CYBERSECURITY

A GENERIC REFERENCE CURRICULUM

CYBERSECURITY

A GENERIC REFERENCE CURRICULUM

National Defence
Office of the Commander
Military Personnel Generation
P.O. Box 17000 Station Forces
Kingston, ON K7K 7B4

Défense nationale
Bureau du commandant
Génération du personnel militaire
CP 17000, Succursale Forces
Kingston, ON K7K 7B4

4500-1 (SSO EE)

6 October 2016

Cybersecurity: A Generic Reference Curriculum (RC)

Dear Partners/NATO Members,

It pleases us to share with you the document entitled *Cybersecurity: A Generic Reference Curriculum (RC)*, developed, on behalf of NATO and the Partnership for Peace Consortium (PfPC) of Defense Academies and Security Studies Institutes, by a multinational team of academics and practitioners. This document aims to provide NATO and partner countries with in-depth learning objectives and curriculum support for academic courses broadly related to Cybersecurity.

The Cybersecurity Reference Curriculum consists of four themes: i) Cyberspace and the Fundamentals of Cybersecurity, ii) Risk Vectors, iii) International Cybersecurity Organizations, Policies and Standards and iv) Cybersecurity Management in the National Context. The four 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.

This document is best understood as a resource to NATO and partner countries looking to develop and gain greater appreciation of the spectrum of issues, national and international, entangled in the practices of cybersecurity. It is presented in the hope that it will be noted by NATO in due time through the appropriate committees. The next envisioned step will be to work with partner defense education establishments in

4500-1 (OSEM PED)

Le octobre 2016

Programme de reference (PR) générique de la Cybersécurité

Chers partenaires/membres de l'OTAN,

Il nous fait grand plaisir de partager avec vous le document intitulé *Programme de référence (PR) générique de la Cybersécurité* dévcloppé par une équipe multinationale d'universitaires et de praticiens au nom de l'OTAN et du Groupement d'institutions d'études de défense et de sécurité du Partenariat pour la paix (PPP). L'objectif de ce document est d'offrir à l'OTAN et aux pays partenaires un appui dans le développement d'objectifs d'apprentissage et de contenu pour les cours liés aux études de la Cybersécurité.

Le programme de référence de la Cybersécurité se compose de quatres étapes : i) cyberespace et les principes fondamentaux de la cybersécurité, ii) vecteurs de risque, iii) organisations internationales cybersécurité , politiques et normes, et iv) la gestion de la cybersécurité dans le contexte national. Les quatre étapes et les thèmes associés ont été choisis avec soin pour englober la plus grande gamme possible de questions et de thématiques de cybersécurité et fournir le niveau le plus pertinent d'éducation.

Ce document sert de ressource à l'OTAN et ses partenaires cherchant à dévclopper une image plus complète de l'ensemble des questions nationales et internationales, empêtré dans les pratiques de la cybersécurité. Il est présenté dans l'espoir qu'il sera entériné par l'OTAN en temps opportun par le biais de comités appropriés. La prochaine étape consistera à collaborer avec les institutions partenaires d'éducation militaire lors de l'adoption et de la

their adoption and implementation of all or parts of this curriculum, guided by their Individual Partnership Action Plan (IPAP).

Only through dialogue and exchange of ideas can this document enhance the professional development and interoperability of alliance and partner military members. I invite your delegation personnel to distribute this document widely in your respective countries.

If you have any questions regarding this curriculum, please have your delegation personnel contact Mr. Sean Costigan, George C. Marshall European Center for Security Studies at sean.costigan@pfp-consortium.org or Dr. Michael Hennessy, Professor of History and War Studies, Royal Military College of Canada at hennessy-m@rmc.ca

Best wishes,

Le commandant,
Major-général

J.G.E. Tremblay
Major-General
Commander

mise en œuvre de ce programme, en tout ou en partie, selon leur plan d'action individuel pour le partenariat (IPAP).

C'est uniquement à travers le dialogue et l'échange d'expériences que ce document contribuera positivement à l'interopérabilité des sous-officiers de l'alliance et des pays partenaires, et à leur éducation militaire. Nous invitons le personnel de votre délégation à le diffuser à grande échelle dans vos pays respectifs.

Pour de plus amples renseignements sur le programme, le personnel de votre délégation peut communiquer avec M. Sean Costigan, Centre George C. Marshall European Center for Security Studies au sean.costigan@pfp-consortium.org ou M. Michael Hennessy, Professeur d'histoire et d'études sur la conduite de la guerre, Collège militaire royal du Canada au hennessy-m@rmc.ca

Nous vous prions d'agréer nos salutations les plus distinguées.

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

5000/TSC TTX 0310/TT-161157/Ser: NU0766(INV)

TO: See Distribution

SUBJECT: Endorsement of the PfPC Emerging Security Challenges Working Group Cybersecurity Reference Curriculum as a NATO Educational Reference Document

DATE: 27 September 2016

1. In an effort to satisfy specific partner education and training needs, the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG) has developed a Cybersecurity Reference Curriculum. The efforts, professionalism and dedication of those who contributed to the development of the curriculum is commendable.

2. The Cybersecurity Reference Curriculum is found compatible with NATO Education and Training on Cyber Defence and I am convinced that it can serve as a reference for partner countries in the design and development of course models and programmes for professional Cybersecurity military education. It will also serve as an enhancement of military interoperability between NATO and its partners and strengthen the collaboration on a responsive education and training system.

3. It is my pleasure to support the PfPC Emerging Security Challenges Working Group through publishing this Cybersecurity Reference Curriculum as a NATO document. I encourage all respective instructional designers of partner countries involved in the development of related learning opportunities to make full use of this guide.

4. Should there be any questions, please contact Mr. Salih Cem Kumsal, NATO Cyber Defence Education and Training Discipline POC at +1 (757) 747-3386, NCN 555-3386, or email cem.kumsal@act.nato.int.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

for
Stefano Vito Salamida
Major General, ITA AF
DCOS Joint Force Trainer

About this Reference Curriculum

This document is the result of the work of a multinational team of volunteer academics and researchers drawn from 17 nations associated with the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG). Our aim was to produce a flexible and generally comprehensive approach to the issue of cybersecurity.

This document aims to address cybersecurity broadly but in sufficient depth that non-technical experts will develop a more complete picture of the technological issues and technology experts will more completely appreciate national and international security policy and defense policy implications. We offer a logical breakdown of the topic by specific categories, suggesting the level of knowledge to be obtained by various audiences and indicating useful key references so that each adopting state can adapt this framework to its needs and the specifics of the target student body.

We are especially grateful to the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, under the leadership of Raphael Perl, and the Chairs of the ESCWG, Dr. Detlef Puhl (NATO) and Dr. Gustav Lindstrom (GCSP), as well as for the support of the PfPC DEEP and Education Working Groups under Dr. Al Stolberg, Mr. Jean d'Andurain and Dr. David Emelifeonwu. In addition, the leadership of several partner nations, including Armenia, Georgia and Moldova, helped make this effort possible through direct and tangible support. Last but most certainly not least, all the volunteers listed as contributors are owed an enormous debt of gratitude. When we asked if they would be willing to commit to a two-year effort that would take them deep into the recesses of cybersecurity education, not one flinched. In particular we wish to thank Scott Knight, Dinos Kerigan-Kyrou, Philip Lark, Chris Pallaris, Daniel Peder Bagge, Gigi Roman, Natalia Spinu, Todor Tagarev, Ronald Taylor and Joseph Vann. Without them, this document simply would not have come together.

Sean S. Costigan and Michael A. Hennessy, eds.

I. AIM OF THIS DOCUMENT

The rapid and unrelenting pace of changes and challenges in cybersecurity[1] 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.

News headlines are replete with references to commercial hacks, data breaches, electronic fraud, the disruption of government service or critical infrastructure, intellectual property theft, exfiltration of national security secrets, and the potential of cyber destruction. 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."

As it is an emergent issue, one in which there remains disagreement over basic terms, the ESCWG has sought to bring some clarity and commonality to this issue through creation of this reference curriculum. We have adopted the agreed spelling "cybersecurity" as one word throughout and employ the term "cyber" as a modifier or to clarify the focus.

In drafting this document, we canvassed all PfPC member institutions and other defense colleges and reviewed military training programs of NATO and PfPC partner countries to establish what is being taught. We sought to identify gaps and shared approaches that cut across traditional boundaries of governmental and military structures. The largest gap we observed was the lack of sufficient understanding of cybersecurity technology and of threat and risk mitigation practices among national security and defense policy leaders. A similar gap in the understanding of national policy frameworks was identified among technical experts.

This reference curriculum provides a coherent launching point from which to develop or enhance the teaching of cybersecurity issues to senior officers, civil servants and mid-level military and civilian staffs. 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, we believe 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. Those with little technical background will find an introduction at a manageable level of complexity and gain a better appreciation of where and why technical depth is required. Those with technical backgrounds may find the material a useful overview of areas they are familiar with and an introduction to broader issues of international, national and legal policies and practices. We trust that everyone will find in it something of value.

Those who desire to use this document as an approach to cybersecurity should analyze their particular and unique national practices and requirements to adapt it to their needs. This document offers guidance in identifying areas that warrant attention and recommends key sources and approaches.

II. CYBERSECURITY AND RISKS

Security measures are most often informed by measures of threats and risks. Both concepts are explored at some length. However, in simple terms, cyberspace is full of threats, but measures to mitigate threats need to be informed by measures of risk. The International Organization for Standardization (ISO) defines risk as "the effect of uncertainty on objectives" (the effect may be positive or negative deviation from what is expected). Since measures taken to secure something must be proportionate to the value of what is being secured, there are various levels of security depending on measures of value and risk. Securing cyberspace, therefore, entails a number of considerations to mitigate risks and threats while encouraging accessibility and openness across various types of interconnected networks and devices. Establishing the necessary balance between access, usability and security is the core challenge. This curriculum explores approaches to threat and risk assessment, identification and mitigation, at the technical level and at an agency and a government policy level, through exploration of recommended best practices and in comparison to the published policies of particular states or organizations.

III. STRUCTURE OF THIS CURRICULUM

As previous reference curriculum documents have stated, a curriculum is a specific learning program, or perhaps a range of courses, that collectively describes the teaching, learning and assessment materials and methods appropriate for a given program of study. The resulting curriculum therefore is a road map of what learners may be exposed to. Like any map, it is crafted

[1] In broad outline, we follow the definition devised for the U.S. Department of Homeland Security: "Cybersecurity is the activity or process, ability or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

at a level of abstraction and may not show all routes or details; however, it outlines what the learner should see.

Typically, a generic curriculum results in a nested structure, with many subtopics and issues nested within a broad framework[2]. These many nested parts are connected to broader objectives of a program of study. Given the interconnectedness of subjects and issues contained within our cybersecurity reference curriculum, we have not recommended that the curriculum be broken into three officer development phases. More will be said on this point below, when we address how to use this curriculum.

In keeping with the structures adopted in other PfPC reference curricula, this document is presented through four 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 (see over).

The four themes of this curriculum are as follows:

Theme 1: Cyberspace and the Fundamentals of Cybersecurity

Theme 2: Risk Vectors

Theme 3: International Cybersecurity Organizations, Policies and Standards

Theme 4: Cybersecurity Management in the National Context

Each theme is described in detail elsewhere in this document, but each has broad specific areas and issues to address.

Subsumed under each theme are several distinct subjects. Each subject is explored in a basic block, which itself may be broken down into distinct learning modules, such as lectures, presentations, demonstrations, tours, scenario exercises or similar activities. For the most part, because this reference curriculum will require local adaptation, we have not suggested distinct modules and lectures because that level of detail is dependent on individual need. The various blocks collectively inform each theme. They suggest learning objectives and outcomes to be achieved; these are in turn connected to the wider objectives of the theme.

Blocks could be delivered as a whole, combined, or subdivided into separate modules. This outline does not suggest which blocks to treat which way, but in either blocks or modules, delivery of the subjects may take the form of lectures, presentations, participatory assignments, tours, demonstrations or participation in scenario exercises.

IV. USING THIS CURRICULUM

The curriculum makes a number of implicit assumptions.

First, all of the material identified in this document is non-classified. Those who adopt this framework may wish to address classified material if the need arises.

Second, it is assumed that institutions adopting this reference curriculum will devote appropriate time and resources with an expert team to identify national policies and procedures at the level of detail required for the target audience. Rote knowledge of transitory technical matters may be necessary, but the objective here is for a broader understanding of the challenges of cybersecurity across the spectrum of issues.

In adapting this curriculum for local use, it may be possible to implement it in a progressive and sequential manner across various career phases, but at all levels the comprehensive outline should be followed. However, the broad objective of this reference curriculum is more strategic-operational than it is tactical. In developing specific courses from this reference curriculum, it is suggested that the local course designers consider the time and resources available, the educational level of the students and the functions that those students are expected to perform or will be expected to perform, regardless of their rank.

Third, there is no block on cyber war, cyber conflict or social media as a conduit for propaganda or disinformation. The design committee elected to leave those focused issues for subsequent development.

Finally, we reiterate that this reference curriculum is not a single or proposed course structure. 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

[2] See previous reference curriculum documents for the origins and utility of this construct.

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.).

V. ADDITIONAL SOURCES

The volume of both general and technical literature related to cybersecurity is expanding rapidly. Course designers are encouraged to generate their own list of key sources; nevertheless, we have included a wide range of sources reflecting many different national and international perspectives relevant to the themes articulated for this reference curriculum, and, where available, we have provided links to active Internet resources. 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. Sources listed at www.natolibguides.info/cybersecurity include the following:

- NATO Review's articles/videos on cyber attacks as well as the June 2013 edition on Cyber—the good, the bad and the bug-free (includes videos, photos, a timeline, infographics, etc.).
- The article NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow by Healey and van Bochoven (February 2012) provides a good overview of NATO's cyber capabilities.
- The report On Cyberwarfare (2012) by Fred Schreier includes a glossary and very good selected and thematic bibliographies (Official Documents, NATO, OECD, by country, Information Warfare, Cyber Security, Books).
- The Cyber Special Edition of *Strategic Studies Quarterly* 6, no. 3 (Fall 2012).
- The Cybersecurity: Shared Risks, Shared Responsibilities edition of *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012).
- The article Cyberspace Is Not a Warfighting Domain (2012) by Martin Libicki.
- *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (2012).
- The 300-page manual was written by a group of 20 researchers at the invitation of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.
- The follow-up "Tallinn 2.0" project to the *Tallinn Manual on the International Law Applicable to Cyber Warfare* is designed to expand the scope of the original *Tallinn Manual*. Tallinn 2.0 will result in the second edition of the *Tallinn Manual* and be published by Cambridge University Press in 2016 (source: NATO CCD COE).
- The National Cyber Security Framework Manual (2012) by the NATO CCD COE.
- The NATO CCD COE's e-learning course on Cyber Defence Awareness (which is available for free but registration is required).
- The Cyber Conflict Bibliography by the Jacob Burns Law Library, George Washington University Law School.
- The briefing Cyber defence in the EU: Preparing for cyber warfare? (31 October 2014) by the European Parliamentary Research Service.
- The Tallinn Paper no. 8, published in April 2015: "The Role of Offensive Cyber Operations in NATO's Collective Defence."

Other useful resources include the following:

- Business Continuity Institute, *Good Practices Guidelines 2013, Global Edition: A Guide to Global Good Practice in Business Continuity* (England, 2013). http://www.thebci.org/index.php/resources/the-good-practice-guidelines
- Gustav Lindstrom, "Meeting the Cyber Security Challenge," *GCSP Geneva Papers—Research Series* no. 7 (June 2012).
- International Auditing and Assurance Standards Board, ISAE 3402 Standard for Reporting on Controls at Service Organizations.
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4.
- ITU-D Study Group 1, Final Report, *Question 22-1/1: Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity,* 5th Study Period 2014. See http://www.itu.int/ITU-D/study_groups or http://www.itu.int/pub/D-STG-SG01.22.1-2014

- J. Lewis and K. Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, Washington, DC, 2011.
- National Initiative for Cybersecurity Careers and Studies http://niccs.us-cert.gov/glossary
- Neil Robinson, Luke Gribbon, Veronika Horvath and Kate Robertson, Cybersecurity Threat Characterisation: A Rapid Comparative Analysis (Santa Monica, CA: Rand Corporation, 2013), prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm.
- NIST Special Publication 800-82: Guide to Industrial Control Systems Security, June 2011.
- Ron Deibert and Rafal Rohozinski, *Shadows in the Cloud: Investigating Cyber Espionage 2.0,* joint report by the Information Warfare Monitor and Shadowserver Foundation, JR-03-2010, April 6, 2010. http://shadows-in-the-cloud.net
- U.S. Department of Defense, *The DoD Cyber Strategy,* April 2015, Washington, DC.
- World Economic Forum, *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats.* Industry Agenda item (in collaboration with Deloitte), Ref. 301214, 2015.

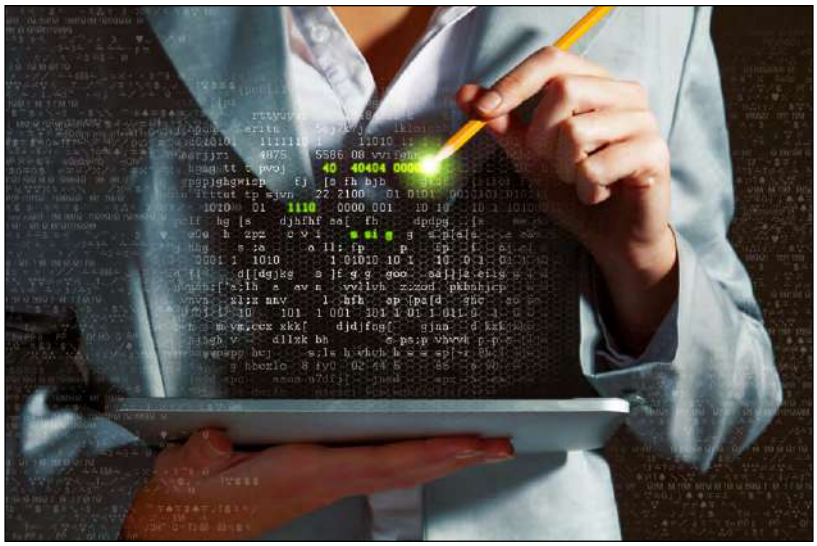


TABLE OF CONTENTS

Theme 1: Cyberspace and the Fundamentals of Cybersecurity

Goal

The object of this theme is to lay the knowledge foundations for all of the instruction that follows by identifying the structural components of cyberspace[3], 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.

Description

The challenges of cyberspace 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. Exploitation of the vulnerabilities may have broad national security implications through deliberate acts of espionage, degradation of command and control facilities, theft of intellectual property and sensitive personal information, disruption of critical services and infrastructure, or economic and industrial damage.

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. Risk analysis must guide and inform the development of cyber architectures and strategy to limit known and unknown vulnerabilities and threats at the organizational and national levels. Accordingly, students are introduced to basic cyber risk analysis methodology and management used to develop systems architecture and strategies aimed at mitigating such risks.

Learning Outcomes

Students will be able to

- describe what is meant by cyberspace and cybersecurity;
- outline some basic vulnerabilities of developed states to cyber threats, such as economic intelligence gathering for national gain, individual and enterprise profiling, data theft, database corruption or the hijacking of industrial control systems or process control systems (e.g., SCADA);
- describe the basic topology of cyberspace, including its physical structures and how it is governed by protocols and procedures; and
- outline the basic considerations for appropriate security architecture.

Suggested References

Lukasz Godon, "Structure of the Internet." http://internethistory.eu/index.php/structure-of-the-internet/

Dave Clemente, "Cyber Security and Global Interdependence: What is Critical?," Chatham House Paper, *The Royal Institute of International Affairs,* ISBN 978-1-86203-278-1, February 2013.

Communications Security Establishment Canada (CSEC), *Harmonized Threat and Risk Assessment (TRA) Methodology,* 23 October 2007.

D.P. Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks,* European Parliament Directorate-General for External Policies of the Union, Directorate B—Policy Department, February 2009, EP/EXPO/B/AFET/FWC/2006-10/Lot4/15 PE 406.997. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem—Full Report,* ENISA, April 2011. http://www.enisa.europa.eu

[3] 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.

R. Tehan, *Cybersecurity: Authoritative Reports and Resources, by Topic,* Congressional Research Service, CRS Report 7-7500 R42507, 15 April 2015. http://www.crs.gov

The White House, *Cyberspace Policy Review,* 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Ethan Zuckerman and Andrew McLaughlin, "Introduction to Internet Architecture and Institutions." https://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html

Cybersecurity Reference Curriculum Writing Team's Workshop in Chisinau.

Block T1-B1: Cybersecurity and Cyberspace — An Introduction

Description

Cyberspace consists of various network-connected computer systems and integrated telecommunications systems. It has become a feature of modern society, enhancing and enabling rapid communication, distributed command and control systems, mass data storage and transfer and a range of highly distributed systems. All of these are now taken for granted by society and have become essential to business, our daily lives and the delivery of services. This ubiquity of and dependency on cyberspace can be seen even in military spheres, where communications, command and control, intelligence and precision strike elements all rely on many "cyber systems" and related communication systems. The ubiquity of these interconnected systems has brought a measure of dependency and vulnerability to individuals, industries, and governments that is difficult to forecast, manage, mitigate or prevent. Some nations view such vulnerable dependencies as an emerging national security or national defense concern and have tasked existing elements of their security forces to respond, while other nations have created wholly new organizations charged with managing or coordinating national cybersecurity policies. Cybersecurity has emerged as an important crosscutting issue that requires responses from individuals, private businesses, non-government organizations, the "whole of government" and a range of international agencies and bodies.

This block aims to familiarize students with the information communication technologies (ICTs) of this domain, revealing their ubiquity and our attendant dependency on such systems. The aim is to develop a broad sociological, technical and cultural appreciation of modern information technology, its multiple roles and the impact of the notional environment of cyberspace to modern life, statecraft and global communications. This block provides a primer for national security students to gain a firm understanding of the topology and constructs of cyberspace and cybersecurity.

For definitional clarity, we have relied on the U.S. National Institute of Standards and Technology (NIST) definition of cyberspace, "the interdependent network of information technology infrastructures, which includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers…." Cybersecurity has been defined as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation." That basic definition shapes what we have included throughout this document.

Learning Outcomes

The student will be able to demonstrate understanding at the appropriate level of

- the significance of information and communication technologies and how they are changing the fabric of modern societies;
- the nuances of cybersecurity in different national and cultural contexts, with an emphasis on their national approach and policies;
- key information communication technology challenges, key providers, key policy sources, key stakeholders, legal responsibilities and functional responsibilities;
- both positive and negative impacts of cyberspace on society;
- broad awareness of the threats and risks to the efficient and secure operation of cyberspace;
- how the Internet is governed, operated and maintained through a network of public, private and not-for-profit institutions;
- the unique national contexts in policy-making and local governance of the Internet;
- the role of standards and protocols in the design of the Internet; and
- the military and political imperatives associated with cyberspace and the governance of the Internet.

Issues for Potential Modules and Approaches to Consider

The depth of exploration will depend on the audience and the time available; however, modules on the national Internet and telecommunications infrastructure, the key service providers and the current division of responsibilities for policies and broad security practices within the national government and defense organization may all be addressed separately for clarity and emphasis.

Learning Method/Assessment

Teaching delivery may include lectures by subject matter experts (SMEs), seminars, demonstrations, exercises and classroom simulations.

Students should be assessed through their participation and discussion in joint reading exercises and debates, followed by a course knowledge test.

References

Jie Wang, A. Zachary Kissel, "Introduction to Network Security: Theory and Practice", Singapore: Wiley, 2015. ISBN 9781118939505. UIN: BLL01017585410.

EU ENISA, "Cybersecurity as an Economic Enabler" Heraklion, Crete, Greece. March 2016. Available at: www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler (Retrieved July 14, 2016).

Bundesamt für Sicherheit in der Informationstechnik (BSI), "The State of IT Security in Germany, 2015". Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2

F. Lantenhammer, A. Scholz, A. Seidel, A. Schuttpelz, A, "Cyber Defence und IT-Security Awareness", in, *Europäische Sicherheit & Technik : ES&T.* No.8,, 2012. Journal ISSN: 2193-746X. UIN: ETOCRN316565061.

SMEs will work with the host country to select appropriate key readings based on planned course focus and time requirements.

Selected readings may include the following:

"'G.I.G.O. Garbage In, Garbage Out' (1969) Computer History—A British View" on YouTube, accessed 25 April 2015. http://youtu.be/R2ocgaq6d5s

James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press), 1986.

Vinton G. Cerf (Chair) et al., *ICANN's Role in the Internet Governance Ecosystem,* report of the ICANN Strategy Panel, 20 February 2014.

Paul E. Ceruzzi, *A History of Modern Computing,* 2nd ed. (Cambridge, Mass.: MIT Press), 2003.

Paul Hoffman, ed., "The TAO of IETF: A Novice's Guide to the Internet Engineering Task Force," Internet Engineering Task Force, 2015.

Barry Leiner, Vinton Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, "Brief History of the Internet," accessed 25 April 2015. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Marie-Laure Ryan, Lori Emerson and Benjamin J. Robertson, eds., *The Johns Hopkins Guide to Digital Media* (Baltimore: Johns Hopkins University Press), 2014.

Lance Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation," *Western Journal of Communication* 63, no. 3 (1999): 382–412. doi:10.1080/10570319909374648

The White House, *International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World* (Washington, DC: Executive Office of the President of the United States, National Security Council), 2011.

T1-B2: Information Security and Risk

Description

Generally, information security (IS) is relevant across broad categories of information—private, public, sensitive, classified, etc.—that require practices and protocols to manage, whether in digital or other formats. In the cyber domain, it is hackers, criminals and foreign intelligence services that are interested in exploiting any weaknesses in the IS regime. This block introduces students to the general concept of information security and risk, with an emphasis on the cyber domain[4]. Later in this course they will be given a more detailed explanation of their national approach to information security (see Theme 4). Here, discussion should move from how information is classified to the distinction between information security and information assurance, and it should progress through an exploration of the various types of cybersecurity vulnerabilities and a review of the attack process or "kill chain" for cyber incidents. Discussion then moves to managing information security risk through approaches such as the Threat and Risk Assessment (TRA) model[5], particularly in light of advanced persistent threats (APTs)[6]. Without detailed exploration at this stage, the students should be made aware of the major national and organizational bodies responsible for articulating their IS polices, procedures and practices.

Background

IS comprises the mechanisms and processes that allow access to physical assets and data contained on or flowing across those systems. Information security is focused on the technology and operations concerned with security applications and infrastructure. Information assurance (which may be given different titles nationally) includes information security issues but also includes a focus on information management, data integrity and protection regimes and protocols to reduce or manage overall risks and mitigate the impact of incidents. The key security objectives generally include confidentiality, integrity, availability, authentication and non-repudiation. There are individual, organizational/enterprise and national-level information security practices and regimes.

Learning Outcomes

The student will demonstrate a familiarity with or knowledge of

- the security classification standards for information and information and electronic systems;
- threat and risk analysis explored at the appropriate level; and
- various sample "cyber kill chains."

Students will

- be able to define key relevant terms (data, knowledge, information, information security, cyber kill chain);
- understand information assurance and the significance of the security objectives of confidentiality, integrity, availability, authentication and non-repudiation;
- be able to explain the role of threat vulnerability risk analysis in the management of information security; and
- be able to identify the organizations responsible for articulating their national information security policies, practices and procedures.

Issues for Potential Modules and Approaches to Consider

- Evolution of information security
- Sources for international good practices
- Identification of the essential national cybersecurity authorities

Learning Method/Assessment

Teaching delivery may include lectures and demonstration with illustrations of actual practices and cases. The students should be able to define information security, the cyber kill chain, APT and TRA.

References

A. Rutowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin and T. Takahashi, "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)," ACM SIGCOMM *Computer Communication Review,* Vol. 40, no. 5, 2010. Available at: http://www.beepcore.org/p59-3v40n5i-takahashi3A.pdf

[4] Electronic IS often aims at a minimum to ensure service continuity, confidentiality, integrity, availability, authentication and non-repudiation—i.e., appropriate access at the appropriate level for authorized users.

[5] As will be explained further, the TRA model weights information assets, threats, vulnerabilities and controls.

[6] Here, the "advanced" means coordinated, purposeful and sophisticated and the "persistent" means continuous. In particular, APTs entail "smart" agents with intent, seeking opportunity to read, alter, corrupt, deny access to, exploit or destroy cyber capabilities.

Babak Akhgar et al "Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies". Amsterdam: Butterworth-Heinemann, 2015. ISBN 9780128019733. British Library Shelfmark: General Reference Collection DRT ELD.DS.28766. UIN: BLL01017039420.

M. Watin-Augouard, "Cyber-Menaces: Un Trait Saillant du Livre Blanc", in, *Administration: Revue d'étude et d'information Publiée par l'Association du Corps Préfectoral et des Hauts Fonctionnaires du Ministère de l'intérieur.* No.239, 2013. Journal ISSN: 0223-5439.

H. Fukatsu, "IT Security Against Cyber Attacks; A Common Thread for Both Developed and Developing Countries", in, Nihon Igaku Ho shasen Gakkai zasshi ; Asian Oceanian Congress of Radiology; AOCR 2014; Kobe, Japan. Journal ISSN: 0048-0428. British Library Shelfmark: 6113.254000. UIN: ETOCCN087891561

Safa, Nader Sohrabi, Rossouw Von Solms, and Lynn Futcher. "Human aspects of information security in organisations." Computer Fraud & Security 2016, no. 2 (2016): 15-18.

Alshaikh, Moneer, Sean B. Maynard, Atif Ahmad, and Shanton Chang. "Information Security Policy: A Management Practice Perspective." arXiv preprint arXiv:1606.00890 (2016).

Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems,* 2nd Edition (Indianapolis, IN: Wiley), 2008.

Australian Government, Department of Defence, Intelligence and Security, 2015 *Australian Government Information Security Manual: Controls,* issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. http://www.protectivesecurity.gov.au

Australian Government, Department of Defence, Intelligence and Security, *2015 Australian Government Information Security Manual: Principles,* issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. http://www.protectivesecurity.gov.au

Communications Security Establishment Canada, *Harmonized Threat and Risk Assessment (TRA) Methodology,* 23 October 2007.

D.E. Gelbstein, *Information Security for Non-Technical Managers,* 1st Edition, 2013. ISBN 978-87-403-0488-6.

Eric M. Hutchins, Michael J. Clopperty and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proceedings of the 6th International Conference on Information Warfare and Security,* Washington, DC, 17–18 March 2011.

Information Systems Audit and Control Association (ISACA), *Advanced Persistent Threat Awareness Study Results,* USA, 2014.

Richard Kissel, ed., *Glossary of Key Information Security Terms,* NIST Interagency Report (IR) 7298 Revision 2, NIST, Computer Security Division, Information Technology Laboratory, May 2013.

Gil Klein, "Unlocking the Secrets of Cybersecurity: Industry experts discuss the challenges of hacking, tracking, and attacking in a virtual world," University of Maryland University College *Achiever* (Spring 2013): 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

Gary Stoneburner, *NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security,* NIST, December 2001.

"Common Criteria for Information Technology Security Evaluation," accessed 17 July 2015. http://www.commoncriteriaportal.org/

International Organization for Standardization Information Technology series:

1) ISO/IEC 27001:2013 Information Technology—Security Techniques—Information Security Management Systems—Requirements
2) ISO/IEC 27005:2011 Information Technology—Security Techniques—Information Security Risk Management
3) ISO/IEC 27031:2011 Information Technology—Security Techniques—Guidelines for Information and Communications Technology Readiness for Business Continuity
4) ISO/IEC 27032:2012 Information Technology—Security Techniques—Guidelines for Cybersecurity

T1-B3: The Structures of Cyberspace: The Internet Backbone and National Infrastructures

Description

This block aims to introduce students to the technical fabric of cyberspace, with a focus on global, national and enterprise infrastructure; this includes the architecture of the Internet, computer networks and cellular networks. The logic of the general structure and the specific national topology (i.e., the specifics of the national infrastructure supporting networks, telecommunications providers and routing conduits) should form the major focus of this block.

Background

The architecture of the Internet backbone comprises the key data routes between the principal large computer network systems and core routers. Commercial, government, academic and other high-capacity network centers host these networks and routers. They control Internet exchange points and network access points, and they exchange Internet traffic between countries and continents. Commonly, large Internet service providers (ISPs) (e.g., Tier 1 networks) participate in the exchange of Internet backbone traffic through privately negotiated interconnection agreements. Internet service providers that manage discrete subdivisions of the Internet called Autonomous Systems (AS) are registered and assigned an Autonomous System Number (ASN). Routing and reachability between autonomous systems are implemented via a set of Internet core routers using the Border Gateway Protocol (BGP). The management of the relationship between domain names (e.g. www.google.com) and the routable Internet addresses controlled by the AS is performed by the Domain Name System (DNS) and its own registration authorities.

A National Internet Registry (NIR) is an organization assigned responsibility for coordination of IP (Internet Protocol) address allocation and other Internet resource management functions at a national level through an international Internet registry. A national government may also regulate the ISPs within its economic region.

Cellular telephone/mobile device networks now make up a large element of the Internet distribution infrastructure. These networks interconnect with the Internet and are referred to as the "mobile Web." Their general architecture and the national specifics should also be explored in this block.

Learning Outcomes

Students will

- have an in-depth understanding the physical and virtual topology and governance of the Internet backbone;
- be able to explain the role of ASNs in the global interconnection of the Internet and the responsibility of the Internet Assigned Numbers Authority (IANA);
- understand the relationship between high-level (Tier 1) ISPs, subordinate ISPs and end-user local area networks (LANs);
- be able to explain the role of authoritative name servers in the global interconnection of the Internet and the responsibility of the Internet Corporation for Assigned Names and Numbers (ICANN);
- understand the topology and geography of their national cyberspace, including national registries and ISP governance authorities; and
- be familiar with the structure and governance of cellular/mobile networks and their Internet connectivity in the national context.

Issues for Potential Modules and Approaches to Consider

To provide an effective introduction to non-technical audiences, those using this reference curriculum to frame a specific course or courses will have to give a good deal of consideration to finding the appropriate level of technical detail to ensure that the material is comprehensible to their students.

National network and telecommunications infrastructures may be explored at some depth.

Learning Method/Assessment

The teaching delivery may be by lecture and demonstration. Tours of national facilities, expert briefings and challenging oral and practical examinations may enliven the curriculum.

References

Konstantinos Moulinos, Rossella Mattioli, EU ENISA, "Communication network interdependencies in smart grids", Heraklion, Crete, Greece. March 2016. Available

at: www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids (Retrieved July 14, 2016).

Abdulrahman Alqahtani. "Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study" Information and computersecurity. Vol 23, No 5; 2015; 532-569. Journal ISSN: 2056-4961. British Library Shelfmark: 4481.796000. UIN: ETOCvdc_100027180236.0x000001

E. Sitnikova, E. Foo, R.B. Vaughn, "The Power of Hands-On Exercises in SCADA Cyber Security Education", International Federation for Information Processing -Publications- IFIP.; Information security education; Heidelberg; Springer; 2013. Journal ISSN: 1868-4238. British Library Shelfmark: 4540.183500. UIN: ETOCCN085265877

O. Netkachov, P. Popov, K. Salako, "Quantification of the Impact of Cyber Attack in Critical Infrastructures", in, *Journal on Data Semantics; Reliability and Security Aspects for Critical Infrastructure Protection,* Florence, Italy, 2014; Sep, 2014, pp 316-327. Journal ISSN: 0302-9743. UIN: ETOCCN088306466.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. The Turn to Infrastructure in Internet Governance. Springer, 2016.

ICANN, "Beginner's Guide to Domain Names," 6 December 2010.

Internet Assigned Numbers Authority, *The IANA Functions: An Introduction to the Internet Assigned Numbers Authority (IANA) Functions,* ICANN, June 2015.

Paul Krzyzanowski, "Understanding Autonomous Systems: Routing and Peering," 5 April 2013, accessed 17 July 2015. https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

Michael Miller, "How Mobile Networks Work," Pearson Education, Que Publishing, 14 March 2013, accessed 17 July 2015.

Ram Mohan, "Attacking the Internet's Core," SecurityWeek website, 16 March 2011, accessed 17 July 2015. http://www.securityweek.com/attacking-internets-core

Jeff Tyson, "How WAP Works," HowStuffWorks website, accessed 17 July 2015. http://computer.howstuffworks.com/wireless-internet3.htm

Rudolph van der Berg, "How the 'Net works: An introduction to peering and transit," 2 September 2008, accessed 17 July 2015. http://arstechnica.com/features/2008/09/peering-and-transit/4/

T1-B4: Protocols and Platforms

Description

Communicating systems use well-defined message formats, called protocols, for exchanging messages. A communication protocol is a system of rules for exchange of data within or between computers (networked or not). The protocols might be thought of as similar to the components of an address on an envelope placed in the mail, identifying the sender, the receiver and their respective coordinates. Each message has an exact meaning intended to elicit a response from a range of possible responses pre-determined for that particular situation. Thus, a protocol must define the syntax (rules), semantics (meaning) and synchronization of communication; the specified behavior is typically independent of how it is to be handled or the various systems that it may pass through in order to reach the intended destination.

Each protocol layer and process has its inherent vulnerabilities and risks, which may be explored at various levels of expertise. This topic may be discussed at a very basic level but, given the appropriate audience, it may be explored at the classified level.

Background

There are two ways to envision and design a network system.

The logical view of how the Internet works can be considered to be protocol-based. A protocol stack is the software implementation of a set of communications protocol standards. Protocol stacks govern how data is packaged and moved. The protocol implementations are typically arranged in a layered architecture (i.e., a stack). Protocol implementations close to the bottom of the stack perform more primitive communications services, such as the basic communication of a small chunk of data to another computer on the local network (for example, Ethernet). Higher up the stack, the protocols provide services such as common addressing for global networks (e.g., IP), error correction and reassembling larger data objects (e.g., TCP, or Transmission Control Protocol). The highest-level protocols provide the most abstract application-level services, such as delivering e-mail (SMTP (Simple Mail Transfer Protocol)) or web page browsing (HTTP (Hypertext Transfer Protocol)). The higher layers in the protocol stack are dependent upon the more basic services of the layers below.

Alternatively, a physical view of the Internet can be described by how protocols are implemented across network devices and platforms (such as switches and routers, gateways, proxies and firewalls) and the forms of interconnection among these network devices. For example, network switches implementing the Ethernet protocol may connect computers on the LAN. The LANs may be connected to network routers implementing the IP to redirect packets of data between networks and perhaps the rest of the Internet. A mail server connected to the network might implement the SMTP.

A straightforward mapping of the relationship between physical devices and their responsibility for protocol implementation is made difficult in contemporary networks by the introduction of virtual devices and networks. In such networks, the network devices and their interconnection can be implemented virtually by software running on large servers (as in the case of "cloud computing"). The virtualization of these systems adds a layer of complication to security and is an emerging issue that must be addressed.

Protocol stacks can be designed and implemented for specialized applications. Industrial control systems (ICSs) such as SCADA (Supervisory Control and Data Acquisition) are an example of network communications protocol stacks being used for reporting sensor measurement data and sending control messages. In a power grid, for instance, they may be responsible for monitoring loading and switching supply connections based on shifting demand. The security of SCADA systems is an important topic in the sphere of national infrastructure security because the systems they control may be of national significance. Many modern weapons systems employ electronic systems similar to those of industrial SCADA and they also may be vulnerable.

Each protocol layer has its inherent risks and vulnerabilities. These can be explored at various levels of expertise, from general knowledge to expert (classified) level.

Definition of network security protocol

In general, network security protocols provide the security and integrity of data in transit over a network connection. Network security protocols define the processes and methodology to secure network data. No security protocol ensures security. Rather, each protocol provides a particular way of thwarting a specific approach to attacking the system or network. Note: there may be specific national or agreed international definitions that apply.

Network security protocols often employ cryptography and encryption techniques to secure the data so that it can be decrypted or altered only with a specific algorithm, logical key, mathematical formula and/or combination of these. Popular network security protocols include Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

Learning Outcomes

Students will be able to

- describe and discuss the role and responsibilities of each of the standard network protocol stack layers (TCP-/IP-based Internet protocol suite);
- describe common network devices such as hubs, switches, routers, gateways and application servers, the relationship between the devices' implementation of network protocol stack layers and their functional role in the network;
- discuss the basic concepts of the virtualization of network devices and software-defined networks, the impact of these concepts on network architecture and their relationship to cloud computing environments;
- describe the basic elements of a SCADA-based ICS environment (this can include ICS-specific components and their operating foundations in standard Internet protocols); and
- identify and describe common security protocols, their relationship to the protocol-based layered network architecture and the particular security vulnerability each protocol is designed to address.

Issues for Potential Modules and Approaches to Consider

Industrial control systems (e.g., SCADA) and military platform IT systems (PIT systems) could be explored in some detail to identify their vulnerabilities and their attractiveness as targets.

Learning Method/Assessment

Lecture, demonstration and case studies are recommended. Assessment should be in written form and grounded at the appropriate level given the particulars of any particular course derived from this curriculum.

References

E. van Baars, R. Verbrugge, R. "A communication algorithm for teamwork in multi-agent environments", *Journal of Applied Non-Classical Logics, Logic and information security;* Leiden, The Netherlands, 2008; Sep, 2009, 431-462, Lavoisier; 2009. British Library Shelf Mark: 4943.400000, UIN: ETOCCN074941483

C.W. Chan "Key Exchange Protocols for Multiparty Communication Services", International Symposium on Cyber Worlds; Tokyo, 2002. Conference ISBN: 0769518621. British Library Shelfmark: 4550.208900. UIN: ETOCCN046776823.

Jan Jatzkowski, Bernd Kleinjohann, "Self-Reconfiguration of Real-Time Communication in Cyber-Physical Systems", 2016. Electronic paper held at the British Library. UIN: ETOCvdc_100033448082.0x000001.

J. Ivimaa, T. Kirt, "Evolutionary Algorithms for Optimal Selection of Security Measures". Proceedings of the 10th European Conference on Information Warfare and Security at the Tallinn University of Technology Tallinn, Estonia July 7-8, 2011, pp. 172-184. Rain Ottis (eds). ISBN 9781908272065 (pbk.) UIN: BLL01015873308.

Qadir, Junaid, Arjuna Sathiaseelan, Liang Wang, and Barath Raghavan. "Approximate Networking for Global Access to the Internet for All (GAIA)." arXiv preprint arXiv:1603.07431 (2016).

IEEE Standards Association, IEEE 802 Standards. http://standards.ieee.org/about/get/

Internet Engineering Task Force, Request for Comments (RFC), accessed 17 July 2015. https://www.ietf.org/rfc.html

Certiology, Network Devices, accessed 17 July 2015. http://www.certiology.com/computing/computer-networking/network-devices.html

Cisco Systems Inc., Virtual LANs VLAN Trunking Protocol (VLANs VTP), accessed 17 July 2015. http://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html

D. Clark, "The Design Philosophy of the DARPA Internet Protocols," *Proceedings of SIGCOMM '88,* 106–14 (New York: Association for Computing Machinery), August 1988.

Kevin R. Fall and W. Richard Stevens, *TCP/IP Illustrated, Volume 1: The Protocols,* 2nd edition, Addison-Wesley Professional Computing Series (Boston, MA: Addison Wesley Professional), 15 November 2011.

Juniper Networks, Inc., "White Paper: Architecture for Secure SCADA and Distributed Control System Networks," 2010, accessed 17 July 2015. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

Radia Perlman, "Tutorial on Bridges, Routers, Switches, Oh My!," accessed 17 July 2015. https://www.ietf.org/proceedings/62/slides/protut-0.pdf

Bart Preneel, "Internet Security Protocols," video of lecture given at SecAppDev 2013, Leuven, Belgium. https://www.youtube.com/watch?v=CZzd3i7Bs2o

Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks,* 5th edition (New York: Pearson), 27 September 2010.

T1-B5: Security Architecture and Security Management

Description

This block deals with basic security architecture (BSA), which includes technological and operational aspects and the human and management contexts that influence its form. The BSA at the national level establishes security architecture and practices to include infrastructure (e.g., telecommunications backbones), national-level content filters and governance structures for cybersecurity. The general goal of this block is to teach the students how to design/construct security environments based on risk analysis so that the risks are within acceptable thresholds. The architecture would include technical controls, physical controls, policies and training. Examples of technical controls are firewalls, intrusion detection systems and log management. Examples of physical controls include access management, fire alarms and moisture control. Students will learn how to conduct risk analysis and security configuration at a national level as well as at individual and organizational levels.

The BSA is informed by national policies, various security standards, system life cycle, design principles and physical architectural elements. In its examination of the design of BSAs, this block explores complementary concepts of appropriate control of assets, physical and environmental control, management plans, human aspects including screening of employees, continuity of operations, contingency plans, and cyber systems resilience.

Background

Security architecture should be policy-driven. That is, it begins with an understanding of the information assets under management. Central to this consideration is the value of the information assets to the defender (i.e., the impact of their loss or alteration) and the value of these assets to potential threat actors. It is this asset identification and valuation phase that drives the development of the policy for controlling access to information.

The threat assessment phase identifies threat actors who could reasonably be expected to compromise the identified assets, and it identifies their technical capability. The development of security architecture is driven by the requirement to design a physical system and the associated assurance criteria and operations procedures that reduce the risk of the identified threat actors being capable of compromising the identified assets. There may be national standards for threat and risk assessment and for design considerations and guidance in the selection of access control mechanisms and architectural layouts.

The selection and organization of enterprise security architecture is often described as a defense-in-depth, in which the coordinated use of multiple security mechanisms protects the integrity of the information assets. The defense of information assets begins with access controls on their data and moves outward, through the security mechanisms in the applications that access the data, the computer hosts that the applications run on and the fabric of the enterprise network, to the security perimeter of the enterprise, where it joins global network infrastructure.

The enterprise security architecture incorporates a suite of mechanisms designed to mitigate the risk for that particular enterprise. Common mechanisms, or architectural elements, for implementing security policy include network zoning, firewalls, intrusion detection systems (IDSs), anti-virus applications, cryptographic techniques and security information and event management (SIEM) systems. No single one of these systems will ensure security. Attack techniques are varied and can exploit vulnerabilities in the many protocols, systems and software applications comprising the enterprise infrastructure.

Security assurance activities are actions taken during development and evaluation of the enterprise security architecture to ensure that the security measures in place for a system are effective. Note: in some instances such measures may prove more notional than real. For example, a data access control product will have an advertised set of security functionalities. A related assurance activity might be methodical testing of this functionality by a recognized standards organization to provide evidence that the product performs the correct function, without error. Other examples of assurance activities are formal or semi-formal design reviews, development of security guidance documents and manuals for the user community and operators of the systems, management of security component life cycles, configuration management, management of the security of the architectural component developer/manufacturer environments, and trusted delivery of the architectural components from the developer/manufacturer to the enterprise environment. Security assurance also

includes programs to provide background checks and security clearances for personnel to establish a level of trust in the users and operators of the systems.

Learning Outcomes

Student will

- Be able to discuss how the multiple layers of security mechanisms are placed throughout a defense-in-depth enterprise architecture to provide redundancy in the event that security controls fail or a vulnerability is exploited;
- Be able to suggest, at a rudimentary level, appropriate security zoning and the placement of measures such as firewalls using a network diagram;
- Be aware of and understand the scope of national standards and guidance documents for conducting threat and risk assessments, setting enterprise/organizational security policy and implementing security architecture;
- Understand the relationship of the asset identification phase of threat and risk assessment (TRA) to the specification of security policy for the enterprise;
- Understand the relationship of the threat assessment phase of the TRA to the identification of exploitable vulnerabilities by expected threat agents and understand how that drives the requirements for security measures deployed across the architecture of the enterprise; and
- Be aware of and understand the scope of the national security classification system for the protection of documents and information and be able to describe its relationship to personnel screening and security clearance programs.

Issues for Potential Modules and Approaches to Consider

Various forms of system architecture management and network security zoning should be discussed to enable the students to assess the models their organization has adopted or should adopt.

Human factors engineering and social engineering exploitation gambits may warrant detailed examination.

The basic national security classification system for physical access, the protection of documents and information, personnel screening and security clearance programs may require review and summation.

Learning Method/Assessment

Teaching delivery may include small-group work on the human, technological and operational aspects.

Guest lectures from private and state organizations can enliven the discussion and learning experience.

Means of assessment will depend on the level of knowledge required as appropriate for the specific students being taught.

References

S.A. Chun, V. Atluri, B.B. Bhattacharya, "Risk-Based Access Control for Personal Data Services", *Statistical Science and Interdisciplinary Research;* International Conference on Information Systems Security; Algorithms, Architectures; Kolkata, India, 2006; Dec, 2009, 263-284. Journal ISSN: 1793-6195. Conference ISBN: 9789812836236; 9812836233. British Library Shelf Mark: 8448.954000. UIN: ETOCCN071364080.

Gérard Desmaretz, *Cyber Espionnage, Ou, Comment Tout le Monde épie Tout le Monde!,* Paris: Chiron, 2007. ISBN 9782702712122 (pbk.) UIN: BLL01014343705.

A. Rutowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin and T. Takahashi, "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)," ACM SIGCOMM Computer Communication Review, Vol.40, No.5, 2010.

I. Atoum, A. Otoom, A.A. Ali, "A Holistic Cyber Security Implementation Framework", in, *Information Management & Computer Security,* Vol.22; No 3, 2014, pp 251-264. Journal ISSN: 0968-5227. UIN: ETOCRN359424579.

Yoo, Hyunguk, and Taeshik Shon. "Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture." Future Generation Computer Systems 61 (2016): 128-136.

Australian Government, Department of Defence, Intelligence and Security, *Australian Government Information Security Manual: Controls,* issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. See www.protectivesecurity.gov.au

Australian Government, Department of Defence, Intelligence and Security, *Australian Government Information Security Manual: Principles,* issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. See www.protectivesecurity.gov.au

Deborah J. Bodeau and D.J. Graubart, "Cyber Resiliency Engineering Framework," MITRE Technical Report MTR 110237 (Bedford, MA: The MITRE Corp.), September 2011.

Communications Security Establishment Canada, *Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22),* June 2007.

Communications Security Establishment Canada, *Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1),* 23 October 2007.

Communications Security Establishment Canada, *Information Technology Security Guideline: Network Security Zoning: Design Considerations for Placement of Services within Zones (ITSG-38),* May 2009.

Communications Security Establishment Canada, *Information Technology Security Guideline: User Authentication Guidance for IT Systems (ITSG-31),* March 2009.

George Farah, "Information Systems Security Architecture—A Novel Approach to Layered Protection: A Case Study," GSEC Practical Version 1.4b, SANS Institute, 9 September 2004. www.sans.org

D.E. Gelbstein, *Information Security for Non-Technical Managers,* 1st Edition, 2013. ISBN 978-87-403-0488-6.

Gil Klein, "Unlocking the Secrets of Cybersecurity: Industry Experts Discuss the Challenges of Hacking, Tracking, and Attacking in a Virtual World," University of Maryland University College *Achiever* (Spring 2013): 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

Alexander Klimburg, ed., *National Cyber Security Framework Manual,* NATO CCD COE Publication, Tallinn, Estonia, 2012. ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

William Pelgrin, "A Model for Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factors, and Leadership", Center for Internet Security.

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?" paper by the Working Group Security Architecture, Information Security Society Switzerland (ISSS), 29 September 2008.

NATO and non-NATO members unite in authoring Cybersecurity Reference Curriculum. Meeting of the Moldovan Minister of Defence with the editors.

Cybersecurity Reference Curriculum Writing Team's Workshop in Tbilisi (Contributors from University of Greenwich and the Royal Military College of Canada).

Cybersecurity Reference Curriculum Writing Team's Workshop in Tbilisi (Contributors from NATO School Oberammergau, i-intelligence and SLCE).

Theme 2: Risk Vectors

Goal

This theme 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 essential component of risk assessment and mitigation policy, as will also be explored.

Description

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 (see Chabinsky 2010 in References): "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.

The broad objective of this theme is to provide a general grounding in the range of vulnerability issues inherent to the components of cyberspace. However, those developing courses informed by this curriculum document may choose do so at an expert and classified level in order to address actual national policies and procedures.

Learning Objectives

Students will be able to

- understand the significance and possible impact of exploited supply chain, remote, proximity and insider access to target cyberspace vulnerabilities and those associated with facilitating enhanced mobility, and
- identify the types of security trade-offs associated with enhanced mobility and the other risk vectors identified in this theme area.

Suggested References

Steven R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line" *Journal of National Security Law & Policy 4,* no. 27 (August 2010): 27–39. http://jnslp.com/wp-content/uploads/2010/08/04_Chabinsky.pdf

Wenke Lee and Bo Rotoloni, *Emerging Cyber Threats Report 2015,* report prepared by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) for the Georgia Cyber Security Summit, 2014. https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf

Louis Marinos, *ENISA Threat Landscape 2013: Overview of Current and Emerging Cyber-threats,* ENISA, 11 December 2013, ISBN 978-92-79-00077-5. http://www.enisa.europa.eu, doi:10.2788/14231

Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka and Jason Frye, *Cyber Threat Metrics,* Sandia National Laboratories, March 2012. http://fas.org/irp/eprint/metrics.pdf

Francesca Spinalieri, *Joint Professional Military Education Institutions in an Age of Cyber Threat,* report, Pell Center for International Relations and Public Policy, Salve Regina University, August 2013.

U.S. Office of Director of National Intelligence, *Understanding Cyber Threats: A Guide to Small and Medium Sized Businesses,* Intelligence Community Analyst, Private Sector Program, 2014.

ISO standards on Risk Assessment/Risk Management.

T2-B1: Supply Chain/Vendors

Description

This block addresses the issue of supply chain vulnerabilities and introduces the concept of best practices for supply chain risk management (SCRM).

The whole supply chain is a known vulnerability. Monitoring and securing of supply chains can be extremely challenging in the global marketplace. Supply chain security challenges include integrity and quality and security assurance as well as prevention of disruptions, exploits and follow-on attacks. Global supply chains include the routes taken by sensitive equipment from the production stage through shipment, for both single components and finished products such as hardware and software. Supply chains are vulnerable to disruption: products may be intercepted and tampered with and defective elements or malicious code may be introduced at various stages of their manufacture, shipping, storage, installation or repair, and valuable data may be extracted during disposal. Thus, tampering may occur anywhere in a product's life cycle. Other nodes of an institutional or national infrastructure can also be compromised through the supply chain or through vendors, resulting in unusual breaches. Can your providers guarantee sufficient security? What needs to be done to create security in the whole supply chain?

Learning Outcomes

Students will

- understand key challenges regarding the life cycle of products, from cradle to grave;
- be able to explain the role of configuration management (i.e., system design) in relation to supply chain security; and
- understand the role and requirements of articulated policies and practices for supply chain risk management.

Issues for Potential Modules and Approaches to Consider

- Vulnerabilities of supply chain to cyber crime and espionage
- Risk mitigation approaches and best practices
- Existing national supply chain risk mitigation policies and practices

Learning Method/Assessment

Teaching delivery may include lectures and case studies of breaches and consequences.

Individual assignment: Find an example of a supply chain breach and identify possible remedies.

Possible: Map a supply chain and identify risk areas.

References

A. Sokolov, V. Mesropyan, A. Chulok, A, Aje, "Supply Chain Cyber Security: A Russian outlook", *Technovation: an International Journal of Technical Innovation and Entrepreneurship.* 2014. Vol 34; No. 7; 2014, 389-391. Journal ISSN: 0166-4972. British Library Shelfmark: 8761.150000. UIN: ETOCRN353289650.

Florin Gheorghe Filip, Luminita Duta, "Decision Support Systems in Reverse Supply Chain Management", Elsevier Paper, 2015. UIN: ETOCvdc_100030799942.0x000001.

Dmitry Ivanov, Alexandre Dolgui, Boris Sokolov, Boris, Frank Werner, Marina Ivanova, "A Dynamic Model and an Algorithm for Short-Term Supply Chain Scheduling in the Smart Factory Industry 4.0", in *International Journal of Production Research,* Vol.54, Issue 2, (2016); 2016; pp 386-402. Journal ISSN: 0020-7543. (Electronic). British Library Shelfmark: ELD Digital store 4542.486000. UIN: ETOCvdc_100031962439.0x000001

J. Sztipanovits, et al. "OpenMETA: A Model-and Component-Based Design Tool Chain for Cyber-Physical Systems", in Journal on Data Semantics. No. 8415, (2014), pp 235-248. Journal ISSN: 0302-9743. UIN: ETOCRN350535700.

Lu, Tianbo, Xiaobo Guo, Bing Xu, Lingling Zhao, Yong Peng, and Hongyu Yang. "Next Big Thing in Big Data: The security of the ict supply chain." In Social Computing (SocialCom), 2013 International Conference on, pp. 1066-1073. IEEE, 2013.

Jon Boyens, Celia Paulsen, Rama Moorthy and Nadya Bartol, Supply Chain Risk Management for Federal Information Systems and Organizations, NIST Special Publication 800-161, Second Public Draft, U.S. Department of Commerce, Washington, DC, 2014.

Steven R. Chabinsky "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines," *Journal of National Security Law & Policy 4,* no. 1 (2010): 27.

Trusted Computing Group. Fact Sheet. 2009. http://www.trustedcomputinggroup.org/files/resource_files/7f38fa36-1d09-3519-add14cb3d28efea6/fact%20sheet%20May202009.pdf

Luca Urciuoli, Toni Männistö, Juha Hinsta and Tamanna Kahn. "Supply Chain Cyber Security—Potential Threats," *Information & Security: An International Journal 29,* no. 1 (2013): 51–68. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

U.S. Government Accountability Office, "Addressing Potential Security Risks of Foreign-Manufactured Equipment," testimony of Mark L. Goldstein, Director, Physical Infrastructure Issues, before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives, U.S. Government Accountability Office, GAO-13-652T, 21 May 2013. http://www.gao.gov/assets/660/654763.pdf

T2-B2: Remote- and Proximity-Access Attacks

Description

Cyber attacks can be considered to be either remote or local. Local attacks, however, can be categorized as those conducted through proximity access to systems or through a trusted insider. Insider attacks are addressed separately in Block T2-B3. Remote access refers to all methods and approaches taken to access or disrupt networks where there is no apparent physical access to the system's hardware. In a remote attack, an attacker may have had no prior physical access to the system under attack; the attacker's access is via a network or other communication device and the attacker may have no previously established privilege on the system. Conversely, in local attacks, an attacker generally has some form of established access or privilege on or to the system and attempts to increase his/her level of privilege to gain unauthorized access to information. Such activity conducted by a malign actor who is not a trusted insider we will address as a proximity-access attack in this document. As Chabinsky (2010) explains, "proximity access–based attack" refers to the ability of a malign actor to disrupt, intercept or otherwise access networks and computer systems while in close proximity to their various components, such as workstations, cables or wireless receivers. Proximity access is a form of remote access. Common techniques such as wireless "sniffing" (interception of and access to information sent over wireless networks), keyboard stroke recording, screen capture, man-in-the-middle interception and insertion of malicious code through physical means are ways in which attackers can use proximity access to exploit vulnerabilities.

This block considers remote- and proximity-access attacks (those that are not insider attacks). This block aims to highlight the most common known risks associated with remote- and proximity-access attacks and discusses various means to mitigate or thwart such efforts.

Background

In classic network applications, there is a concept of client and server. A "client" software application sends requests to a "server" software application in accordance with some protocol, asking for information or for an action to be performed. The client always initiates the communication. The server always waits to be contacted at some known address on the network. Protocols controlling this behavior include web services (HTTP or HTTPS), file transfer services (FTP) and e-mail services (SMTP, POP3 or IMAP). Remote attacks can target vulnerabilities in the server (software or configuration errors) that allow the attacker to access information from or even gain remote control of the server computer.

Remote server-side attacks can be conducted if the attacker can identify a misconfiguration or error in the software implemented on the server. For example, an error in the configuration settings might allow an attacker to inappropriately enter a mode reserved for system maintenance, thus gaining very broad access to the system. Another example is an attack on an HTTP web server that uses a database back end to provide its data resources. Improperly vetted web page requests from an attacker can allow the attacker to pass dangerous database command strings to the back end database; this can give control of the database to the attacker. This style of attack is called "SQL (Structured Query Language) injection."

The advent of better protection for servers (firewalls, access control, etc.) has moved the focus of attack from the server to the client applications. However, client applications cannot be contacted directly on the network; client applications are always the initiators of communication exchanges. Instead, the attacker must find a way to entice the user of the client application to contact a malicious server that can corrupt the client application during the exchange. Such luring or entrapment activities, referred to by a variety of names, are distinct ploys employing principals of social engineering to convince the operator to undertake behaviors such as opening an infected e-mail attachment.

Learning Outcomes

The primary objective of this block is to ensure that students see the range of risks associated with remote- and proximity-access attacks.

Students will

- understand and be able to describe a remote access–based attack scenario, identify the constituent parts of such an attack, and contrast this with proximity access–based attack scenarios;
- be familiar with the structure of client-server-based applications and their network topology and be able to identify how common protocols

such as HTTP, HTTPS, FTP and e-mail protocols fit this model;

- be able describe how server-side attacks are informed through an intelligence-gathering phase using techniques such as network vulnerability analysis tools and fuzzing and explain why network vulnerability analysis tools are valuable to both the attacker and the defender;
- have a rudimentary knowledge of server-side attack scenarios such as exploitation of weak configurations, IP spoofing, Denial of Service and Distributed Denial of Service (DoS and DDoS), SQL injection and network protocol–based buffer overflows;
- be able to describe how the maturing of security at the network perimeter and improvement in server security has led to development and proliferation of client-side attack techniques;
- have a rudimentary knowledge of client-side attack scenarios such as cross-sight scripting, cross-site request forgery, web browser exploits and Trojan documents; and
- be able to identify and discuss the relationship between client-side attacks and social engineering techniques such as phishing and watering hole attacks.

Issues for Potential Modules and Approaches to Consider

- The depth of technical coverage may need to vary greatly, given time constraints and the technical background of students.
- Exploration of various types of attacks employing methods of social engineering

Learning Method/Assessment

Teaching delivery may include lecture and demonstration. Presentations by current network administrators can speak to the constant persistent threats. Real national examples should be generated and identified to illustrate the practical and immediate issues. Various practical assessment measures should be developed, depending on the level of depth the students are expected to reach.

References

Emmanouil Tranos, Peter Nijkamp, Karima Kourtit "The Death of Distance Revisited: Cyber-Place, Physical and Relational Proximities", Journal of Regional Science, Vol.53, No.5, 2013. Journal ISSN: 1467-9787.

E. Anyefru, "Cyber-Nationalism: The imagined Anglophone Cameroon Community in Cyberspace", in African Identities, Vol.6, No.3, (2008), pp 253-274. Journal ISSN: 1472-5843. British Library Shelfmark: 0732.501500. UIN: ETOCRN234554771

A. Almalawi, X Yu, Z Tari, A. Fahad, I. Khalil, "An Unsupervised Anomaly-Based Detection Approach for Integrity Attacks on SCADA systems", in Computers & Security. Vol. 46, (2014), pp 94-110. Journal ISSN: 0167-4048 . British Library Shelfmark: 3394.781000. UIN: ETOCRN359669860 .

Y Li, L Shi, P Cheng, J Chen, D.E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", IEEE Transactions on Automatic Control. Vol.60; No.10, 2015. Journal ISSN: 0018-9286. UIN: ETOCRN375325720.

Steven R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines," *Journal of National Security Law & Policy 4,* no.1 (2010): 27.

Shirley Radack, ed., *Information Technology Laboratory Bulletin: Log Management: Using Computer and Network Records to Improve Information Security,* 1, 2 (October 2006), National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. http://csrc.nist.gov/publications/nistbul/b-10-06.pdf

Murugiah Souppaya and Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops,* NIST Special Publication 800-83, Revision1, U.S. Department of Commerce, July 2013. http://dx.doi.org/10.6028/NIST.SP.800-83r1

U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team, *Using Wireless Technology Securely,* US-CERT, 2008. http://www.us-cert.gov/reading_room/Wireless-Security.pdf

T2-B3: Insider Access (Local-access Attacks)

Description

A computer-based attack of an information system or network exploits a weakness in the system or a software program to carry out some form of malicious action to compromise the confidentiality, integrity or availability of information. Such "exploits" can be considered either remote or local. In local exploits, attackers have previously established access to the system under attack—that is, they already have some privilege on the system and the attacks are attempts to increase this level of privilege to gain unauthorized access to information. This block considers local-access attacks. Malicious insiders who can physically access or use various systems can cause significant damage to an operation, company or organization. They may do this for money, for revenge or because they have a grudge or are ideologically opposed to the organization. However, it is also possible to inflict similar loss or disruption through operator error or other negligence.

Background

"Privilege" in computer security is the permission to perform an action. In this case, permission is a right a particular user has to access a particular system resource, such as a file or an application, to use certain system commands, or to access a particular service, such as a network device. Typically the policy for controlling the level of privilege a user has is controlled through proper authentication of the electronic identity of the user and the employment of a set of access control rules (protocols) that govern the read, write and program execution actions of the user on the system. An attacker may attempt to "raise privilege" and gain access to more information on the system by taking over another user's identity (often by taking over a program being run by a higher-privilege user) or by modifying the imbedded security policy protocols. If attackers gain enough privilege, they can assume administrative control of the system. The attacker in such a scenario may be an authorized user of the system—a malicious insider trying to perform actions that are not permitted. Alternatively, the attacker may be someone outside of the organization, performing a remote attack in order to take over the credentials of a user with limited privilege. From that access point, the attacker may use the stolen credentials to perform a local-access attack to raise his or her privilege level, thus gaining wider access. Technically, it is difficult to distinguish between these two scenarios, both essentially local-access attacks, and many of the mitigation techniques are similar.

One of the foundational principles used to limit local access–based attack vulnerabilities is the "need-to-know" principle, in which users have access to only the information necessary for the conduct of their official duties. The principle of "least privilege" is applied to the design and implementation of the access control policy/rules to ensure that users access only the resources about which they have a need to know. This philosophy is extended to include the principle of "separation of duties"—for example, ensuring that one administrator is not able to both make changes to security policy and also approve those changes.

Compartmentalization is also a classic principle for limiting the impact of local-access attacks. Network security zoning is an effective compartmentalization technique. Network zoning is used to mitigate the risk by segmenting infrastructure services into logical groupings that have the same communication security policies and security requirements. The zones are separated by security perimeters imposed through security and network devices (firewalls, IDSs, data loss prevention software).

Given the range of vulnerabilities identified in this block, the logic of programs and procedures designed to minimize the vulnerabilities inherent to system access using prevention, detection and deterrent approaches should emerge. Such measures will be more fully explored elsewhere in this curriculum.

Learning Outcomes

Students will

- demonstrate an awareness of threats to an organization that may come from individuals within the organization;
- be able to describe local-access attacks and identify the constituent parts of such an attack;
- be able to explain the differences between a remote-access attack and a local-access attack;
- demonstrate an understanding of the concepts of permissions and privilege and how these are used to control user access to information resources on a system;
- display a basic knowledge of techniques used by attackers to abuse their current privilege levels and to raise privilege;

- be able to explain the application of the principle of least privilege and need-to-know and how they can be used to construct security policy; and
- be able to identify how sound network security zoning policy can be used to compartmentalize information.

Issues for Potential Modules and Approaches to Consider

- Policies and programs for personnel training, vetting, threat mitigation and general awareness of the problems inherent to physical access to systems and components should all be takeaways from this block but may be examined at varied levels of detail.
- Working through real-life and national examples would be a good way to engage students with the subject.
- Tools for discovering the presence and discerning the characteristics of threats active in a network may be discussed.

Learning Method/Assessment

Lectures on and demonstrations of examples are recommended.

Case studies, example scenarios and forensic examination of actual cases should be discussed.

A possible sophisticated exercise: Have students, working in teams, find and analyze a real-world example of a malicious insider attack and propose methods whereby the threat could have been avoided. Students could work through an example of a malicious insider abusing his privilege to compromise resources to which he does not have need-to-know access.

Methods of assessment should depend on the level of knowledge the students will be required to demonstrate in accordance with the learning and performance objectives desired for the particular course they may be on.

References

Markus Kont, Mauno Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, Anna-Maria Osula, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015 "Insider Threat Detection Study". Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf

P. Gola and G. Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 5th ed., Cologne, 2009

F. Schwand, "Wenn Mitarbeiter Unternehmens-Laptops privat nutzen, besteht Regelungsbedarf," acant. service GmbH, 23 April 2014. [Online]. Available: http://www.acantmakler.de/2014/04/23/unternehmen-laptops-private-nutzung/ [Accessed 14 September 2015]

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), "Isikuandmete töötlemine töösuhetes," 2011. [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhe58tes%20juhendmaterjal26%2005%202014_0.pdf [Accessed 16 July 2015]

Deutscher Bundestag, "Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes," 15 December 2010. [Online]. Available at: http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf

Centre for the Protection of National Infrastructure, "Insider misuse of IT systems," May 2013. https://www.cpni.gov.uk/documents/publications/2013/2013008-insider-misuse_of_it_systems.pdf?epslanguage=en-gb and also see "Cyber Insiders," https://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/Cyber-insiders/

Communications Security Establishment Canada, *Information Technology Security Guideline: Network Security Zoning: Design Considerations for Placement of Services within Zones* (ITSG-38), May 2009. https://cse-cst.gc.ca/en/system/files/pdf_documents/itsg38-eng_0.pdf

P.A. Legg et al., "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection," Cyber Security Centre, Department of Computer Science, University of Oxford, 2013. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-insider_threat_detection.pdf?epslanguage=en-gb

Jason R.C. Nurse et al., "Understanding the insider threat: A framework for characterising attacks," *IEEE*

2014 Security and Privacy Workshops. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-understanding_insider_threat_framework.pdf?epslanguage=en-gb or http://www.ieee-secrity.org/TC/SPW2014/papers/5103a214.pdf

S. Sagan and M. Bunn, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge MA: American Academy of Sciences), 2014, ISBN 0-87724-097-3. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderthreats.pdf

Derek A. Smith, National Cybersecurity Institute, "The Insider Threat," video. https://www.youtube.com/watch?v=z-CDyZdcGck

U.S. Department of National Defense, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities,* DoDM 5105.21-V3, 19 October 2012. http://www.dtic.mil/whs/directives/corres/pdf/510521m_vol3.pdf

Verizon Enterprise Solutions, "2015 Data Breach Investigations Report". www.verizonenterterprise.com

Cybersecurity Reference Curriculum Writing Team's Workshop in Garmisch (Contributors from Czech Republic, United Kingdom and United States).

T2-B4: Mobility Risks, BYOD and Emerging Trends

Description

The societal shift to mobile communications is irreversible and its security ramifications are poorly understood. Further, the rise of social media such as Facebook and Twitter is transforming interpersonal and global communications. Digital footprints of individuals and organization, distributed access from insecure personal devices to systems that may tie to secure systems, commercial carriers, and a series of similar and new developments pose risks to sensitive data and systems. For instance, the loss or theft of a laptop computer or mobile phone with electronic contacts, documents or shortcuts may prove damaging to an individual, an organization, a company or a country. This block addresses security issues associated with these trends.

BYOD ("Bring Your Own Device") is the policy of permitting employees to bring personally owned mobile devices (laptops, tablets and mobile phones) to their workplace and to use those devices, in the course of their work, to access privileged information and applications. This policy creates tension between the organization, whose security policies are designed to control the confidentiality and integrity of its information resources, and the employees, who wish to maintain ownership of the device and personal data and to protect themselves from monitoring. Organizations must establish policies and practices for situations when an employee leaves a position or when a device is lost, stolen or sold and to ensure that unsecured devices cannot be used by attackers to gain network access to enterprise systems. The use of "the cloud" for storage of data presents similar problems of access and configuration control.

Background

Common enterprise security practice is to build carefully zoned security architecture and provide controlled "choke points" to manage access to the Internet. A BYOD policy for Internet-capable devices introduces new access points that are not likely to be under the control of the enterprise security policy. It is a basic computer security principle that in a computer system, the integrity of lower layers is typically treated as axiomatic by higher layers. This precludes implementation on the personal device of security policies for enterprise applications that cannot be subverted by the person in control of the BYOD operating system, typically the owner. In other words, enterprise security systems (applications, etc.) on personal devices may not be installed consistently, as the owner maintains ultimate administrative control of the device. An insecure device, like a personal smart phone, cannot be made secure by simply installing secure applications or security tools. There are a number of practices that can make personal devices more secure or limit the risks they pose. These rely on the security architecture to limit the device's access to the enterprise network and to limit the information that can be moved to the device. Zoning policies that provide network segmentation and segregation can enable the implementation of workforce mobility and a relatively secure BYOD systems strategy. However, the more secure solutions exist in tension with the usability of the personal devices.

Additionally, the move to the use of infrastructure provided as a service through cloud technologies is leading to a potential loss of control of basic security architecture and security practices. Mobile devices themselves create data streams that may be of interest to both foreign intelligence agencies and commercial entities. The use of social media also exposes individuals to exploitation of information that they have disclosed that is accessed or stored on their mobile devices, exposing a wealth of potentially compromising information on relationships, opinions, locations and habits. Such social media sites may also act as threat vectors by serving as a conduit into various IT systems, making them vulnerable to infection or intrusion. Social media may also be a useful conduit for dissemination of propaganda and disinformation, crowd sourcing, mass messaging for crowd mobilization, and similar activities.

Learning Outcomes

Students will

- demonstrate an understanding of the positive and negative aspects of security policy trade-offs related to social media use in the enterprise environment from the employee's and the employer's perspectives;
- be able to analyze mobility and BYOD policies in the context of enterprise security architecture and identify security and usability trade-offs; and
- be able to analyze cloud computing policies with respect to information storage and processing (e.g., health records, government/military data) in national and international contexts.

Issues for Potential Modules and Approaches to Consider

- Capabilities of threat actors will be addressed at the appropriate level of detail for the specific audience.
- Creating an awareness of the need for adaptability of security to ever-changing technology.
- The unique requirements for and limitations of mobile communications platforms, including BYOD.
- The unique requirements for and limitations of cloud usage.
- The establishment and adoption of best practices in an enterprise setting, based on national and international guidance.
- The exploitation of personal information shared on social media—"Have you Googled yourself today?" discussion and exercise.

Learning Method/Assessment

Teaching delivery may include presentations, in-class discussions, breakout groups and discussion of case studies.

Continual assessment of class and group discussion performance and participation should be conducted.

References

N. Mastali and J. I. Agbinya, "Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper," in 2010 Fifth International Conference on Broadband and Biomedical Communications (IB2Com), 2010.

H. Kärkkäinen, "Apple myy Suomessa vaarallisia puhelimia - ja sulkee kauppiaiden suut," 30 October 2014. [Online]. Available:http://www.digitoday.fi/tietoturva/2014/10/30/apple-myy-suomessa-vaarallisia-puhelimia--ja-sulkee-kauppiaiden-suut/201415103/66. [Accessed July 2016]

Teemu Väisänen, Alexandria Farar, Nikolaos Pissanidis, Christian Braccini, Bernhards Blumbergs, and Enrique Diez. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015 "Defending mobile devices for highlevel officials and decision-makers". Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Defending%20mobile%20devices%20for%20high%20level%20officials%20and%20decision-makers.pdf

Gabriele Costa, Merlo Alessio, Luca Verderame, Konrad Wrona, "Developing a NATO BYOD Security Policy", 2016 International Conference on Military Communications and Information Systems (ICMCIS). IEEEm Brussels, Belguim, May 23-24, 2016. DOI: 10.1109/ICMCIS.2016.7496587. Available at: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=7496587&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7496587

Ree C. Ho , Hiang K. Chua, "The Influence of Mobile Learning on Learner's Absorptive Capacity: A Case of Bring-Your-Own-Device (BYOD) Learning Environment", in, *Taylor's 7th Teaching and Learning Conference 2014 Proceedings,* Singapore: Springer,2015. pp471-479. 2015. DOI: 10.1007/978-981-287-399-6_43. Print ISBN: 978-981-287-398-9. Online ISBN: 978-981-287-399-6.

Suri, Niranjan, Mauro Tortonesi, James Michaelis, Peter Budulas, Giacomo Benincasa, Stephen Russell, Cesare Stefanelli, and Robert Winkler. "Analyzing the applicability of Internet of Things to the battlefield environment." In 2016 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1-8. IEEE, 2016.

Porche III, Isaac R. Emerging Cyber Threats and Implications. RAND Corporation, 2016.

W. Arbaugh, D. Farber and J. Smith, "A Secure and Reliable Bootstrap Architecture," *Proceedings of the 1997 IEEE Symposium on Security and Privacy* (Oakland, CA) 1997, 65–71.

D.P. Cornish, "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks," EU DG-For External Policies of the [European] Union Directorate B—Policy, February 2009. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Ravi Gupta and Hugh Brooks, *Using Social Media for Global Security* (Indianapolis, IN: John Wiley & Sons), 2013, ISBN 978-1-118-44231-9.

Zeb Hallock et al., *Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD,* Cisco Systems, Inc., revised 28 August 2014, accessed 30 July 2015. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf

Raytheon Corp., *Security in the New Mobile Ecosystem,* Ponemon Institute Research Report, August 2014.

Murugiah Souppaya and Karen Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST Special Publication 800-124, Revision 1, NIST, U.S. Department of Commerce, June 2013. http://dx.doi.org/10.6028/NIST.SP.800-124r1

U.S. DNI Defense Cyber Crime Center, *Countering Identity Theft Through Education and Technology,* October 2014.

U.S. Federal CIO Council and U.S. Department of Homeland Security, National Protection and Program Directorate, *Mobile Security Reference Architecture,* 23 May 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf

The editors of the Cybersecurity Reference Curriculum.

Theme 3: International Cybersecurity Organizations, Policies and Standards

Goal

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 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.

Description

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.

Learning Objectives

As it is an emerging security issue, various national and international responses to cybersecurity are taking shape in existing organizations and in new organizations. As a national crosscutting issue, cybersecurity requires high-level policy and coordination, but national responses have been quite varied.

Through exploring the emerging practice of states developing national policies for governmental, commercial and individual cybersecurity and supporting non-state actors in developing regimes to manage the risks and threats, the student will

- develop an awareness that the national and international responses require some form of multi-stakeholder approach;
- identify the chief national organizations responsible for cybersecurity;
- identify and understand the roles and requirements of national and international standards agencies;
- understand the significance of the relationship between cybersecurity, intelligence and military institutions;
- be able to analyze national practices and policies in light of international standards and good practice;
- understand the roles of key international organizations that play a leading role in cybersecurity; and
- be familiar with the evolving international legal framework and the national government's official policy positions within this emerging regime.

Suggested References

European Union External Action, "EU International Cyberspace Policy". http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

IT Governance Ltd., "Information Security & ISO 27001: An Introduction," IT Governance Green Paper, October 2013.

Klimburg, Alexander, ed., *National Cyber Security Framework Manual,* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2012.

National Institute of Standards and Technology, U.S. Department of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations,* Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

PricewaterhouseCoopers LLP, "Why you should adopt the NIST Cybersecurity Framework," May 2014. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

The White House, *Cyberspace Policy Review.* https://www.whitehouse.gov/cyberreview/documents

U.S. Government Accountability Office, *Report to Congress: Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance,* GAO-10-606, July 2010.

T3-B1: International Cybersecurity Organizations

Description

The number of international organizations, governmental and non-governmental, concerned with global or regional cybersecurity issues is large and growing. Their interests range from investigative to regulatory to legal and policy advocacy, oversight and a range of other interests. Many of these organizations work towards collective approaches to solving cyber challenges, while others may serve to amplify national or commercial goals. For various reasons their varied recommendations must be considered critically.

The website maintained by the NATO Cooperative Cyber Defence Center of Excellence (CCD COE), https://ccdcoe.org/, is a good source for links to many regional agencies concerned with broad cybersecurity policy and practice. These include the European Union (see particularly the work of the European Agency for Network and Information Security, ENISA (https://www.enisa.europa.eu/)), the Organisation for Security and Co-operation in Europe, OSCE (http://www.osce.org/), the United Nations (http://www.un.org/en/index.html), and of course NATO (http://www.nato.int/). Beyond those sources there are also agencies such as the Global Forum for Incident Response and Security Teams (www.first.org), the International Multilateral Partnership Against Cyber Threats (IMPACT), and the Armed Forces Communications and Electronics Association (AFCEA). ENISA maintains and regularly updates a list of EU member states' cyber crises response organizations or cyber emergency response teams (CERTs).

Other international bodies concerned with cybersecurity include the International Organization for Standardization (discussed in Block 2 of this theme), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF) and the UN-backed International Telecommunications Union (ITU).

The focus of this block is on how governments interact with these many international organizations and adopt common practices often based on their recommendations.

Learning Outcomes

As pertaining to cybersecurity, students will be able to

- articulate the various challenges affecting governments and their interactions with international organizations;
- identify major international organizations, their policy focus and their role in informing and supporting national cybersecurity; and
- identify the national organizations with responsibilities for international cooperation and engagement.

Issues for Potential Modules and Approaches to Consider

A national SME should be used to identify the nation's most important international bodies on which the nation relies for guidance and through which it expresses its concerns.

Other topics that may be covered may include the following:

- Key international bodies important for informing national practices: the EU, NATO, U.S. Government (Cyber Command, etc.) and Europol (see www.europol.europa.eu/ec3)
- How national interests intersect with international organizations and their goals
- Identification of positive and negative aspects of international organizational approaches to cybersecurity
- National arrangements and mechanisms for resolving international challenges
- The Internet being used for transnational criminal /terrorist/organized crimes purposes

Learning Method/Assessment

Teaching delivery may include analysis of current issues. Students should research and review case studies of international organizational responses and examine trending international challenges and impacts for nations.

Assessment should be through a group project with classroom participation and a written assignment on an international organization's response to cybersecurity.

References

Takeshi Takahashi, Youki Kadobayashi, "Reference Ontology for Cybersecurity Operational Information", *Computer Journal* Vol.50, No 10, 2014. Journal ISSN: 1460-2067.

Farzan Kolini, Lech Janczewski, "Cyber Defense Capability Model: A Foundation Taxonomy", (2015). CONF-IRM 2015. Proceedings. Paper 32. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2015

Feng Xie, Yong Peng, Wei Zhao, Yang Gao, Xuefeng Han, "Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges", in, *Computer Information Systems and Industrial Management,* pp624-635, 2014. Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-45237-0_57.Print ISBN: 978-3-662-45236-3. Online ISBN:978-3-662-45237-0.

Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012". Paper presented at the 'World Congress on Internet Security (WorldCon)' 2014. pp66-73. 10.1109/WorldCIS.2014.7028169. Available from the IEEE at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

In addition to the web resources mentioned previously, see the following:

N. Choucri, S. Madnick and J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development 20,* no. 2 (2013): 96–121. http://dx.doi.org/10.1080/02681102.2013.836699

T3-B2 International Standards and Requirements—A Survey of Bodies and Practices

Description

This block introduces students to the range of international standards set by standards development organizations. Students will come to understand the role of international technical standards and requirements. They will be introduced to the range of ISO (International Organization for Standardization) standards as well as to COBIT (Control Objectives for Information and Related Technology), ISACA (Information Systems Audit and Control Association) and ITIL (the International Technical Infrastructure Library). Discussions will include U.S. National Institute of Standards and Technology (NIST), the British Standards Institute (BSI), Germany's Bundesamt für Sicherheit in der Informationstechnik, and ASIS International (and other standards where possible or desirable) to highlight the types and burdens created by implementing standards and the challenges presented by competing standards. Additionally, this block highlights the national approach to agreeing to international standards. Finally, it addresses the limits of standards and explores the reasons for which military, defense or other governmental organizations may set their own standards.

Learning Outcomes

Students will

- understand the role of international technical standards and requirements;
- be able to identify international standard development organizations (e.g., ISO, NIST);
- be able to identify sources of international standards informing their national cyber strategy;
- appreciate the challenges and complexities involved in implementing international standards; and
- demonstrate knowledge of how and by what body their organization's cybersecurity standards are established, maintained and promulgated.

Issues for Potential Modules and Approaches to Consider

May include the following:

- National and nationally adopted international standards directly addressing cybersecurity
- Related national procedural or organizational standards
- Challenges and complexities involved in implementing international standards

Learning Method/Assessment

The means and methods of assessment should be appropriate for the level of performance established for courses and lessons derived from this reference curriculum.

A national expert will summarize the various standards adopted by the country and explain their relationship to international and emerging standards for cybersecurity.

Students may find and analyze case studies on implementation of international standards.

Group discussion on challenges of implementing international standards should take place. Examples should be developed from local experience.

References

Iñigo Barreira, Izenpe, Jerome Bordier, SEALWeb, Olivier Delos, Arno Fiedler, Nimbus Technologieberatung GmbH, Tomasz Mielnicki, Gemalto, Artur Miękina, Polish Security Printing Works, Jon Shamah, EJ Consultants, Clemens Wanko, TUV Informationstechnik GmbH, Clara Galan Manso, ENISA, Sławomir Górniak, ENISA, "Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards", EU ENISA, July 1, 2016. Available at: https://www.enisa.europa.eu/publications/tsp_standards_2015

Manmohan Chaturvedi, Abhishek Narain Singh, Manmohan Prasad Gupta, Jaijit Bhattacharya, (2014) "Analyses of issues of information security in Indian context", *Transforming Government: People, Process and Policy,* Vol. 8 Issue: 3, pp. 374-397. DOI (available at): http://www.emeraldinsight.com/doi/abs/10.1108/TG-07-2013-0019

L. Zhang, Q. Wang, B.Tian, "Security Threats and Measures for the Cyber-Physical Systems", in, *The Journal of*

China Universities of Posts and Telecommunications, Vol. 20, Supp.1, 2013, pp25-29. Journal ISSN: 1005-8885. UIN: ETOCRN339930374

Blaž Markelj, Sabina Zgaga, "Comprehension of Cyber Threats and their Consequences in Slovenia", in, *Computer Law & Security Review: The International Journal of Technology Law and Practice.* Vol. 32. Issue 3 (2016). Journal ISSN: 2212-473X (Electronic - British Library ELD Digital store). UIN: ETOCvdc_100032209717.0x000001.

Shackelford, Scott, Scott L. Russell, and Jeffrey Haut. "Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks." UC Davis Business Law Journal (2016).

ISACA, *European Cybersecurity Implementation: Overview,* ISACA Whitepaper, 2014. http://www.isaca.org or http://www.isaca.org/knowledge-center

ISACA, European Cybersecurity Implementation Series: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx; see also ISACA's reports on Resilience, Risk Guidance, Assurance and Audit programs.

PricewaterhouseCoopers LLP, *Why you should adopt the NIST Cybersecurity Framework,* May 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Steve Purser, "Standards for Cyber Security" in M.E. Hathaway (ed.), *Best Practices in Computer Network Defense: Incident Detection and Response* (Amsterdam: IOS Press), 2014: 106. doi:10.3233/978-1-61499-372-8-97

Other standards series (in addition to ISO 27000):

- ISO 9000 (quality management)
- ISO 22300 (business continuity management)
- ISO 31000 (risk management)
- BSI PAS 555

T3-B3: National Cybersecurity Frameworks

Description

As a national issue that transcends traditional boundaries between government, industry and citizens, cybersecurity requires high-level policy and coordination. Given the interconnectedness of systems, many governments have recognized that they require a whole-of-government approach just for the security management of their own operating systems, let alone to help minimize the risks to industry and individuals. However, national responses have been quite varied. Some nations have created national bodies responsible for managing national cybersecurity, while other nations have made coordinating bodies responsible for articulating national policies but left management and implementation of the policies to various government departments. Yet other countries struggle to find an appropriate framework.

Many governments have gone beyond articulating or supporting cybersecurity measures only for protecting the machinery of government and have embraced this issue as one of national risk, thus undertaking efforts to support or instill best practices for the private sector and citizens. Championing or mandating such measures has been particularly the case for the protection of critical infrastructures that are often in private ownership. Nevertheless, there are some common requirements, such as establishing structural roles and accountabilities, issuing authoritative technical guidance, defining roles and responsibilities for mitigating risks and responding to active issues.

This blocks aims to make students aware of their nation's cybersecurity policies, strategies and structures. Students need to be informed of the policy strategy framework of their nation (if there is one) and of the organizations responsible for national guidance and technical specifications. Students will compare different national and international cybersecurity strategy documents and approaches in order to better comprehend their own and to assess areas of risk and responsibility.

Learning Outcomes

Students will be able to

- identify the organizations responsible for their national cybersecurity policy;
- identify key features of national cybersecurity policy;
- identify responsible organizations and understand their role in developing and issuing technical guidance/directives;
- identify key features for technical guidance/directives;
- discuss the sources of best practices in organizing national cybersecurity; and
- critically analyze their national approach in comparison to reference policy frameworks.

Issues for Potential Modules and Approaches to Consider

- Centralized vs. multi-stakeholder approach to cybersecurity
- National approaches to cooperation, coordination and collaboration
- International organizations: roles and interaction in the national context
- Reference policy frameworks—review various examples

Learning Method/Assessment

The means and methods of assessment should be appropriate for the level of performance established for courses and lessons derived from this reference curriculum.

Teaching delivery may include discussion, subject matter expert lectures, comparative case studies, identification of good practices, and visits to local cybersecurity bodies.

References

Sławomir Górniak, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, Sławomir Górniak, "Governance Framework of the European Standardization: Aligning Policy, Industry and Research, v1.0", Heraklion, Greece, ENISA, 2015, ISBN 9789292041540.

Tomas Minarik, "National Cyber Security Organisation: Czech Republic", 2nd Revised Ed, Tallinn, 2016. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf

Vytautas Butrimas, "National Cyber Security Organisation: Lithuania", Tallinn, 2015. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf

Lea Hriciková, Kadri Kaska, "National Cyber Security Organisation: Slovakia", Tallinn, 2015. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SLOVAKIA_042015.pdf

Lehto, Martti, and Jarno Limnéll. "Cyber Security Capability and the Case of Finland." In European Conference on Cyber Warfare and Security, p. 182. Academic Conferences International Limited, 2016.

Defense Science Board, U.S. Department of Defense, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

George Farah, *Information Systems Security Architecture: A Novel Approach to Layered Protection—A Case Study,* GSEC Practical Version 1.4b, SANS Institute, 9 September 2004. www.sans.org

Alexander Klimburg, ed., *National Cyber Security Framework Manual,* NATO CCD COE Publication, Tallinn, Estonia, 2012, ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations,* report by NIST Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, NIST, U.S. Department of Commerce, Washington, DC, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

Organisation for Economic Co-operation and Development (OECD), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy,* 2012. http://oe.cd/security

T3-B4: Cybersecurity in National and International Law

Description

Cybersecurity's legal landscape is complex and quickly changing. There are arguments regarding the applicability of existing and emerging international and national laws to address cybersecurity issues and challenges. There is also wide variation in how countries address cybersecurity within domestic law. Some states have specific cybersecurity laws; others do not. The attribution challenge—the difficulties associated with tracking the source of malign, threatening or illegal cyber activity—compounds problems in both the domestic and the international sphere.

There is an evolving body of literature regarding international and national law applicable to cybersecurity. This block introduces students to both international and national laws responsible for a range of cybersecurity issues. Many nations and organizations within them are subject to compliance laws, such as those requiring the reporting of certain types of financial transactions or data breaches. There are also evolving international legal and law enforcement norms and practices (such as cooperation regimes established by Interpol). Legal requirements to report cyber incidents have been adopted by many nations, and efforts are underway to determine an international code of cyber ethics. However, there is no international governing body or organization overseeing the legal aspects of cybersecurity.

Students will be exposed to national positions on domestic and international law relevant to cyberspace, with the emphasis on cybersecurity. Important domestic aspects are privacy, systems assurance, regulatory compliance and commercial insurance implications within the emergent national and international legal regimes.

Learning Outcomes

Students will

- recognize key challenges and policy sources in international cyber law;
- be able to explain the legal responsibilities of national cybersecurity stakeholders and statutes; and
- know the national legal statutes concerning cybersecurity (if any) and identify the key legal authorities within their respective organizations.

Issues for Potential Modules and Approaches to Consider

- Subjects such as the contested international legal status of cyber attacks led by state and non-state actors, cyber issues in domestic law, organizational compliance requirements, and individual legal responsibility may be examined at some length.
- Explore the debate regarding the International Code of Conduct for Information Security proposed to the UN.
- Domestic compliance regulations
- Commercial insurance and liability for cyber risks

Learning Method/Assessment

Lectures should be developed in coordination with responsible legal representatives able to speak definitively to their national position on these issues.

Case studies on international and national legal responses to cybersecurity incidents should be examined.

A short written examination appropriate to the detail taught should be developed as an assessment tool.

References

Hong XU. "Cyber law in China" Alphen aan den Rijn: Kluwer Law International, 2010. ISBN 9789041133335. British Library Shelfmark: YC.2011.a.9251. UIN: BLL01015641102

Radziwill Yaroslav, "Cyber-Attacks and the Exploitable Imperfection of International Law." Leiden: Brill Nijhoff, 2015. ISBN 9789004298330.

Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (2015). NATO CCD COE. E-Book. Full Book Available at: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html

Zeinab Krake, Sheikha Lubna Al Qasimi, *Cyber Security in Developing and Emerging Economies,* 2010, Cheltenham: Edward Elgar Publishing.

Fidler, David P., Richard Pregent, and Alex Vandurme. "NATO, Cyber Defense, and International Law." Journal of International and Comparative Law 4, no. 1 (2016): 1.

Saran, Samir. "Striving for an International Consensus on Cyber Security: Lessons from the 20th Century." Global Policy 7, no. 1 (2016): 93-95.

Dan Arnaudo, "Research Note: The Fight to Define U.S. Cybersecurity and Information Sharing Policy," ASA Institute for Risk & Innovation, 2013. http://www.anniesearle.com/research.aspx?topic=researchnotes

Nils Melzer, *Cyberwarfare and International Law,* United Nations Institute for Disarmament Research (UNIDIR), Geneva, 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

NATO, *Legal Gazette: Legal Issues Related to Cyber* 35 (December 2014). This issue addresses, in separate articles, (1) legal aspects of cybersecurity and cyber-related issues affecting NATO; (2) active cyber defense to responsive cyber defense; and (3) an exploration of the threshold of "armed attack" and related legal issues of attribution and participation in cyber warfare. https://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

NATO Cooperative Cyber Defence Centre of Excellence (Michael N. Schmitt, General Editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press), 2013. https://ccdcoe.org/tallinn-manual.html

Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?," *Stanford Law & Policy Journal* 25 (2014): 269–299.

Theme 4: Cybersecurity Management in the National Context

Goal

The broad objective of this theme is to explore the practice of managing cybersecurity in the national context.

Description

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 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[7].

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.

Learning Objectives

Students will

- understand the systems approach to planning for resilience to threats, attacks and similar events;
- be able to situate the practice of employing resilient systems within the national context;
- be able to analyze the utility of frameworks and matrices for planning and delegation; and
- demonstrate a knowledge of the common types of national response organizations and be familiar with the role, mandate and structure of their current national systems and organizational incident and crisis management organizations.

Suggested References

Deborah J. Bodeau and Richard Graubart, *Cyber Resiliency Engineering Framework,* MITRE Technical Report MTR 110237, The MITRE Corporation, September 2011. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Mohamed Dafir Ech-Cherif El Kettani and Taïeb Debbagh, "A National RACI Chart for an Interoperable 'National Cyber Security' Framework," *Proceedings of the European Conference on Information Warfare & Security,* January 2009.

Nicole Falessi, Razvan Gavrila, Maj. Ritter Kleinstrup and Konstantinos Moulinos, *National Cyber Security Strategies: Practical Guide on Development and Execution,* European Network and Information Security Agency, December 2012. https://www.enisa.europa.eu

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem,* Full Report, ENISA, April 2011.

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?," paper by the Working Group Security Architecture, Information Security Society Switzerland, 29 September 2008.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide,* Carnegie Mellon University, February 2014.

See resources at Carnegie Mellon University CERT Software Engineering Institute, CERT-RMM (CERT Resilience Management Model): www.cert.org/resilience/rmm.html

[7] Derived from the Carnegie Mellon CERT-RMM.

T4-B1: National Practices, Policies and Organizations for Cyber Resilience

Description

Cybersecurity transcends many organizational boundaries. A number of nations have adopted a comprehensive whole-of-government approach to articulating roles and responsibilities for managing cyber resilience. Cyber resilience aims to ensure that national cyber infrastructure remains operational when in crisis mode and recovers rapidly and effectively after disruption. With such resilience in mind, this block addresses national and organizational practices in a comparative context.

In this block, students will be exposed to a number of sample comprehensive approaches to cybersecurity as articulated in published high-level guidance (such as that of the United Kingdom or the United States) in order for them to analyze the strengths and weaknesses of their national policies. The national policies relevant to the student body will be compared and contrasted. Discussion in particular should turn to an examination of existing policies and practices aimed at preventing, protecting, reacting to and managing recovery from cyber incidents. Measures such as audit, verification and the means of independent review should also be addressed.

Learning Outcomes

Students will

- be able to interpret national cyber resilience documents;
- be able to contribute to the development and extension of national cyber resilience procedures;
- be able to articulate the roles and responsibilities of individuals and organizations responsible for national cyber resilience;
- understand the challenges of the coordination of cyber operations during crisis situations; and
- understand decision analysis processes used in making compliance decisions during crisis situations.

Issues for Potential Modules and Approaches to Consider

A national SME should analyze national existing national policies to extract the appropriate level of information for use in the lesson plans.

Learning Method/Assessment

Teaching delivery may include lectures, demonstrations, site visits and written exercises. Assessment should consist of both written and oral verification.

References

Clausewitz Gesellschaft; Bundesakademie für Sicherheitspolitik. "Sicherheitspolitik im Cyber-Zeitalter: Reicht passive Abwehr aus?" Bonn, Germany : Mittler Report Verlag, 2014, British Library Identifier: 016828758. Document Supply Number: 3829.361655 UIN: BLL01016828758

Guido Nannariello, "E-commerce e tutela del consumatore: indagine sui codici di condotta ed i processi di certificazione", Ispra: Joint Research Centre, Institute for the Protection and Security of Citizen, Cybersecurity Sector, 2001. UIN: BLL01011092147.

F. Cassim, "Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players", in, *Comparative and International Law Journal of Southern Africa,* Vol.44, No.1, 2011, pp123-138 (University of South Africa). Journal ISSN: 0010-4051. UIN: ETOCRN296687880.

N. Shirazi, "A Framework for Resilience Management in the Cloud", in, *Elektrotechnik und Informationstechnik,* Vol. 132; No.2, 2015, pp122-132. Journal ISSN: 0932-383X. UIN: ETOCRN370071353.

Kallberg, Jan. "Assessing India's Cyber Resilience: Institutional Stability Matters." Strategic Analysis 40, no. 1 (2016): 1-5.

An SME will have to compile the appropriate national policies and references. More general references include the following:

Deborah J. Bodeau and D.J. Graubart, *Cyber Resiliency Engineering Framework,* MITRE Technical Report MTR 110237 (Bedford, MA: The MITRE Corp.), September 2011.

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem,* Full Report, ENISA, April 2011.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide,* Carnegie Mellon University, February 2014.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance,* Carnegie Mellon University, February 2014.

See resources at Carnegie Mellon University's CERT Software Engineering Institute CERT-RMM (CERT Resilience Management Model): www.cert.org/resilience/rmm.html

Cybersecurity Reference Curriculum Writing Team's Workshop in Tbilisi.

T4-B2: National Cybersecurity Frameworks

Description

This block gives students an understanding of national cybersecurity strategy and its implementation in the context of managing cyber operations, handling national-level cybersecurity incidents and managing national cybersecurity risk. The focus should be on frameworks that assist in allocating resources, define organizational roles and responsibilities and specify the actions along the chain of command for responsibility and reporting.

Drawing from international and national standards, this block considers security foundations and frameworks, examining several comprehensive frameworks for articulating roles and responsibilities for management of cybersecurity risk and response to cybersecurity incidents. Such frameworks are often summarized in the form of a Responsibility, Accountability, Command and Information (RACI) delegation matrix. Such matrix delegation tools lend themselves to managing cybersecurity operations as well. The example of an RACI chart will be used as the teaching example. The students will be exposed to the general design of such tools before addressing their national responsibility and response matrixes. If possible, the actual national policy tools for managing such delegation of responsibilities and tasks will be identified and explored. Discussion will address decision support tools, risk management tools and frameworks, practices and responsibilities. Ultimately, students will examine the cybersecurity delegated management framework adopted by their national government or at least by their organization.

Cyber system resilience may include the following activities: asset management, controls management, configuration and change management, threat and vulnerabilities management, service continuity planning and management, external dependencies management, training, and organizational and individual awareness and active management of situational awareness.

Learning Outcomes

Students will

- demonstrate an understanding of the concept of responsibility matrix planning and delegation;
- explore the broad issues surrounding implementation of their national cybersecurity strategy;
- understand how to interface with national incident response command and control structures;
- understand the delegated management of cyber operations at the national level;
- understand how cyber risk is managed in the context of national policy; and
- understand the positive and negative aspects of formal resource management frameworks applied to the national cybersecurity context.

Issues for Potential Modules and Approaches to Consider

Topics covered may include the RACI system or similar responsibility matrix tools for incident handling and recovery and response management.

Learning Method/Assessment

An SME should devise a brief survey of methods (such as RACI charting) before identifying where national and organizational authorities and explicit guidance exists. The SME can then identify those most germane to the particulars of the student body.

The assessment scheme should be developed in accordance with the level of knowledge and familiarity appropriate to the courses derived from this reference curriculum.

References

IU. V. Nesteriak, (IUrii Vasyl'ovych). "Derzhavna informatsiina polityka Ukraïny: teoretyko-metodolohichni zasady", Kiev, Ukraine, 2014. Monograph. ISBN 9789666193554. UIN: BLL01017709318.

Francis Domingo, "Cyber Policy in China", Europe-Asia Studies, 2015. DOI: 10.1080/09668136.2015.1102519. Available at: http://www.tandfonline.com/doi/full/10.1080/09668136.2015.1102519

Tuija Kuusisto, Rauno Kuusisto, "Leadership for Cyber Security in Public-Private Relations", in R. Koch, G. Rodosek (eds), *Procedings of the 15th Conference on Cyber Warfare and Security,* Munich, July, 2016. ISBN1910810932, 9781910810934.

Mari Malvenishv, "Role and Objectives of the Cyber-security Bureau". Online Presentation by the Cyber-security Bureau of Georgia, 2015. Available at: www./slideplayer.com/slide/9759466/

Sarma, Sanghamitra. "Cyber Security Mechanism in European Union." (2016).

Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,* Special Publication NIST 800-61, Revision 2, U.S. Department of Commerce, August 2012.

Mohamed Dafir Ech-Cherif El Kettani and Taïeb Debbagh, "A National RACI Chart for an Interoperable 'National Cyber Security' Framework," *Proceedings of the European Conference on Information Warfare & Security,* 2009.

Responsibility Charting (RACI). http://www.thecqi.org/Documents/community/South%20Western/Wessex%20Branch/CQI%20Wessex%20-%20RACI%20approach%207Sep10.pdf

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance,* Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

International Standards Organization ISO 22300 series and ISO 27000 series—see earlier list.

T4-B3: Cyber Forensics

Description

Cyber forensics is the application of investigation and analysis techniques to gather, exploit and preserve digital evidence. This domain of activity consists of digital forensics, hardware forensics and human factor forensics. While forensic activity is essential for day-to-day system maintenance and operational efficiency, more rigorous control of these activities may be required to produce evidentiary materials for criminal investigations. Finally, good forensic practices provide important tools for understanding how adversaries seek to exploit access to existing systems by, for example, exposing how they may seek to access command and control nodes or how they design malware.

This block presents the key forensics challenges in managing cyber incidents. Forensics techniques can be applied to the investigation of cyber incidents, intelligence gathering and prosecution by law enforcement. Material to be covered includes tools and techniques to acquire data from multiple sources, to analyze the data and to build a timeline of events. These may be used to build an attribution case or for various forms of follow-up activity, from activity tracking and monitoring to building a criminal case against the perpetrators. Students will also examine forensic data collection and examination for financial crimes such as money laundering.

Students will learn about the issues associated with the collection of data for forensics from multiple sources, including computers, networks, mobile devices, databases and sensors.

Learning Outcomes

Students will demonstrate an understanding of

- the issues associated with the collection of data for forensics from multiple sources, including computers, networks, mobile devices, databases and sensors;
- the importance of analyzing forensic data for the purposes of creating a timeline and assigning attribution; and
- the national laws and regulations for data collection in support of law enforcement.

Issues for Potential Modules and Approaches to Consider

- Creating a resilient system to support recovery after a cyber incident
- Forensic examination of social engineering elements exploited to gain access to systems
- Hardware devices that could be of forensic value
- Uses of forensic investigation results for criminal prosecution
- Automated tools for basic operational forensics

Learning Method/Assessment

Teaching delivery should consist of lecture, demonstration and discussion of several case studies illustrating different forensic elements.

The assessment scheme should be developed in accordance with the level of knowledge and familiarity appropriate to the courses derived from this reference curriculum.

Students should be assessed in oral and written format.

References

Risto Vaarandi, Paweł Niziński, NATO Cooperative, Cyber Defence Centre of Excellence, Tallinn, Estonia. 2013 "A Comparative Analysis of Open-Source Log Management Solutions for Security Monitoring and Network Forensics". Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/VaarandiNizinski2013_Open-SourceLogManagementSolutions.pdf

Xiuzhen Cheng, Miroslaw Kutyłowski, Kuai Xu, Haojin Zhu, "Special Issue on Cybersecurity, Crime, and Forensics of Wireless Networks and Applications." *Security and Communications Networks.* Vol.8, Issue 17. 2015. Journal ISSN:1939-0122.

Å uteva, NataÅ¡a, Mileva Aleksandra; Loleski Mario, "Finding Forensic Evidence for Several Web Attacks", *International Journal of Internet Technology and Secured Transactions,* Vol6., No.1, 2015. Journal ISSN: 1748-5703.

Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012". Paper presented at the 'World

Congress on Internet Security (WorldCon)' 2014. pp66-73. 10.1109/WorldCIS.2014.7028169. Available from the IEEE at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

Choi, Yangseo, Joo-Young Lee, Sunoh Choi, Jong-Hyun Kim, and Ikkyun Kim. "Introduction to a network forensics system for cyber incidents analysis." In 2016 18th International Conference on Advanced Communication Technology (ICACT), pp. 50-55. IEEE, 2016. Santhosh Baboo and S. Mani Megalai, "Cyber Forensic Investigation and Exploration on Cloud Computing Environment," *Global Journal of Computer Science and Technology B: Cloud and Distributed* 15 (Issue 1, Version 1), 2015. https://globaljournals.org/GJCST_Volume15/1-Cyber-Forensic-Investigation.pdf

Ibrahim Baggili and Frank Breitinger, University of New Haven Cyber Forensics Research and Education Lab, "Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer," *Papers from the 2015 AAAI Spring Symposium* (Palo Alto, CA Stanford University), March 2015. http://www.researchgate.net/profile/Ibrahim_Baggili/publication/274065229_Data_Sources_for_Advancing_Cyber_Forensics_What_the_Social_World_Has_to_Offer/links/55134a630cf283ee0833818c.pdf

Santhosh Baboo and S. Mani Megalai, "Cyber Forensic Investigation and Exploration on Cloud Computing Environment," Global Journal of Computer Science and Technology B: Cloud and Distributed 15 (Issue 1, Version 1), 2015. https://globaljournals.org/GJCST_Volume15/1-Cyber-Forensic-Investigation.pdf

T4-B4: National-level Security Audit and Assessment

Description

Assessment of security preparedness is an important role for countries. Assessment helps test the security controls as well as identifying the gaps in security infrastructure and policy. Security assessment can be done at multiple levels. First, individual security controls can be tested using auditing tools. Second, assessment can be done at a holistic, system or organizational level through exercises and real-time simulations. This block introduces the tools and processes of security audits and assessments. This will allow students to learn how the assessment of residual vulnerability in systems can be identified and weighed; moreover, such audits and assessments help establish how to gauge cyber systems readiness to deal with specific types of known threat actors and to prepare for activities where an unknown threat emerges (so-called zero-day threats because there is no warning of their specific means of attack or malign action).

Personal and organization cybersecurity self-awareness tools and techniques are diverse, running from questionnaires to technical tools. This block aims to increase understanding of the role of self-awareness as it relates to cybersecurity for the individual and organization. Analyzing the strengths and weaknesses of different tools and approaches is critical to understanding their value. Ongoing self-assessment can reduce risks. The consideration of potential biases is also crucial for useful self-assessment. Operationalization of results is a necessary component of any self-assessment effort. As the level of security is related to the value, importance or sensitivity of what is being secured, there is no single pattern to simply adopt and apply. Rather, the desired level of cybersecurity will depend on the standards selected and the level of performance that needs to be assured.

Learning Outcomes

Students will

- understand the importance of security audit and assessment tools, and
- be able to evaluate and apply appropriate self-assessment tools and techniques in a national context.

Issues for Potential Modules and Approaches to Consider

Topics to address may include the following:

- Good practices in organizations that use self-assessment
- Discussion of case studies of situations in which self-awareness might have increased security

Learning Method/Assessment

Students should practice using a national self-assessment tool if available and, if not, they can employ the Cyber Security Evaluation Tool (CSET) available through the U.S. Department of Homeland Security (DHS) or a similar approach. It may be fruitful to compare whatever national method exists to that advocated by the U.S. DHS.

The assessment scheme should be developed in accordance with the level of knowledge and familiarity appropriate to the courses derived from this reference curriculum.

References

Ivan Alcoforado, "Leveraging Industry Standards to Address Industrial Cybersecurity Risk", *ISACA Journal,* Vol 6, 2014; Journal ISSN: 1944-1967.

Stefan Laube, Rainer Böhme (Department of Information Systems, University of Munster, Germany; Institute of Computer Science, University of Innsbruck, Austria), "The Economics of Mandatory Security Breach Reporting to Authorities". Available at: http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf

Yulia Cherdantseva, et al. "A Review of Cyber Security Risk Assessment Methods for SCADA systems." Electronic monograph. Available at the British Library, reference: UIN: ETOCvdc_100030733535.0x000001.

Abhijit Gupta, Subarna Shakya, "Information System Audit; A study for security and Challenges in Nepal", in, International Journal of Computer Science and Information Security, Vol.13, No. 11 (Nov 2015) pp 1-4. Journal ISSN 1947-5500.

Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. "Regulatory approaches for cyber security of critical infrastructures: The case of Turkey." Computer Law & Security Review 32, no. 3 (2016): 526-539.

Business Continuity Institute, *The Good Practice Guidelines 2013, Global Edition: A Guide to Global Good Practice in Business Continuity* (England), 2013. www.thebci.org/index.php/resources/the-good-practice-guidelines

International Auditing and Assurance Standards Board, ISAE 3402 Standard for Reporting on Controls at Service Organizations. http://isae3402.com/ISAE3402_overview.html

International Organization for Standardization/International Electrotechnical Commission, *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4,* CCMB-2012-09-001, September 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

Keith Stouffer, Joe Falco and Karen Scarfone, *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security,* National Institute of Standards and Technology, U.S. Department of Commerce, June 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

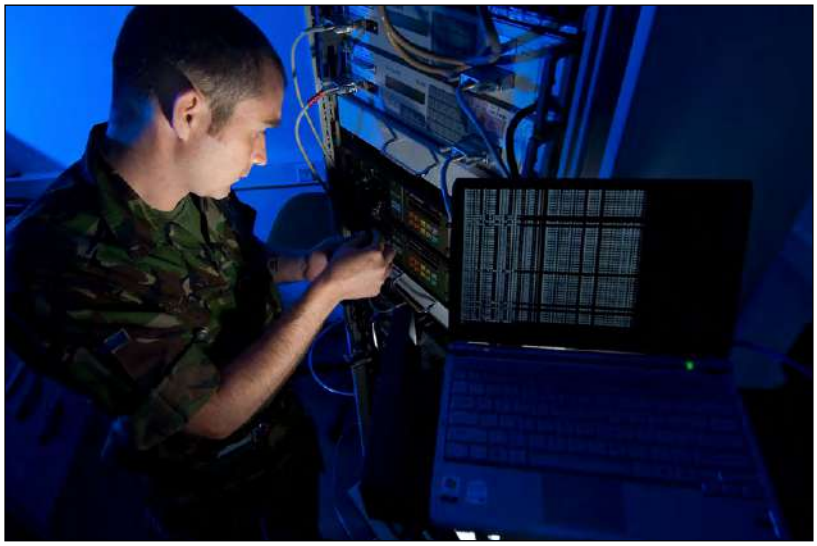
U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Self Assessment Package,* Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance,* Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

Abbreviations

APT	Advanced Persistent Threat
AS	Autonomous System (discrete subdivision of the Internet)
ASN	Autonomous System Number
BGP	Border Gateway Protocol
BSA	Basic Security Architecture
BYOD	Bring Your Own Device
CERT	Cyber Emergency Response Team
COBIT	Control Objectives for Information and Related Technology
COMSEC	Communications Security
CSET	Cyber Security Evaluation Tool
CSET	Cyber Security Evaluation Tool
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
DoS	Denial of Service
ENISA	European Agency for Network and Information Security
ESCWG	Emerging Security Challenges Working Group
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IGF	Internet Governance Forum
IP	Internet Protocol
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
LAN	Local Area Network
NIR	National Internet Registry
NIST	(U.S.) National Institute of Standards and Technology
PfPC	Partnership for Peace Consortium of Defense Academies and Security Studies Institutes
PIT system	Platform IT system
RACI	Responsibility, Accountability, Command and Information
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SME	Subject Matter Expert

SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TRA model	Threat and Risk Assessment model
UNIDIR	United Nations Institute for Disarmament Research



Glossary

Note: Not all terms below appear in the preceding text, but many may prove useful in crafting specific learning exercises, etc.

A

access control mechanism Definition: Security measures designed to detect and deny unauthorized access and permit authorized access to an information system or a physical facility.

active attack Definition: An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data or its operations.

advanced persistent threat(s) Definition: An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical and deception). From: NIST SP 800-53 Rev 4.

antivirus software Definition: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents, sometimes by removing or neutralizing the malicious code.

attack Definition: An attempt to gain unauthorized access to system services, resources or information or an attempt to compromise system integrity.

attack pattern Definition: Similar cyber events or behaviors that may indicate that an attack has occurred or is occurring, resulting in a security violation or a potential security violation.

attack signature Definition: A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

attack surface Definition: The set of ways in which an adversary can enter a system and potentially cause damage. Extended definition: An information system's characteristics that permit an adversary to probe, attack, or maintain presence in the information system. Adapted from: Manadhata, P.K., & Wing, J.M. in Attack Surface Measurement, http://www.cs.cmu.edu/~pratyus/as.html#introduction

authentication Definition: The process of verifying the identity or other attributes of an entity (user, process or device). Extended definition: Also the process of verifying the source and integrity of data.

B

botnet Definition: A collection of computers compromised by malicious code and controlled across a network.

Build Security Definition: A set of principles, practices and tools to design, develop and evolve information systems and software that enhance resistance to vulnerabilities, flaws and attacks.

C

capability Definition: The means to accomplish a mission, function or objective.

cloud computing Definition: A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Computer Network Defense Analysis Definition: Where a person uses defensive measures and information collected from a variety of sources to identify, analyze and report events that occur or might occur within the network in order to protect information, information systems and networks from threats.

critical infrastructure Definition: The systems and assets, whether physical or virtual, so vital to society that their incapacity or destruction may have a debilitating impact on the security, economy, public health or safety, environment or any combination of these matters.

cryptography Definition: The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication.

cyber ecosystem Definition: The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

cybersecurity: Short definition: The "activity or process, ability or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation." Extended definition: Strategy, policy and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009.

cyberspace Definition: The electronic world created by interconnected networks of information technology and the information on those networks.

D

data mining Definition: The process or techniques used to analyze large sets of existing information to discover previously unrevealed patterns or correlations.

denial of service Definition: An attack that prevents or impairs the authorized use of information system resources or services.

digital forensics Definition: The processes and specialized techniques for gathering, retaining and analyzing system-related data (digital evidence) for investigative purposes.

digital rights management Definition: A form of access control technology to protect and manage use of digital content or devices in accordance with the content or device provider's intentions.

distributed denial of service Definition: A denial of service technique that uses numerous systems to perform the attack simultaneously.

E

enterprise risk management Definition: A comprehensive approach to risk management that engages people, processes and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

exploit Definition: A technique to breach the security of a network or information system in violation of security policy.

F

firewall Definition: A capability to limit network traffic between networks and/or information systems.

H

hacker Definition: An unauthorized user who attempts to gain or gains access to an information system.

I

ICT supply chain threat Definition: A man-made threat achieved through exploitation of the information and communications technology (ICT) system's supply chain, including acquisition processes.

inside(r) threat Definition: A person or group of persons within an organization who pose a potential risk through violating security policies. Extended definition: One or more individuals with the access and/or inside knowledge of a company, organization or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products or facilities with the intent to cause harm.

integrated risk management Definition: The structured approach that enables an enterprise or organization to share risk information and risk analysis and to synchronize independent yet complementary risk management strategies to unify efforts across the enterprise.

intrusion Definition: An unauthorized act of bypassing the security mechanisms of a network or information system.

intrusion detection Definition: The process and methods for analyzing information from networks and information systems to determine whether a security breach or security violation has occurred.

K

keylogger Definition: Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously/secretly, to monitor actions by the user of an information system.

M

malicious code Definition: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity or availability of an information system.

malware Definition: Software that compromises the operation of a system by performing an unauthorized function or process.

N

network resilience Definition: The ability of a network to (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.

non-repudiation Definition: A property achieved through cryptographic methods to protect against an individual or entity falsely denying having performed a particular action related to data. Extended definition: Provides the capability to determine whether a given individual took a particular action, such as creating information, sending a message, approving information or receiving a message.

P

passive attack Definition: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system but does not attempt to alter the system, its resources, its data or its operations.

phishing Definition: A digital form of social engineering to deceive individuals into providing sensitive information.

R

redundancy Definition: Additional or alternative systems, sub-systems, assets or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset or process.

resilience Definition: The ability to adapt to changing conditions and prepare for, withstand and rapidly recover from disruption.

risk analysis Definition: The systematic examination of the components and characteristics of risk.

risk assessment Definition: The product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action and informing decision making. Extended definition: The appraisal of the risks facing an entity, asset, system or network, organizational operations, individuals, geographic area, other organizations or society; includes determining the extent to which adverse circumstances or events could result in harmful consequences.

risk management Definition: The process of identifying, analyzing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken. Extended definition: Includes (1) conducting a risk assessment; (2) implementing strategies to mitigate risks; (3) monitoring risk continuously over time; and (4) documenting the overall risk management program.

S

spam Definition: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

spoofing Definition: Faking the sending address of a transmission to gain illegal (unauthorized) entry into a secure system.

spyware Definition: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Supervisory Control and Data Acquisition (SCADA) Definition: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

supply chain Definition: A system of organizations, people, activities, information and resources for creating and moving products, including product components and/or services from suppliers through to their customers.

supply chain risk management Definition: The process of identifying, analyzing and assessing supply chain risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

T

threat Definition: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations or society.

threat actor/agent Definition: An individual, group, organization or government that conducts or has the intent to conduct detrimental activities.

threat assessment Definition: The product or process of identifying or evaluating entities, actions or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations and/or property.

threat vector Definition: The means of introducing the threat to the target or the line of approach taken to actualize a threat.

Trojan horse Definition: A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

U

unauthorized access Definition: Any access that violates the stated security policy.

V

virus Definition: A computer program that can replicate itself, infect a computer without permission or knowledge of the user and then spread or propagate to another computer.

vulnerability Definition: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

W

worm Definition: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Z

Zero-day exploit Definition: An attack exploiting an unrecognized vulnerability, launched without warning and detected only once underway.

Derived and redacted from U.S. DHS National Initiative for Cybersecurity Careers and Studies (NICCS) Glossary. With additional material.

Team Leads and Editors: Sean S. Costigan and Michael Hennessy
Curriculum Team Members and Advisers:

Name	Nationality	Institutional Affiliation	
Dr. Ata ATALAY	Turkey	Head of Department, General Secretariat, National Security Council	
Ms. Mariia AVDEEVA	Ukraine	International Development Manager, Kharkov National Law University	
Ms. Alexandra BIELSKA	Poland	Consultant, i-intelligence	
Mr. Guiseppi CONTI	Italy	CTO, Trilogis	
Mr. Sean S. COSTIGAN	USA	Professor, George C. Marshall European Center for Security Studies	
Mr. Jean d'ANDURAIN	France	Coordinator, Defence Education Programmes NATO International Staff	
LTC Dirk DUBOIS	Belgium	European Security and Defense College	
Dr. David EMELIFEONWU	Canada	Senior Staff Officer, Educational Engagement, Military Personnel Generation Department of National Defence	
Mr. David FRANCO	USA	Supervisory Special Agent, Federal Bureau of Investigation	

Dr. Piotr GAWLICZEK	Poland	Rector's Representative for Innovation National Defense University	
Dr. Sanjay GOEL	USA	Director of Research, NYS Center for Information Forensics and Assurance SUNY Albany	
Mr. Andria GOTSIRIDZE	Georgia	Director of Cyber Security Bureau Ministry of Defence	
Mr. Arman GRIGORYAN	Armenia	Head of Cyber Security Group, Institute for National Strategic Studies	
Dr. Michael A. HENNESSY	Canada	Professor/Associate Vice Principal, Research Royal Military College of Canada	
CDR Andreas HILDENBRAND	Germany	Professor, George C. Marshall European Center for Security Studies	
Dr. Dinos KERIGAN-KYROU	Ireland	Instructor, Department of Computer & Mathematical Sciences University of Greenwich	UNIVERSITY of GREENWICH
Dr. Scott KNIGHT	Canada	Professor/Head, Department of Computer and Electrical Engineering Royal Military College of Canada	
Mr. Frederic LABARRE	Canada	Program Manager, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes	
Mr. Philip LARK	USA	Director, Program on Cyber Security George C. Marshall European Center for Security Studies	

Dr. Gustav LINDSTROM	Sweden	Head of Programme, Emerging Security Challenges Geneva Centre for Security Policy	
Dr. Vakhtang MAISAIA	Georgia	Professor, MA Program in International Security Caucasus International University	
Dr. Petar MOLLOV	Bulgaria	Associate Professor, Defense Advanced Research Institute	
Mr. Chris PALLARIS	United Kingdom	Director, i-intelligence	
Mr. Daniel PEDER BAGGE	Czech Republic	Cyber Security/Policy Specialist, National Security Authority	
Mr. Raphael PERL	USA	Director, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes	
Ms. Maka PETRIASHVILI	Georgia	Head of Human Resources, Ministry of Defence	
Ms. Stela PETROVA	Bulgaria	Consultant, European Leadership Network	
Dr. Benyamin POGHOSYAN	Armenia	Deputy Director, Institute for National Strategic Studies	
Mr. Oleksandr POTIL	Ukraine	Professor of IT Security, Kharkiv Air Force University	

Dr. Detlef PUHL	Germany	Senior Advisor, Emerging Security Challenges Division, NATO International Staff	
Mr. Neil ROBINSON	United Kingdom	Research Leader RAND Europe	
Mr. Gigi ROMAN	Romania	ADL, NATO School Oberammergau	
LTC Ghenadie SAFONOV	Moldova	Communications and Informatics Department Moldova Military Academy	
Mr. Danylo SHEVCHENKO	Ukraine	Project Manager, Center for Strategic Research and Innovation	
Ms. Natalia SPINU	Moldova	Chief, Cyber Security Center, State Chancellery of Moldova	
Dr. Alan G. STOLBERG	USA	Coordinator, Defense Education RAND	
Dr. Todor TAGAREV	Bulgaria	Professor/Head, "IT for Security" Department & Centre for Security and Defence Management	
Dr. Ronald TAYLOR	USA	President, Center for Strategic Leadership in Complex Environments	
Mr. Bodgan UDRISTE	Romania	Information Systems Security Expert, European Union Monitoring Mission	
Mr. Joseph VANN	USA	Professor, George C. Marshall European Center for Security Studies	

Editorial Team and Distribution

Editors:

Sean S. Costigan
Professor
George C. Marshall European Center for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
sean.costigan@pfp-consortium.org

Michael A. Hennessy, PhD
Professor of History and War Studies
Associate Vice Principal – Research
Royal Military College of Canada
P.O. Box 17000 STN FORCES
Kingston, ON Canada
K7K 7B4
Hennessy-m@rmc.ca

Layout Coordinator / Distribution:

Gabriella Lurwig-Gendarme
NATO International Staff
lurwig.gabriella@hq.nato.int

1217-16 NATO Graphics & Printing — ISBN 978-92-845-0196-0