AGILE EDUCATION IMAGINED

A report from the Cybercampus workshop on Agile Education

Skills and knowledge

Gunnar Karlsson and Paola Lundén

Illustrations by Open AI Dall•E 2

CONTENTS

Reference to this report:

Gunnar Karlsson, Paola Lundén, *Agile Education Imagined: A report from the Cybercampus workshop on Agile Education*, KTH TRITA-EECS-RP 2023:1, January 2023.

INTRODUCTION

Cybercampus Sweden is a national initiative to provide education, research, innovation and advice in cybersecurity and cyber-defense. This brochure addresses needs for cybersecurity training and education: There is a manifest imbalance between the cybersecurity workforce required in Sweden and the number of skilled graduates being produced by Swedish universities. There is also a gap between the needed cybersecurity skillset and the contents of existing education programs. For these reasons, Cybercampus Sweden aims at building capacity for work force training and to facilitate new cross-university cybersecurity programs, taking advantage of the specific teaching and research expertise from different universities. These comprise bachelor-level programs that provide a strong base with deep technical knowledge, and master-level and continuous education programs that train the cybersecurity workforce needed in Swedish organizations through applied and advanced courses with direct contact to ongoing research.

The contents of this brochure are fictitious courses created from the outcomes of a planning workshop on agile education, conducted by the planning project for *Cybercampus Sweden*[1]. The workshop, held on October 17, 2022, provided two sets of results. First, we obtained a list of concerns for the establishment of agile education, ordered in importance and urgency. And, second, we received desired topics for education with side information on target groups and formats, also ordered according to urgency. These topics have been expanded into imagined educational offerings, such as courses and programs, in this report. The concerns are addressed in the listed activities and in appendix 1: Concerning the concerns.

NO MAGIC – CONTINUOUS EDUCATION THAT WORKS

Educating professionals can be hard. They try to learn while meeting deadlines at work and commitments to family, friends and associations, and they need time for their own interests; they struggle with prior knowledge that might seem unrecoverable from memory and with study practices that lie years back. Yet, it is possible to create valuable training that provides new skills and knowledge. The training must simply be designed for working people to fit the conditions they might have while studying.

REVEALING THE TRICKS

The expectation at universities for continuous education is that at most half of the enrolled course participants complete their courses. The reasons are mentioned above and are further described in a report[2]. The conclusion in brief is that the target group of working professionals is different from regular students

[1] www.cybercampus.se
[2] Sverker Janson and Gunnar Karlsson, *PROMPT Learnings*, RISE Report 2021:52.

who are studying full-time on a campus and whose financial support is conditioned on their progress.

Agile education is the term we use for training that is fit for the people who need it: It is purposeful; it relies on participants working together and supporting one another, and it is clear on expectations and schedules. The latter is needed for interested persons to decide whether they are capable of taking a course and to know how they can arrange their lives to manage it.

ABOUT THE IMAGINED: A READER'S GUIDE

The listing of educational courses, programs, and activities more generally, follows this format.

Title: Descriptive name
Purpose: Why participating in this activity
Audience: Whom it is for, from expert to beginner
Contents: Summary and topic listings
Format: Online or campus; duration, intensity, and recognition
Provider: Organizations responsible or contributing to the activity

The lists are categorized into: activities for those without any prior knowledge of cybersecurity and for whom general awareness might be the goal – these activities are under the heading *Upwards from the START;* activities for those who plan to work in the area, under *Unstuck in the middle,* and activities for professionals in the area, both academics and active practitioners – we call this category *When the top is not the summit.*

CYBERCAMPUS AND PROVIDERS OF EDUCATION

Cybercampus is a national endeavor in cybersecurity that brings together interested institutions of higher education and higher vocational education, educational companies and non-profit organizations. The courses and other educational activities listed in this brochure are to be developed by experts from these parties and represent curated contents based on state-of-the-art scientific research and industrial and organizational best practices. The contents are then organized and formatted for efficient learning by modern didactic and pedagogic theories and methods. The modes of instruction vary from online to campus, from interactive to asynchronous, and from massive to small scale classes.

The courses and activities may be *freely provided* by any organization affiliated with Cybercampus. In this manner, Cybercampus ensures the development of high-quality, updated and in-demand contents and teaching methods, and the participating organizations provide scalable capacity for offering the menu of educational activities presented herein.

IMAGINED EDUCATION AT A GLANCE

Title	Type	Status	Format	Level
CYBER-SECURITY FOR ALL	SURVEY	UNDER DEVELOP-MENT	< 40 HOURS PARTTIME, ONLINE	INTRO-DUCTORY
MASTER IN CYBER-SECURITY	ACADEMIC, INDEPTH	IDEATION	FULL- OR HALFTIME, ON SITE, 60 CR	BACHELOR DEGREE REQUIRED
MANAGING CYBER-SECURITY	EXECUTIVE	IDEATION	PARTTIME, ON SITE	PRO-FESSIONAL EXPERIENCE
POWER TRAINING IN CYBER-SECURITY	PRO-FESSIONAL	IDEATION	CONTINUOUS EDUCATION, ONLINE, ON SITE	EXPERT EXPERIENCE, HIGHER EDUCATION
SMALL AND MEANING-FUL	GENERAL PUBLIC, ACDEMIC, AND PRO-FESSIONAL	IDEATION	CONTINUOUS EDUCATION, MICRO-LEARNING, ONLINE	BEGINNER, INTER-MEDIATE AND EXPERT EDITIONS
SUMMER IN CYBER	SUMMER CAMPS	IDEATION	TWO WEEKS ON SITE	INTRO-DUCTORY, INFORMAL, RECRE-ATIONAL
TRAINING CAMPS	ACADEMIC, PRO-FESSIONAL	IDEATION	TWO WEEKS ON SITE	EXPERT, RESEARCH

UPWARDS FROM THE START

Courses and other educational activities in this section are aimed at people who do not have any prior knowledge of cybersecurity. Common to all activities is that they are motivating for learning more and perhaps also for taking a full program to work in the area. Special attention will be given for reaching women and people from minorities.

Title: Cybersecurity for all

Purpose: Establish awareness for the importance of cybersecurity and to provide knowledge and skills to better handle dangers, systems and services. The course will motivate participants to continue learning.

Audience: This course is for everyone who has not worked or studied cybersecurity (or any guise thereof).

Contents: The participants will learn to reason about security, manage their own devices and settings for services and to install updates and useful tools for improved safety online (eg password handlers). Cybersecurity is seen from an individual's perspective:

- Understanding the threats and the actors
- Social engineering and the personal exposure
- Personal services and social networks
- Personal devices and self-managed systems
- Cloud and managed services

Format: The course is provided *online* with the option to use the material in study circles and organized courses. Expected time for completion is 40 hours. After completing the course, the participants will be provided regular repetition exercises and updates through the course *Small and meaningful – the up and coming edition*. Official badges will be provided for those passing the examination; no formal university credits are given. Regular repetition will be required to keep the badge active.

Providers: Vocational training institutions, commercial and non-profit providers, such as (Swedish) *studieförbund*.

Title: Prévenir le déluge – managing cybersecurity

Purpose: An intensive course for high-level managers and decision makers to understand the threats that cyberattacks may cause for their organization. The course will provide skills for security assessment of the organization and for commissioning and managing projects to address lacking security culture, insufficiently secured systems and services, and to restore operations and confidence should an attack be successful.

Audience: The course is only open for professionals in leading positions. It assumes introductory knowledge of cybersecurity, equivalent to the course *Cybersecurity for all*. Technical skills will be taught as needed and may prolong the course. The course is taken under the Chatham House Rule[3] for all participants; non-disclosure agreements may be required.

Contents: The course provides two strands of contents: one for managers and others with operational responsibilities, and one for investors, board members, politicians and others responsible for strategic decisions. Some parts of the course are common to both strands to ensure that all participants also understand the other strand's aspects and meet the persons attending.

- *Operations*
  The participants are expected to report on the security culture of their organization, to make a self-assessment of their own preparation with a plan for continuous education beyond this course, and an action plan for the organization in terms of threat analysis and improvements.
- *Strategy*
  Impact of cybersecurity risks and how to assess the financial vulnerabilities of the organizations they own, run, or govern. The participants are expected to report on the security exposure of their organization, with a strategic plan for the organization in terms of incentivizing the organization for continual improvements and readiness for handling contingencies.

Summary and topic listings for meetings to be decided together with the participants ahead of the course. The contents change from year to year and the course may be taken repeatedly for credits and diploma.

Format: The course extends over forty weeks and follows a well-established format for executive training with four weekends of intensive training (60 hours); weekly seminars and discussions (80 hours), and independent preparation for the weekly activities (80 hours). Time for applying the learning in the own organization is not included. Contract education (for employers).

Providers: Universities, research institutes, security companies and commercial and non-profit educational providers.

---

[3] "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

Title: A summer in Cyber

Purpose: Summer camp for families, youth and adults to get hands-on experience with cybersecurity. To build interest for further training, to have fun around technology and to interest more women and minorities in cybersecurity.

Audience: No prior training expected; programming and basic IT knowledge will be included as needed.

Contents: Same overall contents as *Cybersecurity for all*; challenges provided by Hack the Box and other public services.

Format: Two week camps at several sites nationally with good possibilities for sports and recreation.

Providers: Cybercampus is responsible for the contents; the camps are offered by camping grounds, scouting and sports associations, youth hostels and folk high schools that can provide accommodation, meals and recreation and that can provide staff for running the camps.

Title: Small and meaningful – the up-and-coming edition

Purpose: Staying up to date requires access to both the latest discoveries and developments as well as the insights of leading experts. This education is an indefinite series of micro-education installments for people who want to understand cybersecurity and follow the developments.

Audience: For anyone with prior knowledge from or equivalent to the introductory course *Cybersecurity for all*, as well as students and professionals whose work is related to cybersecurity and who want to learn more.

Contents: Provides easy access to the latest research and internationally leading researchers as invited lecturers. The contents will to a large extent rely on expertise at the national universities, research institutes and public agencies.

Format: A wealth of online formats from blog posts, videos to regular lectures and tests; some may be provided as live transmissions, and all contents will be available asynchronously. Discussion forums are provided for each new topic along with resources for further information. Expected time is two hours per provided installment. High participation in the series will be recognized by a Cybercampus open badge (new for each year).

Providers: Universities, research institutes, vocational training institutions, companies, public agencies, commercial and non-profit education providers.

UNSTUCK IN THE MIDDLE

Courses and other educational activities in this section are aimed at people who have a professional interest in cybersecurity but whom are not presently served by the education provided by vocational training institutions and universities. The main target group is professionals who want to work with cybersecurity for the domains in which they have advanced professional training and work experience, such as retail, health care, law, media and public services (taxation, welfare). The main vehicle forward for them is a full master's program to work in the area. Special attention will be given for attracting more women and people from minorities to contribute to the cybersecurity field.

Title: One year to a future – master program in cybersecurity for professionals

Purpose: The program provides a solid technology basis in cybersecurity with application to the business areas of the respective participants. After a completed program, the participants will be able to work on cybersecurity problems with respect to their professions.

Audience: Persons with professional experience and at least a bachelor's degree. Relevant areas are health care, retail, finance, legal services and transportation.

Contents: Summary and topic listings: see example syllabus from KTH in Appendix 2 (in Swedish).

Format: Onsite at the Cybercampus with scheduled work time and mandatory attendance. The program is given as full-time work four days a week over 44 weeks, with additional time necessary for individual studies. The program is highly intensive and participants are recommended to organize their lives for total focus for the duration of the program. A version at half pace will be developed later. The program is provided as contract education to the employers of the participants. Successful completion is awarded a formal and internationally recognized one-year master's degree in cybersecurity from one of the Cybercampus partner universities.

Providers: Universities.

Title: Small and meaningful – the middle edition

Purpose: Staying up to date requires access to both the latest discoveries and developments as well as the insights of leading experts. This education is an indefinite series of micro-education installments of special interest to people who work with applied cybersecurity.

Audience: For professionals in different fields who work with cybersecurity concerning security analysis, security cultures, implementation of new directive and deployment of new systems. Particularly aimed as continuous education for graduates from the master's program in cybersecurity for professionals.

Contents: Provides easy access to the latest research, business developments, legal frameworks and policies from internationally leading researchers and experts. The contents complement the up-and-coming edition of *Small and meaningful* series and both may beneficially be taken simultaneously.

Format: A wealth of online formats from blog posts, videos to regular lectures and tests; some may be provided as live transmissions, and all contents are available asynchronously. Discussion forums are provided for each new topic along with resources for further information. Topics will be labelled by the category for ease of selection (eg technical, business, legal). Expected time is two hours per provided installment. High participation in the series will be recognized by a Cybercampus open badge (new for each year).

Providers: Universities, research institutes, vocational training institutions, public agencies, commercial and non-profit education providers.

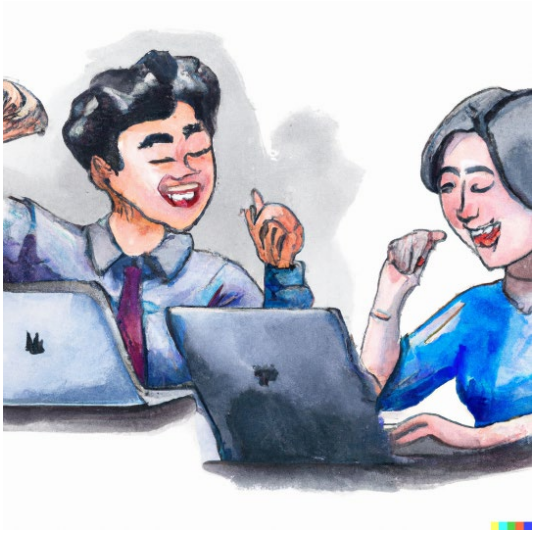
WHEN THE TOP IS NOT THE SUMMIT

Professionals working in cybersecurity often have their preferred sources for staying up to date. Consequently, the main educational offering that Cybercampus will provide experts is easy access to the research in the partner universities. For this, we will work on format and language to make research results accessible in summaries of plain language and in tutorial videos. In addition, all advanced courses (master and doctoral levels) from universities will be listed on the campus site. Here are select activities aimed at professional security experts and academic researchers.

Title: As hard as it gets – power training in cyber security

Purpose: Why participating in this activity? Because you have become smug and complacent and believe you know it all. Or, you simply want to improve.

Audience: For the elite professionals and those aiming for that rank. Some activities may require security clearance.



Contents: An unpredictable mixture of activities from in-depth lectures on new tools from leading providers and methods from top researchers over to competitions and challenges. Content examples include:

- Artificial intelligence to the rescue and attack
- Post-quantum cryptography and then what?
- Weird machines and instructions
- Dark nets and the Internet netherworld
- Threat intelligence and novel attack modes
- The hard problems of social engineering

Participants may be expected to contribute their own contents to the course.

Format: Running series of activities. Online, campus and at other locations (Campus partners'). Two weekends per year are run as bootcamps. Contract education with a pay-per-activity price model (for employers). Credits reported once a year in installments of 3 higher-educational credits.

Providers: Universities, research institutes, commercial and non-profit providers; security services and consultants (white, gray and black hats).

Title: Summers in deep water – training camps for doctoral students, faculty and professionals

Purpose: Staying up to date and improving requires periods of immersive training. The national summer camps of the Cybercampus provide intensive training and networking experiences beyond what any university or company can achieve on their own.

Audience: For elite professionals, doctoral students and faculty in cybersecurity and closely related fields. Some international participants may be accepted.

Contents: Provides access to the latest research and to internationally leading researchers as invited lecturers. A blend of lectures with practical exercises and group projects. New contents every year. Several training camps may be offered each summer (given willing organizers and participants).

Format: Two weeks on site at selected rural locations in Sweden for various recreational activities (mountain, costal and woodland). Contract education for employers; free for university participants for two training camps. Winter camps pending.

Providers: Universities, research institutes, security services.

Title: Small and meaningful – the expert edition

Purpose: Staying up to date requires access to both the latest discoveries and developments as well as the insights of leading experts. This education is an indefinite series of micro-education installments.

Audience: For elite professionals, doctoral students and faculty in cybersecurity and closely related fields.

Contents: Provides easy access to the latest research and internationally leading researchers as invited lecturers. The contents will to a large extent rely on doctoral research at the national universities and each new thesis published by the partner universities will be presented in the *Small and meaningful* series.

Format: Online with live transmitted seminar with direct discussion as well as recorded material. The material is provided in form of a brief video, a digest and sources for further study. Each presented topic is given its own discussion forum for questions and answers as well as comments.

Providers: Universities, research institutes.

APPENDIX 1: CONCERNING THE CONCERNS

Cybercampus is a national initiative, based on collaboration and cooperation between universities, institutes, government agencies and companies across Sweden. The educational activities are developed as joint efforts and the diversity of the stakeholders and locations renders strength and relevance. Cybercampus operates as an agile cybersecurity *education platform and think-tank*, which enables quick response to changing demands in cybersecurity education. Within two years of its inauguration, Cybercampus Sweden will provide the services accounted for below with regard to educational services and attracting more people to the cybersecurity field.

Educational resources

Cybercampus will offer extensive educational resources, such as a competence pool of lecturers and security professional who may provide educational activities and assist in giving existing courses. It will furthermore provide a database with cybersecurity open educational resources (OER)[4] including labs, software and tools.

Cybersecurity training can be conducted on-line and on-site in a controlled, virtual environment at the RISE testbed Cyber Range. In addition, Cybercampus will provide hacker labs and makerspaces where students can experiment and examine devices for vulnerabilities.

Life-long learning is supported through a continuous series of micro-education installments through the series of educational activities called *Small and meaningful*, given in the course listing above.

Attracting more people to the cybersecurity field and retaining them

Cybersecurity is a fast-paced and dynamic field. It is also faced with a number of challenges. Among these are a general understaffing of the workforce, a lack of specialists and difficulty in retaining them in some areas and positions. The persistent increase in demand for their expertise can oftentimes lead to extremely high pressure and demands on the existing workforce.

Cybercampus will address these challenges by attracting – and retaining – more professionals to the cybersecurity field and to support them in maintaining a sustainable work life. An important effort in increasing the recruitment base and workforce is to encourage interest in cybersecurity among the general public, particularly women and minorities, who are underrepresented in the field. The courses and educational activities that are aimed at people who do not have prior knowledge in cybersecurity play an especially important part in this endeavor, as well as innovative marketing strategies. These strategies could emphasize the

[4] UNESCO Open Educational Resources

role that increased cybersecurity capabilities have in strengthening societal resilience in the deteriorating security situation in Europe.

To support and motivate cybersecurity professionals in sustaining a healthy work-life balance, Cybercampus will offer workshops and training aimed at HR-functions to increase understanding of this occupational category and its challenges.

Cybercampus will make the field of cybersecurity an attractive as well as accessible career choice for many, and it will profile Sweden as an innovation-focused, knowledge-driven nation with an exceptionally competent cybersecurity workforce.

Reports on needs for education in cybersecurity

Education providers cannot blindly develop courses and training activities without a clearly articulated need. For each new course, a provider must to decide on:

- *Subject and contents; level of the material and needed prerequisites*
- *Volume of work and awarding of credits or other recognitions*
- *Format and mode of teaching*
- *Collaborations in course development and teaching*
- *Channels for marketing and pricing model*

A mismatch in neigh any of these aspects might render an otherwise attractive course uninteresting for the market, such as a course on a "hot" subject that is too large or that is taught on campus when the interested only can attend online.

To avoid developing unsuccessful courses, Cybercampus will survey employers for their needs in terms of competence building through education. The needs will be reported to member educators, allowing them to invest in developing activities and courses that are likely to be well received by the market.

Raising awareness

A frequently voiced concern in the community of cybersecurity is the lack of awareness in the population in general and in working professionals who are not involved in security work. A particular concern is a perceived dearth of understanding of risks and exposure among company board members and upper-level management as well as among political representatives in regions, municipalities and the parliament.

All of these categories are addressed in the listed educational activities with different instruments from the basic *Cybersecurity for all* (and the intensive version *A summer in Cyber*) to *Managing cybersecurity* for decision makers. None of these offerings will be successful unless they reach their target groups. For the general population, open badges[5] may give pride and recognition to those completing the basic course, similarly to the internationally certificate Computer Driving License.

Particular marketing efforts will be aimed at decision-makers in the private sector, public agencies, and government.

[5] Open badges may be displayed on personal profiles in social networks; see OpenBadges.me

APPENDIX 2: *UTKAST TILL* MAGISTEREXAMEN I CYBERSÄKERHET VID KTH

Bakgrund

Samhällets behov av säkerhetskunniga personer överskrider stort den tillgängliga kompetensen. (IST)[2] bedömer att det saknas ungefär 200 000 personer i Europa som kan arbeta med cybersäkerhet[6]. Flertalet tjänster kräver såväl en teknisk kunskap som branschkunskap från verksamheten där säkerhetsarbetet bedrivs. Detta gäller exempelvis vårdsektorn, detaljhandeln och finansbranschen.

Det nyligen inrättade omställningsstudiestödet[7] möjliggör vidareutbildning för yrkesverksamma med en kompensation för inkomstbortfall under studietiden som motsvarar upp till 80 procent av nettoinkomsten. Stödet gäller för 44 veckor vilket svarar väl mot en magisterexamen på avancerad nivå[8].

Vi föreslår därför att ett ettårigt utbildningspaket av kurser för personer som saknar tekniska förkunskaper. Det vänder sig till yrkesverksamma som önskar arbeta med cybersäkerhet inom olika branscher. Utbildningen ska vara tillgänglig genom anslagsfinansierade platser såväl som uppdragsfinansierade platser. Vi kommer att beakta antagning till kurserna utifrån reell kompetens[9].

Planen är att erbjuda kurser som går läsa enskilt men som tillsammans kvalificerar de studeranden för en magisterexamen i cybersäkerhet.

Pedagogiskt upplägg

Utbildningen är utformad för yrkesverksammas behov och möjligheter till vidareutbildning och de bör gå att läsa på hel- och halvfart. Kurserna ska ges med schemalagda arbetstider för att underlätta planering gentemot deltagarnas övriga åtaganden. Deltagarna ska även ha en arbetsplats på KTH där de kan samarbete med varandra och delta i undervisningen. Viss förberedelse kan ske utanför schemat, exempelvis läsning och videor.

Kurserna i utbildningen läggs upp med utmaningsdriven undervisning och studentcentrerat lärande med eget ansvar för att genomföra arbetet. Studierna bedrivs därför i grupp och medlemmarna ansvarar för varandras lärande; examinationen sker individuellt. Detta koncept är beprövat och har visat sig framgångsrikt för försvarsmaktens utbildning av cybersoldater, som ges i samarbete med KTH CDIS.

Utbildningen planeras så att i regel ges en kurs åt gången och kurserna samverkar för att ämnena ska sammanfogas till en meningsfull helhet. Detta kommer även främjas genom seminarier, gästföreläsningar och studiebesök som

---

[6] (ISC)[2] Cybersecurity workforce study, 2021, läst 2022-06-30
[7] Omställningsstudiestöd – För dig som är mitt i arbetslivet, CSN, läst 2022-06-30
[8] Se Gunnar Karlsson, *Snabbt om fortbildning – en lathund*, KTH TRITA-EECS-RP 2022:4, juni 2022.
[9] Så fungerar validering av reell kompetens, KTH, läst 2022-06-30

ligger utanför de examinerade delarna. Arbetsintegrerat lärande ska erbjudas i möjligaste mån utifrån tillgänglighet.

Utkast till innehåll

Hösttermin

Grundläggande programmering, 5 hp (DD1331)
Förstå datornät och -system, 4 hp (ny, utifrån EP1100 och EP1200)
Grundläggande datalogi, 6 hp (DD1327)
Cybersäkerhet översiktskurs, 7,5 hp (DD2391)
Tillämpad kryptografi, 7,5 hp (DD2520)

Vårtermin

Säkerhetsanalys av storskaliga datorsystem, 7,5 hp (EP2790)
Etisk hackning, 7,5 hp (EP 2720)
Examensarbete i cybersäkerhet med branschtillämpning, 15 hp

Anmärkningar: Utkastet visar att det går att sammanställa en utbildning som i stort bygger på nuvarande kurser. Det är inte meningsfullt att erbjuda valbara kurser som kan kräva olika förkunskaper än dem som ges och uppdelningen av gruppen bryter den sammanhållning som är nödvändig för ett studentcentrerat lärande.