ISSN 2392-0300 „Civitas et Lex" 2020 / 1(25)
DOI 10.31648/cetl.4906

BEZPIECZEŃSTWO / SECURITY STUDIES

Piotr Jerzy Gawliczek

E-LEARNING AS TOOL TO SUPPORT CYBERSECURITY EDUCATION. CASE STUDY – GENERIC REFERENCE CURRICULUM, RECOMMENDED BY NATO, AVAILABLE AS E-LEARNING COURSE

Introduction

Since 2008, the Partnership for Peace Consortium (PfPC) of Defense Academies and Security Studies Institutes, working in coordination with the NATO International Staff, has developed a number of different curricula – designed for employment by defense education institutions. They are designed to provide partner countries with in-depth learning objectives and curriculum support for academic courses in professional military education (PME) schools. NATO has noted that these reference curricula can serve as tools for partner countries in the design and development of courses, modules and programs for professional officer military education and the enhancement of military interoperability between NATO and partners within Defence Education Enhancement Programs (DEEP).

Until now, NATO and the PfP Consortium have jointly developed six reference curricula, and another one is being developed. First one is the Partnership Plan for Defence Institution Building (PAP-DIB), which aims to provide in-depth learning objectives and curriculum development support for academic courses focused on defence institution building or reform. *The PAP-DIB reference curriculum* informs that in part by the typical academic programs and courses found in Western civilian and military academic institutions[1].

Second one is on Professional Military Education for Officers (PME)[2], developed by a multinational team of defence educators and practitioners, aims to provide in-depth learning objectives and curriculum support for academic courses

Piotr Jerzy Gawliczek – Uniwersytet Warmińsko-Mazurski w Olsztynie Filia w Ełku, ORCID: https://orcid.org/0000-0002-0462-1168, e-mail: piotr.gawliczek@uwm.edu.pl

[1] *PAP-DIP Reference Curriculum*, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2009_09/20090908_PAB-DIB_en.pdf> (Accessed 2019-10-19).

[2] *Generic Officer Professional Military Education Reference Curriculum*, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20111202_Generic-Officer-PME-RC.pdf> (Accessed 2019-10-21).

related to officer professional military education; an important contribution to defence education and enhancement of military interoperability between NATO and its partners.

Third one is on Professional Military Education for Non-Commissioned Officers[3]. Is also developed by a multinational team of defence educators and practitioners, is designed to provide in-depth learning objectives and curriculum support for academic courses related to Non-Commissioned Officer (NCO) professional military education; an important contribution to defence education and enhancement of military interoperability between NATO and its partners.

Fourth reference curriculum one is on Counterinsurgency[4] and the document aims to serve as a reference, a starting place, for individuals or organizations in NATO member states and partner countries looking to develop and/or supplement their professional military education (PME) in the area of Counterinsurgency (COIN).

Fifth one is on Building Integrity (BI)[5], was developed by NATO International Staff-led working group of subject matter experts (SMEs) from Allied and partner nations, aims to assist both NATO Allies and partners in enhancing education and training, and the mainstreaming of BI. In addition, this document provides BI specific topics that can be embedded into existing courses on good governance and anti-corruption or tailored to meet specific national requirements and objectives in both of these areas or related subjects DEEP features specialised engagement on pedagogy to provide institutions and instructors with access to the latest teaching methods and to support their efforts to foster critical thinking in the classroom. This document was the inspiration to develop e-learning course, due to the availability of the Information and Communications Technologies[6]. This course is available i.e. on the JADL platform of the NATO Allied Command Transformation in Norfolk.

Cybersecurity. A generic RC as the document and e-learning course

Apart from five already mentioned documents, of special importance is the reference curriculum on Cyber Security[7] which aims to provide in-depth learning objectives and curriculum support for academic courses broadly related

[3] *Non-Commissioned Officer (NCO) Professional Military Education Reference Curriculum*, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_10/20151013_151013-non-comm-officer-eng.pdf> (Accessed 2019-10-21).

[4] *Counterinsurgency Reference Curriculum*, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_09/20170904_1709-counterinsurgency-rc.pdf> (Accessed 2019-10-21).

[5] *Building Integrity (BI) Reference Curriculum*, <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_10/20171129_171031-bi-ref-cur17.pdf> (Accessed 2019-10-21).

[6] P. Gawliczek, *Technologie informacyjno-komunikacyjne jako narzędzia kształcenia. Studium przypadku – Filia w Ełku Uniwersytetu Warmińsko-Mazurskiego w Olsztynie*, „Civitas et Lex" 3(2019), pp. 33–39.

[7] *Cyber Security: A Generic Reference Curriculum*, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf> (Accessed 2019-10-21).

to Cybersecurity. This curriculum consists of four themes: 1) Cyberspace and the Fundamentals of Cybersecurity, 2) Risk Vectors, 3) International Cybersecurity Organizations, Policies and Standards and 4) Cybersecurity Management in the National Context. The themes and associated blocks have been carefully chosen to encompass the broadest spectrum of Cybersecurity issues and topics, and to provide the most pertinent level of education. Of importance are the recommendations stemming from the unique document, which was endorsed by the NATO Supreme Allied Commander Transformation on 27 September 2016 as the result of the work of a multinational team of volunteer academics and researchers drawn from 14 nations associated with the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG). The document is found compatible with NATO Education and Training on Cyber Defence and can serve as the reference for partner countries in the design and development of course models and programs for cybersecurity education.

On the other hand, within NATO DEEP ADL Ukraine agenda, the document was transformed into a framework e-learning course, consisting of the respective equivalents. It is available on the NATO DEEP ADL Portal and LMS ILIAS platform of the Elk Campus Branch of the University of Warmia and Mazury in Olsztyn.

Figure 1 shows the general layout of the e-learning course.

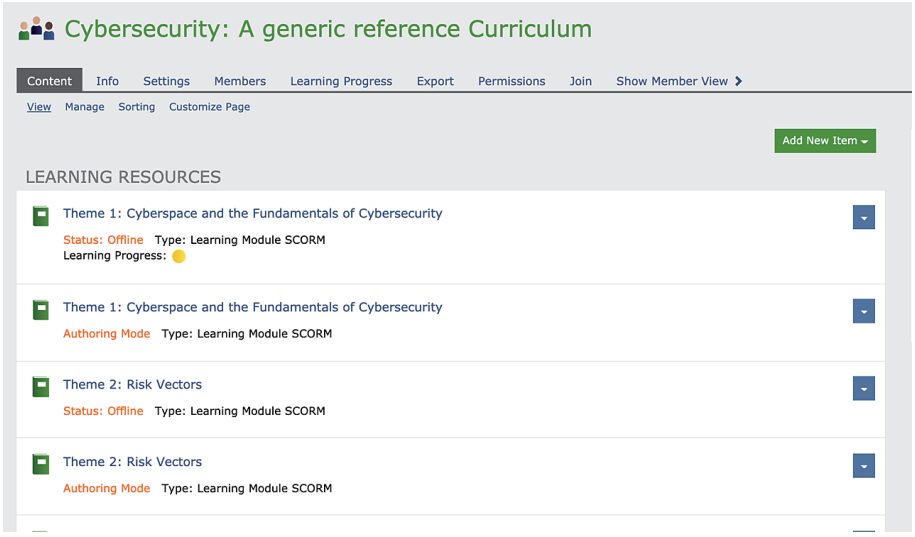

Figure 1
Source: <https://deepportal.hq.nato.int/ilias.php?ref_id=1505&cmdClass =ilrepositorygui&cmdNode=1h&baseClass=ilRepositoryGUI> (Access: 2019-10-22).

By the way of introduction, in the section "Aim of this document", it is stated, that he rapid and unrelenting pace of changes and challenges in cybersecurity was the driving force that prompted the ESCWG to request this curriculum effort, in accordance with NATO's increased emphasis on improving cybersecurity

awareness, preparedness and resilience. The domains once simply considered as electronic warfare, or information warfare once dominated by network security experts, is today transforming into a much broader domain, referred to as "cybersecurity"[8].

In keeping with the structures adopted in other PfPC reference curricula, the document is presented through the aforementioned themes, each of which is separated into blocks that naturally could be further subdivided. These divisions are designated Themes (T) and Blocks (B), as reflected in the Table of Contents. As far as next paragraph – "Using this Curriculum" is concerned, the document makes a number of implicit assumptions. Rather, the document is best used as a key reference providing a broad outline of issues and topics across the spectrum of cybersecurity. It may serve as a guide for technical personnel to know where their particular focus falls within this broad spectrum of issues. Similarly, it may guide introductory courses for senior national security policy makers, so that they might better appreciate and situate their national policies with knowledge of the technical context. The three elements of greatest concern when deriving any single course from this outline will be the aim or purpose of the course; the proposed students, particularly their level of technical knowledge and the nature of their employment; and the time available. Those three elements should guide the level of technical detail discussed and the nature of the learning exercises (lectures, examples, field trips, demonstrations, war games, etc.). It is stated that the volume of both general and technical literature related to cybersecurity is expanding rapidly. In addition to the many sources listed throughout this document, the NATO website provides many current articles and information on issues of interest to the NATO community.

Theme 1

First theme is focused on cyberspace and the fundamentals of cybersecurity. It comprises following blocks: (1) Cybersecurity and Cyberspace—An Introduction, (2) Information Security and Risk, (3) The Structures of Cyberspace: The Internet Backbone and National Infrastructures, (4) Protocols and Platforms, (5) Security Architecture and Security Management.

Figure 2 shows the screenshot related to this part of the document.

Main object of this theme is to lay the knowledge foundations for all of the instruction that follows by identifying the structural components of cyberspace[9], its basic architecture and the rudiments of cybersecurity. Identification and management of risk is the major shared challenge linking the disparate themes and subjects addressed in this curriculum. The challenges of cyberspace

[8] P. Gawliczek, *Cybersecurity. A generic reference curriculum. Towards unified approach*, in: *Cybeprezstrzeń. Zagrożenia w sieci*, ed. M. Koziński, S. Kosznik-Biernacka, J. Grubicka, Słupsk 2017, pp. 293–306.

[9] Cyberspace has been defined here as the electronic world created by interconnected networks of information technology and the information on those networks. Derived from *Canada's Cyber Security Strategy*, 2014.

Figure 2
Source: <https://deepportal.hq.nato.int/ilias.php?baseClass=ilSAHSPresentationGUI&ref_id=1508> (Access: 2019-10-22).

and cybersecurity require more than a simple rechristening of government organizations responsible for information technology security (IT security) or communications security (COMSEC). The ubiquity of modern computer systems and the ability to communicate or interact through a variety of means, from mobile devices to wearable computers, present a number of inherent vulnerabilities and possible attack vectors for both state and non-state actors. Through the five blocks of this theme, students will be exposed to the basic structure of cyberspace and to a risk-based approach to cybersecurity. T1-B1, Cybersecurity and Cyberspace–An Introduction, explores the origins and general shape of cyberspace and introduces the concept of cybersecurity. T1-B2, Information Security and Risk, addresses the basics of information security risk analysis methodology and explores a threat-based approach to assessment. T1-B3, The Structures of Cyberspace: The Internet Backbone and National Infrastructures, explores the operation and architecture of the global Internet and its governance. T1-B4, Protocols and Platforms, introduces network technology and information technology standards in order to explore the basics of network design and operations. Finally, T1-B5, Security Architecture and Security Management, introduces the basics of security architecture based on threat, risk and vulnerability analysis.

Theme 2

Second theme is focused on risk vectors. It comprises following blocks: (1) Supply Chain/Vendors, (2) Remote- and Proximity-access Attacks, (3) Insider Access (Local-access Attacks), (4) Mobility Risks, BYOD and Emerging Trends. Figure 3 shows the screenshot related to this part of the document.

This theme area offers an introductory survey of the vulnerabilities inherent to cyberspace and the ways and means to exploit those vulnerabilities through various attack chains or vectors. Understanding these vulnerabilities is an

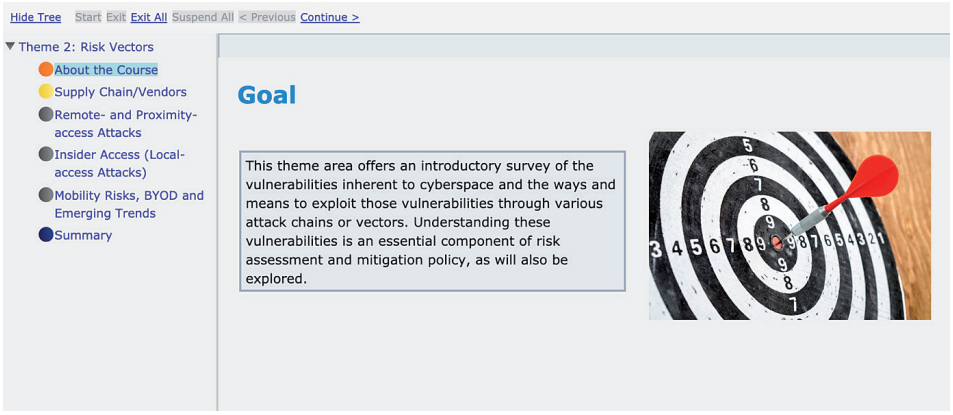

Figure 3
Source: <https://deepportal.hq.nato.int/ilias.php?baseClass=ilSAHSPresentationGUI&ref_id=1507> (Access:2019-10-22).

essential component of risk assessment and mitigation policy, as will also be explored. This reference curriculum has adopted the suggestion of the U.S. National Cyber Study Group report to the U.S. Director of National Intelligence, which argued that all of the various cyber vulnerabilities can be readily categorized under the following risk vector rubrics: "supply chain and vendor access; remote access; proximity access; and insider access." Therefore, within this theme, T2-B1 addresses the Supply Chain/Vendors rubric, highlighting security issues from the production floor through sub-contractors, shipment, warehousing and maintenance controls; T2-B2, Remote- and Proximity-access Attacks, explores the vulnerabilities associated with unauthorized (unprivileged) access; T2-B3, Insider Access (Local-access Attacks), explores vulnerabilities associated with privileged systems access; and T2-B4, Mobility Risks, BYOD and Emerging Trends, discusses risks associated with BYOD ("Bring Your Own Device") policies, "cloud" computing and other mobility issues.

Theme 3

Third theme is focused on international cybersecurity organizations, policies and standards**.** It comprises the blocks: (1) International Cybersecurity Organizations, (2) International Standards and Requirements – A Survey of Bodies and Practices, (3) National Cybersecurity Frameworks, (4) Cybersecurity in National and International Law. Figure 4 shows the screenshot related to this part of the document.

The broad objective of this theme is to expose students to international standards and organizations, such as the U.S. NIST and the British BSI (and possibly others), and the ways in which these relate to national contexts. Students will come to identify the role of international standards bodies and identify the major international organizations with cybersecurity roles

Figure 4
Source: <https://deepportal.hq.nato.int/ilias.php?baseClass=ilSAHSPresentationGUI&ref_id=1510> (Access: 2019-10-22).

or functions. Further, they should examine their national cybersecurity policies in light of international standards and recommended best practices and do so by comparing them to several example national policies. Finally, this theme area will address evolving international legal regimes for cybersecurity. Each nation will have to tailor this section to its needs, identifying its national bodies responsible for cybersecurity policy and practices and how these affect their respective cybersecurity policies and organizations. While particulars will vary for each nation, the approach taken to present this theme may follow these lines: T3-B1, International Cybersecurity Organizations, as relevant to the national context; T3-B2, International Standards and Requirements–A Survey of Bodies and Practices; T3-B3, National Cybersecurity Frameworks, which is aimed at analyzing national frameworks in comparison to those of other nations; and T3-B4, Cybersecurity in National and International Law.

Theme 4

Fourth theme is focused on Cybersecurity Management in the National Context. There are flowing blocks: (1) National Practices, Policies and Organizations for Cyber Resilience, (2) National Cybersecurity Frameworks, (3) Cyber Forensics, (4) National-level Security Audit and Assessment.

Figure 5 shows the screenshot related to this part of the document.

The broad objective of this theme is to explore the practice of managing cybersecurity in the national context. It is underlined, that approaches to managing national cybersecurity issues will differ significantly among countries. While challenges and responses may differ in detail, the general problems will be similar among nations. National frameworks for cybersecurity may differ in specifics, but in general a comprehensive regime often includes the following issues, which require active management and coordination: (1) physical

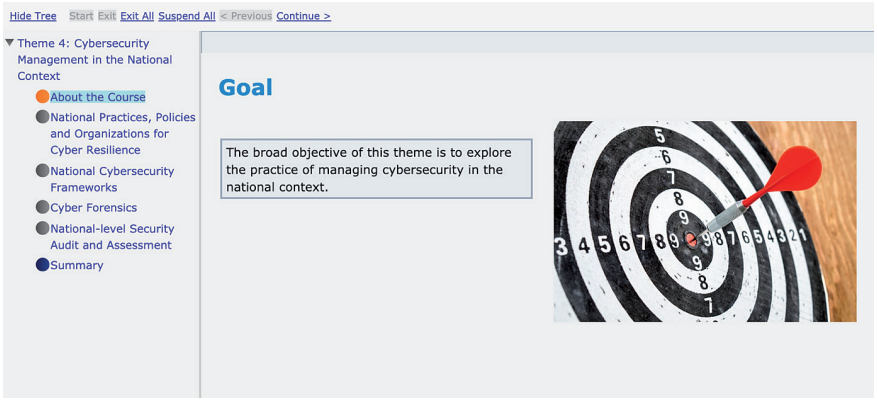

Figure 5
Source: <https://deepportal.hq.nato.int/ilias.php?baseClass=ilSAHSPresentationGUI&ref_id=1512> (Access 2019-10-22).

IT-related asset management; (2) controls management; (3) systems configuration and configuration change management; (4) vulnerability identification and management; (5) incident management; (6) service continuity management; (7) threat identification and handling management; (8) external dependences and linkages management; (9) training and awareness; and (10) maintaining situational awareness. This theme explores national cybersecurity management practices in depth and contextualizes national security readiness in a risk framework. In particular, T4-B1, National Practices, Policies and Organizations for Cyber Resilience, delves into contingency planning and recovery from cyber incidents so as to minimize disruption. T4-B2, National Cybersecurity Frameworks, introduces national cybersecurity management practices, which include operations, incident response and risk mitigation. T4-B3, Cyber Forensics, teaches students forensic tools, practices and procedures to collect, analyze and interpret data for attribution and intelligence. T4-B4, National-level Security Audit and Assessment, introduces students to best practices in assessing national cybersecurity readiness.

Additional sections

At the end of the document there are three additional sections: (1) abbreviations, (2) glossary – not all terms below appear in the text of the curriculum, but many may prove useful in crafting specific learning exercises, etc., (3) curriculum team members and advisers – total 40 persons.

Conclusions

This reference curriculum on cyber security provides a coherent launching point from which to develop or enhance the teaching of cybersecurity issues. Like the other reference curricula developed by the PfPC, the aim of this document is conservative. It does not present a single master course outline for all to follow. It is not exhaustive as to content, details or approaches to the subject. However, it furnishes a useful heuristic approach to the various domains, comprising a comprehensive introduction to the spectrum of issues entangled in the practices of cybersecurity.

Actually, e-learning is becoming an essential part of professional military education and is also one of the fastest growing areas of NATO's technological education and training capabilities, and a tool the DEEP uses to provide support to partner countries. It is of importance to stress that the rapid and unrelenting pace of changes and challenges in cybersecurity and NATO's increased emphasis on improving cybersecurity awareness, preparedness and resilience are the driving forces to develop new courses on cybersecurity. The "Cybersecurity Awareness Micro Course – 10 Principles of Cybersecurity", is the good example to follow as far as other NATO DEEP programs are concerned.

As already stated, a new curriculum is being developed – on Counterterrorism. Relying on voluntary contributions, NATO steers policy and the PfP Consortium leads on academic support facilitating the network of institutions and individual academics and practitioners who contribute through the PfP Consortium's Education Development Working Group. NATO draws on an ad-hoc network of contributors who offer their services through an annual Clearing House on Defence Education that serves as a forum for Allies and partners to coordinate efforts and inform institutions and countries about the status of the various DEEP programmes. Led by Bulgaria, Canada, the Czech Republic, France, Italy, Lithuania, Poland, Romania, Slovakia, Spain, Switzerland and the United States, with the support of the PfP Consortium, the annual Clearing House is an effective tool to identify partner requirements and align them with donor expertise[10]. It is connected with the strategic communications specificity – to deliver message[11].

BIBLIOGRAPHY

Building Integrity (BI) Reference Curriculum, <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_10/20171129_171031-bi-ref-cur17.pdf> (Accessed 2019-10-21).

Counterinsurgency Reference Curriculum, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_09/20170904_1709-counterinsurgency-rc.pdf> (Accessed 2019-10-21).

[10] *Defence Education Enhancement Programme (DEEP)*, <https://www.nato.int/cps/en/natohq/topics_139182.htm> (Accessed 2019-10-21).

[11] P. Gawliczek, *Rola komunikacji strategicznej w kreowaniu wizerunku NATO. Refleksje po szczycie w Warszawie. Wykład inauguracyjny 2016/*2017, „Zagadnienia Społeczne" (2)2016, pp. 302–313.

Cyber Security: A Generic Reference Curriculum, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf> (Accessed 2019-10-21).
Defence Education Enhancement Programme (DEEP), <https://www.nato.int/cps/en/natohq/topics_139182.htm> (Accessed 2019-10-21).
Gawliczek P., *Cybersecurity. A generic reference curriculum. Towards unified approach*, in: *Cyberprzestrzeń. Zagrożenia w sieci*, ed. M. Koziński, S. Kosznik-Biernacka, J. Grubicka, Słupsk 2017, pp. 293–306.
Gawliczek P., *Rola komunikacji strategicznej w kreowaniu wizerunku NATO. Refleksje po szczycie w Warszawie. Wykład inauguracyjny 2016/2017*, „Zagadnienia Społeczne" 2(2016), pp. 302–313.
Gawliczek P., *Technologie informacyjno-komunikacyjne jako narzędzia kształcenia. Studium przypadku – Filia w Ełku Uniwersytetu Warmińsko-Mazurskiego w Olsztynie*, „Civitas et Lex" 3(2019), pp. 33–39.
Generic Officer Professional Military Education Reference Curriculum, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20111202_Generic-Officer-PME-RC.pdf> (Accessed 2019-10-21).
Non-Commissioned Officer (NCO) Professional Military Education Reference Curriculum, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_10/20151013_151013-non-comm-officer-eng.pdf> (Accessed 2019-10-21).
PAP-DIP Reference Curriculum, <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2009_09/20090908_PAB-DIB_en.pdf> (Accessed 2019-10-19).

E-LEARNING AS TOOL TO SUPPORT CYBERSECURITY EDUCATION. CASE STUDY – GENERIC REFERENCE CURRICULUM, RECOMMENDED BY NATO, AVAILABLE AS E-LEARNING COURSE

SUMMARY

The aim of the article is to address the challenges and opportunities for academic education, as a consequence of the technological revolution, with particular emphasis on the context of the e-learning solutions and applications. The aim is also to formulate recommendations regarding the best practices within the information and communication technologies in education. In this context the cooperation between Partnership for Peace Consortium (PfPC) of Defense Academies and Security Studies Institutes, and the NATO International Staff, aiming to develop the reference curricula, is presented – designed for employment by the defense education institutions. The respective documents are available, also for the Defence Education Enhancement Program (DEEP) partner countries. As the case study, the Reference Curriculum on Cybersecurity is shown as the e-learning solution, available on the NATO DEEP ADL Portal and LMS ILIAS platform of the Elk Campus Branch of the University of Warmia and Mazury in Olsztyn.

KEY WORDS: cybersecurity, NATO DEEP, education, LMS ILIAS, e-learning