Information & Security

B. Nikolov
vol. 46, no. 1 (2020): 27-35
https://doi.org/10.11610/isij.4602

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

A Concept for Establishing a Security Operations and Training Centre at the Bulgarian Naval Academy

Borislav Nikolov

Nikola Vaptsarov Naval Academy, Varna, Bulgaria
http://www.naval-acad.bg

ABSTRACT:

The provision of cybersecurity is a responsibility not only of the IT department but every employee. Cybersecurity training of IT specialists and cybersecurity awareness for other employees are the first steps in creating effective cyber defence. These two types of educations must be provided in a realistic environment for which the computer virtualization is the best choice. The purpose of this article is to present a concept for building and developing a fully functional Security Operations and Training Centre (SOTC) at Nikola Vaptsarov Naval Academy (NVNA). This SOTC will operate as a training environment for IT specialists and as a Security Operations Centre for the academy's computer network. The author presents all design steps that must be implemented during establishing and enhancing the SOTC at NVNA, including key resource requirements and utilised technologies.

ARTICLE INFO:

RECEIVED: 19 JULY 2020
REVISED: 02 SEP 2020
ONLINE: 15 SEP 2020

KEYWORDS:

cybersecurity, security operations and training centre, cyber range, virtualization, exercise team

Introduction

The digitalization of human life is leading to an increase in cyber threats. The targeted cyber-attacks conducted by hackers are becoming vaster, both in terms of used resources, and in terms of the damage caused. The damage inflicted also has a significant financial impact.

✉ Corresponding Author: nikolov@naval-acad.bg

The cybersecurity of the corporate computer network is the responsibility of all employees, not only the IT department. The high qualification of the specialists from the IT department and the good level of awareness about cybersecurity of the other employees are inseparably connected and are required to achieve a certain level of security for the whole network. To achieve them, periodic training is required. In addition, it is necessary to provide the necessary technical devices to implement the security measures.

There are many cybersecurity training centres in the world. Many of them specialize in a certain field, while others enable their clients to build and use SOC. In order to define the tasks, goals and functionalities for designing and building of a combined training and operational centre, world trends must be taken into account.

The Persistent Cyber Training Environment (PCTE) provides cyber simulations that will allow cyber mission forces from all military branches to train together in a realistic environment. It will support individual instruction and certification to allow cyber operators to practice and rehearse missions simultaneously from locations around the world, meeting the needs of all four services and the U.S. Cyber Command.[1]

Every year, authorized users of the U.S. DoD information systems must complete the Cyber Awareness Challenge to maintain awareness of, and stay up-to-date on new cybersecurity threats. The training also reinforces best practices to keep the DoD and personal information and information systems secure, and stay abreast of changes in DoD cybersecurity policies. Other agencies use the course to satisfy their requirements as well. There is also a Knowledge Check option available within the course for individuals who have successfully completed the previous version of the course. The course [2] provides an overview of cybersecurity threats and best practices to keep information and information systems secure.

The Cyber Awareness Challenge is developed by the Defence Information Systems Agency for the DoD Chief Information Officer.[3] Content is based on input from the Workforce Improvement Program Advisory Council. DoD and other agencies use this course to satisfy mandatory training. The course addresses the DoD 8570.01-M Information Assurance Workforce Improvement Program (WIP), 10 November 2015, incorporating Change 4, Office of Management and Budget Circular NO. A-130, and the Federal Information Security Modernization Act (FISMA) 2014.

The Cyber Awareness Challenge begins with a message from the future describing serious vulnerabilities that were the result of certain decisions made in the present. The student is asked to help prevent these incidents by making proper cybersecurity decisions about events from the evidence provided. Through this process, the student learns proper cybersecurity practices. Students are given the opportunity to take the knowledge check track. This knowledge check option allows users to answer questions related to subtopics in each area. If these questions are answered correctly, students are given credit and are able to move to other subtopics.

Most of the known cybersecurity training centres, including pointed out so far, perform only the function of preparing their clients to deal with cyber-attacks and respond to cyber incidents. Combining the operational work of an SOC with a cybersecurity training centre is extremely rare. For this reason, the building of SOTC at NVNA can be described as an innovative idea with a practical focus.

Security Operations and Training Centre – Purpose and Requirements

The building and commissioning of a centre with both training and operational purposes poses significant challenges. The main question to be answered is what will be the main function of a centre of this type. With an answer of this question, it will be possible to move to the design stage so that the implemented project is as functional and operational in terms of its tasks.

The variety of learning tasks that have to be covered in such type of training centre is a serious challenge at the design stage. The wide range of possible simulation scenarios, both for beginners and advanced, implies a wide range of functional capabilities of the training centre, so that you can quickly move from one task to another. This in turn leads to the need for the technical parameters of the individual structural components of the training centre to cover a wide range of requirements, both in terms of performance and in terms of their functional capabilities.

On the other hand, SOC has a clearly defined functional purpose – to provide cyber protection of the corporate computer network. In this way, the range of tasks can be clearly defined, as well as the technical requirements for the structural components can be determined.

SOTC Purpose

It is expected SOTC at NVNA to have two main purposes – a training centre and a SOC for the academy's computer network. These two purposes are both complementary and mutually exclusive. It should be noted that the use of a productive environment to provide learning goals carries many risks related to compromising the functioning not only of the centre itself, but also of the computer network of the academy.

Although the main reason for the realization of the project for building SOTC is the training at all levels of competence, the leading functionality in the design stage is that of SOC for the academy's computer network. It is more accurate to say that at the heart of SOTC, the SOTC Datacentre should be implemented all necessary measures to ensure a certain level of cybersecurity for the computer network not only of SOTC, but also of the academy.

The mission of each SOC can be compared to providing physical security at the sites of the organization. Nathans[4] defines the purpose of SOC as „to provide a real-time view into a network or an organization's security status, assuring that systems are not being negatively affected and has the ability to execute agreed upon protocols and processes in a consistent manner when issues arise as well as someone keeping an eye on the facilities at all times". In terms of cyber-security, the focus of the SOC is network security. It can be said that SOC

is an upgraded version of the functions of the Network Operations Centre (NOC), which is used to monitor the operation of the computer network and maintaining this operation based on defined parameters. To the purpose of NOC are added the responsibilities for securing the data in the computer network, it is safely used and policies to respond to incidents with cybersecurity. In short, it can be said that the main purpose of SOC is to maintain the continuous in the business pro-cesses in the organization, realizing all aspects of the security of the used systems. Achieving this mission is unthinkable without utilizing up-to-date information technology.

SOTC Requirements

Based on the above functional purposes of SOTC can be defined and the requirements for its individual structural components. The key resources needed for the successful development of any business project can be categorized into four categories [5] – physical resources, intellectual resources, human resources and financial resources. The specifics of the implementation of SOTC at NVNA excludes the independent assessment of the required financial resource, as SOTC will not function independently. This does not exclude the creation of a business plan for the use of SOTC in its second main function - education and training. The purpose of this plan should be to ensure a return on investment and financial resources for maintenance of the Centre operation, including its development.

The requirements for the structural components of the SOTC can be divided into two main groups depending on the function provided namely the training centre and the SOC for the academy's computer network. In each of these two groups, three separate categories of key resources can be defined, for which separate requirements for availability and functionality can be imposed. The correlation between the same types of key resource categories from the two groups, without giving any priority to either group, will be used to determine the recommended requirements for the building and operation of the SOTC.

The three categories of key resources from each group are:

- Hardware – physical resources;
- Software – intellectual resources;
- Staff – human resources.

Utilised technologies at Nikola Vaptsarov Naval Academy SOTC

The availability of hardware resources and trained staff are necessary conditions for building a functional IT infrastructure. However, without software usage the IT infrastructure cannot be exploited on the merits. Various software products are used to provide IT services. Various software products are also used to support the administration of the IT infrastructure. Conducting a learning process requires appropriate software products not only for the presentation of learning content, but also for tests, simulations, emulations and for more.

Each element of the IT infrastructure is associated with different IT technology solutions on which it is based. The individual elements of the IT infrastructure cannot work separately – the data from the servers operating in a virtual environment cannot reach the end-users devices without the presence of network connectivity between them. The last example shows the relationship between four separate categories of IT technologies, whose general purpose is end-users to receive certain information. These are network technologies, server virtualization technologies, technologies for providing a specific IT service and technologies related to the work of end user's devices. Of course, it is possible to go into details and to describe these technologies through separate technological solutions, which are applicable depending on the specific implementation.

SOTC Datacentre

The main purpose of the SOTC datacentre is to ensure the functioning of all hardware components and software platforms related to the provision of IT services in the IT infrastructure, as well as the management of the infrastructure itself.[6] When setting the task for designing SOTC, the main goal of its data-centre is formulated. It is to provide the necessary computing resources and technical tools to ensure the operation and provision of services in the IT infrastructure of the centre and the academy, as well as all necessary technical tools to achieve a certain level of cybersecurity for the entire IT infrastructure.

Because of the defined goal, all the necessary IT technologies are determined, through which to achieve it. The main IT technical solutions used in the SOTC datacentre are:

- Server virtualization;
- Storage systems;
- Different network technologies;
- Technologies for filtering and controlling network traffic.

Server virtualization is a technology that allows the creation of multiple virtual machines on a single physical machine (server).[7] One of the main advantages of server virtualization is the isolation of running virtual machines – in virtual machines run different operating systems simultaneously, sharing the same hardware resources without sharing the data being processed.

Into the SOTC's datacentre server virtualization is the leading technology that ensures the provision of all necessary IT services for the operation of the centre, by creating an infrastructure of virtual servers and desktops. Among the main necessary IT services for the SOTC are:

- Service for locating hosts;
- Service for dynamic configuration of workstations IP protocol parameters;
- Service for users authentication and access control to IT infrastructure resources;

- Service for providing information through hyperlinks;
- Service for access to structured learning content;
- Service for videoconferencing and chat;
- Service for starting cyber-attacks simulation models and simulations management;
- Service for access to virtual desktops.

In addition to the above, it is possible to provide other IT services needed to perform a specific task. For their deployment, it is extremely convenient to use pre-configured virtual appliances.

IT and Cybersecurity Software Relevant to Training at SOTC

SOTC will perform two main functions and one of them is related to the training process of IT specialists and cybersecurity specialists. Regarding this, the technologies used in the creating of the SOTC's datacentre should be considered as technologies that are related to the ongoing learning process. It can be said that the learning process of IT specialists should be conducted using all IT technologies that are used into the real productive IT infrastructures, including their datacentres. In order to not compromise the SOC function of the centre, productive devices should not be used for conducting a learning process. Similar devices should be used for this purpose. In other words, the mentioned above technologies also apply to SOTC training activities, but should be applied by separate devices. To increase performance for one of the two main functions if this is necessary, it is recommended that the hardware devices supported each of the functions should be interoperable.

If we need to assess the technologies discussed above from the point of view of the learning activity, then the server virtualization will be ranked first among the others. The reason for this is that using the server virtualization during the learning process it will be possible to simulate different situations in an IT infrastructure without affecting the performance of the real infrastructure. The functionalities of the server virtualization allow the rapid deployment of various IT services in a short time, their rapid recovery in its original state, as well as the isolation of the processes in the virtual environment from the real one.

Designing SOTC at NVNA

The design of the SOTC is conducted in accordance with the planned purposes of the centre. The point of intersection between the two main purposes of the centre is its datacentre, ensuring the functioning of the necessary computing resources. Conducting a learning process requires specific rooms related to the possibility of training in various aspects of both IT specialists and cybersecurity specialists.

If the design of the datacentre is aimed to provide the necessary computing resources with given parameters for availability and accessibility, the design of the rest of the SOTC is related to the learning function. It must be taken into account how the simulations of cyber-attacks and incidents will be conducted.

In addition, it is necessary to take into account all aspects of IT technologies for which integrated training can be conducted. After the design, a construction phase must be undertaken, after which the SOTC will be able to fulfil its two main purposes.

Rooms Layout at SOTC

The design of the classrooms takes into account the peculiarity of the use of SOTC as an SOC, as well as a centre for conducting exercises using simulation models of the Cyber range platform. The need for the following types of classrooms is defined:

- Lecture hall;
- Computer laboratories;
- Specialized laboratory for studying computer hardware;
- Specialized laboratory for study, analysis and testing of IT technologies under the conditions for CIPA;
- Simulation control room.

The planned workspace of the rooms in the SOTC for ensuring the learning pro-cess is presented on Fig. 1.

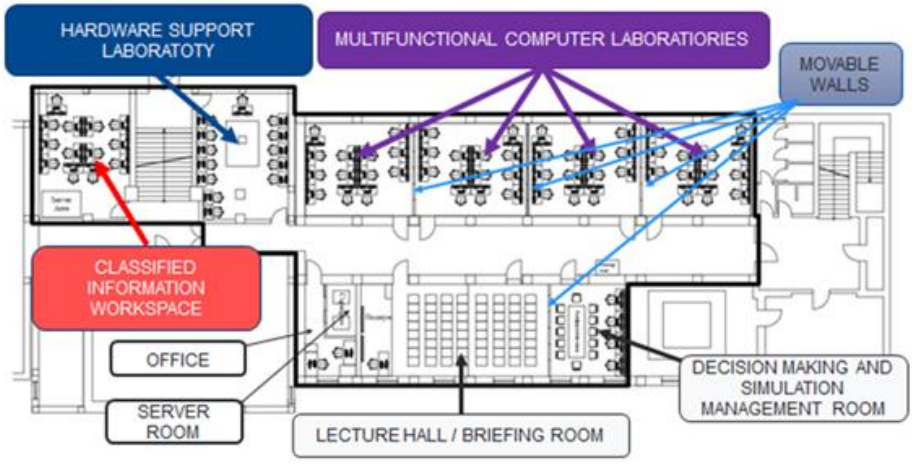

Figure 1: IT training rooms' placement.

Usage Scenarios

The design of the classrooms takes into account the peculiarity of the use of SOTC as an SOC, as well as a centre for conducting exercises using simulation models of the Cyber range platform. The need for the following types of classrooms is defined:

In addition to the described location of workplaces, providing a standard learning process, the SOTC should be able to conduct specialized practical

classes for conducting cyber operations and implementation of cybersecurity measures. In most cases, this requires trainees to be divided into teams. The names of teams may correspond to the generally accepted notions of the types of hackers – white and black hackers. Another approach is to name the teams in accordance with the accepted notions in the armed forces for denoting their own and enemy's forces - blue and red. Of course, it is possible use another principle of naming teams depending on the current scenario.

Because the military nature of the NVNA, the division of a blue and a red team is considered the main naming of teams in cybersecurity exercises. An exemplary division of the workrooms to provide these teams is shown on fig. 2. The location of the two teams is principle and their places can be exchanged. This division of teams assumes that each of them will include up to $^{2}4$ participants. To achieve a common workspace for each of the teams, two of the movable walls are removed. This scenario also requires workplaces to be reconfigured as is shown on Fig. 2.

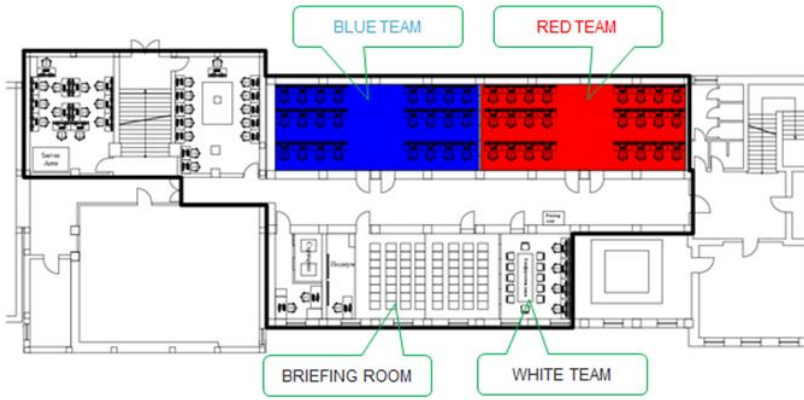

Figure 2: A variant of cyber operations training rooms' placement.

Conclusions

Building the SOTC in the way discussed so far will create the conditions for conducting cybersecurity exercises. At the same time, the centre will function as an SOC for the academy's computer network.

Assessing the cybersecurity of marine equipment or systems from other industries remain outsides the range of options for using the SOTC described so far.[8]

The building and development of the SOTC aims to solve several key tasks at NVNA. First, this is the achievement of a certain level of cybersecurity in the computer network of the academy. Next, an environment is expected to be created for cybersecurity training at all levels of competence. Last but not least, the possibility of integrating the SOTC with NVNA's maritime simulation

complexes will allow the research in the field of cybersecurity of the maritime industry, in which the problems are many, but there are no real tools for their assessment and impact forecasting.

References

1 Persistent Cyber Training Environment, https://www.raytheonintelligenceandspace.com/capabilities/products/persistent-cyber-training-environment, last accessed July 13, 2020.

2 Cyber Awareness Challenge, https://public.cyber.mil/training, last accessed July 13, 2020.

3 Security education, training, and certification for DoD and Industry, www.cdse.edu/catalog/index.html, last accessed July 13, 2020.

4 David Nathans, *Designing and Building a Security Operations Centre* (Syngress, 2014).

5 Alexander Osterwalder and Yves Pigneur, *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers* (John Wiley, 2010).

6 Hwaiyu Geng, *Data Centre Handbook* (John Wiley, 2015).

7 Matthew Portnoy, *Virtualization Essentials* (John Wiley, 2012).

8 Dimo Dimov and Yuliyan Tsonev, "Result Oriented Time Correlation between Security and Risk Assessments, and Individual Environment Compliance Framework," In: *Proceedings of the International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning, Smart Innovation, Systems and Technologies,* 2019, pp. 373-383, https://doi.org/10.1007/978-3-030-03577-8_42.

About the Author

Borislav **Nikolov** is assistant professor in the Information Technologies Department, Nikola Vaptsarov Naval Academy. Currently he is working on his PhD degree in the same university. His current research interests are in the field of system administration and server virtualization.
https://orcid.org/0000-0002-6055-8538