão, a Coordenação, a Partilha de Informação e o treino das Capacidades Técnicas [15]. Desta forma assumem-se com principais objetivos de treino a

Capacidade de Decisão com base nas informações disponíveis, escolhendo as melhores ações a realizar perante a natureza do incidente, o que devido à grande variedade de ameaças e de fontes de informação disponíveis, requer um treino específico. Outro aspeto que é essencial treinar, é a Coordenação das equipas e dos vários atores que participam no processo de responder a um incidente. É normal o incidente ser detetado, por exemplo numa plataforma de segurança e que os mecanismos de resposta desencadeados com vista à resolução do incidente ou à mitigação da vulnerabilidade, envolvam entidades externas à equipa que está a gerir o incidente, como por exemplo a equipa de administração dos serviços ou comunicações, sendo fundamental que estas ações sejam bem coordenadas de modo a que atinjam o máximo de eficácia. Na sequência das atividades de coordenação apresentadas, surge como natural o objetivo de treinar a Partilha da Informação. Quando a resposta ao incidente tem de envolver entidades externas é expectável que surjam algumas dificuldades, relacionadas com a utilização de ferramentas e processos distintos, que não permitam uma ação coordenada. Estas dificuldades devem ser detetadas durante as ações de treino, levando à procura e desenvolvimento de processos de comunicação comuns ou pelo menos compatíveis, com vista a uma normalização de procedimentos e de taxonomia. Outro grande objetivo é o treino das Capacidades Técnicas dos vários elementos que compõem as equipas de resposta a incidentes. Para tal é importante que durante o treino sejam simuladas situações tão próximo quanto possível do real, que coloquem os elementos das equipas em situações imprevistas, que os obriguem a explorar completamente as ferramentas que utilizam diariamente, sendo assim possível identificar lacunas na sua formação ou inadequabilidade das ferramentas utilizadas em face da ameaça.

MATERIAL

Como vimos anteriormente, no modelo DOTMLPI-I o Material refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais, desde os equipamentos, à tecnologia e às infraestruturas de comunicações. No caso específico da tecnologia utilizada numa capacidade de resposta a incidentes de segurança da informação, iremos considerar quatro categorias distintas, os equipamentos de

proteção e monitorização que geram a *informação em bruto*[5], os equipamentos que realizam a agregação e arquivo dessa informação e a correlacionam de modo a gerar informação com mais valor, os equipamentos ou tecnologias que permitem fazer a gestão da informação sobre os incidentes, e por ultimo, as tecnologias de análise que permitem a investigação do incidente, nomeadamente a investigação forense.

Na primeira categoria temos então os diferentes equipamentos e tecnologias que a organização utiliza, com o objetivo de proteger a informação e as comunicações, adotando estratégias de defesa em profundidade que passam também por estabelecer perímetros de segurança lógicos e físicos, segmentando a infraestrutura da informação em níveis de grau de segurança distintos. Para obter este efeito utilizam-se equipamentos de proteção do tipo *firewall* para controlar e filtrar o acesso aos fluxos de informação entre os diferentes níveis. A comunicação entre níveis é inevitável, bem como a disponibilização e o acesso de serviços de e para o exterior da organização, utilizando-se tecnologias que permitem a autenticação dos utilizadores, que definem diferentes graus de autorização, bem como o registo de toda a atividade realizada. Outra ferramenta que é indispensável na estrutura de segurança da organização, são os equipamentos de inspeção e prevenção do tipo IPS[6] que analisam todo o tráfego dados que circulam na rede, detetando padrões de comportamento potencialmente perigosos, podendo agir preventivamente através do bloqueio automático dessas comunicações. Consideramos ainda nesta categoria as tecnologias de anti *malware* como sejam os programas de antivírus de gestão centralizada ou as plataformas de proteção de correio eletrónico. A utilização destas ferramentas permite ter um conhecimento situacional do ciberespaço da organização, através da análise da informação disponibilizada através dos vários registos de atividade (*logs*) ou dos quadros informativos que disponibilizam.

O conjunto de equipamentos e tecnologias que protegem a informação da organização, abordados no parágrafo anterior, geram eventos de informação em tal quantidade que numa organização de média dimensão (cerca de 8000 utilizadores) pode chegar facilmente aos 1000 eventos por segundo, tornando impossível um tratamento eficaz da informação recebida, que permita realmente saber o que está a

[5] Por informação em bruto entendemos a informação tal como é gerada pelos equipamentos de segurança, ou seja, não foi alvo de qualquer tratamento prévio, servindo como exemplo os registos de atividade, de comunicações ou processamento de informação, normalmente designados por *logs*.
[6] IPS - Intrusion Prevention System

acontecer na infraestrutura de informação e comunicações da organização. Para solucionar estes problemas são utilizados os equipamentos da segunda categoria indicada anteriormente. As tecnologias de *Security Information and Events Management* (SIEM) permitem agregar toda a informação gerada nas várias plataformas de segurança, correlacioná-las entre si e com outras fontes de informação externa, como a análise de vulnerabilidades ou informações de inteligência.[7] Assim, os milhares de eventos são transformados em algumas poucas dezenas de potenciais incidentes. Caberá à equipa de resposta a incidentes analisá-los, classificá-los e reagir no caso de estarmos perante um verdadeiro incidente. Os equipamentos que implementam esta tecnologia têm também a capacidade de armazenar os vários registos que recebem, no seu formato original, servindo como fonte de evidências com valor legal, no caso de uma investigação para apuramento de responsabilidades.

A categoria de tecnologias que permitem fazer uma efetiva gestão do incidente está relacionada com a necessidade de existir uma plataforma única que permita seguir o incidente ao longo de todos o seu ciclo de vida, registando todas as ações com este relacionada, desde o relato dos eventos, as ações de triagem realizadas e que levaram à sua escalada para incidente. Nesta plataforma são igualmente registadas as várias ações e iterações efetuadas com vista à resolução do incidente pelos técnicos intervenientes no processo e finalmente as recomendações ou lições aprendidas. Toda esta informação é assim registada numa plataforma associada a uma base de dados, com um interface que permite registar todas as ações relativas à gestão do incidente[8]. Algumas plataformas deste tipo têm também associado um sistema de seguimento das várias ações realizadas, por quem as realizou, disponibilizando ainda um conjunto de ferramentas básicas de apoio à gestão do próprio incidente.[9]

Na última categoria consideramos os equipamentos ou tecnologias utilizados para a análise dos dados e informações disponíveis, com vista à investigação das causas e os efeitos, provocados pelo incidente. Para identificar todos os acontecimentos

---

[7] Estas informações de inteligência, conhecidas por Cyberfeeds, são informações recolhidas e divulgadas em tempo quase real sobre eventos de segurança, recolhidos em todo o mundo e pre-processados para as organizações subscritoras destes serviços [16].

[8] Devido à potencial importância da informação recolhida, relevamos a necessidade de existirem mecanismos de salvaguarda da informação armazenada, recorrendo a tecnologias de *backup* e a procedimentos de *disaster recovery*, que deverão ser testados periodicamente.

[9] O *Request Tracker for Incident Response* (RTIR) é uma das plataformas mais populares de gestão de incidentes, possuindo um sistema de seguimento das ações realizadas e por quem (*tickting)*, apresentando um *workflow* próprio para apoio à gestão de incidentes [17].

relacionados com um incidente, é necessário utilizar tecnologias que permitam capturar e analisar pacotes de dados, analisar as configurações base dos sistemas de informação, bem como detetar as alterações introduzidas nos sistemas de ficheiros ou nos registos de configuração dos sistemas operativos, no decorrer do incidente. As plataformas que implementam estas tecnologias têm de estar preparadas para lidar com enormes quantidades de dados, em diversos formatos, e ainda de recolher evidências sem introduzirem qualquer alteração à informação original, para não comprometer a utilização da informação recolhida, no âmbito de uma possível investigação legal.[10]Este material deve estar disponível no local principal de trabalho da equipa de resposta a incidentes, no entanto deve também de existir sob a forma de *Kit* de investigação forense, que seja transportável, para permitir a mobilidade dos técnicos da equipa, mantendo toda a sua operacionalidade ou seja, a capacidade de recolher e investigar evidências.[11]

LIDERANÇA

Na edificação de qualquer capacidade, o fator Liderança apresenta-se sempre como um fator muito importante. No caso da Capacidade de Resposta a Incidentes de Segurança da Informação, existe como fator determinante a abrangência da ação da equipa de resposta, e o impacto das suas ações de forma transversal em toda a organização. Assim, é muito importante que a implementação desta capacidade tenha o apoio inequívoco dos líderes da própria organização. Por outro lado, esta é uma capacidade que está associada a uma forte componente tecnológica, como tal é fundamental a preparação das chefias das equipas para uma abordagem profissional das operações, ou seja, ao desenvolvimento da competência profissional para comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão. Nesta perspetiva, o líder da equipa é visto mais como um decisor que tem de possuir um conhecimento holístico da estrutura da organização e dos seus sistemas. A tomada de decisão ocorre

[10] O *Forensic ToolKit* (FTK) é uma das plataformas mais completas, incluindo funções muito variadas para a investigação forense, como por exemplo a recolha e análise do conteúdo de memória RAM, suporta a análise de todos os sistemas de ficheiros mais importantes, ferramentas de apoio à desencriptação de informação, cópia integral de discos entre outras [18].

[11] Devido à importância destas ferramentas para o sucesso da investigação, consideramos de particular importância mantê-las sempre atualizadas, quer do ponto de vista de segurança (eg atualizações do fabricante), quer do ponto de vista tecnológico.

muitas vezes em plena ação e desenvolvimento dos acontecimentos, sendo assim importante que o líder esteja preparado para lidar com a gestão de crises no seu ciberespaço organizacional, que conheça os fatores que afetam e irão ser afetados pela sua decisão, de maneira a que o habilite a tomar decisões prontas e fundamentadas. No apoio ao líder podem existir sistemas de apoio à decisão baseados em multicritérios que não serão abordados no âmbito deste trabalho.

Outro ponto que assume especial importância, na gestão da capacidade de resposta a incidentes de segurança, está relacionado com o posicionamento do líder e da sua equipa, na estrutura hierárquica da organização. Devido à abrangência das ações a realizar no âmbito da auditoria aos sistemas e análise de vulnerabilidades, transversal aos vários departamentos, parece-nos particularmente importante assegurar na estrutura da organização, a total separação entre a equipa responsável pela gestão de incidentes e as equipas responsáveis pela administração e configuração dos sistemas de segurança e de suporte aos serviços. Esta separação evita situações de conflito de interesse entre os membros das duas equipas e evita situações de "promiscuidade" técnica, como por exemplo o de um técnico ter de avaliar a vulnerabilidade de um sistema por si configurado. Finalmente, as ações e as recomendações relativas à segurança da informação, resultantes da análise de vulnerabilidades, da avaliação do risco e das lições aprendidas, devem ter um peso institucional elevado, devendo por isso o líder e a sua equipa estarem posicionados na dependência direta da Direção da organização.

PESSOAL

Numa capacidade de resposta a incidentes de segurança, mesmo existindo todo o material necessário para a sua operacionalização, o Pessoal ou fator humano é determinante, pois tem sempre de existir uma fase muito importante de análise e decisão das ações a seguir. A organização deve disponibilizar os elementos mais capazes para o desempenho das tarefas a realizar, garantindo que estes são possuidores das qualificações técnicas necessárias para o desempenho da missão. Neste sentido é particularmente importante definir os diferentes papeis que cada membro da equipa terá de desempenhar, aprovar o percurso de formação necessário para o desempenho dessas funções e selecionar os elementos. Nas organizações em que existe implementado o conceito de rotatividade de pessoal, é importante garantir a

estabilidade dentro das equipas de resposta a incidentes, devido à especificidade das suas ações e da sua formação técnica.

O número e a especialização dos elementos da equipa está obviamente dependente, da estrutura definida para a capacidade que a organização pretende implementar. Uma estrutura exclusivamente interna à organização, com uma configuração centralizada, terá necessidades de pessoal diferentes, de outra de configuração distribuída ou então apoiada por entidades externas.[12]

Tomando como exemplo uma estrutura de resposta a incidentes interna à organização e centralizada, que será a que melhor se adapta à organização fortemente hierarquizada e centralizada da infraestrutura de Tecnologias da Informação e Comunicações (TIC) da Marinha Portuguesa, segundo *Killcrece et al* [19] a estrutura deverá ser composta por um gestor (garantindo um elemento alternativo para assumir as suas funções), um elemento administrativo e a equipa técnica com formação que lhe permita assegurar os serviços a que a equipa tem de responder, em numero suficiente para garantir a operacionalidade desejável de 24x7x365. São ainda apresentados exemplos de outros papéis a serem preenchidos como o de apoio jurídico, o de investigador ou de relações públicas que por não terem caracter permanente não são considerados como responsabilidade direta da equipa.

Killcrece et al [20] identifica como principais fatores para o pessoal, a variedade de competências. As equipas de maior sucesso caracterizam-se por serem dedicadas, inovadoras, flexíveis, analíticas, orientadas para a solução, bons comunicadores e capazes de trabalhar em situações de *stress*. *Killcrece* destaca ainda competências técnicas necessárias, ao nível de experiência na administração de redes e de sistemas, experiência em diferentes sistemas operativos, compreensão básica de protocolos de *Internet* e conhecimento básico sobre os ataques mais comuns a computadores e sobre vulnerabilidades. Na área mais específica da segurança, indica como fatores importantes, a experiência na gestão de incidentes e a capacidade de resolver os problemas.

[12] A universidade de Carnegie Mellon apresenta cinco modelos de organização diferentes para as equipas de resposta a incidentes de segurança, o modelo "equipa de segurança", o modelo interno distribuído, o interno centralizado, um modelo interno misto centralizado e distribuído, modelo coordenador [19].

INFRAESTRUTURAS

Uma capacidade de resposta a incidentes de segurança da informação não é muito exigente ao nível das Infraestruturas requeridas. Atendendo a que a informação a proteger tem diferentes níveis de segurança, que implicam muitas vezes a segregação física ao nível da própria infraestrutura, é essencial que essa segregação se estenda até ao local onde a equipa de resposta a incidentes monitoriza e analisa os diversos eventos, bem como ao armazenamento da informação relativa aos incidentes de segurança. Assim, nesta dimensão consideramos como fator mais importante, a segurança física das instalações. O edifício onde está operar a equipa de resposta a incidentes, para além da necessária proteção elétrica que permita manter a operar os seus sistemas, mesmo em caso de corte de energia[13], e das condições ambientais, terá também de possuir comunicações redundantes, áreas de segurança para a operação dos sistemas, com os devidos mecanismos de controlo de acessos e de videovigilância.

INTEROPERABILIDADE

A Interoperabilidade é fundamental no processo de responder aos incidentes de segurança da informação de modo eficaz e eficiente, de forma a não só resolver o incidente e recuperar a operacionalidade, mas também a mitigação das vulnerabilidades. É um processo complexo que muitas vezes envolve não só a própria organização mas também entidades externas, sejam elas prestadoras de serviços de comunicações, serviços de internet, ou mesmo entidades congéneres. Estas entidades externas naturalmente terão os seus processos próprios de operação, com procedimentos e taxonomias diversas das nossas. As ameaças cibernéticas à segurança da informação são globais e na maioria das vezes afetam todas as organizações, independentemente da sua natureza ou área de negócio. O estabelecimento de relações de confiança entre as várias entidades responsáveis por assegurar a resposta a incidentes de segurança, permite a partilha de informação e mesmo de apoio mútuo, na resolução de incidentes de natureza global, permitindo assim um conhecimento situacional do ciberespaço que vai para além do da própria organização. Para que estas partilhas de informação sejam possíveis, é necessário

[13] O edifício deverá apresentar duas linhas principais de energia elétrica, uma associada a sistemas de proteção do tipo U*ninterrupted Power Supply* (UPS), ao qual se associaram todos os sistemas críticos para a operação, e outra associada a um sistema de mecânico de geração de energia.

estabelecerem-se não só as já referidas relações de confiança mas também mecanismos que permitam a comunicação clara, com procedimentos e taxonomias comuns.[14]

4.CONCLUSÃO

A análise que realizámos das diferentes dimensões DOTMLPI-I com base os conceitos relacionados com a implementação de uma capacidade operacional de resposta incidentes no âmbito da Cibersegurança permitiu identificar alguns dos aspetos essenciais à implementação de uma capacidade desta natureza. Da Doutrina é relevada a importância de estarem definidos os princípios legislativos, que irão enquadrar a ação da equipa de resposta a incidentes relativamente aos seus objetivos e o âmbito da sua ação. A Organização é muito importante nomeadamente na articulação e comunicação da capacidade dentro da própria organização. Do Treino sobressai como mais importante a realização de exercícios à escala nacional e internacional que permitam testar e desenvolver competências ao nível da capacidade de decisão, coordenação, partilha de informação e capacidades técnicas. O Material na capacidade de resposta a incidentes assume relevância no sentido que devem de existir os meios necessários que permitam a monitorização do ciberespaço com mecanismos de deteção e registos de eventos, que eventualmente escalarão para incidentes, assegurando os meios para os acompanhar ao longo do seu ciclo de vida. Da Liderança destaca-se a importância de os níveis superiores de chefia da organização estarem envolvidos em todo o processo de edificação da capacidade, apoiando o seu desenvolvimento, motivados pela sua necessidade operacional, dotando-a dos recursos humanos e materiais necessários. Para que esta capacidade seja efetiva, os recursos ao nível do Pessoal devem possuir a formação e o treino que permitam alcançar com sucesso os objetivos elencados na Doutrina, sendo muito importante conseguir garantir a estabilidade das equipas. A Interoperabilidade assume-se como vital na construção da Capacidade de Resposta a Incidentes de

[14] Como exemplo do esforço de criação de uma verdadeira interoperabilidade a nível nacional, temos o exemplo da Rede Nacional de CSIRT que possui mais de vinte membros efetivos, abrangendo um vasto leque de entidades, que inclui o Centro Nacional de Cibersegurança, as Forças Armadas, vários operadores públicos de telecomunicações, Bancos e instituições universitárias. A Rede assume-se como "fórum de cooperação entre equipas de resposta a incidentes de segurança informática (CSIRT)" tendo acordado entre os seus membros os "termos de referência" que permitirão garantir as condições para uma verdadeira Interoperabilidade [21].

Segurança. A complexidade de muitos dos ataques cibernéticos faz com que apenas uma ação concertada de várias entidades permita a sua mitigação. Por outro lado, a partilha de informação e conhecimentos é determinante na construção de um conhecimento situacional do Ciberespaço. A verdadeira Interoperabilidade apenas se concretiza se estiverem considerados dois elementos chave: a existência de relações sólidas de confiança entre os diversos atores que contribuem para a Cibersegurança e os mecanismos de comunicação compatíveis (plataforma de comunicação segura, taxonomia, comum, entre outros).

A metodologia DOTMLPI-I, desenvolvida para a identificação dos elementos críticos de uma capacidade operacional de natureza militar, mostra-se assim igualmente eficaz quando aplicada à Cibersegurança, nomeadamente na edificação de uma resposta a incidentes de segurança da informação.

REFERÊNCIAS

[1] NATO. (2014). NATO Cyber Defence Taxonomy and Definitions. Norfolk: Consultation, Command and Control Board (C3B).

[2] Bravo, R. & Matias, A. (18 de 10 de 2014). Geopolítica, geoestratégia e ciberespaço: Notas introdutórias. Obtido de academia.edu: http://www.academia.edu/ 5543845/Geopolitica_geoestrategia_e_ciberespaco Notas_introdutorias.

[3] IDN, I. d. (2013). Estratégia da Informação e Segurança no Ciberespaço. Obtido de idn.gov.pt: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

[4] EC, E. C. (2013). Cybersecurity Strategy of European Union: An Open, Safe and Secure Cyberspace. Bruxelas.

[5] DR, D. d. (2014). Instalação do Centro Nacional Cibersegurança, DR, 1.ª série - N.º 89 - 9 de maio de 2014. Lisboa: Assembleia da República.

[6] DR, D. d. (2015). Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015. Lisboa: Assembleia da República.

[7] ACQuipedia. (30 de junho de 2005). DOTMLPF.P Analysis. Obtido em 29 de outubro de 2014, de ACQuipedia: https://dap.dau.mil/acquipedia/Pages/ ArticleDetails.aspx?aid= d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2.

[8] DoD, D. o. (2013). Guidance for development and implementation of joint concepts. Chairman of the Joint Chiefs of Staff.

[9] NATO. (2010). NATO Concept Development and Experimentation (CD&E) Process MCM-0056/2010. NATO.

[10] NATO. (2009). Policy for NATO concept development and experimentation MC 0583. NATO.

[11] E-Maps. (22 de agosto de 2013). DOTMLPF-P. Obtido em 03 de novembro de 2014, de e-mapsys: http://www.e-mapsys.com/ DOTMLPFP(3).pdf.

[12] Bergamini, C. (maio/junho de 1994). Liderança: A administração do sentido. Revista de Administração de Empresas, pp. 102-114.

[13] NATO. (2014). AAP-6 NATO Glossary of Terms and Definitions. NATO.

[14] DR, D. d. (2009). Lei do Cibercrime, Lei nº 109/2009 de 15 de Setembro. Lisboa: Assembleia da República.

[15] NATO. (2014). Cyber Coalition CC14 Training Objectives. NCIA.

[16] Anubisnetworks. (2015). Cyberfeed. Obtido em 17 de janeiro de 2015, de anubisnetworks.com: https://www.anubisnetworks.com/products/threat-

intelligence/cyberfeed.

[17] JANET. (s.d.). RTIR incident handling work-flow. Obtido em 17 de janeiro de 2015, de bestpractical.com: https://www.bestpractical.com/static/rtir/janet-workflow.pdf.

[18] Accessdata. (2015). Forensic Tool Kit. Obtido em 17 de janeiro de 2015, de accessdata.com: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.

[19] Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). Pittsburg: Carnegie Mellon.

[20] Killcrece, G., & Ruefle, R. (2008). Creating and Managing Computer Incident Response Capability (CSIRTs). Pittsburg: Carnegie Mellon University.

[21] RCTS. (2015). Serviço de Resposta a Incidentes de Segurança da RCTS - objetivos. Obtido em 18 de janeiro de 2015, de cert.rcts.pt: http://www.cert.rcts.pt/ index.php/rede-nacional-csirt/objectivos.