Cyber Security Syllabus (IY 3612/4612) — Academic Year 2021–2022

S. Wolthusen

December 28, 2021

1 Introduction

Cyber security can be considered as a specialised area of information security in that it focuses on an understanding of information systems with physical systems as is reflected by the etymology of the *cyber* prefix in κυβερνήτης who, fittingly, was not only the title of the helmsman but also the officer responsible for safety on a trireme.

The objective of this module is hence to develop an understanding of advanced adversaries and threats to information systems, and particularly the interaction of information with physical systems at scales ranging from embedded and industrial control systems up to critical infrastructures at national and supra-national scales. Recent events have perhaps confirmed that this is no longer an entirely hypothetical endeavour.

To this end, models of adversaries and interactions with adversaries will be studied together with approaches for modelling dependencies and interdependencies in networked systems including cyber-physical interactions. Based on this, advanced and persistent threats are studied, also to networks, embedded and control systems.

The module also aims to impart an understanding of assurance mechanisms for both the development and operation of security-sensitive and other high-integrity systems and will therefore provide a critical review of relevant standards and evaluation criteria as well as of issues arising in the development of high assurance systems.

2 Learning Outcomes

Having completed the course, students should have

- gained an overview of core concepts of cyber security problems, and particularly their relation to critical (information) infrastructures and national cyber security strategies to defend such critical assets

- developed an understanding of dependencies and interdependencies in particularly larger-scale networks employing different modelling techniques
- the ability to analyse cyber-physical systems, particularly involving control systems and to analyse attacks on such systems
- the ability to demonstrate critical awareness of advanced threats and attacks, and of methods for modelling and analysing such threats and attacks
- demonstrate a conceptual grasp of problems pertaining to specifying, measuring, and validating assurance including through formal assurance mechanisms
- the ability to evaluate problems and approaches related to information sharing, including security-related, legal, and ethical considerations
- a critical awareness of problems related to conflicts involving attacks on information systems including issues surrounding attribution and asymmetric conflicts

3 Formal Aspects

3.1 Faculty Contact Information

Stephen Wolthusen (main point of contact)
Office: Bedford 2-31
Telephone: 01784 443 270
Email: stephen.wolthusen@rhul.ac.uk

3.2 Prerequisites

The module benefits from a sound understanding of computer and network security. It is therefore desirable to have read the IY5512 (*Computer Security*) module and to satisfy the prerequisites for this module, or to have an equivalent background; in addition or in case that further material is required. Examples of background reading material at the advanced undergraduate or beginning postgraduate levels on on modern operating systems include the books by Tanenbaum [74] or Silberschatz *et al*. [67]. Similarly, it is also recommended to have read the module IY5511 (*Network Security*); in this case background reading on network security is e.g. provided by the books of Stallings [68] or [69], while further general networking background can e.g. be found in the books of Comer [17].

3.3 Course Requirements and Objectives

Students will be expected to have a sound understanding of information security concepts as well as a solid grasp of core concepts in computer science and selected aspects of discrete mathematics mainly required for modelling as well as some understanding of elementary probability theory.

On completion of the module, students will have gained insight into selected aspects of cyber security beginning with high-level concepts such as national cyber security policies and their interactions with technical implementations. As the subjects of cyber security particularly at high levels will often exhibit dependencies, students will have gained exposure and the ability to analyse dependencies, and interdependencies using different modelling approaches varying in their level of detail including for critical infrastructures.

On completion of the module, students will further have achieved critical awareness of the cyber security issues found in cyber-physical systems and techniques employed in their security analysis including for sophisticated threats and attacks as well as incident response and recovery approaches. Students will also have gained a systematic understanding of assurance models and approaches for certification and accreditation.

3.4 Assessment and Academic Integrity

3.4.1 Assessment

The outcome of the course will be based on three assessment elements.

An examination during the assessment period contributes 60% to the final outcome; the remaining assessment is formed by a quiz contributing 10%, and an essay (term paper) contributing 30% to the outcome.

3.4.2 Quiz

The quiz is a timed (1h) assessment in which a small number of problem-solving questions, typically 3-4 questions, need to be answered concisely.

3.4.3 Term Paper

The term paper is an essay on a topic that is within the scope of the module, but should delve into an area either covered by the lectures in some more depth, or should study an adjacent area; the topics identified in this syllabus documents can act as a guide.

If the chosen topic does not match with these requirements, it will be considered an invalid submission.

Term papers will usually take the form of a *literature survey*, but should be based on one or two *research questions* to guide the selection of articles

and book chapters used to construct the review and the formulation of the essay structure.

The length of the essay will vary depending on the module code under which the module is taken. For IY3612, the length should be 2000 words, for IY4612 the length should be 3000 words, and in case of IY5612 it should be 4000 words.

As with any academic work, it is expected to be structured in support of its argument with clear and concise writing one of the key objectives. All arguments need to be supported, whether by direct evidence or proof, or more commonly by reference to the literature.

When relying on supporting evidence from the literature, every argument or claim should be supported by a clear, separate reference. The apparatus containing citations must follow a consistent format; whilst not required, use of the ACM citation style is recommended. When using LaTeX[1] for writing the term paper, this is supported by a dedicated BibTeX style.

3.4.4 Academic Integrity

Penalties will particularly be imposed for academic dishonesty. Academic dishonesty is defined as any action or practice that provides the potential for an unfair advantage to one individual or one group.

Academic dishonesty includes the misrepresentation of facts, the fabrication or manipulation of data or results, representing another's work or knowledge as one's own, disrupting or destroying the work of others, or abetting anyone who engages in such practices. Academic dishonesty is not absolute because the expectations for collaboration vary. However, unless given specific permission, any and all results submitted must be the result of individual effort, performed without the help of other individuals or outside sources.

If a question arises about the type of external materials that may be used or the amount of collaboration that is permitted for a given task, each individual involved is responsible for verifying the rules with the lecturer or teaching assistant before engaging in collaborative activities, using external materials, or accepting help from others.

3.5 Schedule

Lectures will be given in the *second term*, beginning the week of January 10, 2022 on *Monday*. Lectures will take place from 9am until 12 noon in the *Boilerhouse Auditorium*. To facilitate time-keeping, attendees should be in the lecture theatre well before the starting time to complete any necessary preparations and seating arrangements.

[1] Available for virtually all operating systems, see the LaTeX Project for links to distributions.

4 Required Reading

There is no single textbook on which the module is based; please refer to the notes for each unit. Several initial units make reference to chapters from [52]; note that these are available electronically through the college library subscription.

5 Lecture Schedule

The following sections contain both descriptions of the contents of each individual lecture together with required and recommended reading materials.

Lecture materials, exercise sheets, and a *mock exam* are posted on Moodle together with information on the blocks covered in each week's lecture. This mechanism also provides timely information on any changes to the schedule and should be reviewed regularly for any significant changes.

5.1 Unit 1: Introduction

Objectives

- Introduction to the concepts of cyber security
- Introduction to critical infrastructures, critical information infrastructures,
  and their relation to cyber security
- Overview of national cyber security strategies

Topics

Block 1 Administrative Matters

- Overview of the Cyber Security module and topics covered
- A review of exercises, tutorials, and formative feedback provided

Block 2 Introduction to Cyber Security and Critical Infrastructures

- Defining Critical Infrastructures (CI) and
  Critical Information (CII) Infrastructures
- The relation between Cyber Security and CI/CII
- Threat actors and their classification

Block 3 National Cyber Security Strategies

- The relation between overall national security strategy and
  Cyber Security strategies
- The UK Cyber Security strategy
- Selected national Cyber Security strategies

Required and recommended reading The chapter by Dunn Cavelty and Suter provides an overview of the embedding of cyber security in the overall national security stratgy context and the relationship to critical infrastructures [23], while Luiijf provides a survey of cyber threats [54].

The United Kingdom's overarching national security strategy in its publishable form is outlined in [35], while the UK Cyber Security strategy is found in [36]; an earlier revision and updates sketching out developments are found in [31, 34, 33]. More recent highlights are found in [37].

The U.S. cyber security policy stance has shifted considerably in 2021 with Executive Order 14028 ("*Improving the Nation's Cybersecurity*") [84] with renewed emphasis not only on governmental and critical national infrastructure cyber security, but explicitly targeting the software supply chain security. A more dated but comprehensive general U.S. policy perspective can be found in the 2009 review document [79], whilst the U.S.

Department of Defense's published perspective particularly on operational considerations in the cyber domain was published in 2011 [77] with a more recent overview document on U.S. DoD strategy dating from 2015 [78]; strategies for protecting critical infrastructures were only published in draft form. Whilst the European Union does not have defence matters within its remit, several policy areas including related to national and European critical infrastructures such as payment and clearing systems, energy, and commerce are immediately affected; hence the Commission published a European Cyber Security strategy augmenting the respective national strategies is found in [38].

A more comprehensive survey of national cyber security strategies can be found in the NATO framework document [45]; related to this is a guide released by the ITU [86]; for a collection of national strategy documents see https://ccdcoe.org/cyber-security-strategy-documents.html.

5.2 Unit 2: Complex Attacks

Objectives

- Introduce complex attacks
- Understanding the cyber attack lifecycle and defences
- Case studies of cyber attack campaigns

Topics

Block 4 Complex Attacks

- The Cyber Kill Chain
- Advanced persistent threat campaigns and selected countermeasures
- Deception defences

Block 5 APT Case Studies

- Early examples: Solar Sunrise, Moonlight Maze, and Titan Rain
- Aurora, APT1, and other "professional" groups
- Case study: The Regin toolkit
- State and non-state actors: Sofacy/Fancy Bear (APT28)

Required and recommended reading For an early example of an espionage campaign conducted in computer networks see Stoll's entertaining account [70].

The concept of cyber kill chains was introduced in [42], while the book [43] offers some recent academic perspectives on key problems including attribution, deterrence, adversary profiling, and human factors; attribution is also studied in the article by Lindsay [50]. An unclassified view of cyber operations is provided by [80] while a discussion of related policy issues can be found in [75]; a NATO perspective on offensive operations is contained in [49] with a discussion on models of offensive operations in [28].

The more recent MITRE ATT&CK framework [72] offers a more narrative mechanism for describing adversary behaviour in the form of a taxonomy that had later been extended also to pre-attack behaviour. This more extensive taxonomy is suitable for describing attacks, although for analysis it presents challenges in mapping activities [81].

Some theoretical underpinnings on cyber attack can also be found in the article by Michael [56]; the Mandiant (purchased by FireEye in 2013 and de-merged again in 2021) report on the APT1 group and its activities as well open source as attempts to identify these can be found in [25], while the Kaspersky analysis of the Regin platform is found in [44]. The APT28 group that seems to have played a certain role recently [83] is described in

the FireEye report [26], while stealthy mechanisms using Twitter employed by the APT29 group as a vector are discussed in [27].

FireEye was, ironically, also one of the targets of the SolarWinds supply chain attacks in 2020–21 [82].

5.3 Unit 3: Networks and Dependencies

Objectives

- Develop systematic understanding of basic concepts in network modelling
- Conceptual understanding of network robustness and the effects of failures
  in networks for selected network models
- Synthesis of network robustness concepts developed for the case of the global
  Internet structure

Topics

Block 6 Models of Large-Scale Networks

- Elements and concepts in graph theory
- Methods for characterising graphs
- Basic network models: Random graphs

Block 7 Robustness of Networks

- Further properties and metrics for characterising graphs
- Matching existing physical and logical networks to the Erdős-Rényi random graph
- The Watts-Strogatz Small-World model
- Scale-free graphs and the Barabási-Albert graph model

Required and recommended reading A brief survey of network models is provided in the book chapter [73]. Whilst this is sufficient for the purposes of this lecture, a far more comprehensive and leisurely survey of networks and network science covering a number of ancillary areas is provided by [58] with chapters 7 and 8 of particular interest, while chapter 16 gives further insights into network resilience.

Although this module requires mainly a conceptual grasp of graph theory, the book by van Steen (on which the exposition of graph theoretic concepts is partly based) may provide valuable further reading at the advanced undergraduate level [85]. For further reading as well as a somewhat more rigorous but still accessible presentation, many alternative texts exist including [21].

5.4 Unit 4: Network and Internet Robustness

Objectives

- Understanding Internet Robustness to Random Faults and Attacks
- Robustness and attacks against the Internet infrastructure
- Understanding economic models of critical infrastructure dependencies

Topics

Block 8 Internet Robustness

- Modelling the global Internet structure
- An introduction to network robustness

Block 9 Robustness and attacks against the Internet Infrastructure

- Robustness of BGP routing
- Robustness of the DNS infrastructure
- Large-scale distributed denial of service attacks

Block 10 Economic Models of Critical Infrastructures

- Introduction to modelling approaches for dependencies and interdependencies
- Input-Output economic models
- Case Study: Centrality Measures for the Analysis of Financial Networks

Required and recommended reading Willinger and Roughan give a critical overview of Internet topology mapping research and associated problems [88]; at different abstraction levels this will yield quite variable insights and is subject to intensive research into methods for minimising any such errors. The only somewhat specious observation about the trade-off between the fidelity and necessary abstraction in the lecture was made by Wiener and Rosenblueth [62].

A seminal, but also often criticised, contribution on network robustness that is worth reviewing is the original article by Albert, Jeong, and Barabási [4], while the exposition of robustness aspects in the latter part of the unit is derived from the article by Deng *et al*. [20].

No current textbook covers routing protocols and security to a meaningful extent, so the primary RFC 4271 for BGP [61] may be reviewed. The survey papers [12, 41, 3] give a good insight into security problems and some approaches for protecting BGP from attacks and in part also misconfiguration. For in-depth but somewhat dated reading on routing protocols [29] or [40] may be more readable than the protocol specifications.

Economic and other qualitative as well as partially quantitative models of critical infrastructures are covered in the book chapter [73].

5.5 Unit 5: Critical Infrastructures and Interdependencies

Objectives

- Conceptual understanding of interdependency models at different abstraction levels
- Synthesis of dependency concepts and their effect on risk and vulnerability analysis in interdependent networks
- Understanding of power network concepts and their relation to critical infrastructures and control

Topics

Block 11 Critical Infrastructure Interdependency Models

- Graph-based models
- Flow problems and network robustness
- Agent-based models of interdependence
- Game-theoretical models

Block 12 Power Systems: A Case Study for Critical Infrastructures

- Power (and Smart) Grid Structrure
- Grid Requirements and Operation
- Communication and Control in the (Smart) Grid

The discussion of centrality measures for identifying systemically critical entities in the financial services sector is based on the article by Battiston *et al*. [9].

Cárdenas *et al*. discuss centrality and betweenness centrality results for a real communication network that would be considered carefully designed (yet still exhibits scale-free properties, as noted by the authors) [15]. For a study of betweenness measures for several electrical grids, consider the study by Hawick [30] detailing not only the immediate betweenness of a network, but also changes in betweenness on removal of some high-betweenness nodes as would be expected in an attack.

Schrijver describes the history of maximum flow problems arising from transportation networks and the study of their capacity and robustness [66].

The study of cascading failures has attracted considerable research interest, using a variety of formalisms and abstraction levels. The work by Buldyrev *et al*. [11] referenced in the lecture notes provides an example of this line of inquiry.

The lecture can give only a very brief motivation for the types of problems making agent-based modelling attractive in the analysis and simulation of computer and infrastructure networks; instead, only a simple example is provided. The main outline of the currently-used Tor protocol

(an overlay network intended to provide privacy and anonymity) as described by Dingledine and Mathewson [22] is analysed in an example of an agent-based simulation for studying strategies of enhancing the robustness to failure and attack when changing the entry-points ("guards") of the overlay by Elahi *et al*. [24].

Similar to agent-based models, the study of game-theoretical models for analysing security controls and properties is an active research area which is only introduced briefly; the specific question of resource allocation for security controls is e.g. studied by An *et al*. [8].

A basic introduction to power systems can e.g. be found in the work by Weedy *et al*. [87]

5.6 Unit 6: Security of Cyber-Physical Systems

Objectives

- Develop an understanding of key concepts in control systems theory and control systems architecture
- Synthesis of security challenges arising from cyber-physical interactions

Topics

Block 13 Introduction to Cyber-Physical Systems and Control Systems

- Control Systems Fundamentals
- Interaction Between Computation and Physical Environment
- Modelling, Specification, and Analysis of Cyber-Physical Systems

Block 14 Control Systems Architecture

- Basic Control Systems
- Components of Industrial Control Systems
- Real-Time Systems

Block 15 Attacks on Cyber-Physical Systems and Hybrid Attacks

- Attacks on Sensors and Actuators
- De-Synchronisation Attacks
- Altering Physical Parameters

Required and recommended reading The unit touches only on the very fundamentals of control systems theory and aims to be broadly qualitative, so if a deeper appreciation of problems and concepts is sought, this will require further self-study.

A very gentle introduction is e.g. the volume by Albertos and Mareels [5]; there exist a number of books on control systems theory where one approach may be more suitable to personal taste and background than another; one relatively comprehensive text at the advanced undergraduate level is the volume by Ogata [59]. While the title by Polderman and Willems is slightly older and currently out of print, it can be found online [60].

Chapter 2 of [71] gives a basic overview of the general control systems architecture. The bulk of [71] is concerned with control systems attacks; this will largely be covered in Unit 6 (see section 5.6), but for the purposes of this unit a more high-level perspective suffices.

A more in-depth view of attack modes on process control systems can e.g. be found in the article by Huang *et al*. [39].

5.7 Unit 7: Control Systems Security

Objectives

- Overview of basic concepts in control system implementations
- Conceptual understanding of state estimation problems
- Overview of security issues in control systems implementations

Topics

Block 16 SCADA and DCS Systems

- Introduction to Supervisory Control and Data Acquisition (SCADA) architectures
- Distributed Control Systems
- Control System Protocols

Block 17 State Estimation

- Linear State Estimators
- Non-Linear State Estimator
- Attacks on State Estimators

Block 18 Security of Control System Components

- Threats to Availability and Integrity
- Intrusion Detection in Control Systems

Required and recommended reading The NIST Special Publication 800-82 provides a good overview of current issues and challenges in control systems security [71].

A more network-oriented perspective is provided by Klein [46], with chapter 4 in particular dealing with the network protocols in industrial control systems. The UK CPNI also provides guidance for different aspects of control systems security [19].

A more in-depth view on some protocol vulnerabilities is e.g. provided by Rrushi in [64], while a discussion of cyber vulnerabilities in current (not necessarily "smart") power networks is provided by Bompard *et al*. in [10].

A set of examples of attacks on state estimation in power networks is found in the article by Liu *et al*. [51] (see [1] for a detailed monograph on power system state estimation).

A very brief outline of more practical attacks and techniques used in the analysis of control systems components is found in the white paper by Luallen [53], while some selected attacks on GPS systems are described in the paper by Tippenhauer *et al*. [76].

5.8 Unit 8: Attack Modelling Techniques

Objectives

- Survey of static risk and attack models
- Overview of selected dynamic attack and adversary models
- Introduction to the problem of concurrency in modelling adversary behaviour

Topics

Block 19 Static Risk and Attack Models

- Basic Risk Metrics
- Attack Trees

Block 20 Dynamic Attack and Adversary Models

- Attack-Defence Trees
- Game-Theoretic Models

Block 21 Concurrency in Adversary Models

- The problem of concurrency in attacker-defender interaction
- Petri nets for adversary modelling

Required and recommended reading A number of methods for analysing attacks based on approaches such as Fault Tree Analysis and Failure Mode and Effects Analysis have been described in the literature, partly intended for documenting analytical steps as in the case of [57], but also earlier e.g. in Amoroso's Threat Trees [7]. The term *Attack Tree* was then popularised by Schneier [65] and formulated rigorously by Mauw and Oostdijk [55].

Given the limitations of Attack Trees in becoming somewhat large and unwieldy for more complex scenarios and also the need to incorporate responses, a number of approaches have been put forward, including exensions of the earlier work by Mauw and Oostdijk by Kordy *et al*. [47] in the form of *Attack-Defence Trees*. This formalism can be extended further and has also been shown to be equivalent to a game-theoretical formulation.

A related approach which also includes a distinction between detection and mitigation events in the modelling of attacks was proposed by Roy *et al*. in the form of Attack Countermeasure Trees (ACT) [63]; as in the case of Attack Trees this allows both qualitative and quantitative study of attacks, including the cost effectiveness of detection and mitigation strategies where quantitative studies are used.

The article by Korzhyk *et al*. provides a summary of security games [48] and also contains further references to a number of existing models where different variants of security games are studied and deployed.

The article by Chen *et al*. gives a brief overview of different Petri net based concurrency formalisms for capturing concurrency in adversary behaviour, and also provides a case study in the cyber-physical interaction of the smart grid environment [16].

Reading List

[1] ABUR, A., AND GÓMEZ-EXPÓSITO, A. *Power System State Estimation: Theory and Implementation*. CRC Press, Boca Raton, FL, USA, 2004. 16

[2] AGUTTER, C. *ITIL Foundation Handbook*, 3rd ed. ed. H.M. Stationery Office, Norwich, UK, 2012.

[3] AL-MUSAWI, B., BRANCH, P., AND ARMITAGE, G. BGP Anomaly Detection Techniques: A Survey. *IEEE Communications Surveys & Tutorials 19*, 1 (Mar. 2016), 377–396. doi:10.1109/COMST.2016.2622240. 11

[4] ALBERT, R., JEONG, H., AND BARABÁSI, A.-L. Error and Attack Tolerance of Complex Networks. *Nature 406* (July 2000), 378–382. doi:10.1038/35019019. 11

[5] ALBERTOS, P., AND MAREELS, I. *Feedback and Control for Everyone*. Springer-Verlag, Heidelberg, Germany, 2010. 15

[6] ALBERTS, C., AND DOROFEE, A. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley, Reading, MA, USA, 2002.

[7] AMOROSO, E. G. *Fundamentals of Computer Security Technology*. Prentice-Hall, Upper Saddle River, NJ, USA, 1994. 17

[8] AN, B., KEMPE, D., KIEKINTVELD, C., SHIEH, E., SINGH, S., TAMBE, M., AND VOROBEYCHIK, Y. Security Games with Limited Surveillance: An Initial Report. In *Proceedings of the 2012 AAAI Spring Symposium on Game Theory for Security, Sustainability, and Health* (Stanford, CA, USA, Mar. 2012), AAAI, pp. 2–8. 14

[9] BATTISTON, S., PUGLIA, M., KAUSHIK, R., TASCA, P., AND CALDARELLI, G. DebtRank: Too Central to Fail? Financial Networks, the FED and Systemic Risk. *Nature Scientific Reports 2*, 541 (Aug. 2012), 1–6. doi:10.1038/srep00541. 13

[10] BOMPARD, E., CUCCIA, P., MASERA, M., AND FOVINO, I. N. Cyber Vulnerability in Power Systems Operation and Control. In *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Heidelberg, Germany, Sept. 2012), J. Lopez, R. Setola,

and S. Wolthusen, Eds., vol. 7130 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 197–234. doi:10.1007/978-3-642-28920-0_10. 16

[11] BULDYREV, S. V., PARSHANI, R., PAUL, G., STANLEY, H. E., AND HAVLIN, S. Catastrophic Cascade of Failures in Interdependent Networks. *Nature 464*, 7291 (Apr. 2010), 1025–1028. doi:10.1038/nature08932. 13

[12] BUTLER, K., FARLEY, T. R., MCDANIEL, P., AND REXFORD, J. A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE 98*, 1 (Jan. 2010), 100–122. doi:10.1109/JPROC.2009.2034031. 11

[13] CALDER, A., AND WATKINS, S. *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*, 5th ed. Kogan Page, London, UK, 2012.

[14] CARALLI, R. A., STEVENS, J. F., YOUNG, L. R., AND WILSON, W. R. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. CMU/SEI 2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, May 2007.

[15] CÁRDENAS, J. P., BENITO, R. M., MOURONTE, M. L., AND FELIU, V. The Effect of the Complex Topology on the Robustness of Spanish SDH Network. In *Proceedings of the 5th IEEE International Conference on Networking and Services (ICNS 2009)* (Valencia, Spain, Apr. 2009), IEEE Press, pp. 86–90. doi:10.1109/ICNS.2009.28. 13

[16] CHEN, T. M., SANCHEZ-AARNOUTSE, J. C., AND BUFORD, J. Petri Net Modeling of Cyber-Physical Attacks on Smart Grid. *IEEE Transactions on Smart Grid 2*, 4 (Dec. 2011), 741–749. doi:10.1109/TSG.2011.2160000. 18

[17] COMER, D. *Internetworking with TCP/IP, Volume 1*, 6th ed. Prentice-Hall, Upper Saddle River, NJ, USA, 2013. 2

[18] COMMUNICATION ELECTRONICS SECURITY GROUP (CESG). HMG Information Assurance Standard No. 1: Technical Risk Assessment. Her Majesty's Cabinet Office, Oct. 2009.

[19] CPNI. *Securing the Move to IP-Based SCADA/PLC Networks*. Centre for the Protection of National Infrastructure, London, UK, Nov. 2011. 16

[20] DENG, W., KARALIOPOULOS, M., MÜHLBAUER, W., ZHU, P., LU, X., AND PLATTNER, B. k-Fault tolerance of the Internet AS graph. *Computer Networks 55*, 10 (July 2011), 2492–2503. doi:10.1016/j.comnet.2011.04.009. 11

[21] DIESTEL, R. *Graph Theory*, 4th ed., vol. 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Heidelberg, Germany, 2010. 10

[22] DINGLEDINE, R., AND MATHEWSON, N. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th USENIX Security Symposium* (San Diego, CA, USA, Aug. 2004), M. Blaze, Ed., USENIX, pp. 303–320. 14

[23] DUNN CAVELTY, M., AND SUTER, M. The Art of CIIP Strategy: Taking Stock of Content and Processes. In *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Heidelberg, Germany, Sept. 2012), J. Lopez, R. Setola, and S. Wolthusen, Eds., vol. 7130 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 15–38. doi:10.1007/978-3-642-28920-0_2. 6

[24] ELAHI, T., BAUER, K., ALSABAH, M., DINGELDINE, R., AND GOLDBERG, I. Changing of the Guards: A Framework for Understanding and Improving Entry Guard Selection in Tor. In *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society* (Raleigh, NC, USA, Oct. 2012), ACM Press, pp. 43–54. doi:10.1145/2381966.2381973. 14

[25] FIREEYE. APT1: Exposing One of China's Cyber Espionage Units. Tech. rep., Mandiant Inc., Milpitas, CA, USA, Feb. 2013. 8

[26] FIREEYE. APT28: A Window into Russia's Cyber Espionage Operations? Tech. rep., FireEye Inc., Milpitas, CA, USA, Oct. 2014. 9

[27] FIREEYE. APT29: Hammertoss: Stealthy Tactics Define a Russian Cyber Threat Group. Tech. rep., FireEye Inc., Milpitas, CA, USA, July 2015. 9

[28] GRANT, T., BURKE, I., AND VAN HEERDEN, R. *Leading Issues in Cyber Warfare & Security Research*, vol. 2. ACPI, Reading, UK, 2015, ch. Comparing Models of Offensive Cyber Operations, pp. 35–. Proceedings of the 7th International Conference on Information Warfare and Security. 8

[29] HALABI, S. *Internet Routing Architectures*, 2nd ed. Cisco Press, Indianapolis, IN, USA, 2000. 11

[30] HAWICK, K. A. Betweenness Centrality Metrics for Assessing Electrical Power Network Robustness against Fragmentation and Node Failure. Computational Science Technical Note CSTN-119, Institute of Information and Mathematical Sciences, Massey University, Auckland, New Zealand, Nov. 2010. 13

[31] HER MAJESTY'S GOVERNMENT. The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. Her Majesty's Stationery Office, Nov. 2011. 6

[32] HER MAJESTY'S GOVERNMENT. HMG Security Policy Framework, Version 8. Her Majesty's Cabinet Office, Apr. 2012.

[33] HER MAJESTY'S GOVERNMENT. Progress Against the Objectives of the National Cyber Security Strategy. Her Majesty's Stationery Office, Dec. 2013. 6

[34] HER MAJESTY'S GOVERNMENT. The National Cyber Security Strategy: Our Forward Plans. Her Majesty's Stationery Office, Dec. 2013. 6

[35] HER MAJESTY'S GOVERNMENT. National Security Strategy and Strategic Defence and Security Review 2015. Her Majesty's Stationery Office, Nov. 2015. 6

[36] HER MAJESTY'S GOVERNMENT. National Cyber Security Strategy 2016 to 2021. Her Majesty's Stationery Office, Nov. 2016. 6

[37] HER MAJESTY'S GOVERNMENT. National Cyber Strategy 2022. Her Majesty's Stationery Office, Dec. 2021. 6

[38] HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY. *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace*. European Commission, Brussels, Belgium, Feb. 2013. 7

[39] HUANG, Y.-L., CÁRDENAS, A. A., AMIN, S., LIN, Z.-S., TSAI, H.-Y., AND SASTRY, S. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection 2*, 3 (Oct. 2009), 73–83. doi:10.1016/j.ijcip.2009.06.001. 15

[40] HUITEMA, C. *Routing in the Internet*, 2nd ed. Prentice Hall, Upper Saddle River, NJ, USA, 1999. 11

[41] HUSTON, G., ROSSI, M., AND ARMITAGE, G. Securing BGP — A Literature Survey. *IEEE Communications Surveys & Tutorials 13*, 2 (May 2011), 199–222. doi:10.1109/SURV.2011.041010.00041. 11

[42] HUTCHINS, E. M., CLOPPERT, M. J., AND AMIN, R. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In *Proceedings of the 6th Annual Conference on Information Warfare and Security (ICCWS 2011)* (Washington, D.C., USA, Mar. 2011), E. Armistead, Ed., ACI, pp. 1–11. 8

[43] JAJODIA, S., SHAKARIAN, P., SUBRAHMANIAN, V., SWARUP, V., AND WANG, C., Eds. *Cyber Warfare: Building the Scientific Foundation*, vol. 56 of *Advances in Information Security*. Springer-Verlag, Heidelberg, Germany, 2015. 8

[44] KASPERSKY LAB'S GLOBAL RESEARCH & ANALYSIS TEAM. The Regin Platform: Nation-State Ownage of GSM Networks. Tech. rep., Kaspersky Lab, Moscow, Russia, Nov. 2014. 8

[45] KLIMBURG, A. *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Talinn, Estonia, Dec. 2012. 7

[46] KNAPP, E. D. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Elsevier (Syngress), Amsterdam, The Netherlands, 2011. 16

[47] KORDY, B., MAUW, S., AND OOSTDIJK, M. Foundations of Attack-Defense Trees. In *Proceedings of the 7th International Workshop on Formal Aspects of Security and Trust (FAST 2010)* (Pisa, Italy, Sept. 2010), P. Degano, S. Etalle, and J. Guttman, Eds., vol. 6561 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 80–95. doi:10.1007/978-3-642-19751-2_6. 17

[48] KORZHYK, D., YIN, Z., KIEKINTVELD, C., CONITZER, V., AND TAMBE, M. Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness. *Journal of Artificial Intelligence Research 41* (May 2011), 297–327. doi:10.1613/jair.3269. 17

[49] LEWIS, J. A. The Role of Offensive Cyber Operations in NATO's Collective Defence. Tallinn Paper 8, NATO CCD COE, Tallinn, Estonia, May 2015. 8

[50] LINDSAY, J. R. Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity 1*, 1 (Nov. 2015), 53–67. doi:10.1093/cybsec/tyv003. 8

[51] LIU, Y., NING, P., AND REITER, M. K. False Data Injection Attacks against State Estimation in Electric Power Grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (Chicago, IL, USA, Nov. 2009), S. Jha and A. D. Keromytis, Eds., ACM Press, pp. 21–32. doi:10.1145/1653662.1653666. 16

[52] LOPEZ, J., SETOLA, R., AND WOLTHUSEN, S., Eds. *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*

(Heidelberg, Germany, Sept. 2012), vol. 7130 of *Lecture Notes in Computer Science*, Springer-Verlag. doi:10.1007/978-3-642-28920-0. 5

[53] LUALLEN, M. E. Critical Control System Vulnerabilities Demonstrated — And What to Do About Them. SANS White Paper, Nov. 2011. 16

[54] LUIIJF, E. The Art of CIIP Strategy: Taking Stock of Content and Processes. In *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Heidelberg, Germany, Sept. 2012), J. Lopez, R. Setola, and S. Wolthusen, Eds., vol. 7130 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 52–67. doi:10.1007/978-3-642-28920-0_4. 6

[55] MAUW, S., AND OOSTDIJK, M. Foundations of Attack Trees. In *Proceedings of the 8th International Conference on Information Security and Cryptology (ICISC 2005)* (Seoul, South Korea, Dec. 2005), D.-H. Won and S. Kim, Eds., vol. 3935 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 186–198. doi:10.1007/11734727_17. 17

[56] MICHAEL, A. Cyber Probing: The Politicisation of Virtual Attack. Special Series 10/12, Defence Academy of the United Kingdom, London, UK, Sept. 2010. 8

[57] MOORE, A. P., ELLISON, R. J., AND LINGER, R. C. Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, Mar. 2001. 17

[58] NEWMAN, M. *Networks: An Introduction*. Oxford University Press, Oxford, UK, 2010. 10

[59] OGATA, K. *Modern Control Engineering*, 5th ed. Prentice Hall, Upper Saddle River, NJ, USA, 2009. 15

[60] POLDERMAN, J. W., AND WILLEMS, J. C. *Introduction to Mathematical Systems theory: A Behavioral Approach*. Springer-Verlag, Heidelberg, Germany, 1998. 15

[61] REKHTER, Y., LI, T., AND HARES, S. A Border Gateway Protocol 4 (BGP-4). IETF Request for Comments 4271, Jan. 2006. 11

[62] ROSENBLUETH, A., AND WIENER, N. The Role of Models in Science. *Philosophy of Science 12*, 4 (Oct. 1945), 316–321. 11

[63] ROY, A., KIM, D. S., AND TRIVEDI, K. S. Attack Countermeasure Trees (ACT): Towards Unifying the Constructs of Attack and Defense

Trees. *Security and Communication Networks 5*, 8 (Aug. 2012), 929–943. doi:10.1002/sec.299. 17

[64] RRUSHI, J. L. SCADA Protocol Vulnerabilities. In *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Heidelberg, Germany, Sept. 2012), J. Lopez, R. Setola, and S. Wolthusen, Eds., vol. 7130 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 150–176. doi:10.1007/978-3-642-28920-0_8. 16

[65] SCHNEIER, B. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, New York, NY, USA, 2000. 17

[66] SCHRIJVER, A. On the History of the Transportation and Maximum Flow Problems. *Mathematical Programming 91*, 3 (Feb. 2002a), 437–445. doi:10.1007/s101070100259. 13

[67] SILBERSCHATZ, A., GAGNE, G., AND GALVIN, P. B. *Operating System Concepts*, 10th ed. John Wiley & Sons, Chichester, UK, 2018. 2

[68] STALLINGS, W. *Cryptography and Network Security*, 7th ed. Prentice Hall, Upper Saddle River, NJ, USA, 2017. 2

[69] STALLINGS, W. *Network Security Essentials*, 6th ed. Prentice Hall, Upper Saddle River, NJ, USA, 2017. 2

[70] STOLL, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday, 1989. 8

[71] STOUFFER, K., PILLITTERI, V., LIGHTMAN, S., ABRAMS, M., AND HAHN, A. *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security Revision 2*. U.S. National Institute of Standards and Technology, Gaithersburg, MD, USA, May 2015. 15, 16

[72] STROM, B. E., APPLEBAUM, A., MILLER, D. P., NICKELS, K. C., PENNINGTON, A. G., AND THOMAS, C. B. MITRE ATT&CK: Design and Philosophy. Tech. Rep. MP180360, MITRE Corporation, Cambridge, MA, USA, July 2018. 8

[73] SVENDSEN, N. K., AND WOLTHUSEN, S. Modelling Approaches. In *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Heidelberg, Germany, Sept. 2012), J. Lopez, R. Setola, and S. Wolthusen, Eds., vol. 7130 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 68–97. doi:10.1007/978-3-642-28920-0_5. 10, 12

[74] TANENBAUM, A. S. *Modern Operating Systems*, 4th ed. Prentice-Hall, Upper Saddle River, NJ, USA, 2014. 2

[75] THEOHARY, C. A., AND HARRINGTON, A. I. Cyber Operations in DoD Policy and Plans: Issues for Congress. United States Congressional Research Service, Jan. 2015. 8

[76] TIPPENHAUER, N. O., PÖPPER, C., BONNE RASMUSSEN, K., AND ČAPKUN, S. On the Requirements for Successful GPS Spoofing Attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (Chicago, IL, USA, Nov. 2011), Y. Chen, G. Danezis, and V. Shmatikov, Eds., ACM Press, pp. 75–86. doi:10.1145/2046707.2046719. 16

[77] UNITED STATES DEPARTMENT OF DEFENSE. Department of Defense Strategy for Operating in Cyberspace. U.S. Government Printing Office, July 2011. 7

[78] UNITED STATES DEPARTMENT OF DEFENSE. The Department of Defense Cyber Strategy. U.S. Government Printing Office, Apr. 2015. 7

[79] UNITED STATES EXECUTIVE OFFICE OF THE PRESIDENT. Cyberspace Policy Review. U.S. Government Printing Office, May 2009. 6

[80] UNITED STATES JOINT CHIEFS OF STAFF. JP 3-12: Cyberspace Operations. United States Department of Defense, Feb. 2013. 8

[81] US CISA. Best Practices for MITRE ATT&CK Mapping. Tech. Rep. 20210602, US CISA Cyber Security & Infrastructure Agency, Washington D.C., USA, June 2021. 8

[82] US CISA. Malware Analysis Report AR21-105A. Tech. Rep. MAR-10327841, US CISA Cyber Security & Infrastructure Agency, Washington D.C., USA, Apr. 2021. 9

[83] US DHS NCCIC. Grizzly Steppe — Russian Malicious Cyber Activity. Joint Analysis Report JAR-16-20296, U.S. Department of Homeland Security NCCIC and Federal Bureau of Investigation, Washington D.C., USA, Dec. 2016. 8

[84] U.S. FEDERAL REGISTER. Improving the Nation's Cybersecurity. United States Federal Register, May 2021. 6

[85] VAN STEEN, M. Graph Theory and Complex Networks: An Introduction. Maarten van Steen, Apr. 2010. 10

[86] WAMALA, F. *ITU National Cyber Security Strategy Guide*. International Telecommunications Union, Geneva, Switzerland, Sept. 2011. 7

[87] WEEDY, B. M., CORY, B. J., JENKINS, N., EKANYAKE, J. B., AND STRBAC, G. *Electric Power Systems*, 5th ed. John Wiley & Sons, Chichester, UK, 2012. 14

[88] WILLINGER, W., AND ROUGHAN, M. *Recent Advances in Networking*. ACM Press, 2013, ch. Internet Topology Research Redux, pp. 1–59. 11