# Det allra senaste - Trender och kunskapsluckor inom cybersäkerhet i smarta nät
# (Verkställande rapport)


Författare:

Jirapa Kamsamrong, Björn Siemers, Shadi Attarha,
Sebastian Lehnhoff, Maria Valliou, Andrejs Romanovs,
Jana Bikovska, Janis Peksa, Ruta Pirta-Dreimane,
Janis Grabis, Nadezhda Kunicina, Julija Srebko
Tero Vartiainen, Bahaa Eltahawy, Mike Mekkanen



Kursplansrekommendationer för cybersäkerhet i smarta nät (CC-RSG)

Strategiskt partnerskapsprojekt inom Erasmus+

Kunskapsproduktion 1

April 2022

Granskare: Foivos Palaiogiannis

Samordnare: Vasas universitet
Samarbetsparter: University of Oldenburg, Riga Technical University, National Technical University of Athens

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

Europeiska kommissionens stöd till upprättandet av denna publikation utgör inte ett godkännande av innehållet, som endast återspeglar författarnas

åsikter, och kommissionen kan inte hållas ansvarig för eventuell användning av informationen i den.

# Innehåll

List of Tables ..... 4
List of Figures ..... 4
Abbreviations ..... 5
1. Introduction ..... 6
1.1 Objectives ..... 6
1.2 Structure of the document ..... 6
2. Research Methodology ..... 7
3. Cybersecurity Policy in European Union ..... 7
3.1 EU Policies and Strategic Directions ..... 7
3.2 Organization related to cybersecurity ..... 8
3.3 Industry Studies and Recommendations ..... 8
3.4 Industry Studies and Recommendations ..... 8
4. State of the art and trends in cybersecurity in smart grids ..... 9
4.1 Categorization ..... 9
4.2 Technology and Education Development ..... 10
4.3 Gaps analysis ..... 11
5. State of the art in education in smart grids and cyber security ..... 12
5.1 Higher education study programs ..... 12
5.2 Continuing education programs ..... 12
5.3 Massive open online courses (MOOC) ..... 13
6. Identification of skill gaps in cyber security in smart grids ..... 13
7. Identification of useful tools for education in cyber security in smart grid ..... 14
7.1 Basic tools for active learning about cybersecurity ..... 14
7.2 Advanced tools for vulnerabilities experiments ..... 14
8. Conclusion and recommendations ..... 15
9. Bibliography ..... 16

# Innehållsförteckning

Table 1 Cyberattacks classification considering CIA..... 10
Table 2 Gap analysis for existing CPES laboratory/testbed..... 11
Table 3 Cybersecurity Risks in the CPES..... 12
Table 4 Recommendation from the stakeholder workshop [70] ..... 13
Table 5 Educational Approaches in Smart Grids and Cyber Security ..... 14
Table 6 Cybersecurity tools for smart grids ..... 14

# Förteckning över figurer

Figure 1 Research methodology of WP1 ..... 7
Figure 2 Cybersecurity education curriculum thought model ..... 8
Figure 3 Categorization of skill gaps based on the literature review ..... 9

# Förkortningar

| | |
|---|---|
| ACM | Association for Computing Machinery |
| AES | Advanced Encryption Standard |
| CIA | Konfidentialitet, integritet och tillgänglighet |
| CPES | Cyber Physical Energy System |
| DdoS | Överbelastningsattack |
| DMZ | Demilitariserade zoner |
| DoS | Denial of Service |
| ENISA | Europeiska byrån för nät- och informationssäkerhet |
| EU | Europeiska unionen |
| HPC | Hårdvaruräknare |
| ICS | Industriella styrsystem |
| ICT | Informations- och kommunikationsteknologi |
| IDS | Intrångsdetekteringssystem |
| IEC | Internationella elektrotekniska kommissionen |
| IoT | Sakernas internet |
| IP | Internetprotokoll |
| KUs | Kunskapsenheter |
| MOOC | Storskaliga öppna nätkurser |
| VET | Yrkesutbildning |
| WP | Arbetspaket |

# 1. Inledning

Under de senaste åren har energisektorn avsevärt ökat sin digitala mognadsgrad genom att integrera olika system och tekniker för digital databehandling, kommunikation och industriell kontroll i ett moderniserat och avancerat elnät. Dessutom strävar Europa efter att helt integreras genom ett gränsöverskridande utbyte av marknadsdata i realtid. På grund av den enorma mängden data och den breda användningen av sakernas internet har energisektorn blivit allt mer attraktiv för hackare. Det kräver ett brett spektrum av tvärvetenskapliga kunskaper, bland annat om energisystem, datornätverk, programvaror, integrerade system, kritisk infrastruktursäkerhet och säkerhetshantering.

Europeiska kommissionen (EC) har lanserat EU:s strategi för cybersäkerhet för att öka Europas kollektiva motståndskraft mot cyberhot och säkerställa att alla medborgare och företag till fullo kan dra nytta av tillförlitliga och pålitliga tjänster och digitala verktyg. Strategin omfattar säkerhet för grundläggande service, inklusive energinät och det ständigt ökande antalet uppkopplade objekt i medborgarnas hem och på deras kontor. I strategin anges att EU:s nuvarande cybersäkerhetskapacitet inte är tillräcklig. För att förbättra cybersäkerhetskapaciteten belyser både EU:s strategi för cybersäkerhet och programmet för Ett digitalt Europa behovet av att öka samhällets medvetenhet om cybersäkerhet och en förbättring av nya specialisters kunskaper om cybersäkerhet.

## 1.1 Mål

WP1-rapporten har följande mål:

- Analysera aktuella trender och den senaste utvecklingen inom den akademiska världen
- Analysera nuvarande och framtida kursplaner inom högre utbildning inom EU
- Analysera branschens kompetensbehov
- Identifiera kunskapsluckorna mellan den högre utbildningen och industrins behov baserat på ovanstående analys

## 1.2 Dokumentets struktur

Dokumentet är uppbyggt på följande sätt:

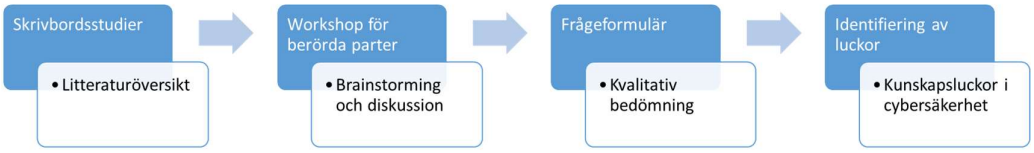
- I avsnitt 2 presenteras forskningsmetoden som har använts i denna studie för att samla in data och analysera resultatet, inklusive studiens omfattning.
- Avsnitt 3 illustrerar EU:s politik för cybersäkerhet i det smarta nätet.
- I avsnitt 4 presenteras den akademiska världens perspektiv i form av en litteraturöversikt. Syftet med litteraturöversikten är att hitta den senaste tekniska utvecklingen och de aktuella trenderna inom utbildning inom det kombinerade området smarta nät och cybersäkerhet.
- I avsnitt 5 presenteras en sammanfattning av befintliga utbildningsprogram inom cybersäkerhet, inklusive högre utbildning, fortbildning och MOOC-utbildning.
- I avsnitt 6 identifieras branschen och de kompetensbehov som den behöver för bemanning. Kartläggningen av kompetensbehoven uppnåddes genom en workshop för berörda parter och en särskild undersökning som genomfördes.
- I avsnitt 7 presenteras användbara verktyg för utbildning i cybersäkerhet som analyseras utgående från litteraturöversikten och intressentenkäten.
- Avsnitt 8 ägnas åt slutsatser och inledande krav och rekommendationer för utbildningar

i cybersäkerhet i smarta nät.

Detta dokument kompletteras med slutsatserna och en litteraturförteckning.

# 2. Forskningsmetod

För att få insikt i och få med det senaste om cybersäkerhet i smarta nät är litteraturöversikten ett första steg för att samla ihop forskningstrender och utveckling, samt utbildningsmetoder och befintliga kursplaner. Forskningsmetoden för arbetsprogram 1 visas i Figur 1




Figur 1 Forskningsmetod för WP1

Skrivbordsstudier ger endast information baserad på specifika ämnen och områden beroende på forskningssammanhanget och forskningsmålen. För att få en bredare syn på kompetensbrister inom cybersäkerhet, särskilt ur industrins perspektiv, är workshoppen för berörda parter avgörande för att brainstorma och utbyta åsikter mellan den akademiska världen och industrin.

# 3. Cybersäkerhetspolitik i Europeiska unionen

## 3.1 EU:s politik och strategiska riktlinjer

Cybersäkerhetspolitiken kan hjälpa nationen att ta itu med de väsentliga aspekter som behövs för att förhindra de negativa effekterna av cybersårbarheter. Europeiska kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik har fastställt en ny femårig EU-strategi för cybersäkerhet (2020–2025) för att stärka och säkra den digitala systemomställningen mot cyberhot. I strategin betonas också vikten av en arbetskraft med IT-kompetens inom EU. Cyberberedskapen och medvetenheten hos företag och individer är fortfarande låg, och det råder en betydande brist på arbetskraft inom cybersäkerhet.

EU:s strategi för cybersäkerhet anpassar EU:s reviderade handlingsplan för digital utbildning [1], som syftar till att öka medvetenheten om cybersäkerhet bland enskilda personer, särskilt barn och ungdomar, och organisationer, särskilt små och medelstora företag. Planen har två prioriteringar [1] att främja ett högpresterande digitalt utbildningsekosystem och [2] förbättra digitala färdigheter och kompetenser för den digitala omställningen. För att möta den ökande efterfrågan på ICT-personal har ICT-säkerhetsexperter med operativ kunskap på energiområdet getts en utmaning, och kan behöva uppdatera kursplanerna på ingenjörs- och ICT-utbildningar. Dessutom har man i handlingsplanen för utbildning föreslagit utbildning och fortbildning av intressenter under hela livscykeln för nya säkerhetslösningar för smarta nät. Där anges att utbildningsprogram måste motivera berörda parter att tänka på olika, innovativa sätt och erfara nya strategier. Utbildnings- och lärandeprogrammen måste rikta in sig på att

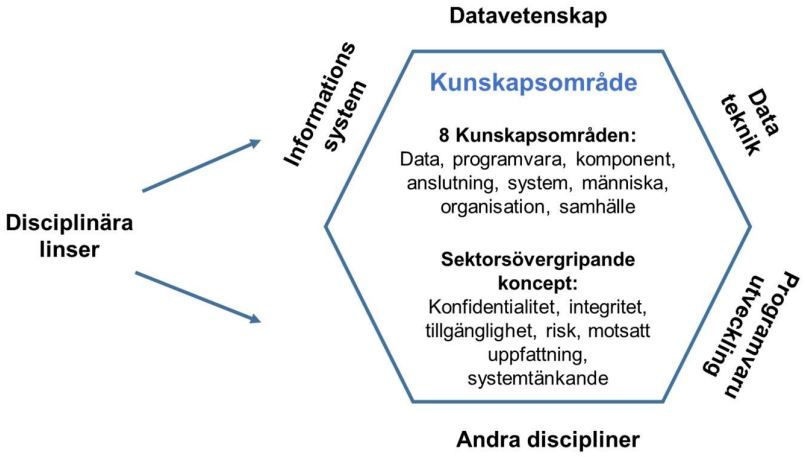
öka (och uppdatera) medvetenheten, ge insikt och perspektiv genom verkliga scenarier och utveckla, experimentera och uppleva nya (cybersäkerhets) koncept.

## 3.2 Organisation kopplad till cybersäkerhet

EU:s cybersäkerhetsbyrå (ENISA) ansvarar för cybersäkerhet i EU enligt cybersäkerhetslagen [2]. Genom cybersäkerhetslagen stärks ENISA-organet med ett permanent mandat med konkreta resurser och uppgifter för att öka den operativa verksamheten på EU-nivå. ENISA har fått i uppdrag att ge EU-medlemsstaterna stöd för genomförande av cybersäkerhet genom att inrätta en europeisk cybersäkerhetscertifiering [3]. Företag inom EU måste uppfylla det särskilda kravet på sina produkter och tjänster enligt direktivet.

## 3.3 Branschstudier och rekommendationer

Branschorganisationer och intressegrupper har studerat den senaste utvecklingen inom den befintliga cybersäkerhetsutbildningen och utarbetat rekommendationer för kursplaner i cybersäkerhet. Förslagen om utbildning i cybersäkerhet i smarta nät är dock fortfarande begränsade. Den gemensamma arbetsgruppen för cybersäkerhetsutbildning består av flera organisationer som har utarbetat riktlinjer för läroplaner i eftergymnasial utbildning i cybersäkerhet [4]. Den gemensamma arbetsgruppen delar åsikten att det råder en aktuell och växande brist på kvalificerad personal och yrkesverksamma inom cybersäkerhet. De föreslagna utbildningsprogrammen för cybersäkerhet visas i Figur 2.




Figur 2 Utbildningsplan för cybersäkerhet [4]

## 3.4 Branschstudier och rekommendationer

Energisektorn har nyligen inlett en digital omvandlingsprocess som introducerar smarta nät. Detta ger upphov till ett behov av att omskola den åldrande arbetskraften och utbilda den kommande arbetskraften. En utbildningsplattform för att främja aktivt lärande bör tillhandahållas enligt följande [5]:

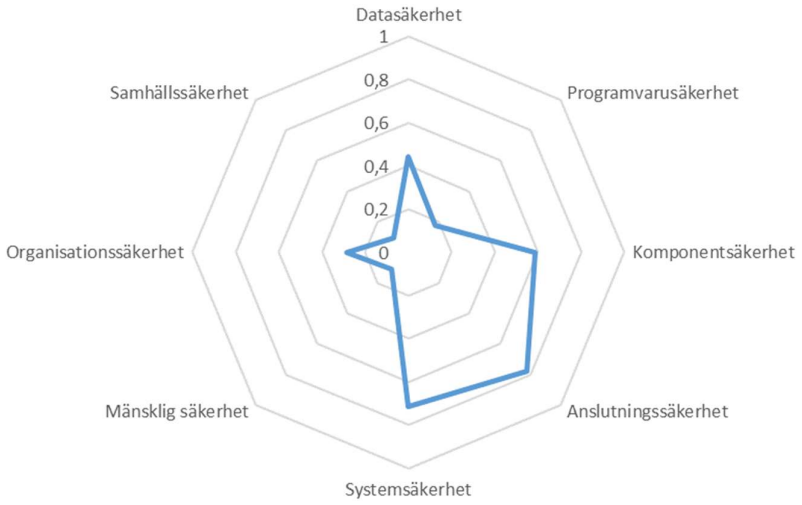
- Cyberinfrastruktur i elnätet.
- Övervakning och situationsmedvetenhet.
- Infrastruktur för avancerad mätning.
- Vägledningsdokument för smarta nät.

- Mognadsmodell för elsektorns kapacitet.
- Integritet i det smarta nätet.
- Exempel på och konsekvenser för säkerheten i kritisk infrastruktur.
- Ett säkerhetsperspektiv.
- Säkerhetsutmaningar inom automatiserad distribution.
- Inbäddad bedömning.
- SCADA-grundprinciper och Robust-kontrollsystem

# 4. Det allra senaste och trender inom cybersäkerhet i smarta nät

## 4.1 Kategorisering

Google Scholar och Microsoft Academic används för att samla in relevanta studier från 2017–2020 genom att använda nyckelorden ”cybersäkerhet” och ”smarta nät”. Resultaten framgår av titeln och även av studiernas innehåll, vilka bestod av cirka 164 dokument. Alla dessa studier granskas på hög nivå för att välja relevanta studier som rör cybersäkerhet och smarta nät. Därefter kategoriseras de valda undersökningarna med hjälp av ACM:s cybersäkerhetsram enligt Figur 3. Varje vald studie granskas i detalj för att identifiera undersökningens syfte, metod och resultat. Ju högre antal, desto fler studier fokuserade på området. Det bör noteras att en studie kan omfatta mer än en aspekt.




Figur 3 Kategorisering av kompetensbrister baserat på litteraturöversikten

Det är uppenbart att fokus på organisationssäkerhet, mänsklig säkerhet och samhällssäkerhet är mycket lågt jämfört med systemsäkerhet, anslutningssäkerhet och komponentsäkerhet. Utredningen av säkerheten inom teknik, system och komponenter utförs med hjälp av specifika testbeds och/eller CPES-laboratorier (cyberfysiskt energisystem) för experimentet och/eller för undervisning av studerande.

## 4.2 Utveckling av teknik och utbildning

### 4.2.1 Cybersäkerhetshot i smarta nät

En CPES omfattar flera områden inom teknik- och kommunikationsdiscipliner som kräver relevanta kursplaner och nödvändiga verktyg för att identifiera sårbarheter. För att förhindra tidigare och nya cyberattacker i framtiden är det mycket viktigt med passiva och aktiva motåtgärder. Systemansvariga och operatörer kräver en testbed i en realistisk miljö för att undersöka verkliga scenarier och motåtgärder. Cyberattacker inbegriper nätverksanslutna enheter vars programvara infekteras av skadlig kod. Under de senaste åren har det förekommit många cyberattacker mot smarta nätsystem. Dessa cyberattacker kan ske medvetet eller omedvetet och påverka konfidentialitet, integritet och tillgänglighet (CIA). Cyberattackklassificeringen med hänsyn till CIA-aspekten finns i Tabell 1.

Tabell 1 Klassificering av cyberattacker med beaktande av CIA

| Cyberattacktyp | Kort beskrivning | Exempel |
|---|---|---|
| Konfidentialitet | Skydd av uppgifter genom att förhindra obehörigt utlämnande av information | Man-in-the-middle, Stuxnet, kampanj med nätfiske, SQL-injektionsattack, Side-channel-attack, utökning av rättigheter, AES Cache-Timing Attack |
| Integritet | Avlyssning och ändring av meddelande | Injicering av falska data, Load Altering-attack, kampanj med nätfiske, Manipulering |
| Tillgänglighet | Antingen blockera eller försena meddelandet/trafiken | Dos/DDoS, Utpressningsprogram, Blockeringsattack, utökning av rättigheter, AES Cache-Timing Attack, Buffertöverskridning |

### 4.2.2 Motåtgärder

Det finns ingen enda motåtgärd för att möta alla attacker. Varje attack kräver motåtgärder beroende på kontexten för attacken. Flera typer av forskning om cybersäkerhet i det smarta nätet har föreslagit gemensamma motåtgärder såsom intrångsdetekteringssystem (IDS), demilitariserade zoner (DMZ), hårdvaruräknare (HPC), interlock, logghantering, multifaktorautentisering, aktiv nätverksövervakning, IP-adress och appvitlistor, nätverkssegmentering och smarta switchar/routrar, utbildning i säkerhetsmedvetenhet.

### 4.2.3 Laboratorium för cyberfysikaliska energisystem (CPES)

Hittills har universiteten, regeringen och industrin inrättat testbeds för att experimentera med cybersäkerhetsforskning och cybersäkerhetsutveckling. Cybersäkerhetsfrågor är komplexa och omfattar flera kunskapsbakgrunder, t.ex. datateknik, elteknik och industriteknik. Sammanlänkning mellan domäner gör det möjligt för yrkesverksamma att förstå och få en bred överblick över hur olika domäner är sammankopplade. En testbed med flera syften och domäner har en större fördel jämfört med att ha ett enda syfte och/eller en enda domän. En enkel och billig testbed gör det möjligt för studerande att återskapa och utforska de grundläggande principerna om cybersäkerhet. Ett sofistikerat laboratorium är kostsamt, ett samarbete mellan industrin och universitetet kan påskynda en toppmodern, innovativ forskning.

### 4.2.4 Kommunikationsprotokoll

Forskning och utbildning om cybersäkerhet fokuserar också på kommunikationsprotokollen mellan enheterna och/eller systemen. Protokollen testas i laboratoriet och i en särskild testbed. Det är viktigt att ha standardprotokoll, som definierar vissa regler för kommunikationen, för all dataöverföring inom ett nätverk. Det finns flera kommunikationsprotokoll som använts i smarta nät beroende på fördröjning, tillförlitlighet, datahastighet, skalbarhet och säkerhet. IEC 61850 möjliggör samverkan mellan olika komponenter och funktioner från olika tillverkare.

Eftersom IEC 61850 blir alltmer populärt i elautomationssystem, på grund av den enkla anslutningen via Ethernet och standardiserade meddelandestrukturer, har man påpekat sårbarheten för att få tillgång till konfidentiella data och störa tjänsten på grund av datautbytets integritet. För att stärka cybersäkerheten i energikommunikation kan IEC 62351 ge fullständig informationssäkerhet för styrfunktioner av energisystem. I direktivet fastställs olika krav för säker datakommunikation och databehandling i energisystem. Standarden IEC 62351 fokuserar på säkerheten för IEC TC 57-protokoll som kan stödja autentisering och kryptering. IEC 62351 kan säkra IEC61850-meddelanden som GOOSE, SV, R-GOOSE, R-SV.

## 4.3 Analys av luckor

Energisystemet är komplext och hanterar olika enheter och protokoll. Den testbed som universitetet utvecklat saknar oftast verklig praxis från industrin. För att utbilda studerande och yrkesutövare måste en testbed installeras och utrustas med inbyggda komponenter och en realistisk miljö för att genomföra helhetsexperimentet med flera domäner. Sammanfattningen av analysen av luckor i det befintliga CPES-laboratoriet och/eller testbed visas i Tabell 2.

Tabell 2 Analys av luckor för befintligt CPES-laboratorium/testbed

| Aspekt | Analys av luckor |
|---|---|
| **Syfte** | Begränsad analys av en enda domän, antingen energisystem eller kommunikationsnätverk |
| **Trovärdighet** | Ren simulering testbed<br>Brist på intensiv kunskap om ICS-komponenter, fysisk process och praktiskt genomförande |
| **Tillgänglighet** | Endast fysisk åtkomst<br>Brist på stöd för gränssnittsplattformar |
| **Flexibilitet** | Bristande flexibilitet för att välja mellan simulering och fysiska processer<br>Det går inte att konfigurera den verkliga komponenten på grund av det äganderättsligt skyddade protokollet<br>Bristande förmåga att integrera olika simulatorer |
| **Skalbarhet** | Bristande förmåga att skala upp experimentet på grund av begränsade resurser |
| **Användarvänlighet** | Flera programmeringsverktyg<br>Brist på GUI |
| **Kostnadseffektivitet** | Höga investeringskostnader för verklig/fysisk utrustning och komponenter |
| **Möjlighet att upprepa** | Låg granulering av testbed-arkitektur för repeterbarhet och tillförlitlighet<br>Osäkerhet i mätningar<br>Kan inte upprepas på grund av äganderättsligt skyddad industriell process |
| **Standard och protokoll** | Bristande stöd för olika maskinvaru- och kommunikationsprotokoll<br>Kräver en ny ICS-testbed som kombinerar nya och gamla protokoll<br>Avsaknad av IoT-gateway och verkliga enheter |
| **Kunskap** | Brist på tvärvetenskaplig bakgrund, har endast datorteknisk eller elteknisk bakgrund |

Från de cyberattacker som världen hittills har upplevt har hotaktörernas tekniska kapacitet utvecklats avsevärt. Därför måste den kritiska infrastrukturen i det smarta nätet kunna upptäcka och återhämta sig från en cyberattack. Tabell 3 identifierar cybersäkerhetsluckor i CPES enligt CPES-applikationen.

Tabell 3 Cybersäkerhetsrisker i CPES

| Område/applikation | Cybersäkerhetsrisk |
|---|---|
| **Gränsskydd** | - Oupptäckt obehörig aktivitet i kritiska system<br>- Svagare gränser mellan ICS och företagsnätverk. |
| **Tilldelning av resurser** | - Ingen reservpersonal eller alternativ personal som kan fylla positionen om den primära inte kan arbeta<br>- Förlust av kritisk kunskap om kontrollsystem |
| **Kontohantering** | - Äventyrad oskyddad lösenordskommunikation<br>- Äventyrande av lösenord kan tillåta obehörig åtkomst till system |
| **Identifiering och autentisering** | - Bristande ansvarsskyldighet och spårbarhet för användaråtgärder om ett konto äventyras<br>- Ökade svårigheter med säkerhetskonton när personalen lämnar organisationen, särskilt känsligt för användare med administrativ åtkomst. |
| **Fysisk åtkomstkontroll** | - Obehörig fysisk åtkomst till fältutrustning och placeringar ger ökad möjlighet att:<br>o Illvilligt ändra, ta bort eller kopiera program och inbyggd programvara<br>o Komma åt ICS-nätverket<br>o Stjäla eller vandalisera cybertillgångar<br>- Lägga till falska enheter för att fånga och återöverföra nätverkstrafik |
| **Minsta funktionalitet** | - Ökade vektorer för illvilliga parters åtkomst till kritiska system.<br>- Otillåtet internt tillträde har fastställts |

# 5. Den senaste tekniken inom utbildning i smarta nät och cybersäkerhet

## 5.1 Studieprogram för högre utbildning

Totalt 84 universitet som erbjuder studieprogram inom säkerhetsrelaterad IT undersöktes. Från listan motsvarar 14 av 84 universitet inte de allmänna kriterierna. Särskilda studieprogramkriterier med cybersäkerhet, studier i informationsteknik, datavetenskap eller informatik ger dock inga djupa kunskaper om cybersäkerhet. Den tekniska utvecklingen av cybersäkerhetsutbildningen påskyndas, men i allmänhet är anpassningen av kursplanerna vid universiteten långsam. Att överbrygga klyftan mellan industrins behov och utbildningsresultat, när det gäller de blivande forskarna och ingenjörerna, är alltid en utmaning. En av de viktigaste åtgärderna är att regelbundet se över kursplanerna för att förbättra den aktuella kontexten och undervisningsmetoderna.

## 5.2 Program för vidareutbildning

Det finns yrkesutbildningskurser [6] som försöker förbereda studerande och yrkesutövare för karriärer inom det framväxande området cybersäkerhet i smarta nät. Olika specialiserade certifieringskurser gör det möjligt att öka specialisternas kompetens, förmågor och färdigheter och presentera ett specifikt kunskapsområde. En studie [7] har visat att många länder erbjuder

en högre täckning av kunskapsenheterna. Till exempel täcker Spanien, Frankrike, Tyskland och Italien 75 % av kunskapsenheterna (KE) med obligatoriska kurser. Landets storlek är dock inte en avgörande faktor [7]. Tillgången till och främjandet av olika yrkespraxis kan observeras, vilket gör det möjligt att utöka kunskaperna och stärka den tekniska specifika erfarenhet som industrin i allmänhet kräver.

### 5.3 Storskaliga öppna nätkurser (MOOC)

Nätkurser blir alltmer populära när de når ut till fler människor. Det finns tillgängliga nätkurser om cybersäkerhet via edX. De tillgängliga utbildningskurserna i cybersäkerhet är dock ordnade på basis av ämnet i stället för använda verktyg, vilket gör det svårt för studerande att utöva specifik kunskap om cybersäkerhet. Storskaliga öppna nätkurser (MOOC) har fortfarande utrymme att utveckla sin kapacitet inom cybersäkerhet och utbildning i smarta nät. Detta kan göras genom att ge praktiska exempel som studerandena har möjlighet att uppleva verkliga laboratorier, dvs. simuleringar i realtid.

## 6. Identifiering av kompetensbrister i cybersäkerhet i smarta nät

För att uppnå en bättre förståelse för den verkliga situationen för industrin och den akademiska världen genomförde vi en virtuell workshop för att sprida resultaten av litteraturöversikten och tillhandahålla ett sammanhang för att diskutera nödvändiga verktyg och färdigheter för cybersäkerhetsämnet på energiområdet. Tabell 4 visar resultatet av workshoppen för berörda parter. De förslag som samlats in från workshoppen visar de grundläggande kunskaperna om cybersäkerhet inom olika områden (t.ex. kommunikationsnät, kritisk infrastruktur). Det krävs mer praktisk erfarenhet, det är nödvändigt att de arbetar mer med olika verktyg för cybersäkerhet i den akademiska världen. Det är viktigt att nämna att det inte räcker med att undervisa och presentera teorin i kursplanerna för kurser i cybersäkerhet för studenter som strävar efter att arbeta inom industrin i framtiden.

Tabell 4 Rekommendation från workshoppen för berörda parter [8]

| Domän | Starta | Fortsätt | Gör mer | Mindre av |
|---|---|---|---|---|
| **Den akademiska världen** | • Överbrygga kunskap om energisystem och kommunikationsinfrastruktur.<br>• Designa, utveckla och övervaka proaktiva åtgärder och strategier för cybersäkerhet.<br>• Anslå mer budget för forskning. | • Testbud.<br>• Nödvändiga verktyg för utveckling och testning<br>• Kunskap om cybersäkerhet inom flera domäner (t.ex. kritisk infrastruktur, kommunikationssystem, kraftsystem.<br>• Praktisk erfarenhet. | • Kännedom om komponenten i energisystemet (RTU, IED, PMU).<br>• Bedriva internationell forskning om cybersäkerhet.<br>• Professionell utbildning.<br>• Certifikat (t.ex. CISM/CISSP/CISA/CEH) | • Endast teori |
| **Industriell** | • Djupgående förståelse för de olika typerna av säkerhetshot | • Självstudier.<br>• Förståelse för flera domäner (t.ex. energisystem, kommunikationsnät).<br>• Zero trust | • Självstudier.<br>• Kännedom om sårbarheter i energisystem och kommunikationsnät.<br>• Användbara mjuka färdigheter.<br>• Lära sig ny teknik.<br>• Kunskap om de mest populära SCADA-plattformarna.<br>• Exempel på konkreta användningsområden<br>• Grundläggande verktyg för hotanalys. | - |

# 7. Identifiering av användbara verktyg för utbildning i cybersäkerhet i smarta nät

## 7.1 Grundläggande verktyg för aktiv inlärning om cybersäkerhet

Det finns många metoder för kunskapsspridning som kan användas på områdena cybersäkerhet i allmänhet och smarta nät i synnerhet. Tabell 5 visar utbildningsstrategier inom smarta nät och cybersäkerhet för att bygga upp djup kunskap om och förståelse för de viktigaste begreppen på området samt de analytiska färdigheter som krävs för fortsatt utveckling.

Tabell 5 Utbildningsstrategier för smarta nät och cybersäkerhet

| Metod | Syfte | Exempelverktyg |
|---|---|---|
| **Fjärrstyrda och virtuella laboratorier** | Självlärande och att skapa en verklighetstrogen interaktion som i klassrummet | Labview, OMWeb, NI ELVIS, Labster, LabAlive |
| **Förstärkt verklighet** | Interaktivt lärande | Worklink, CoSpaces, Merge Cube |
| **Datavisualisering** | Visualisering och analys | Tableau, Microsoft Power Bi, IBM Congos Analytics |
| **Molndatatjänster** | Avancerade algoritmer och funktioner som datautvinning och djupinlärning | Google Classroom, Microsoft Education Center, Amazon Web Services |
| **Omvänt lärande** | Aktivt tekniskt lärande | Storskaliga öppna nätkurser (MOOC) |
| **”Spelifiering” (gamification) och spelteori** | Analys av sannolikhets- och cybersäkerhetsscenarier | Kahoot, Gimkit |
| **Simulering** | Övning och testning av olika fall | MATLAB, Simulink |

## 7.2 Avancerade verktyg för sårbarhetsexperiment

Smarta nätsystem är komplexa då de inkorporerar elnät och kommunikationsnät. Det har förekommit flera cyberattacker på smarta nätsystem under de senaste åren som har orsakat betydande konsekvenser. Störningarna är till sin natur komplexa och kan tillskrivas ett stort antal källor, däribland naturliga händelser och händelser orsakade av människan. Tabell 6 visar avancerade verktyg kategoriserade efter deras funktioner för att hantera och testa sårbarheter.

Tabell 6 Cybersäkerhetsverktyg för smarta nät

| Verktyg | Funktionalitet |
|---|---|
| **Säkerhetsplattform** | Enhetlig säkerhetshantering för att tillhandahålla centraliserad kontroll och åtgärder mot hot som påverkar en organisations infrastruktur |
| **Nätverksövervakning** | Övervakning av nätverkets kvalitet mot fel eller störningar, för att på så sätt säkerställa kontinuitet och prestanda |
| **Sårbarhetsavsökning** | Att skanna olika system och programvarukomponenter i ett försök att identifiera brister och svagheter som kan utnyttjas |
| **Penetrationsprovning** | För att utvärdera systemens säkerhet genom att utnyttja påträffade sårbarheter |

| Verktyg | Funktionalitet |
|---|---|
| **Paketanalyserare och portskannare** | Övervakning av nätverkstrafik, identifiera tjänster som körs och utvärdera säkerhetsprinciper |
| **Kryptering** | För att bevara informationens konfidentialitet och enhetlighet och på så sätt skydda data från obehörig åtkomst |
| **Antivirus** | Identifiera och vidta åtgärder mot skadlig kod och annan olaglig programvara som utpressningsprogram, verk, trojanska hästar osv. |
| **Brandväggar** | För att skydda mot attacker genom att förhindra att skadlig trafik kommer in i ett visst nätverk eller en viss smart enhet |
| **Trådlös säkerhet** | För att förhindra obehörig åtkomst till det trådlösa nätverket och skydda den överförda trafiken genom att säkerställa en hög nivå av datakryptering |
| **Lösenordshantering** | För säker kontroll av konton |

De befintliga avancerade verktygen täcker främst de teknikrelaterade problem som är förknippade med fysiska cybersystem. De avancerade verktygen bör kunna hantera sådana felaktiga och felidentifierade hot samt långsammare detektions- och svarstid. Detta skulle hjälpa studerandena att få praktisk erfarenhet genom aktivt lärande.

# 8. Slutsatser och rekommendationer

Utbildning i cybersäkerhet har identifierats som en strategisk digital färdighet i EU som behöver stärkas genom att tillhandahålla formell och informell utbildning (inklusive yrkesutbildning, fortbildning) och ämnen för praktisk tillämpning (praktik) i FoU-projekt inom organisationer. Cybersäkerhet representeras i olika utbildningsformer, såsom högre utbildning, livslångt lärande och MOOC-utbildningar. De viktigaste kraven för att förbättra läroplanerna för cybersäkerhet för utveckling av smarta nät är följande:

- Utbildning måste vara tillgänglig för olika grupper av EU-medborgare (inklusive företag, chefer på C-nivå, vuxna som vill öka sin kompetens och skola om sig och för nya specialister).
- Det är rekommenderat att tillhandahålla cybersäkerhetsavstånd, onlinemöjligheter och blandade möjligheter för utbildning för att göra kompetenshöjning och omskolning mer tillgänglig för vuxna.
- Utbildningen måste behandla allmänna grunder i cybersäkerhet och branschspecifika ämnen (som cybersäkerhet i energiförsörjningskedjan och verktyg/metoder och åtgärder för att övervaka och kontrollera den).
- Den måste tillhandahålla teoretiska föreläsningar och praktisk utbildning, som användning av verktyg för hantering av cybersäkerhet och virtuella laboratorier, och utföra simuleringar och experiment med digitala tvillingar och liknande miljöer. Inom utbildning i cybersäkerhet i smarta nät är både specifika cybersäkerhetsverktyg kopplade till smarta nät, och verktyg för övervakning av energiska domänkontrollanter lika viktiga.
- Utbildningsprogram måste utvecklas i samarbete med relevanta partners (t.ex. universitet och företrädare för näringslivet).
- I program för cybersäkerhet i smarta nät bör uppmärksamhet ägnas åt alla dessa områden [9]: Sekretess, integritet och tillgänglighet (inklusive prestanda och aktualitet) samt dataskydd (kombination av organisation, integritet och konfidentialitet) och oavvislighet (t.ex. elektroniska kontrakt). Därför är

tillämpningsområdet bredare än enbart datasäkerhet, eftersom det bara är en av säkerhetsaspekterna (även om den är viktig) när smarta nät implementeras i Europa.

- Teman för cybersäkerhet bör integreras som en obligatorisk del av energistudieprogrammen.
- För att göra utbildning i cybersäkerhet mer interaktiv och attraktiv för studerande rekommenderas att man integrerar spelelement, såsom hotspel, cyberintervall och escape rooms för cybersäkerhet.
- Studerandena bör ha tillgång till infrastrukturer för simulering i realtid och praktiska scenarier samt till grundläggande och avancerade verktyg för aktivt lärande.
- Inom ramen för relevant högre cybersäkerhetsutbildning bör studentutbyten betraktas som en del av programmet.

# 9. Litteraturförteckning


[1] Europeiska kommissionen, den reviderade handlingsplanen för digital utbildning. Europeiska kommissionen, 2020.

[2] Europaparlamentet, Cybersäkerhetsakten, 2019.

[3] Europeiska kommissionen, EU:s ramverk för cybersäkerhetscertifiering.

[4] J. T. F. om utbildning i cybersäkerhet, riktlinjer för kursplaner i eftergymnasiala utbildningsprogram i cybersäkerhet. Association for Computing Machinery, 2017.

[5] Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) https://tcipg.org/.

[6] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, “Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application,” i 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, 2014.

[7] N. Dragoni, A. Lluch Lafuente, F. Massacci and A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]," i IEEE Security & Privacy, vol. 19, no. 1, pp. 81-88, Jan.-Feb. 2021, doi: 10.1109/MSEC.2020.3037446

[8] B. Siemers et al., "Modern Trends and Skill Gaps of Cyber Security in Smart Grid: Invited Paper," IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, 2021, pp. 565-570, doi: 10.1109/EUROCON52738.2021.9535632.

[9] Europeiska kommissionen, Europeiska kommissionens expertgrupp för säkerhet och motståndskraft i kommunikationsnät och informationssystem för smarta nät. Europeiska kommissionen, 2019.