The Impact of Changing Technology on International Cybersecurity Curricula

Huw Read[1,2(✉)], Iain Sutherland[1,4], Konstantinos Xynos[5],
Tom Drange[1,3], and Ernst Sundt[1]

[1] Noroff University College, Kristiansand, Norway
{iain.sutherland, tom.drange, ernst.sundt}@noroff.no
[2] Norwich University, Northfield, VT, USA
hread@norwich.edu
[3] University of Sunderland, Sunderland, UK
[4] Edith Cowen University, Perth, Australia
[5] Darkmatter LLC, Dubai, United Arab Emirates
konstantinos.xynos@darkmatter.ae

Abstract. Cyber Security degree programs vary in scope; from those that are constructed around traditional computer science degrees with some additional security content, to those that are strongly focused on the need to develop a dedicated cyber security professional. The latter programs typically include a grounding in computer science concepts such as programming, operating systems and networks to specialised security content covering such disparate areas as digital forensics, information assurance, penetration testing and cryptography. The cyber security discipline as a whole faces new challenges as technology continues to evolve, and therefore significant changes are being faced by educators trying to incorporate the latest technological concepts into courses. This presents cybersecurity educators with a number of related challenges to ensure that changes to degree programs reflect not only the educational needs of students, but of the needs of industry and government. The evolving use of technology therefore presents both opportunities and problems, in how these changes are demonstrated in the curriculum. This paper highlights the accreditation, standards and guidelines (from three of the countries where the authors of this paper have sought accreditation) that shape the way educators are encouraged to develop and structure degree courses and considers these in lieu of factors relating to incorporating new technology in cybersecurity curriculum, particularly in the presentation of technical exercises to students.

Keywords: Standards · Education · Curriculum

1 Introduction

Bachelor programs in the area of computer security and in particular computer forensics started to gain traction around 2006 with some of the earliest UK courses being taught in Royal Holloway and the University of Glamorgan (now University of South Wales). Currently universities across the UK and further afield now offer degrees

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 518–528, 2017.
DOI: 10.1007/978-3-319-58460-7_36

in computer security and related crime investigation programmes (Keystone Academic Solutions 2017). There is a need for differentiation and specialisation although the drive for certification and accreditation limits the potential curriculum. In addition to increasing competition in this area, universities have had to deal with a continued rapid expansion in technology. Furthermore if courses are to remain current, there is a need to investigate and incorporate the impact of the changing environment and changing technologies into the degree itself.

2 Changing Environment

Technology continues to develop with the inclusion of processing power and data storage into a continuing wide variety of end-user devices. These devices are oft described as being part of systems such as ‘smart cities’, ‘smart’ houses, ‘smart clothing’ and other ‘smart’ devices. At the present it could be argued that these so-called smart devices are providing little more than additional automation and not intelligent processing and decision-making functions, although these features are gradually being added to different systems. One example of this type of technology is the Verisure alarm company (Verisure 2016) in Norway provides alarm systems with additional functionality including flood senses and the ability to monitor temperature and humidity in addition to intrusion warnings. Technology is now being incorporated into a variety of devices; examples include wearable devices and clothing (Hexoskin 2016), drinking containers (Disney Food Blog 2016, Glassify 2016) and smart housing (Amazon 2017). This now provides a challenging and information rich environment for capture, analysis and presentation in the classroom or via online laboratories. Universities therefore have to respond to these changes to train graduates that are ready for these future workplace challenges. A question is how to respond to the challenges in the way in which courses and degrees are designed and structured; which topics to focus and prioritise and how to best integrate these into taught content, in particular how to provide exposure to new systems and technologies. Consultation of nationally recognised accreditation schemes, in particular those recognising Universities as centres of national excellence in the Cyber discipline should be used to identify challenges in adopting subject matter into courses.

3 Accreditation, Standards and Guidelines

There are a number of accreditation schemes and guidelines that attempt to address the specific needs of the discipline that can be used as an indication of the types of topics that should be addressed at a technical level in university courses. These vary considerably both in terms of the prescribed content required to achieve the accreditation or standard and in terms of the level of detail required. The authors have explored accreditation options in three countries; Norway, USA and the UK.

One of the most comprehensive and detailed systems is that used in the USA. The National Security Agency (NSA 2016) has been recognising higher-education institutions in cyber since 1998 with the Centre of Academic Excellence (CAE) in Information Assurance Education (IAE). Originally open only to 4-year universities, the NSA (later joined by the Department of Homeland Security in 2004), in 2008 began recognising postgraduate universities by awarding the Information Assurance Research (IAR) certification. Furthermore in 2010, 2-year institutions could also apply for the IAE designation.

Today, the process has been updated considerably with the gradual phasing out of the IAE designation, being replaced with Cyber Defence Education (CDE) to reflect the more active component in defending against threat actors in addition to focusing on the assuring of information security (IAE). There are 214 accredited institutions (NIETP 2017a) out of 4,700 (NSF 2016) across the United States, or 4.5% penetration at the time of writing. With a shortfall of 209,000 employees in the US (Morgan 2016) and with higher-education producing about 10,000 skilled graduates per year any designation programme needs to ensure the right practical skills are being given to undergraduates so they can make an effective transition into the workforce. To assist with this, the CAE application process has 17 specialist designations (NIETP 2017b), or focus areas, including cyber investigations, health care security, digital forensics, secure software development and systems security administration to name a few. Of the 214 accredited, it has been said about 20% of institutions have been designated as a CAE with a defined focus area, the rest achieving the general CAE-CDE.

The application process is comprehensive, the actual programme path/degree path being assessed had to meet certain Knowledge Units (KUs) which themselves contain a number of topics that academic institutions must provide evidence for. Evidence can be a reference to chapters of a book, an academic product such as a lecture or tutorial or an assessment exercise. A large part of the evidence must demonstrate technical, practical, hands-on experience in different cyber areas. Considering the high-cost of entry into the cyber-education market for a University, it is no small feat. For example, specialist software, hardware, complex real/virtual network configuration for red/blue team vulnerability assessment scenarios, disparate wide-ranging vulnerable devices found in the market (e.g. Internet of Things (IoT)) and understanding how students should interact with specialist cybersecurity subjects (i.e. KUs) is the best way to ensure effective use of University resources.

For the generic NSA cybersecurity designation, CAE-CDE, 4 year institutions must collect evidence for a minimum of 22 of these KUs. Many cover core cyber principles in the degree curriculum but others relate to special focus areas. For a specialist focus area, the number of KUs can change, for example the digital forensics designation requires 20 KUs but many of these courses are specialisms in the discipline. For example, those seeking a designation of CAE-CDE with a focus area of digital forensics, the following KUs are required in the degree.

Basic Scripting or Introductory Programming, IA Fundamentals, Intro to Cryptography, IT Systems Components, Networking Concepts, Policy Legal Ethics and Compliance, System Administration, Networking Technology and Protocols, Operating Systems Concepts, Data Structures, Device Forensics, Digital Investigations, Forensic Accounting, Hardware Reverse Engineering, Host Forensics, Media Forensics, Network

Forensics, Operating Systems Theory, Software Reverse Engineering and Vulnerability Analysis.

The combination of Topics comprising the different KUs provides robust definition of a Cyber curriculum in the USA. However, the impact of new technology can make such curricula age rapidly. A recent development in the process has been the addition of a Wiki whereby academics can propose changes to the KUs that, if accepted, will be required when an institution seeks designation (Cyberedwiki 2017). It is not yet known the timeframe in which changes in the Wiki will be reflected in the CAE requirements, however if successful, this may be an opportunity to ensure programs are dynamically updated during each NSA redesignation cycle (5 years) to more effectively keep up with the changing threat landscape.

In terms of practical advice on actual procedures, standards like those proposed by NIST (NIST 2016) are a useful indicator of skills and knowledge required by those working in this area. The NICE Cybersecurity Workforce Framework (NCWF) is, at the time of writing, in draft stage and is currently open for comment and contributors are encouraged to "…ensure it applies to all cybersecurity workforce needs" (NIST 2016). In particular, it seeks to identify and more clearly articulate the Knowledge, Skills and Abilities (KSAs) required by industry. Of particular importance to educators is how it is anticipated to become a "cybersecurity workforce dictionary that will allow employers, educators, trainers, and those in the workforce to use consistent terms to describe cybersecurity work" (NIST 2016). The implications will be felt by those teaching cyber security who will need to ensure that common terminology is used for consistency; this is not a bad thing considering what was known as computer forensics several years ago became digital forensics to highlight that evidence is not limited to what is found on the PC. Now the term also includes the non-device specific elements of acquisition (e.g. Cloud storage or automated sensor networks, etc.).

Where the NCWF is emphasising the workforce, the CSEC2017 (CyberSecurity Curricula 2017) Curriculum task force (comprising of ACM, IEEE-CS, AIS SIGSEC and IFIP WG 11.8) represents an expansion of the ACM's education initiative to provide the "…first set of global curricula recommendations in cybersecurity education". The knowledge area comprises of six categories; data security, software security, system security, human security, organisational security, and societal security. The first three are technical in nature, whilst the latter are in areas significant to cybersecurity but not commonly taught in such programmes. CSEC2017 is working towards implementing a roadmap to achieve parity with the NCWF. The intention appears to provide course roadmaps that demonstrate a pathway for knowledge acquisition between the two.

Such guidelines may be one way for those countries that have not yet developed standards to use as a starting point. For example, Norway has no explicit governmental requirements for cyber security education, however there are several organisations that have provided advice or influence to academia. The Norwegian Educational Quality Assurance Agency (NOKUT) prescribes some aspects of IT curricula. However for other subjects such as engineering, a more detailed approach is taken. There are several organisations that have developed broader advice or policy relating to cyber security.

The Norwegian Business and Industry Security Council (NSR) serves the Norwegian business sector in an advisory capacity on matters relating to crime, and works actively to prevent losses. One aspect they address is that professional competence should contain three factors; Academic foundation, Practical skillset and Authorisation or Certification. These parts can act as guidelines for security programs (Stranden 2010).

In addition the governmental Norwegian Center for Information Security (Norsis) state in their publication (Malmedal and Røislien 2016), the need for a holistic approach. The public and private sector need a common methodology to establish a culture of incorporating all the aspects of cybersecurity (Norsis 2016).

The UK has an approvals system that the EPSRC and Government Communication HeadQuarters (GCHQ 2011) issues for research, recognising Academic Centres of Excellence in Cyber Security Research (ACE-CSR). There was discussion of recognising contributions by education-focused institutions with the Academic Centre of Excellence in Cyber Security Education designation (ACE-CSE (GCHQ 2014)), but there is little mention of ACE-CSE on the GCHQ website at the present time.

However, as mentioned in (GCHQ 2014), ACE-CSE will require certified postgraduate Master's degrees. To this end, courses already certified include Cyber Security, Cyber Defence, Digital Forensics and Information Security (GCHQ 2016). An initial call for certifying undergraduate Bachelor's was issued in November 2016 (GCHQ 2016b), the closing date of which has only recently passed at the time of writing. Whereas the NSA identifies 17 different cybersecurity focus areas, GCHQ recognises 4 distinct areas (GCHQ 2016c). Each area comprises of security disciplines/principles/computer science subject areas, which contain skills groups. These skills groups contain a number of indicative topics. These topics provide the institution with the level of detail as to what should be covered in a cybersecurity degree to attain certification.

Additionally in the UK, the Chartered Society of Forensic Sciences (CSFS) has a scheme for approving the content of a wide range of courses within the forensic science domain. It is interesting to note that out of 31 universities that have gained approval for programs, so far only two have been in the cyber-realm (digital forensics) the vast majority has been focused in the area of traditional forensic methods (Chartered Society of Forensic Sciences 2016).

One issue with standards and both commercial/government accreditation is that they tend to trail new development due to the length of time required to create and agree on a standard. The NSA-CAE, as of Nov 2016, has a wiki where changes can be updated by the academic community, However participation is voluntary, and it remains to be seen how this might be adopted by those who drive the research in the area, the academic community. Furthermore, how Universities choose to adopt new recommendations, in lieu of cost, remains to be seen.

Table 1 below summarises the different accreditation and standardisation programs outline above, highlighting in which country the program is located, for whom the program will ultimately assist, and a brief summary.

Table 1. Summary of accreditation, standards and guidelines influencing cybersecurity education by region

Standard	Country	Subject focus area	Summary
National Security Agency, Centre of Defence Excellence	U.S.A.	Government	Gov't centric knowledge units identify topics to be covered, skills required by NSA
NICE Cybersecurity Workforce Framework	U.S.A.	Workforce	Skills identifiable and referenceable by employers
ACM, Cybersecurity Curricula 2017	Global	Academia	Topics should be included in cyber degrees
Nasjonalt organ for kvalitet i utdanningen (NOKUT) The Norwegian Agency for Quality Assurance in Education	Norway	Academia	Academic Quality assurance
Norsk senter for Informasjonssikring (Norsis) The Norwegian Center for Information Security	Norway	Industry	Serves as an advisory body on matters relating to a security, focussing on preventable loss
Næringslivets Sikkerhetsråd (NSR) Norwegian Business and Industry Security Council	Norway	Industry	Industry related security body
Government Communication HeadQuarters (GCHQ)	UK	Government	Gov't centric topic areas
The Chartered Society of Forensic Sciences (CSFS)	UK	Industry	Four key objectives including providing opportunities for education, training and development

4 Current Educational Methods

The idea of universities and other institutions of higher learning teaching cyber-related curricula is not new; the first undergraduate degree to feature the term "hacking" appeared in 2006 (University of Abertay 2017), whilst many programmes and courses in information security were available as far back as the 1990s (Kessler and Ramsay 2013). The typical forms of teaching cyber within higher-education has aggressively moved away from the more traditional forms of teaching (lectures, reading literature, understanding concepts in principle, often referred to colloquially as "the sage on the stage") as they have been identified to not be adequate enough for cyber security training as the student cannot apply the academic principles they have learnt to a realistic environment (Willems and Meinel 2012). Available literature in the public domain shows that the "Capture The Flag" (CTF) genre, whereby a specific aim or goal is set typically for an offensive exercise such as obtaining a particular file from a system, has remained very popular as an educational tool to help students understand how to configure, respond, defend, attack and exploit networked systems. Indeed, many organisations have taken to using this model as a recruiting tool in recent years

(NSA 2016b, GCHQ 2011b, Telegraph 2011). Others encourage a team-based model; Conklin (2007) describes an information security practicum course whereby students, working as part of a team, make amendments in a simulated small business environment. Changes are issued via memos deliberately sent outside of assigned student class contact hours, such as introducing malware or the "accidental" deletion of a file. The real world simulation is kept by maintaining system states between classes providing the sense of continuity and by incorporating the input of industry professionals whom can prevent the instructor from doing the "same old thing" (Conklin 2007). By focusing on business aspects (business processes, business continuity, etc.) students are prevented from treating the simulations like their "personal playgrounds" (Conklin 2007), i.e. taking risks and performing actions that would not be considered during a real exercise. Rege (2015) recognises other issues with the prevailing CTF model, namely novice encouragement, temporal constraints, and skewed experiences (barriers to entry based on prior knowledge). Furthermore the focus of the paper is on applying cyber curricula, taught traditionally to those with a strong background in computing to those in criminal justice majors.

Similar practical educational exercises have been developed for other, more focused areas within the cyber-realm. Sitnikova et al. (2013) discuss their experiences taking the experiential model in cybersecurity learning and applying it to the realm of Supervisory Control and Data Acquisition (SCADA) systems. Practical exercises were designed, which help to maximise a student's education of cyber within this area whilst minimising the amount of time needed overseas at specialist training facilities.

Those courses typically focusing on a more investigative angle such as forensics tend to focus analytical and investigative challenges. These are commonly in the form of smaller practical exercises.

Dopplick (2015) summarises up these worldwide trends in experiential cybersecurity learning; technical project-based activities, competitions, training and research are becoming commonplace as are universities "…teaming with companies to provide structured programs on an ongoing basis".

5 Educational Challenges to Changes in Technology

Universities needed to respond to the changing environment as education/training and certification has been highlighted as a key issue in the discipline for a number of years (Rodgers et al. in 2004).

A number of the standards outlined above indicate the need for students to develop specific skills that can only be achieved in depth with hands on experience of hardware, which will continue to be a challenge in cybersecurity. As discussed in the Current Educational Methods section, it is clear that there are established hands-on practical exercises in areas such as CTF (Capture The Flag) competitions, which have been particularly successful at interfacing between subject matter and the student's ability to learn. However, within the specialisms of cybersecurity, such as digital forensics, there are a vast array of skills that a future investigator may be expected to have upon leaving university. Knowledge of the acquisition process and how it applies to disparate evidence sources e.g. encrypted computers, mobile phones, tablets, embedded systems such as games consoles, IoT, SCADA systems, network traffic, malware acquisition, live vs. dead acquisition, data recovery from deliberately damaged devices, etc. Knowledge of the analysis process, different operating system artefacts, file systems, root cause analysis, structured vs. unstructured data, and so on. Knowledge of the presentation process, developing concise expert witness reports, the courtroom process, public speaking, giving expert testimony under oath or affirmation, etc. The fact that many cases involving digital evidence contain all of these areas does not make for an easy task in creating effective teaching interfaces to transmit such knowledge to students.

The analysis process lends itself rather well to the virtualised lab environment. Using the "here's-one-I-made-earlier" approach, devices and hardware can be acquired forensically prior to the lab exercise and easily copied into pre-configured virtual machines with appropriate forensic software (commercial offerings such as Access-Data's FTK, Guidance Software's EnCase or open source alternatives such as Autopsy/The Sleuth Kit or the Digital Forensics Framework). Such exercises can be conducted remotely as part of online course offerings rather well. However, a large part of digital forensics is in understanding the importance of evidence seizure and data acquisition and the practical challenges that go with these areas. This requires students to adequately explore and experience some of the problems and challenges with actual equipment and devices.

Universities then have to respond to both the need to incorporate new technologies and to do so in a way that gives students an appropriate interface to obtain the practical skill set required to meet learning objectives and outcomes.

In terms of meeting the demands of the subject specialisation, one route is to develop a broader range of specialised electives to enable students to focus in particular technologies. However while it is desirable to have, for example, digital forensics investigators or penetration testers with a common understanding and knowledge of core concepts, there is the question as to how much additional specialist content is required. The cost of implementing advanced forensic data recovery or advanced kernel exploitation for classes require specialist staff training, specialist equipment, at a considerable additional cost.

An alternative to developing several specialised courses covering the breadth of cybersecurity is the development of degree programmes that concentrate on specific focus areas. This approach is inline with the current NSA method of evaluating higher education institutions. As mentioned previously, universities may seek certification as an academic centre of excellence in 17 different areas of specialization. The advantage of this approach is that there is a core set of transferrable cyber security skills that are common across all the specialisations, whilst allowing individual universities to play to the strengths of their academics. Further advantages of the specialist centre model are that, as new and novel ways of implementing practical learning into tutorials, labs and other exercises are developed by a specialist institution, the university can share the material with others whilst continuing research, development and investment in the focus area. As centres of excellence are expected to engage in outreach activities (considering both the NSA and GCHQ certifications), there is also the impetus to disseminate the specialist knowledge beyond enrolled college students, to make the subject matter accessible for those of school-going age, for other university cyber-programmes and to the general populace as a whole (e.g. Continuing Professional Development).

This will enable many other universities to rapidly adapt to a changing environment (as it is far easier to develop courses for existing programs and incorporate ideas and suggestions from these specialist centres) and better keep par with changes in technology. Therefore this will enable universities to put individuals into the workplace that have a broader understanding of cyber with a common understanding of key concepts that are developed early on in the degree program before students seek specialisation, perhaps at a defined centre of excellence in a particular discipline.

6 Summary and Conclusions

It is clear that the expansion in the adoption of technology is presenting a number of challenges in terms of the breath of new technologies that need to be incorporated into cybersecurity courses. Universities have a number of options to look towards for guidance as to what to include in cyber security programmes, whether generic or in a specific focus area. Such guidance covers content for academic programmes directly, what universities should be addressing in terms of the workforce or the needs of Government organisations or industry.

Two ways of responding to the challenges are discussed - new specialisation courses for existing degree programs - and the need for new degree programs. Clearly both approaches are equally valid and will depend on existing specific university provisions and resources. Perhaps both approaches are required as the specialism develops. A number of educational challenges to incorporating new technology were also presented; the cost barrier to entry for incorporating specialist courses may be too high for smaller institutions and that existing models for incorporating technical teaching material (e.g. virtualised capture-the-flag exercises) may not translate well to new technologies.

There is much to be done in this field. With several types of accreditation/guidance available for academic institutions focusing on different categories of industry, further work needs to be conducted into how specific subject/topic areas can be delivered to students in a way that facilitates hands-on experiential learning with the appropriate technological tools.

Acknowledgements. This project was supported by work funded by the Senter for internasjonalisering av utdanning (SIU), project no. PNA-2015-10010, Forensics and Security Teaching Educational Resources (FASTER).

References

ACM: Cybersecurity Curricula 2017, Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity (2017). http://www.csec2017.org/csec2017-v-0-5

Amazon: Smart Home (2017). https://www.amazon.com/smart-home/b?node=6563140011. Accessed 18 Apr 2017

Chartered Society of Forensic Sciences: Component Standards (2016). http://www.csofs.org/Digital-Forensics. Accessed 10 Nov 2016

Conklin, A.: The design of an information security practicum course. In: Proceedings of the AIS SIG-ED IAIM 2007 Conference (2007)

Cyberedwiki: 2017. http://cyberedwiki.org/mediawiki/index.php?title=Welcome_to_CyberEd_Wiki. Accessed 31 Jan 2017

Disney Food Blog: Disney Refillable Mugs (2016). http://www.disneyfoodblog.com/disney-refillable-mugs/. Accessed 12 Nov 2016

Dopplick, R.: Experiential cybersecurity learning. ACM Inroads **6**(2), 84 (2015). http://dx.doi.org/10.1145/2743024

GCHQ: Scheme to Recognise Academic Centres of Excellence in Cyber Security Research (2011). https://www.epsrc.ac.uk/files/funding/calls/2011/scheme-to-recognise-academic-centres-of-excellence-in-cyber-security-research/. Accessed 15 Nov 2016

GCHQ: Can you crack it (2011b). http://www.canyoucrackit.co.uk/. Accessed 15 Nov 2016

GCHQ: Working with academic to increase the UK's capability in cyber security (2014). http://www.nationalarchives.gov.uk/documents/information-management/cesg-aces-partnerships.pdf. Accessed 31 Jan 2017

GCHQ: GCHQ certifies six more Masters' degrees in Cyber Security (2016). https://www.gchq.gov.uk/news-article/gchq-certifies-six-more-masters-degrees-cyber-security. Accessed 15 Nov 2016

GCHQ: New call to certify Cyber Security Degrees (2016b). https://www.gchq.gov.uk/news-article/new-call-certify-cyber-security-degrees. Accessed 31 Jan 2017

GCHQ: Certification of Bachelor's and Master's Degrees in Cyber Security… is your degree in scope? (2016c). https://www.ncsc.gov.uk/content/files/protected_files/article_files/degrees-at-a-glance.pdf

Glassify: The Smart Glass (2016). http://www.glassify.me/. Accessed 12 Nov 2016

Hexoskin Wearable Body Metrics (2016). http://www.hexoskin.com/collections/all. Accessed 13 Nov 2016

Kessler, G.C., Ramsay, J.: Paradigms for cybersecurity education in a homeland security program. J. Homel. Secur. Educ. **2**, 35–44 (2013). http://www.journalhse.org/v2-kesslerramsay.html

Keystone Academic Solutions (2017). https://www.bachelorstudies.com/BSc/IT/Cyber-Security/. Accessed 18 Apr 2017

Malmedal, B., Røislien, H.E.: The Norwegian Cyber Security Culture, Norsk senter for informasjonssikring (Norsis) (2016). https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

Morgan, S.: One Million Cybersecurity Job Openings in 2016, Forbes (2016). http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#209e17d77d27. Accessed 11 Nov 2016

National Science Foundation: https://www.nsf.gov/statistics/seind14/index.cfm/chapter-2/c2s1.htm. Accessed 11 Nov 2016

NCSC: GCHQ Degree Certification - Call for New Applications (2016). https://www.ncsc.gov.uk/articles/gchq-degree-certification-call-new-applicants. Accessed 31 Jan 2017

NIETP: Current CAE Designated Institutions (2017a). https://www.iad.gov/nietp/reports/current_cae_designated_institutions. Accessed 11 Nov 2016

NIETP: NSA/DHS National Centers of Academic Excellence for Cyber Defense (2017b). https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_Focus_Areas.pdf. Accessed 11 Nov 2016

NIST: DRAFT NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education, SP 800-181 (2016). http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-181

NSA: National Centers of Academic Excellence in Cyber Defense (2016). https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/. Accessed 10 Nov 2016

NSA: 2016 NSA Codebreaker Challenge (2016b). https://codebreaker.ltsnet.net/home. Accessed 10 Nov 2016

Rege, A.: Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation. In: Proceedings of the 2015 USENIX Summit on Gaming, Games and Gamification in Security Education, Washington DC, 11 August 2015 (2015)

Rodgers, M., Siegfried, K.: The future of computer forensics: a needs analysis survey. Comput. Secur. **23**(1), 12–16 (2004). http://www.sciencedirect.com/science/article/pii/S0167404804000100

Sitnikova, E., Foo, E., Vaughn, R.B.: The power of hands-on exercises in SCADA cyber security education. In: Dodge, R.C., Futcher, L. (eds.) WISE 2009. IAICT, vol. 406, pp. 83–94. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39377-8_9

Stranden, R.: Sikkerhet – en profesjon? Næringslivets Sikkerhetsråd (NSR) (Norwegian Business and Industry Security Council (2010). https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

The Telegraph: GCHQ spy recruitment code solved (2011). http://www.telegraph.co.uk/news/uknews/defence/8928088/GCHQ-spy-recruitment-code-solved.html. Accessed 11 Nov 2016

University of Abertay: Ethical Hacking Degree (2017). http://www.abertay.ac.uk/studying/undergraduate/bsc-ethical-hacking/

Verisure: 2016. https://www.verisure.no/. Accessed 11 Nov 2016

Willems, C., Meinel, C.: Online assessment for hands-on cybersecurity training in a virtual lab. In: Proceedings of the 3rd IEEE Global Engineering Education Conference (EDUCON 2012). IEEE Press, Marrakesh, Morocco (2012)