Färdplan för utveckling och implementering av kunskapsbasen för utbildning om cybersäkerhet i smarta nät
(Verkställande rapport)

Författare:

Rūta Pirta-Dreimane, Jana Bikovska, Andrejs Romānovs, Maria Valliou, Bahaa Eltahawy, Jānis Pekša

Kursplansrekommendationer för cybersäkerhet i smarta nät (CC-RSG)

Strategiskt partnerskapsprojekt inom Erasmus+

Kunskapsproduktion 4

Riga Technical University, University of Vaasa, National Technical University of Athens, University of Oldenburg

Detta projekt har fått finansiering från Europeiska unionens Erasmus+program inom ramen för bidragsavtal nr 2020-1-FI01-KA203-066624.

Innehåll

Förkortningar 3

1. Inledning 4

2. Modell för läroplaner 4

2.1 Modell för innehåll i läroplaner 5

2.2 Utformningsmetod för utbildningsprogram 7

2.3 Metoder och verktygsbank 9

3. Rekommendationer för läroplaner 9

3.1 Studentprofiler 9

3.2. Arbetsroller och uppgifter 10

3.3. Kunskapsområden och kunskapsenheter 10

3.4. Metod- & verktygsbank 10

Referenser 12

Förkortningar

ACM	Association for Computing Machinery
NICE	Nationellt initiativ för utbildning inom cybersäkerhet
CC-RSG	Kursplansrekommendationer för cybersäkerhet i smarta nät
CPES	Center for Power Electronics Systems
ENISA	Europeiska byrån för nät- och informationssäkerhet
EU	Europeiska unionen
JTF	Gemensam arbetsgrupp
IT	Informationsteknik
IO	Kunskapsproduktion
MOOC	Storskaliga öppna nätkurser
NIST	National Institute of Standards and Technology
PMU	Phasor Measurement Unit
OT	Driftteknik
SCADA	Supervisory control and data acquisition
SME	Små och medelstora företag
VET	Yrkesutbildning
WP	Arbetspaket

1. Inledning

Cybersäkerhet definieras som en av EU:s strategiska kapaciteter och man har konstaterat att EU måste förbättra sin digitala kapacitet avsevärt på cybersäkerhetsområdet [1]. Detta inbegriper införande av digital teknik samt nödvändiga digitala färdigheter för alla personalstyrkor inom EU. Cybersäkerhet är ett tvärvetenskapligt ämne [2]- [3] som måste integreras i utbildningsprogram, såsom datavetenskap, ingenjörsvetenskap, psykologi, sociologi och lagstiftning för att säkerställa alla kritiska kompetenser, inom flera dimensioner och discipliner. Cybersäkerhetsspecialister måste ha djupgående tekniska kunskaper, men även allmänna färdigheter är nödvändiga, särskilt i krissituationer.

En miljö med smarta nät innebär ytterligare komplexitet när det kommer till cybersäkerhet. Smarta nät integrerar olika sensorer, kontrollsystem och kommunikationsnätverk, vilket ökar cyberattackens yta. Specialister på cybersäkerhet som arbetar med smarta nät måste ha en rad olika kompetenser för att kunna skydda infrastrukturen. De ska kunna balansera cybersäkerhet och kunskap om elteknik med mjuka färdigheter.

Detta dokument representerar projektet ”Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)” resultat från WP4. Syftet med detta arbete är att konceptualisera kunskap som förvärvats i projektet och ge rekommendationer för utveckling av kursplaner för cybersäkerhet i smarta nät.

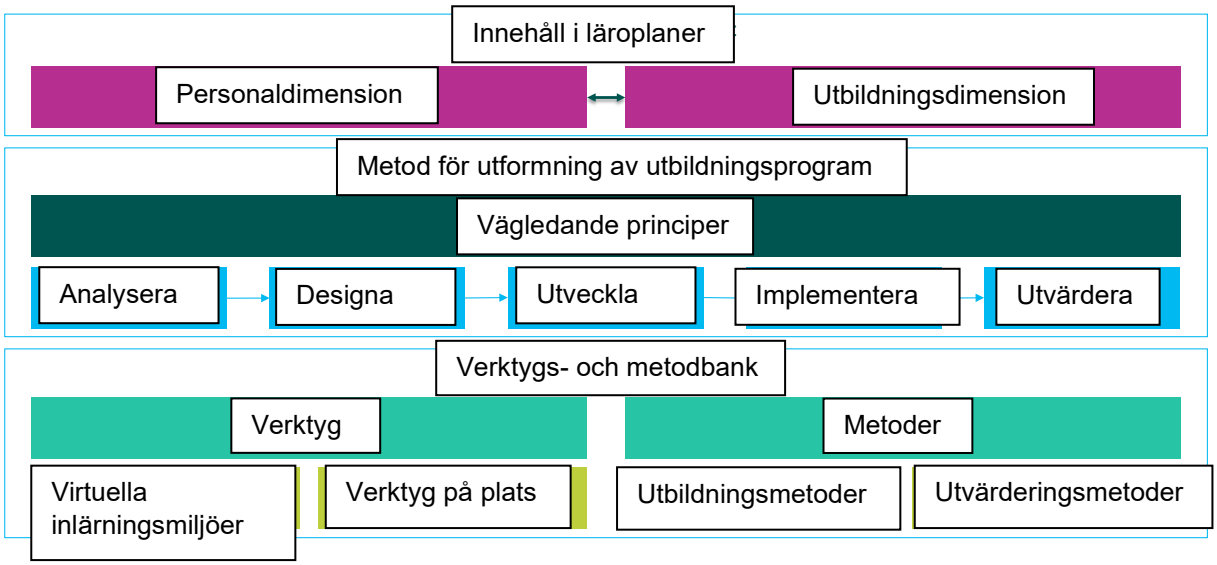
Huvudsyftet med dokumentet är att ge rekommendationer till lärare och andra relevanta parter för utveckling av utbildningsprogram, med beaktande av industrins behov, arbetskraftskrav, studentcentrerade utbildningsmetoder och framväxande stödverktyg.

2. Modell för läroplaner

Syftet med modellen är att ge vägledning för kompetensdrivna utbildningsprogram i cybersäkerhet i smarta nät vad gäller utformning, utförande och utvärdering. Modellen förklarar hur en kunskapsbas (t.ex. detta dokument) bör användas för att möjliggöra integration av arbetskraft och utbildningsdimensioner.

Modellen bygger på den metod som föreslås i [4] och består av tre viktiga byggstenar (figur 1):

1. **Innehållet i läroplanen** definierar roller och uppgiftsspecifika kompetenser och tillhörande kunskapsområden, kunskapsenheter, läroämnen och läranderesultat.
2. **I utformningsmetoden för utbildningsprogram** finns förslag på principer och processer för utformning, genomförande och utvärdering av studieprogram och kurser.
3. **Verktygs- och metodbanken** innehåller metoder och verktygslistor och användningsvägledning (mönster) för dem, som kan användas för utformning, utförande och utvärdering av utbildningsprogram för cybersäkerhet i smarta nät.

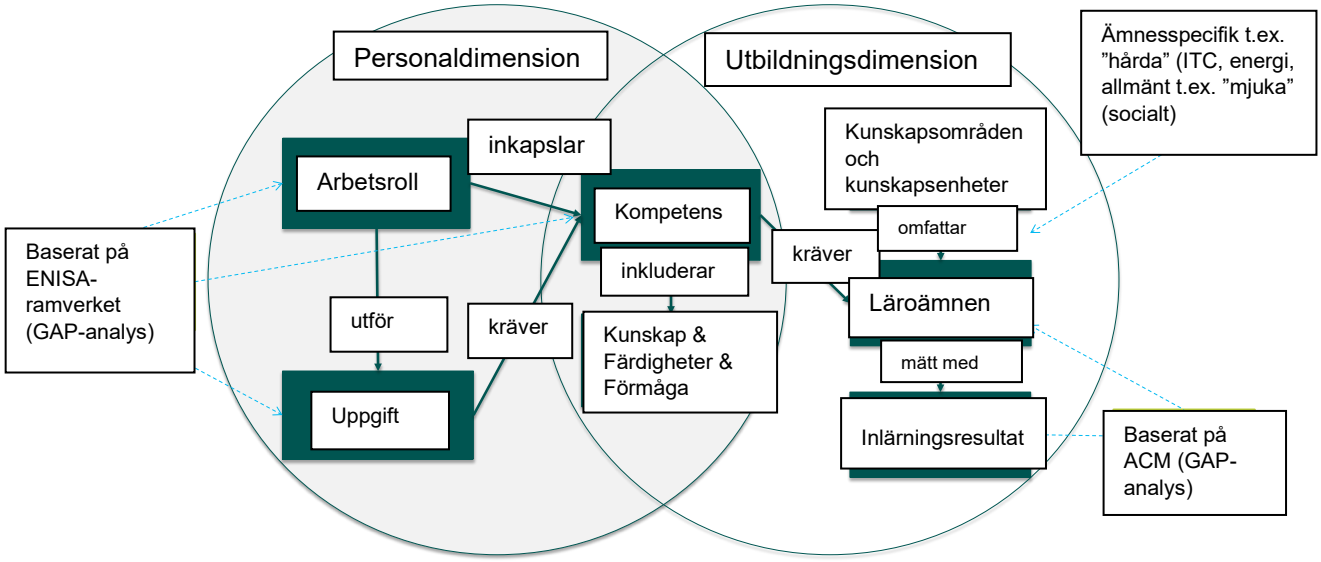


Figur 1 Modell för läroplansöversikt

2.1 Modell för innehåll i läroplaner

Läroplaner måste utformas på grundval av personalkrav för att säkerställa att kompetensen hos cybersäkerhetsspecialister tillgodoser industrins efterfrågan, inklusive kompetens som behöver läras ut och kompetensområden som måste omfattas [2].

Den föreslagna modellen för läroplaner omfattar två dimensioner: arbetskraftsdimensionen och utbildningsdimensionen (diagram 2).



Figur 2 Modell för läroplansöversikt

Sysselsättningsdimensionen omfattar följande nyckelbegrepp [5]:

- **Arbetsroller** är de mest detaljerade grupperingarna av cybersäkerhetsrelaterat arbete, inklusive en förteckning över attribut, dvs. kunskap, färdigheter och förmågor som krävs för att utföra uppgifter som hör samman med rollen.

- **Uppgifter** representerar specifika definierade arbetsdelar som, i kombination med andra identifierade uppgifter, sammanställer arbetsomfattningen i ett specialområde eller en arbetsroll.
- **Kompetenser** beskriver förmågan att tillämpa eller använda kunskaper, färdigheter, förmågor, beteenden och personliga egenskaper för att framgångsrikt utföra kritiska arbetsuppgifter, specifika funktioner eller verka i en viss roll eller befattning. Det är viktigt att särskilja kapaciteten mellan ämnesspecifika (t.ex. ”hårda färdigheter”) och allmänna (t.ex. ”mjuka färdigheter”). Hårda färdigheter omfattar teknisk eller administrativ kompetens. Mjuka färdigheter är ett kluster av produktiva personlighetsdrag som kännetecknar ens relationer i en social miljö. Dessa färdigheter kan omfatta socialt uppträdande, kommunikationsförmåga, språkkunskaper, personliga vanor, kognitiv eller emotionell empati, tidshantering, teamarbete och ledarskapsegenskaper.

I flera ramar definieras cybersäkerhetsrelaterade roller, tillhörande uppgifter och erhållen kompetens, t.ex. det nationella initiativet för utbildning i cybersäkerhet (NICE) Workforce Framework (NIST NICE-ramverket) [5] och kompetensramen för Europeiska byrån för nät- och informationssäkerhet (ENISA) [6].

För utbildning i cybersäkerhet i smarta nät föreslås att ENISA-kompetensmodellen ska användas som grund för utformningen av utbildningsprogram, eftersom den har en enklare arbetsrollsstruktur jämfört med NIST. NIST-roller är främst utformade för stora företag, och de representerar därför avskild cybersäkerhetskapacitet uppdelad över organisationer. Empiriska observationer visar att företag vanligtvis kombinerar liknande roller och möjliggör T-formade kompetenser och multifunktionella team.

Befintliga kompetensmodeller för cybersäkerhet fokuserar på cybersäkerhetsstyrning och IT-specifika cybersäkerhetsaspekter, men de tar inte upp cybersäkerhetsroller, uppgifter och kompetenser i smarta nät. Därför ingår cybersäkerhetsspecifika uppgifter i ENISA-modellen (avsnitt 3.2). Projektexpertgruppen föreslår uppgifter och kompetenser (avsnitt 3). I detta dokument fastställs därför en referensmodell för cybersäkerhetsroller och uppgifter med smarta nät som grund för utformningen av relevanta utbildningsprogram.

Sysselsättningsdimensionen påverkar utbildningsdimensionen via kompetenser, inklusive färdigheter, förmågor och kunskap. Utbildningsdimensionen omfattar följande nyckelbegrepp [7]:

- **Kunskapsområden** och **kunskapsenheter** är tematiska grupperingar som omfattar flera relaterade **läroämnen**.
- **Läranderesultaten** är mer detaljerade än kompetenserna och kan ses som läranderesultat eller lärdomar. Läranderesultat betonar vad studenterna kan göra framför vad studenterna vet.

I flera rekommendationer i läroplanen för cybersäkerhet föreslås huvudsakliga kunskapsområden, kunskapsenheter, läroämnen och läranderesultat. Exempelvis Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) utarbetad av Association for Computing Machinery Committee for Computing Education in Community Colleges [7] and CSEC2017 Gemensamma arbetsgruppen för utbildning i cybersäkerhet (JTF) Global cybersecurity curricular recommendations [3].

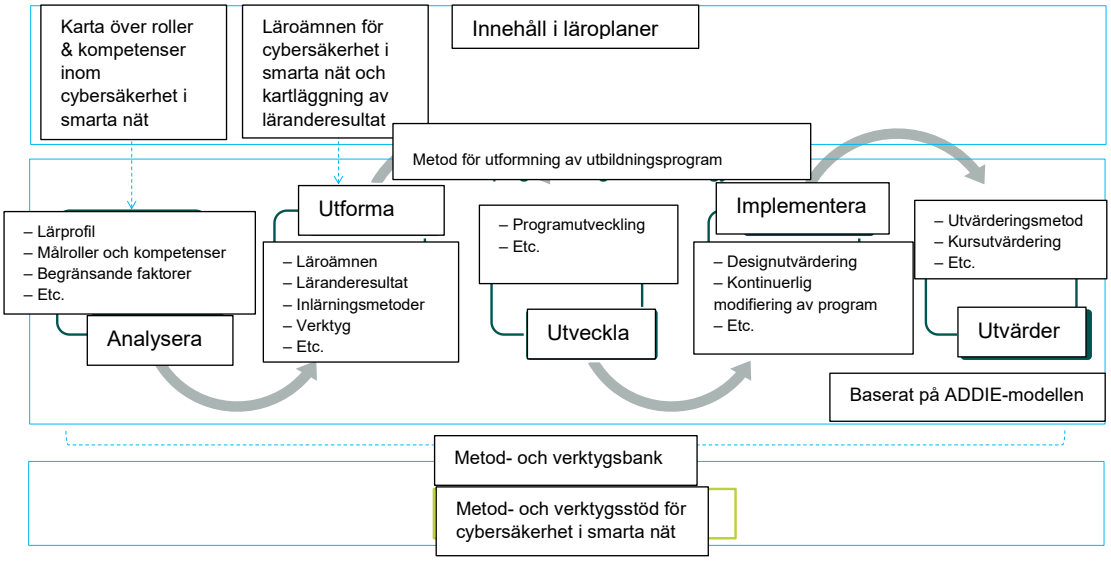
När det gäller utbildning i cybersäkerhet i smarta nät föreslås att man tillämpar Cyber2yr2020-riktlinjer för IT-specifika kunskapsenheter för cybersäkerhet, kunskapsområden, ämnen och definition av läranderesultat. Specifik utbildning i cybersäkerhet i smarta nät har konstaterats vara begränsad av befintliga ramar, och därför inkluderas cybersäkerhetsspecifika kompetenser, läroämnen och läranderesultat i Cyber2yr2020-modellen. Projektexpertgruppen föreslår kompetenser, läroämnen och läranderesultat för smarta nät (avsnitt 3.3).

I det här dokumentet är kompetenserna indelade i fyra grupper:

- IT-specifika kompetenser definierar de kunskaper, färdigheter och färdigheter som krävs för att utföra IT-specifika cybersäkerhetsuppgifter. Dessa kompetenser bygger på riktlinjer för Cyber2yr2020 (endast grundläggande kompetenser). Dessa kompetenser definierar ”vad som bör göras”-aspekter [7].
- Smarta nät – specifika kompetenser definierar kunskap, förmågor och färdigheter som krävs för att utföra smarta nätspecifika cybersäkerhetsuppgifter. Dessa kompetenser utarbetas av projektexperter och valideras med branschexperter. Dessa kompetenser definierar ”vad som bör göras”-aspekter [7].
- Operativa kompetenser sammanställer förvaltnings- och operativa kompetenser som definierar ”hur aktiviteter bör utföras” inom både IT-specifika och smarta nätspecifika områden.
- Allmänna färdigheter definierar förväntade ”mjuka färdigheter”.

2.2 Utformningsmetod för utbildningsprogram

I utformningsmetoden för utbildningsprogram definieras allmänna principer som bör följas och huvudsakliga steg i hur utbildningsprogram bör definieras (figur 2). I programdefinitionen kan utförande- och utvärderingsutbildare använda kompetensmodellen för smarta nät för cybersäkerhet och rekommendationer för kursplansinnehåll som beskrivs i detta dokument. Det exakta innehållet måste dock anpassas till programprofilerna och deras behov (målroller osv.).



Figur 3 Utformningsmetod för utbildningsprogram

Utbildningsprogram bör utarbetas enligt flera vägledande principer. Enligt utformningstänkadet när det gäller användning i utbildningsdesign [8] används [9]

designprinciper ofta för att ange huvudriktningen som måste följas i programdesign och genomförande [10]. Utformningsprinciperna definieras som [9]: ''...ett mellansteg mellan vetenskapliga fynd, som måste vara generaliserade och reproducerbara, och lokala erfarenheter eller exempel som dyker upp i praktiken. På grund av behovet av att tolka designprinciper är de inte lika lättförståeliga som vetenskapliga lagar. Principerna genereras induktivt från tidigare exempel på framgång och är föremål för förfining över tid när andra försöker anpassa dem till sina egna erfarenheter". Designprinciper hämtar designkunskap från framgångsrika inlärningsmiljöer [10] och sammanfattar återanvändbara bästa praxis.

Det föreslås att följande nyckelprinciper ska följas i utbildning i cybersäkerhet i smarta nät:

1) **Målroller och uppgiftsstyrd kompetensutformning** – kompetenser måste definieras utifrån de studerandes målroller för att möjliggöra integration av arbetskraft och utbildningsdimensioner.
2) **Studerandecentrering och individanpassning** – studieprogrammen måste fokusera på studenternas behov och tillhandahålla profilspecifik kompetensutveckling.
3) **Ämnesspecifika och allmänna kompetenssynergier** – allmänna kompetenser måste integreras i varje läroämne tillsammans med ämnesspecifika kompetenser.
4) **Integrering av verkliga erfarenheter** - studieprogram och kursinnehåll måste återspegla verkliga utmaningar och anpassas med tiden.
5) **Vertikal integration** – cybersäkerhet är ett tvärvetenskapligt ämne. Program måste integrera samhällsvetenskaper (som psykologi) för att möjliggöra utvecklingen av allmänna kompetenser.
6) **Feedbackbaserad kontinuerlig förbättring** – kontinuerlig förbättring måste planeras utgående från studenternas och arbetskraftens feedback.

Den föreslagna utformningen av utbildningsprogrammet baseras på ADDIE-modellen [11]. ADDIE-modellen är den generiska process som traditionellt används av instruktionsdesigners och utbildningsutvecklare. Modellen innehåller fem faser:

1. **Analys** – studentprofilanalys (inklusive deras egenskaper, befintlig kompetens, förväntade målroller och utbildningsbehov), definition av instruktionsmål och mål. Programmet måste utformas så att det omfattar kompetenser som krävs för studenternas målroller. Detta dokument innehåller typiska cybersäkerhetsroller som berikas med smarta nätspecifika cybersäkerhetsuppgifter och cybersäkerhetskompetenser (avsnitt 3.2). Detta dokument kan användas som referensmodell för kartläggning av studenternas målroller. Rollerna är utformade på grundval av identifierade typiska cybersäkerhetsprofiler för smarta nät (avsnitt 3.1) som definieras utgående från projektexperters erfarenheter.
2. **Design** - studieprogramsmål, läroämnen, läranderesultat och definition av undervisningsmetoder. I detta dokument definieras den uppsättning läroämnen och läranderesultat som definierade roller måste ha (avsnitt 3.3.). Ämnena är inkapslade i kunskapsområden och enheter. Arbetsroller, uppgifter, kompetenser och ämneskarta för lärande läggs till i bilaga 1. Ämnena måste väljas på grundval av identifierade studentmålroller. Studenterna kan ha individuella planer, baserade på sina befintliga kompetenser (t.ex. om studenten har tidigare utbildning i IT-specifik cybersäkerhet och han/hon

strävar efter att bli säkerhetsarkitekt vid institutioner inom energisektorn måste han/hon erhålla kompetens för smart nätspecifik cybersäkerhet). Dokumentet innehåller en metodbank (avsnitt 4) och en verktygsbank (avsnitt 5) som kan användas för att utforma utbildningsprogram.

3. **Utveckling** - utveckling och laddning av programmaterial i e-lärandesystem (om tillämpligt).
4. **Implementering - faktisk leverans av program och kurser.**
5. **Utvärdering** – återkoppling och datainsamling för identifiering av förbättringsområden. Dokumentet innehåller metodbank (avsnitt 4) och verktygsbank (avsnitt 5) som kan användas för stöd till utvärdering av utbildningsprogram.

2.3 Metoder och verktygsbank

Metod- och verktygsbanken (avsnitt 4) ger förslag på metoder och verktyg som utbildningsprogramdesigners och utbildare kan använda i alla utbildningsutvecklingsfaser (analys, utformning, utveckling, genomförande och utvärdering). Metoder och verktyg definieras i form av återanvändbara mönster som utgör en kunskapsbas för att utforma och genomföra kurser. Metoder och verktyg som kopplas till utbildningsutformning och genomförandeprocesser beskrivs på varje metod /verktygskort.

3. Rekommendationer för läroplaner

Rekommendationer för läroplaner utgör en referensmodell för arbetskraft och utbildningsintegration. Den innehåller följande huvudbegrepp:

- Studentprofiler – typiska studentprofiler för smarta nät för cybersäkerhet utgör grunden för definitionen av arbetsroller.
- **Arbetsroller och uppgifter** representerar studentmålroller, uppgifter och erhållna kompetenser (inklusive IT-specifik cybersäkerhetskompetens, smarta nätspecifika cybersäkerhetskompetenser, operativa och allmänna kompetenser).
- **Kunskapsenheter och kunskapsområden** definierar **läroämnen och läranderesultat** som krävs för att erhålla kompetens.

3.1 Studentprofiler

Syftet med studentprofilen är att lyfta fram studentgrupper som läroplansmodellen kan tillämpas på.

Här kan två grupper av utexaminerade som kan vara intresserade av att fortsätta sin utbildning på området cybersäkerhet i smarta nät lyftas fram: utexaminerade inom datorområdet och utexaminerade inom kraftsystem. De andra två grupperna är antingen IT&OT-proffs eller proffs på hantering av smarta nät. De har arbetserfarenhet av kraftsystem och smarta nät men behöver dock mer avancerad kunskap om cybersäkerhet i smarta nät.

Följande attribut beaktas för profilen:

- med bakgrund avses en studerandes utbildningsresultat eller yrkesfärdigheter,
- utbildningsbehoven är klyftan mellan den studerandes nuvarande kunskaps-, kompetens- och attitydnivå och den önskade, för att anpassa sig till en ny situation som kan uppnås genom utbildning.

- Förväntningar beskriver de kunskaper och färdigheter som studenterna förväntas uppvisa i slutet av studierna.

Energiindustrin behöver arbetskraft med kunskap om cybersäkerhet, och den högre utbildningen kunde spela en värdefull roll för att överbrygga klyftan.

3.2. Arbetsroller och uppgifter

Arbetsrollerna för cybersäkerhet i smarta nät har byggts på förslag från ENISA: Chef för informationssäkerhet (CISO), svarsperson för cyberincidenter, cyberjurist, policy- och regelefterlevnadsansvarig, cybersäkerhetsarkitekt, cybersäkerhetsrevisor, cybersäkerhetsimplementerare och cybersäkerhetsriskhanterare. Rollerna, uppgifterna och kompetenserna har kompletterats i enlighet med det smarta nätets särdrag.

ENISA-rollerna har kompletterats med nya roller med tanke på särdragen hos smarta nät – energimedborgarskap, förvaltare av nättillgångar och kommunikationstekniker. De gemensamma affärsmålen för smarta nät är [12]: att upprätthålla säkerheten, upprätthålla energisystemets tillförlitlighet, upprätthålla energisystemets motståndskraft och stödja nätmodernisering.

3.3. Kunskapsområden och kunskapsenheter

Kunskapsområden och enheter baseras på ”ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020 Cyber2yr2020” Association for Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC): Datasäkerhet, programvarusäkerhet, komponentsäkerhet, anslutningssäkerhet, systemsäkerhet, mänsklig säkerhet, organisationssäkerhet, samhällssäkerhet. De är berikade med de smarta nätspecifika kompetenser som krävs för definierade arbetsroller (avsnitt 3.2.). Det nya kunskapsområdet ”Smart-Grid Security” kompletterar ramen för ACM.

3.4. Metod- & verktygsbank

Metoderna och verktygen specificerar föreslagna metoder och verktyg som ska användas inom utbildning i cybersäkerhet i smarta nät: Simuleringsverktyg, CPES-laboratorier och testbäddar, spel, problem- och projektbaserad inlärning och spegelvänd inlärning. Ett snabbt sätt för lärare/utbildare som vill formulera en läroplan för att se de grundläggande inslagen i metoden och dess vanliga användningsfall när det gäller cybersäkerhet och/eller smarta nät. Tillsammans med utbildningsmetoderna beskrivs också verktyget för simuleringstestbäddar medföljande användningsfall.

Testbäddar används för att simulera verkliga system i varierande grad. Vissa testbäddar använder programvarusimulering för delar av systemet och andra använder endast maskinvarukomponenter. Dessutom finns det testbäddar som endast simulerar en komponent i systemet och andra som simulerar hela systemet. Att använda en realtidssimulator i kombination med verklig maskinvara (t.ex. växelriktare och PMU) för att simulera ett helt mikronät är det mest realistiska och fullständiga sättet att studera ett elnäts beteende under en cyberattack.

Spel är en undervisningsmetod där element och mekanismer från speldesign används för att öka elevernas engagemang [13]. Sådana element och mekanismer kan till exempel vara en berättad historia, begränsad tid för att utföra en uppgift, poäng, märken och nivåslagning.

I problembaserat lärande undersöker en grupp studerande ett olöst, verkligt problem och försöker hitta den lämpligaste lösningen som gruppen sedan presenterar för sina

andra medstuderande. Projektbaserat lärande bygger på samma idé, men i allmänhet har det en längre varaktighet och ett konkret resultat snarare än en teoretisk lösning.

Den huvudsakliga egenskapen hos omvänt lärande är att studenterna studerar det material som vanligtvis studeras under klassrummet hemma. På så sätt har de möjlighet att reflektera över det undersökta materialet och ha tid för experiment.

Referenser

[1] European Commission, “The EU’s Cybersecurity Strategy for the Digital Decade,” 2020. [Online]. Tillgängligt: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[2] Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta och R. De Nicola, ”Framework, Tools and Good Practices for Cybersecurity Curricula”, IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3093952.

[3] Joint Task Force on Cybersecurity Education, *Curricula 2017 Cybersecurity Curriculum - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, vol. Version 1., no. December. 2017.

[4] R. Pirta-Dreimane, A. Brilingaite, E. Roponena, and K. Parish, “Multi-dimensional Cybersecurity Education Design: A Case Study,” in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, IEEE, Sep. 2022, pp. 1–8. doi: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931.

[5] D. S. M. C. S. K. A. W. and G. W. R. Petersen, “Workforce Framework for Cybersecurity (NICE Framework),” 2020.

[6] E. European Union Agency for Cybersecurity, “European cybersecurity skills framework,” *https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles*, 2022.

[7] Cyber2yr2020 Task Group, *Cybersecurity Curricular Guidance for Associate-Degree Programs*. 2020. doi: 10,1145/3381686.

[8] I. Wrogemann, L. Sarp, N. Susser, and J. Falk, “D-Learning – Design Thinking as a means to innovative product development in adult learning,” *https://cesie.org/media/ d-learning-manual-en.pdf,* 2021.

[9] S. Panke, “Design Thinking in Education: Perspectives, Opportunities and Challenges,” *Open Education Studies*, vol. 1, no. 1. 2019. doi: 10.1515/edu-2019-0022.

[10] Y. Kali, R. Levin-Peled, and Y. Dori, “The role of design-principles in designing courses that promote collaborative learning in higher-education. Computers in Human Behavior,” *Comput Human Behav*, vol. 25, 2009.

[11] G. Morrison and S. Ross, *Designing Effective Instruction, 7th Edition*. 2013.

[12] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, “Cybersecurity framework smart grid profile,” Gaithersburg, MD, Jul. 2019. doi: 10.6028/NIST.TN.2051.

[13] S. Deterding, K. O’Hara, M. Sicart, D. Dixon, and L. Nacke, “Gamification: Using game design elements in non-gaming contexts,” in *Conference on Human Factors in Computing Systems - Proceedings*, 2011. doi: 10.1145/1979742.1979575.