Information & Security: An International Journal

Tagarev, vol.35, 2, 2016, 181-184 https://doi.org/10.11610/isij.3510

A GENERIC REFERENCE CURRICULUM ON CYBERSECURITY

Todor TAGAREV

Abstract: A volunteer group of academics and practitioners embarked on a two-year project to develop a generic reference curriculum on cybersecurity on behalf of NATO and the Partnership for Peace Consortium. This paper provides a brief overview of the result of this work – a curriculum that is recommended as a starting point for any university or training organization considering a program in the field of cybersecurity.

Keywords: Cybersecurity, competence framework, policy-making, technical expertise, education, training.

Introduction

As our societies are getting ever more reliant on data, information, and networks, expertise in information and cyber security is in high demand.[1] That applies to numerous fields and public and private sectors, and the expectation of professional performance by defense and security sectors are particularly strong.

Universities address this demand by providing respective educational programs, and many excel in the fields of information and communications technologies and computer science. Others provide advanced education in policy and management. There have been, however, few attempts to bring together people with policy-making experience and technical experts, so that the two—so far distinct—communities can come together, understand each other, and work jointly to find adequate solutions to the cybersecurity challenges of today and in the foreseeable future.

To address this void, NATO and the Partnership for Peace Consortium of the Defense Academies and Security Studies Institutes (below, PfP Consortium[2]) launched a two-year project to produce a reference cybersecurity curriculum.

Publication

Cybersecurity: A Generic Reference Curriculum was produced by a multinational team of volunteers, both academics and practitioners, coming from 17 nations, on behalf of NATO and the PfP Consortium.

Sean S. Costigan and Michael N. Hennessy led the work and served as editors for the final publication. Scott Knight, Dinos Kerigan-Kyrou, Philip Lark, Chris Pallaris, Daniel Peder Bagge, Gigi Roma, Natalia Spinu, Todor Tagarev, Ronald Taylor, and Joseph Vann were also among the core contributors to the Curriculum. Dr. Raphael Perl, Executive Director of the PfP Consortium, NATO's Defence Education Enhancement Program (DEEP),[3] the Emerging Security Challenges Working Group and the education working groups of the PfP Consortium provided valuable guidance and support to the development of the Curriculum.

Major-General J.G.E. Tremblay, Commander of Canada's "National Defence" wrote the foreword to the publication. The curriculum includes as well an endorsement by Major-General Stefano Vita Salamida, Italian Air Force, ACT Deputy Chief of Staff (DCOS) Joint Trainer, on behalf of the Supreme Allied Commander Transformation.

Overview of the Curriculum's Structure

The Curriculum is structured along four themes:

The first theme introduces the student to cyberspace and the fundamentals of cybersecurity, with an introductory block and blocks dedicated to information security and risk, the Internet backbone and national infrastructures, protocols and platforms, and security architecture.

Theme 2 looks into risk vectors and includes four blocks: supply chain and vendors, remote- and proximity-access attacks, insider access and respective attacks, mobility risks, BYOD,[4] and emerging trends.

The third theme is dedicated to good practices coming from national and international cybersecurity organizations, policies and standards. Its four blocks look respectively into international cybersecurity organizations, international standards and requirements, national cybersecurity frameworks, and national and international law on cybersecurity.

Theme 4 sets the ground for management of cybersecurity in a national context. It also includes four blocks presenting respectively national practices, policies, and organizations for cyber resilience, cybersecurity frameworks, cyber forensics, and national level audit and assessment of security.

The Curriculum includes also a list of abbreviations and an extensive glossary, as well as a list of all contributors and advisors with their organizational affiliation.

The document provides even experienced readers with a better grasp of the broad spectrum of issues to be taken into account in addressing cybersecurity. Both NATO and partner countries, as well as any interested organization, that wants to develop or enhance an existing cybersecurity curriculum, can use that document as a reference source that can be tailored to their specific needs and teaching capacity.

The anticipation is that partner countries, interested in adapting and implementing the whole or parts of this Curriculum, can use their Individual Partnership Action Plan (IPAP) to request and manage support from NATO and the PfP Consortium and thus further their own and our collective security.

Bibliographic Information

Costigan, Sean S. and Michael N. Hennessy, eds. *Cybersecurity: A Generic Reference Curriculum*, with Foreword by Major-General J.G.E. Tremblay. Kingston, ON: National Defence, 2016. ISBN 978-92-845-0196-0

The Curriculum is available for download in pdf format, for free, from:

- NATO's website at http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf, and
- the website of the PfP Consortium at http://pfp-consortium.org/index.php/pfpc-products/education-curricula/item/262-cybersecurity-reference-curriculum.

References

[1] See, for example, Emily Garthwaite, "Cyber security expertise in high demand as threats increase," *ITProPortal*, September 15, 2015, available at http://www.itproportal.com/2015/09/15/cyber-security-expertise-high-demand-threats-increase/.

[2] See http://pfp-consortium.org for more details.

[3] NATO – Topic: Defence Education Enhancement Programme (DEEP), available at www.nato.int/cps/en/natohq/topics_139182.htm.

[4] BYOD – Bring Your Own Device. See, for example, "Bring Your Own Device (BYOD)," *Gartner IT Glossary*, available at http://www.gartner.com/it-glossary/bring-your-own-device-byod.

About the Author

Todor TAGAREV is Editor-in-Chief of *Information & Security: An International Journal*. He was member of the group that developed the reference curriculum, contributing primarily to policy and management topics.