Proelium X (10) (2016) 141 - 160

Sensibilização e Treino em Cibersegurança - Exercício de Recolha de Informação -

José Martins [1a], José Silva [2b], Carlos Pimentel [3b], António Galindro [4c], João Rocha [5c], Marco Custódio [6c]

[a] Departamento de Ciências e Tecnologias de Engenharia, Academia Militar & Empresa "FeelSec"

[b] Departamento de Ciências e Tecnologias de Engenharia, Academia Militar

[c] Departamento de Ciências Exatas e Naturais, Academia Militar

RESUMO

Este artigo apresenta um método de planeamento para a execução de exercícios académicos de recolha de informação através do ciberespaço, e centrados na sensibilização e treino em cibersegurança dos colaboradores de uma organização. Está orientado principalmente para as organizações que procuram realizar a sensibilização e treino dos colaboradores de modo a mitigar o risco de obtenção e divulgação da informação classificada da sua organização por parte de uma organização oponente. A importância deste estudo é fundamental pois as organizações necessitam cada vez mais de optar por formações ajustadas a problemas concretos, à sua especificidade, e de medir o retorno dos seus investimentos em segurança da informação.

O *design* do método de planeamento proposto tem por suporte uma revisão de literatura e a realização de um exercício académico de recolha de informação realizado no âmbito da Academia Militar / Exército Português. É um trabalho em progresso, onde através do método de investigação *Action Research* se procura identificar as principais fases, atividades e tarefas do método. Está ligado à prática do "saber fazer", sendo necessário a realização de mais instâncias do exercício, em organizações com diferentes topologias, para a sua validação.

Como principais resultados obtidos da realização deste tipo de exercício salientam-se, a importância: (i) do treino individual na utilização das aplicações necessárias para recolha de informação; (ii) da forma de organizar o grupo para executar

[1] Contactos: Email – jose.carloslm@gmail.com

[2] Contactos: Email – jose.silva@academiamilitar.pt

[3] Contactos: Email – pimentel.cam@gmail.com

[4] Contactos: Email – ajog1964@gmail.com

[5] Contactos: Email – rocha.jppb@mail.exercito.pt

[6] Contactos: Email – mpmcustodio@gmail.com

Recebido em 18 de setembro de 2015 / Aceite em 30 de outubro de 2015

as atividades; (iii) e dos colaboradores possuírem conhecimentos técnicos do funcionamento das Redes de Computadores e da Internet, com especial atenção para os protocolos utilizados (por exemplo, o TCP-IP) e tecnologias de suporte (por exemplo, ativos de rede, *firewalls*).
Perceciona-se ainda que numa primeira iteração deste tipo de exercícios é preferível: (i) a sua execução em ambientes virtuais, em virtude de se notar algum receio dos participantes em interagir com a organização real (alvo), face à sua inexperiência na utilização das ferramentas disponibilizadas; (ii) utilizar grupos de reduzida dimensão para permitir uma melhor interação entre os seus membros (e.g., três a seis pessoas); (iii) necessidade de software de *business intelligence* para integrar e analisar a informação recolhida.
Este artigo procura lançar as bases para o *design* de um método de planeamento para execução de exercícios académicos de cibersegurança focados na recolha de informação ao nível organizacional, e em partilhar lições aprendidas com outras organizações militares e civis.

Palavras-Chave: Exercício de Cibersegurança, Sensibilização e Treino, Cibersegurança, Segurança da Informação, Recolha de Informação.

ABSTRACT

This article seeks to establish a framework of planning cyber security academic exercises, focused on gathering information at the organizational level, and to share lessons learned with other military and civilian organizations.
This paper presents a method of planning academic exercises of collecting information through cyberspace. The focus is to raise the awareness of employees in cyber security and train the employees in this area. It is mainly oriented to organizations looking for improving awareness and training of employees in order to mitigate the risk of obtaining and disclosure of classified information of your organization. The importance of these exercises is fundamental because organizations increasingly need to adjust training to real problems, and be able to measure the return of the investment in information security.
The design of the proposed planning method is supported on literature review and in the completion of an academic exercise carried out in the Portuguese Military Academy. It is a work in progress, which through Action Research method is sought to identify the main phases, activities and tasks of the method. It is based in the "know-how" practice, being necessary to carry out more instances of the exercise, on organizations with different topologies, for an academic validation.
The main results obtained with the exercise are: (i) the importance of the individual training in the use of the necessary applications to collect information; (ii) the correct role distribution to the group elements to perform the activities; (iii) the employees must have technical knowledge of the operation of Computer

Networks and the Internet, with special attention to use the protocols (eg TCP-IP) and supporting technologies (eg, network assets, firewalls).
In the first trial of this type of exercise is advisable: (i) its performance in virtual environments, some participants are afraid to interact with the real organization (target), because their inexperience in use of the available tools; (ii) use small groups to allow a better iteration among its members (eg, three to six people); (iii) the need of business intelligence software to integrate and analyze the information collected.

Keywords: Cyber Security Exercise, Awareness and Training, Cyber Security, Information Security, Information Retrieval.

1. INTRODUÇÃO

A segurança da informação é fundamental para as organizações (Andress: 2011) (Whitman e Mattord: 2012), em especial para a militar, consequentemente deve ser mitigado o risco da recolha de informação através do ciberespaço por parte de um adversário, de modo a evitar a sua superioridade de informação, ou seja, deve-se garantir a capacidade operacional de uma organização recolher, processar e disseminar um fluxo ininterrupto de informação, enquanto se explora ou nega a capacidade de um adversário fazer o mesmo.
A gestão eficaz da informação nas suas múltiplas dimensões, como seja a preservação da informação das nossas forças e a disrupção dos sistemas do adversário, é um multiplicador de força que aumenta significativamente o potencial de combate dessa força e amplifica a probabilidade de sucesso do cumprimento da missão.
O ciberespaço levanta desafios novos e complexos à segurança da informação para as organizações e Estados (Martins: 2014) pela possibilidade de um adversário anónimo, sem restrições temporais e geográficas explorar as vulnerabilidades dos componentes principais dos seus Sistemas de Informação (SI). Consequentemente pode atingir as propriedades de segurança da informação, a confidencialidade, a integridade e a disponibilidade (Dhillon: 2007) (ISO / IEC 27001, 2013) (Pfleeger & Pfleeger: 2007).
Os efeitos de alguns dos métodos de ataque lançados através do ciberespaço e suportados essencialmente nas Tecnologias de Informação (TI) foram observados no ciberataque lançado contra a Estónia em abril e maio de 2007, que levaram à paralisação de praticamente todas as atividades do Estado (Tikk: 2008) e no conflito da Geórgia em 2008 (Tikk, et al.: 2008). Perspectivam-se também nas possíveis capacidades de alguns países para a condução de *Cyber Warfare e de Computer Network Operations* (Andress & Winterfeld: 2011) (Carr: 2012) (JP 3-12: 2013).
Podem identificar-se múltiplos e diferenciados métodos de ataque através de diferentes taxonomias, como seja a *Common Attack Pattern Enumeration and Classification* (CAPEC), de *framework*s de testes de penetração (NIST 800-115: 2008), de certificações reconhecidas pela indústria (e.g., a *Certified Ethical Hacker*) (Walker: 2012) ou em relatórios internacionais (Ponemon. 2012) (Symantec: 2014).

Documentos estes que transmitem uma visão geral sobre as modalidades de ação de um adversário e consequentemente permitem orientar a organização no treino individual e coletivo dos seus colaboradores.

Embora exista uma multiplicidade de ações possíveis de serem realizadas por um adversário, um aspeto central para o planeamento e execução de um método de ataque por parte de um adversário é a necessidade de conhecer o oponente (ou seja, a organização alvo). *SunTzu*, na sua obra, A Arte da Guerra, afirmava que "*Conhece o teu inimigo e conhece-te a ti próprio e em cem batalhas nunca serás derrotado. Se não conheces o teu inimigo e apenas te conheces a ti mesmo, por cada vitória sofrerás uma derrota*".

O sucesso nos conflitos militares depende da obtenção de informação acerca do adversário e da cada vez mais eficiente utilização das Tecnologias de Informação (Arquilla & Ronfeldt: 1999). Um dos manuais de Operações de Campanha do Exército Português refere que "*a informação constitui um fator que não pode deixar de ser tido em conta no ambiente operacional moderno, que faz sentir a sua importância de três formas distintas: (i) Na capacidade de a ela aceder; (ii) Na capacidade em a negar ao adversário; (iii) Na capacidade em disponibilizar ao adversário a informação que nos interessa que ele obtenha*" (RC130-1, 2005: 2.5).

Consequentemente é importante identificar as formas de obtenção de informação no âmbito das organizações militares. De acordo com as caraterísticas da fonte de informação, e segundo uma abordagem militar de pesquisa e tratamento de informação, estas formas de obtenção podem ser divididas nas seguintes categorias (AJP-2.0,2003): (i) HUMINT (*Human Intelligence*): cujo objetivo é a obtenção de informação com origem nos seres humanos (por exemplo, através de ataques de Engenharia Social); (ii) MINT (*Imagery Intelligence*): que visa a obtenção de informação através de satélite ou fotografia aérea (por exemplo, utilizar o google earth); (iii) SIGINT (*Signals Intelligence*): permite a obtenção de informação através da interceção de sinais com origem na emissão de energia eletromagnética (por exemplo, interceção e captura das ondas eletromagnéticas emitidas através de monitores, impressoras); (iv) MASINT (*Measure and Signature Intelligence*): é uma forma de aquisição de informação que não se enquadra na HUMINT, na IMINT e na SIGINT (por exemplo, origem acústica); (v) OSINT (*Open Source Intelligence*): centra-se na obtenção de informação através de fontes públicas (por exemplo, sites na Internet, relatórios, listas telefónicas); (vi) TECHINT (*Technical Intelligence*): foca-se na análise de equipamento e armamento militar (por exemplo, análise da informação armazenada num portátil); (vii) CI (*Counter Intelligence*): inclui todas as ações tomadas para detetar, identificar, rastrear, explorar e neutralizar as atividades de intelligence de organizações amigas, adversários ou inimigos, procurando fundamentalmente contrariar ou neutralizar os esforços de recolha de informação de um oponente.

A história recente tem mostrado que a tipologia dos conflitos tem vindo a alterar-se. Desenrolam-se no seio das populações e apelam massivamente à opinião pública,

pois sabe-se que os decisores políticos relevam a forma como as populações vêm o emprego das Forças Armadas. Como diz a publicação doutrinária do Exército Português, PDE 3-00, "*este facto alterará de modo significativo a forma como as forças armadas poderão aplicar a força militar para alcançarem o sucesso nas suas operações. Embora a guerra continue a ser um conflito de vontades, assume particular relevo a disputa pelo controlo da população*" (2012: 1-7).

Este controlo da população é realizado com a utilização das Operações de Informação, cujo objetivo principal é negar à população em geral a informação divulgada pelo adversário e promover uma informação das nossas forças. As organizações terroristas, os grupos de crime organizado, os grandes grupos económicos ao serviço de interesses não revelados, poderão assumir o poder (ou parte deste) dentro de alguns Estados, e não se coíbem de empregar os meios de comunicação social, as redes sociais e as infraestruturas tecnológicas para atingir os seus fins.

Como refere o PDE 3-00,

> "*para atingir este objetivo as suas operações tendem a evoluir, tornando-se mais sofisticadas e empregando todo o tipo de táticas e técnicas à sua disposição (sejam elas convencionais, não convencionais, irregulares e criminais) tendo como principal objetivo criar condições de instabilidade, procurando afastar o poder legítimo e as suas forças da respetiva população. Uma vez atingido o controlo local, procurarão alargar a sua influência utilizando as redes globais, através de Operações de Informação (INFO OPS - Information Operations), não se coibindo de empregar a violência sempre que necessário, sendo esta empregue sem limitações de qualquer tipo, sejam elas de ordem moral, humanitária ou outras*" (2012: 1-7).

Como exemplo recente pode-se ver as ações de violência extrema do atual denominado "Estado Islâmico" que usa a Internet, as redes sociais e os media como meios de suporte às Operações de Informação. Se lhe for possível negar acesso a estes meios, o seu sucesso será severamente comprometido. Foi com base nestes pressupostos que o grupo de hacktivismo Anonymous declarou ciberguerra ao ISIS.

As Tecnologias da Informação permitem às forças militares aceder, através das operações centradas em rede, a estados de superioridade de informação face ao adversário (AR 25-1, 2013: 2). Para isto ser possível é fundamental que todos os militares estejam cientes das potencialidades e vulnerabilidades dos Sistemas de Informação. "*As forças contendoras lutam continuamente pela obtenção de vantagens no ambiente de informação ao mesmo tempo que conduzem operações de combate. As ações de informação moldam o ambiente operacional e ao mesmo tempo desestabilizam o comando e controlo do adversário ou inimigo* "(PDE 3-00, 2012: 50). Logo a recolha e a análise de informação, bem com a sua segurança são aspetos centrais no planeamento de operações militares. A *Intelligence* Militar

considera o ciberespaço como origem cada vez mais relevante para este processo (JP 2-0: 2013) (JP 3-12: 2013) (Mattern, Felker and Borum: 2014).
Deste modo é crítico a sensibilização e treino dos colaboradores de uma organização militar na atividade de recolha e análise de informação. E fundamental conhecer os modos de atuação do adversário, nesta nova dimensão do campo de batalha, o que vai permitir proteger de forma mais eficiente a organização, mas também possibilitar planear ações futuras sobre um adversário, quer no âmbito de operações defensivas, quer ofensivas.
Só o treino real (ou simulado, através de jogos de guerra) permite obter experiência e partilhar lições aprendidas, i.e., aprender de forma eficiente, o que vai possibilitar alterar o modo de fazer as coisas, a fim de melhorar o desempenho. Pois o valor de uma lição aprendida está na sua implementação em atividades futuras (PDE 0.32.00: 2012).
Tendo em consideração a importância do treino no âmbito desta temática o objetivo central deste artigo é apresentar um método de planeamento para a execução de exercícios académicos de recolha de informação através do ciberespaço, e centrados na sensibilização e treino em cibersegurança dos colaboradores de uma organização. De forma a descrever o método de planeamento e enunciar as lições aprendidas, o artigo está estruturado em cinco seções. Nesta primeira identifica-se e enquadra-se o problema. Na segunda analisa-se a questão da sensibilização e treino dos colaboradores, salientando a importância das organizações possuírem um programa de sensibilização e treino, e ainda se analisam alguns dos principais fatores a considerar nesse programa. Na terceira seção descreve-se o planeamento e a execução de um exercício de recolha de informação através do ciberespaço, realizado numa organização militar (Academia Militar, Portugal). Posteriormente, na quarta seção, discutem-se os resultados obtidos da investigação e por fim apresentam-se os principais resultados da investigação, as limitações do estudo e os trabalhos futuros a realizar.

2. SENSIBILIZAÇÃO E TREINO EM CIBERSEGURANÇA

A sensibilização e o treino dos colaboradores de uma organização, centrado nos modos de atuação do adversário, abordagem tradicional na doutrina militar para o planeamento de operações, é fundamental também em cibersegurança, pois possibilita complementar uma visão mais tradicional, focada na maioria das vezes unicamente na implementação de controlos de segurança da informação e SI. O que possibilita que os colaboradores possam passar a atuar como sensores da organização para prevenir, detetar, deter, desviar, recuperar e reagir a possíveis ataques e consequentemente proteger de forma mais eficiente a organização a que pertencem.
A necessidade da sensibilização e treino dos colaboradores para a cibersegurança é identificada por diversos autores, organizações Nacionais e Internacionais (ISO / IEC 27001: 2013) (SANS: 2015) (Walker: 2012). Identifica-se também uma especial

preocupação com os métodos de ataque de Engenharia Social (Mann: 2008) (Peltier: 2006), especialmente os que utilizam ações ativas de recolha de informação, como seja os ataques de *phishing* ou a exploração das redes sociais.

A primeira fase da execução de um ataque, quer manual, quer automático, através da Internet, passa na maioria das vezes pelo reconhecimento do alvo, ou seja, pela recolha de informação, o que vai possibilitar, posteriormente ao adversário definir cenários de atuação, através da modelação de métodos de ataque (por exemplo, através do uso da técnica de árvores de ataque) (Correia e Sousa: 2010). Consequentemente é fundamental a sensibilização e treino dos colaboradores de uma organização para este tipo de atividades de um adversário, focadas na recolha de informação. Tem ainda a vantagem de poderem ser treinados sem custos elevados, quer pelo reduzido tempo necessário para o seu treino, quer pela possibilidade de utilizar *software open source*.

É essencial que a entidade responsável pelas ações de sensibilização e treino tenha em consideração à partida a diferença entre sensibilização (*awareness* em Inglês) e treino; Awareness: "*which is used to stimulate, motivate and remind the audience what is expected of them*", Training: "*the process that teaches a skill or the use of a required too*l" (Peltier, 2005: 1). Para além disso é ainda importante que ao nível organizacional se considere, para o planeamento e execução, diferentes grupos de formandos (por exemplo, utilizadores no geral, gestores de nível intermédio, utilizadores especialistas de tecnologias de Informação, profissionais da segurança da informação e SI), pois é necessário ajustar a sensibilização e o treino para cada um dos grupos definidos (NIST 800-50: 2003).

Considera-se que para realizar a sensibilização e o treino dos colaboradores é necessário ter em consideração no planeamento os seguintes eixos principais, ou seja, conhecer: (i) os principais componentes de um programa de sensibilização e treino (NICE: 2015) (NIST 800-50: 2003) (NIST 800-16: 2013) (Peltier: 2005) (Siponen: 2001); (ii) O tipo de exercícios que podem ser realizados, i.e., a sua abordagem (ENISA: 2009); (iii) as ações e ferramentas que podem ser utilizadas (Chauhan and Panda: 2015) (Walker: 2012); (iv) e por fim a gestão das lições aprendidas (PDE 0-32-00: 2012).

Deste modo, para realizar a sensibilização e treino dos colaboradores através de exercícios de cibersegurança deve-se ter em consideração os seguintes aspetos principais:

(1) Identificar as competências individuais e coletivas a desenvolver nos colaboradores da organização.
(2) Escolher o tipo e a abordagem do exercício mais adequado à organização e à audiência de treino.
(3) Identificar claramente os objetivos do exercício e as suas métricas de avaliação.
(4) Escolher o cenário geral, as *storylines* e a lista de eventos do exercício
(5) Escolher a organização alvo, ou o ambiente de simulação que a representa.
(6) Identificar e avaliar os riscos da execução do exercício.
(7) Identificar os principais *stakeholders* envolvidos no apoio direto e indireto.

(8) Selecionar os grupos de colaboradores a treinar.
(9) Selecionar a forma de garantir a competitividade entre os grupos.
(10) Identificar o software a utilizar (preferencialmente *open source*).
(11) Definir o processo de planeamento e de execução (ver Quadros I e II).
(12) Elaborar a fita do tempo ajustada aos objetivos definidos de acordo com as listas de eventos a realizar.
(13) Identificar os diversos apoios críticos (por exemplo o suporte logístico).
(14) Identificar e treinar os tutores, ou seja os especialistas que acompanham o exercício.
(15) Obter e gerir as lições aprendidas de modo a partilhar os ensinamentos por toda a organização.
(16) Gerir e classificar toda a informação recolhida do exercício.

Tendo em consideração os aspetos identificados anteriormente planeou-se um exercício de cibersegurança que possibilita aos colaboradores da organização, neste caso particular aos alunos da Academia Militar, percecionar as modalidades de ação do adversário que podem ser executadas para recolha de informação e deste modo sensibilizá-los para boas práticas no âmbito da segurança da informação e da cibersegurança, as quais devem ser responsabilidade de todos os colaboradores de uma organização.

3. EXERCÍCIO DE RECOLHA DE INFORMAÇÃO

O exercício consistiu fundamentalmente na recolha de informação de uma organização, em ambiente de *Competitive Intelligence*, de modo passivo, utilizando ferramentas *Open Source* (Hadnagy, Watson, Mason, Ackroyd: 2014) (Chauhan, Panda: 2015) Walker: 2012) e focado no "*saber fazer*".
Numa organização este tipo de exercício permite motivar os colaboradores para a necessidade do cumprimento das regras internas de segurança da informação, pois possibilita que estes verifiquem a informação que a sua organização na realidade tem disponibilizada ao público em geral e ainda conhecer algumas das principais ações que um adversário pode executar para obter informação da sua organização através de fontes abertas.
No caso da Academia Militar a utilização deste tipo de exercícios é triplamente vantajoso, pois possibilita: (i) motivar os alunos para a temática da segurança da informação e da cibersegurança, complementando a unidade curricular E361 - Segurança da Informação, SI e Ciberdefesa; (ii) prepará-los para executar esta atividade em situações operacionais reais, pois na organização militar cada soldado é um "sensor de recolha e proteção da informação"; (iii) possibilita iniciar a sua preparação no âmbito das *Computer Network Operations*, na vertente ofensiva.

A abordagem deste exercício é a tradicional "*Capture of Flag*", em que se procura obter o máximo de informação de uma organização adversária. Ganha a equipa que obtiver maior pontuação e em caso de igualdade, a equipa que sugerir um método de ataque com maior probabilidade de sucesso.
Tem como principais objetivos: (i) criar e desenvolver competências na área da Segurança da Informação, Sistemas de Informação e Cibersegurança nos discentes da AM; (ii) e fomentar a reflexão e a partilha de conhecimento entre docentes, discentes e as organizações participantes.
A "*Blue Team*". *i.e.*, a equipa das forças amigas, foi constituída por grupos de alunos da AM, com a missão de recolher informação e a "*Red Team*", ou seja, o adversário, é a organização alvo, objeto da ação de recolha.
A execução do exercício decorreu de acordo com seis regras principais: (i) as ações de recolha de informação, antes da sua execução, devem ser aprovadas pelo tutor (docente especialista que acompanha cada grupo de alunos) e pelo representante da organização alvo, de modo a controlar possíveis riscos operacionais; (ii) é permitida apenas a utilização de fontes abertas, particularmente a Internet; (iii) só é permitida a utilização de aplicações que não interajam com os Sistemas de Informação da organização, de modo a evitar a detecção das ações da "*Blue Team*" pela organização alvo; (iv) respeitar a fita do tempo aprovada para execução do exercício, reforçando a importância da gestão do tempo disponível para planeamento e execução das operações militares; (v) elaborar um relatório final com template aprovado, a entregar ao escalão superior (importância das lições aprendidas); (vi) os documentos com a informação obtida sobre a organização alvo devem ser destruídos ou armazenados com segurança após a realização do exercício (importância da classificação e tratamento da informação).
O planeamento e a execução do exercício foi efetuado de acordo com o processo referenciado no Quadro 1 e as atividades nucleares identificadas no Quadro 2.

Quadro 1: Processo de Planeamento do Exercício	
Objectivo	Recolha e tratamento de Informação da organização alvo através da Internet.
Entradas	Organização alvo; Grupos de alunos participantes.
Saídas	Relatório de lições aprendidas; Questionário de avaliação do exercício.
Controlo	Regras de realização do exercício; Fita do tempo de planeamento e execução; Correta utilização das ferramentas *Open Source* disponibilizadas.
Meios (recursos)	Salas de apoio ao funcionamento do exercício; Rede de computadores com acesso à Internet; Aplicações *Open Source*; Plataforma de apoio aos conteúdos necessários (moodle); Google Survey.
Principais Stakeholders	Organização militar alvo; Tutores (acompanhamento dos grupos de alunos); Avaliadores externos da organização alvo; Entidades da cadeia de comando das organizações participantes.
Identificação e Avaliação dos Riscos	(Omitido por questões de segurança militar)
Documentação Principal	Guião do exercício; Lista de itens de informação a obter pelos alunos; Modelo de relatório de recolha de informação a apresentar pelos grupos; Documentos de suporte ao funcionamento das aplicações utilizadas.

No Quadro 1 identifica-se de modo sumário, o objetivo principal do exercício, as principais entradas e saídas do processo de planeamento, bem com o modo de controlo de execução do exercício. Identificam-se ainda os principais recursos críticos utilizados e as entidades que participam. É fundamental a identificação e avaliação do risco, atividade que foi realizada, mas que por motivos de segurança militar é omitida no artigo. E por fim listam-se alguns dos principais documentos utilizados no planeamento e execução.

No Quadro 2, identificam-se as principais atividades a desenvolver para a realização de um exercício deste tipo. A lista de tarefas não é exaustiva, mas representativa das que foram necessárias desenvolver para esta instância e de algumas que se prevê que futuramente serão realizadas (assinaladas com *).

Quadro 2: Atividades Nucleares de um Exercício Académico de Cibersegurança	
Actividade	**Finalidade**
Gestão de Projetos	Gerir o exercício segundo as boas práticas da gestão de projetos.
Comité de Gestão do Exercício	Nomear e gerir uma equipa responsável pelo planeamento do exercício.
Equipa Operacional	Nomear e gerir uma equipa responsável por operacionalizar o exercício.
Equipas Participantes	Gerir as equipas que participam no exercício.
Tutores e Avaliadores	Selecionar e gerir a equipa que realiza o acompanhamento e a avaliação.
Stackholders	Gerir todas as organizações e entidades nacionais e internacionais envolvidas.
Guião do Exercício	Desenvolver o guião de apoio ao exercício (e.g., cenários, lista de eventos, templates de apoio, software a utilizar, regras).
Identificação e Avaliação do Risco	Identificar e avaliar todo o risco que envolve a realização do exercício (e.g., financeiro, organizacional, de execução).
Laboratórios Virtuais (*)	Desenvolver laboratórios virtuais para treino das tarefas a realizar ao longo do exercício (e.g., software *open source* e máquinas virtuais).
Métricas, Monitorização e *Data Mining* (*)	Definir as métricas de avaliação do exercício, o processo de monitorização e de análise dos dados produzidos.
Análise Forense Computacional (*)	Selecionar e gerir a equipa que identifica e valida os resultados dos métodos de ataque executados.
Logística	Planear e preparar toda a logística de apoio (e.g., instalações).
Cadeia de Comando e Comunicações	Definir a cadeia de comando e os sistemas de apoio ao comando e controlo do exercício (e.g., sistema de vídeo conferência).
Plataformas Colaborativas	Implementar e gerir todas as aplicações de apoio à divulgação de informação relevante para o exercício (e.g., moodle, site de divulgação).
Gestão Documental	Gerir toda a documentação produzida no exercício, de modo a produzir lições aprendidas.
Relações Públicas (*)	Divulgar interna e externamente as atividades executadas (e.g., Estado Maior do Exército, comunicação social, revistas).

A realização deste exercício decorreu em duas fases, numa primeira fase foi efectuada a preparação dos alunos (2º e 3º Ano) para o exercício e numa segunda fase decorreu a execução. A fase de planeamento demorou aproximadamente um mês e a fase de execução teve a duração de três horas.
Salienta-se que: (i) a organização dos grupos foi proposta pelos alunos, tendo a sua maioria três elementos na constituição (sugestão dos responsáveis pelo exercício); (ii) existiu um docente tutor para acompanhar cada turma (com aproximadamente 12 grupos); (iii) já existia um conhecimento do tipo de exercício; (iv) disponham

de uma *framework* conceptual teórica base sobre as temáticas abordadas (ministrada durante a UC E361: segurança da informação, Sistemas de Informação e Ciberdefesa); (v) os alunos possuiam na sua maioria o sistema operativo Windows 7/8 e utilizaram como ambiente de virtualização a Virtual Box; utilizaram para acesso à internet Pen´s de banda larga móvel USB dos próprios.
No final do exercício todos os participantes estiveram presente numa reunião de lições aprendidas e cada grupo de alunos respondeu a um inquérito *online*, o que permitiu obter informação relevante para o planeamento de exercícios futuros. Perspectivaram-se ainda um conjunto de atividades nucleares que permitiria futuramente gerir um exercício académico de dimensão nacional, algumas das quais não foram implementadas no exercício realizado, mas que estão identificadas no Quadro 2.

4. RESULTADOS E DISCUSSÃO

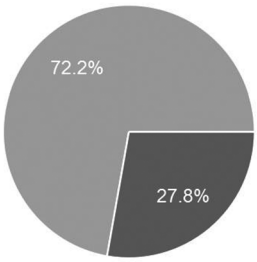
O exercício decorreu com grande empenho dos alunos, sendo este um dos principais objetivos, que consequentemente foi atingido. Face à experiência obtida neste exercício, é importante em futuros exercícios introduzir as seguintes melhorias: (i) realizar ações de formação e treino com as principais aplicações a utilizar, pois verificou-se que uma percentagem elevada dos alunos não tinha instalado e testado as ferramentas recomendadas; (ii) reforçar a prática da utilização das máquinas virtuais nas unidades curriculares E316 e E315; (iii) introduzir e utilizar a *Framework Kali* (testes de penetração) na unidade curricular E361; (iv) utilizar a rede Wifi da Academia Militar; (v) clarificar e introduzir melhorias no documento base para recolha de informação ("Lista de Itens"); (vi) possibilitar a recolha de informação através de ações de Engenharia Social do tipo "humano-humano", via telemóvel ou mail (por exemplo, através de ataques de *phishing*)"; (vii) e utilizar ferramentas de *business intelligence* para agrupar, analisar e apresentar a informação recolhida aos decisores.
Notou-se em diversos grupos uma "*ansiedade*" em ligar diretamente, via telefone, à organização alvo, mas simultaneamente percecionou-se uma certa relutância em usar as aplicações sugeridas, por dois motivos: primeiro, pela necessidade de instalação de software nas máquinas pessoais dos alunos (opção escolhida para facilitar o treino e a execução); em segundo, por questões éticas, pois estes sentiam que estavam a recolher informação, embora autorizada, de uma Unidade Militar.
Em termos gerais, para próximos exercícios, é importante para melhorar os resultados obtidos que (i) que os grupos estejam localizados num único edifício, para facilitar a logística de apoio; (ii) garantir que as salas possuam tomadas de energia eléctrica e pontos de rede em número suficiente; (iii) planear o exercício para uma data onde a solicitação académica aos alunos seja menor (i.e., realização de testes e trabalhos); (iv) introduzir um factor de avaliação académica no exercício; (v) aumentar a duração da reunião de lições aprendidas, de modo a que todos os coordenadores dos grupos possam intervir e manifestar a sua opinião.

4.1 Resultados do Inquérito

Após a realização do exercício com a duração de aproximadamente três horas, os grupos participantes preencheram um questionário online composto por 22 perguntas agrupadas em 4 seções. Os alunos dividiram-se por 18 grupos, sendo cada um composto por 2 a 4 alunos (maioritariamente de três). Cada grupo respondeu ao inquérito, correspondendo a um total de 18 respostas. De uma forma breve, são indicadas as questões mais relevantes. Na primeira seção, para caracterização dos participantes, foram colocadas as questões:

i) Questão: Qual o ano que frequenta?

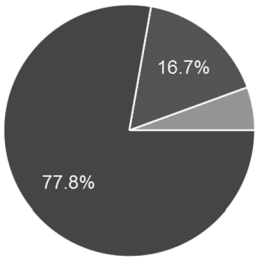
Respostas:	Nº respostas	Percentagem Respostas
2º Ano	5	27.8%
3º Ano	13	72.2%



O número de respostas, muito superior no 3º ano, quando comparado com o 2º ano é justificado por no 3º ano existirem mais alunos a frequentar a Academia Militar. Por outro lado, não existem respostas de outros anos uma vez que no Exercício apenas participaram alunos do 2º e 3º anos.

ii) Questão: Qual o curso que frequenta?

Cursos:	Nº Respostas	Percentagem Respostas
Armas	14	77.8%
Engenharia	3	16.7%
Administração	1	5.6%



A distribuição dos alunos na Academia Militar pelos cursos reflete as necessidades do Exército, sendo notório o predomínio do Curso de Ciências Militares (vulgo Curso de Armas) com especialidades em Infantaria, Cavalaria e Artilharia.

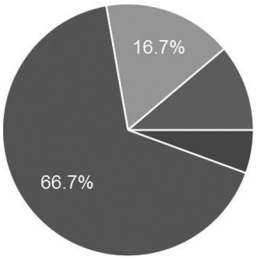
iii) Questão: Como organizou o grupo de trabalho?

Método de Organização	Nº de Respostas	Percentagem Respostas
Divisão do trabalho por todos os elementos do grupo	15	83.3 %
Todos os elementos do grupo procuravam responder a todas as questões	2	11.1 %
Uns procuram respostas e outro regista	1	5.6 %

Permitiu-se aos grupos fazerem a gestão do trabalho da forma que consideravam mais produtiva. Considerando que todos os elementos possuem um grau de conhecimento similar, a opção da quase totalidade dos grupos foi de distribuir o trabalho de pesquisa / recolha de informação, por todos os elementos do grupo.
A segunda seção incluiu perguntas sobre as ferramentas usadas para a recolha de informação. A totalidade dos grupos usaram o Google como o motor de pesquisa preferido. Em complemento, metade dos grupos visitaram o website da organização alvo para obtenção de informação. Note-se ainda que as redes sociais também foram utilizadas por quase metade dos grupos para a obtenção de informação.
A terceira secção incluiu questões relativas ao conhecimento adquirido ao longo do exercício.

iv) Questão: Este exercício foi relevante para a sua formação?

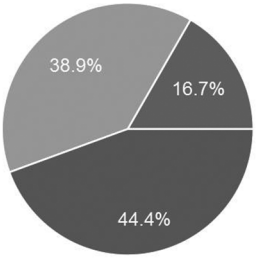
Resposta:	Nº de Respostas	Percentagem Respostas
Pouco útil	1	5.5%
Razoavelmente útil	12	66.7%
Muito útil	3	16.7%
Extremamente importante	2	11.1%



É notório que a quase totalidade dos grupos considerou que o exercício realizado foi útil para a sua formação. Atendendo a este resultado, este exercício será repetido anualmente, com detalhes adicionais, para melhoria da execução e refletir os objectivos / motivações dos participantes.

v) Questão: Aprendeu algo de novo?

Resposta:	Nº de Respostas	Percentagem Respostas
Nada de novo	0	0.0%
Aprendi alguma coisa	8	44.4%
Aprendi diversas coisas novas	7	38.9%
Aprendi muitas coisas novas	3	16.7%



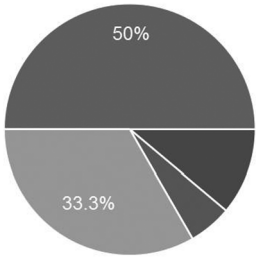
A resposta a esta questão indica que todos os participantes aprenderam algo de novo, o que é motivador para a realização de um novo exercício, na continuidade deste. Observa-se ainda que mais de metade dos participantes aprendeu “diversas coisas novas” ou “muitas coisas novas”, o que sugere que o presente exercício foi um êxito.

vi) Questão: Usou conhecimentos obtidos noutras unidades curriculares?

Cinco grupos responderam a esta questão afirmando que não usaram conhecimentos de outras unidades curriculares, para além da UC E361. Os grupos que usaram conhecimentos obtidos de outras unidades curriculares, indicaram Sistemas Computacionais e de Comunicação (4 grupos), Programação (2 grupos), Base de Dados (1 grupo) e Metodologia da Comunicação (1 grupo). A quarta secção teve como objectivo recolher a opinião dos participantes sobre a duração do exercício, os aspectos que mais / menos gostaram, e ainda quais as espectativas para futuros exercícios.

vii) Questão: A duração do exercício foi:

Respostas:	Nº de respostas	Percentagem respostas
Curta, mas está bem assim	2	11.1%
Curta, e deveria ser mais longa	1	5.6%
Longa, mas está bem assim	6	33.3%
Longa, e deveria ser mais curta	9	50%



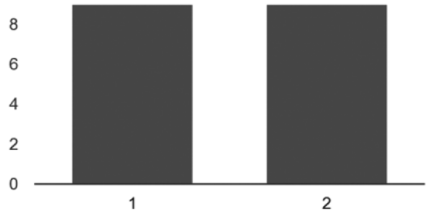
Genericamente os participantes consideraram que a duração do exercício foi longa; de todos os participantes, metade sugere que a duração do exercício deveria ser mais curta. Este resultado é facilmente entendido em virtude de alguma falta de conhecimento e prática na utilização das aplicações.

viii) Questão: O que gostaria de ver explorado num futuro exercício?

As respostas a esta questão foram muito diversas, existindo uma concentração (sete grupos) que sugerem ataques de penetração / obtenção de passwords. As restantes sugestões são: (i) descobrir passwords de emails e de redes sociais (dois grupos); (ii) métodos para proteger a informação pessoal (dois grupos); (iii) recolha de informação de forma ativa (um grupo); (iv) ver em tempo real a execução do exercício (um grupo); (v) obter dados pessoais de colaboradores de uma instituição (um grupo); (vi) recolher mais informação de cariz tecnológico e não tanto informação humana (um grupo).

ix) Questão: As instalações foram adequadas?

Respostas possíveis	Nº de respostas	Percentagem Respostas
1-Sim	9	50%
2-Não	9	50%



No que respeita às instalações as opiniões dos participantes dividiram-se, em que apenas 50% considera as instalações adequadas. Os aspetos que poderão ter influenciado um número considerável de respostas negativas poderá ser a inexistência de ar condicionado, o reduzido número de tomadas eléctricas, e o facto de uma das salas ter sido um anfiteatro.
É relevante ainda mencionar que os participantes têm preferência por um exercício com visualização em tempo real dos progressos efectuados pelos vários grupos, sendo este aspecto uma motivação adicional para acompanhar o desenrolar do exercício.
Estes resultados permitem concluir que o método preferencial de abordagem para a resolução do problema pelos alunos foi "dividir para conquistar", ou seja, repartir as múltiplas tarefas por todos os elementos do grupo tal que seja possível atingir o objectivo no menor período de tempo possível.
Os alunos usaram preferencialmente o Google, talvez por desconhecerem outros motores, apesar de existirem meta-pesquisadores (motores de busca que combinam o resultado de vários motores de busca). As redes sociais (por exemplo, o facebook) também foram usadas para pesquisa, pois permitem explorar a vulnerabilidade de alguns "humanos" que expõem muitos detalhes pessoais e da sua organização nas redes sociais.
Saliente-se que 100% dos participantes afirmou que aprendeu algo de novo e 94% dos participantes considerou este exercício relevante para a sua formação, o que motiva os responsáveis pelo exercício a efectuar diligências para a continuidade e melhoria deste tipo de exercício, refletindo o que os participantes gostariam de explorar em futuros exercícios.

5. CONCLUSÕES

O artigo apresenta um método de planeamento para a execução de exercícios académicos de cibersegurança, focado na recolha de informação através do ciberespaço e divulga algumas das principais preocupações associadas à sensibilização e treino em cibersegurança ao nível organizacional.
Constatou-se que a realização deste tipo de exercícios académicos de abordagem prática são mais motivantes para os discentes (e docentes) do que os de "caneta e papel" e que os discentes ganham reais competências centradas no "saber fazer", pois não basta dizer o que fazer, é necessário executar. Verificou-se ainda a importância do treino individual na utilização das aplicações, antes de iniciar o treino coletivo.
Em próximos exercícios é importante ultrapassar as dificuldades identificadas anteriormente, com especial relevância, para a necessidade de realizar ações de formação e treino com as principais aplicações e explorar ainda durante o exercício os métodos de ataque focados no *Phishing* e na análise das *Redes Sociais*.
É também importante a presença de especialistas militares da área de ciberdefesa

que interliguem os conhecimentos teóricos e práticos ministrados em ambiente académico com as verdadeiras necessidades operacionais do Exército Português. A reflexão dos docentes intervenientes neste exercício (autores do artigo) permite propor desde já melhorias em futuros exercícios para colmatar algumas das deficiências detetadas, que passarão: (i) pela criação de uma atividade extra curricular anual de *Ethical Hacking* que permita desenvolver as competências necessárias aos alunos e futuros oficiais do Exército; (ii) aumentar a coordenação multidisciplinar entre unidades curriculares que possam contribuir para o ensino desta temática; (iii) implementar uma actividade laboratorial para treinar as competências associadas às temáticas da segurança da informação, Sistemas de Informação e cibersegurança (já se encontra em fase de implementação); (iv) estreitar as relações e partilha de lições aprendidas com outras entidades que desenvolvem conhecimento nesta temática.
De modo a optimizar e validar o *método* de planeamento do exercício é necessário a sua execução em diversas organizações, com diferentes topologias no âmbito das Forças Armadas. Em termos de trabalhos futuros é também importante explorar a vertente dos Jogos de Guerra / Simulação e a *Cyber Intelligence*.
Nesta temática só equipas multidisciplinares e com elevada competência técnica, centrada no saber fazer podem ultrapassar os desafios que se colocam em termos de cibersegurança às Organizações e aos Estados.

AGRADECIMENTOS

Um agradecimento especial ao Professor Henrique dos Santos da Universidade do Minho, ao Professor Rui Silva do Instituto Politécnico de Beja (UbiNET), pelas sugestões e ensinamentos partilhados, e ao Centro de investigação Geoespacial do Exército (CIGeoE), na pessoa do Major (Eng.) Francisco Salvador, pelo apoio como representante da organização alvo e pelos conhecimentos partilhados.

REFERÊNCIAS BIBLIOGRÁFICAS

AJP - 2.0 (2003). *Allied Joint Intelligence: Counter Intelligence and Security Doctrine*, NATO.

ANDRESS, Jason (2011). *The Basics of Information Security*, Elsevier.

ANDRESS, J., and Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*: Syngress Media Inc.

Army Information Technology.USA AR 25-1 (2013).

ARQUILLA, J., & Ronfeldt, D. (1999). The Advent of Netwar: Analytic Background, *Studies in Conflict & Terrorism*, 22(3), 193-206.

CARR, J. (2012). *Inside Cyber Warfare* (Second Edition ed.): O´Reilly.

CHAUHAN, Sudhnshu and PANDA, Nutan, Kumar K. (2015). *Hacking Web Intelligence*, Syngress.

CORREIA, M. P., & SOUSA, P. J. (2010). *Segurança no Software*. Lisboa: FCA.

DHILLON, G. (2007). *Principles of Information Systems Security*, Text and Cases, Wiley.

ENISA (2009). *Good Practice Guide on National Exercises*, December, EU.

HADNAGY, Chris, Watson, Gavin, Mason, Andrew and Ackroyd, Richard (2014). *Social Engineering Penetration Testing*, Syngress.

ISO / IEC 27001 (2013). *Information technology – Security techniques – Information Security Management Systems - Requirements*.

JP 2.0 (2013). *Joint Intelligence*, Joint Chiefs of Staff, USA.

JP 3-12 (2013). *Cyberspace Operations*, USA.

MANN, I. (2008). *Hacking the human: Social Engineering Techniques and Security Countermeasures*: Gower Publishing Company.

MARTINS, José Carlos L. (2014). *Método de Planeamento de Segurança da Informação para Organizações Militares em Ambiente de Guerra de Informação*, Tese de Doutoramento, Universidade do Minho.

MATTERN, Troy, Felker, John, Borum, Randy and Banford, George (2014). *Operational Levels of Cyber Intelligence*, International Journal of Intelligence and Counter Intelligence, Nº 27, pp. 702-719.

NICE (2014). *The National Cybersecurity Workforce Framework*, USA.

NIST 800-115 (2008). *Technical Guide to Information Security Testing and Assessment*, USA.

NIST 800-50 (2003). *Computer Security, Tecnology Awareness and Training Program*, USA.

NIST 800-16 (2013). *A Role-Basead Model for Cyber Security Training*, V2.0, USA.

PDE 0.32.00 (2012). *Lições Aprendidas*: Ministério da Defesa Nacional, Exército Português.

PELTIER, Thomas R. (2005). *Implementing an Information Security Awareness Program*, The EDP Audit, Control, and Security Newsletter, Vol. XXXIII, Nº 1.

PELTIER, Thomas R. (2006). *Social Engineering: Concepts and Solutions*, The EDP Audit, Control, and Security Newsletter, Vol. XXXIII, Nº 8.

PFLEEGER, C. P., and Pfleeger, S. L. (2007). *Securiy in Computing*, Prentice Hall, 4ed, United States of America.

PONEMON (2012). *The Human Factor in Data Protection*, Research Report, Ponemon Institute.

RC 130-1 (2005). *Regulamento de Campanha - Operações*. Lisboa: Instituto de Estudos Superiores Militares.

SANS (2015). *Twenty Critical Security Controls for Effective Cyber Defense* (Version 4.1).

SIPONEN, Mikko (2001). *Five Dimensions of Information Security Awareness,* Computer and Society, June 2001, pp. 24-29.

SYMANTEC (2014). *Internet Security Threat Report, 2013 Trends*, Volume 19, Published April 2014.

TIKK, E. (2008). *National Defense Policies for Cyber Space – Background and Effect of the Estonian Cyber Attacks* (Cooperative Cyber Defence Centre of Excellence), Academia Militar, Lisboa, Portugal.

TIKK, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., & Vihul, L. (2008). *Cyber Attacks Against Georgia: Legal Lessons Identified, NATO Unclassified Report v1.0. Tallin*, Estonia: Cooperative Cyber Defense Centre of Excellence.

WALKER, Matt (2012). *Certified Ethical Hacker*, Exam Guide, McGraw-Hill.

WHITMAN, Michael E. and MATTORD, Herbert J. (2012). *Principles of Information Security, Course Technology*, Cengage Learning.

JOSÉ MARTINS

Professor Regente na Academia Militar nas temáticas de Segurança da Informação, Sistemas de Informação e Ciberdefesa. Doutorado em Tecnologias e Sistemas de Informação na área da "Gestão de Segurança da Informação e de SI". É fundador e gestor da empresa FeelSec que se dedica à implementação de programas de sensibilização e treino de SegInfo, SI e cibersegurança em organizações públicas e privadas.

JOSÉ SILVA

É docente do Departamento de Ciências e Tecnologias de Engenharia, da Academia Militar, e lecciona as unidades curriculares Sistemas Computacionais e de Comunicação, Programação de Sistemas e Análise de Circuitos.

JOÃO ROCHA

Professor Regente na Academia Militar nas temáticas de sistemas Operativos e Programação. Engenheiro Electrotécnico Militar interessa-se pelas áreas de data mining, data farming e segurança da Informação. Actualmente é chefe do Departamento de Ciências Exactas e Naturais da Academia Militar (DCEN).

ANTÓNIO GALINDRO

Professor Regente na Academia Militar nas temáticas de Programação, Algoritmos e Estruturas de Dados e Bases de Dados. Mestre em Engenharia Informática, interessa-se pelas áreas de Segurança da Informação.

MARCO CUSTÓDIO

Professor Regente na Academia Militar da disciplina de Introdução à Programação e Professor Auxiliar nas cadeiras de Redes de Computadores e de Tecnologias de Informação e Plataformas de Internet. Mestre em Engenharia Informática e de Computadores. É Tenente-Coronel do Exército Português, a prestar serviço na Direção de Comunicações e Sistemas de Informação.

CARLOS PIMENTEL

Professor Adjunto na Academia Militar nas temáticas de Segurança da Informação, Sistemas de Informação e Ciberdefesa. É Instrutor permanente da GNR nos cursos de Transmissões, Informações e Investigação Criminal. Publicou um livro pela FCA com o título "CyberWar – O Fenómeno, as Tecnologias e os Actores". Interessa-se fundamentalmente pelas áreas de Segurança da Informação e comunicações seguras.