FOI Memo

Projekt
AI:s påverkan på förutsättningar för informations- och cybersäkerhet

Sida
1 (10)

Uppdragsnummer
E64087

Uppdragsgivare
Myndigheten för samhällsskydd och beredskap

Forskningsområde
Ledningsteknologi

Handläggare
Teodor Sommestad, Joel Brynielsson, Stefan Varga

Datum
2019-05-31

Memonummer
FOI Memo 6737

Möjligheter för automation av roller inom cybersäkerhetsområdet

1 Inledning

Autonoma lösningar har påvisat stor potential inom cybersäkerhetsområdet. Att både informationsinhämtning och många andra arbetsmoment i cyberdomänen, särskilt sådana som inte innefattar fysisk aktivitet, i sin helhet kan lösas i cyberdomänen, gör det relativt enkelt att skapa autonoma lösningar. En annan faktor som talar för autonomi är att mänskligt beslutsfattande omöjliggörs då händelser inom cybersäkerhetsområdet ibland sker under mycket snabba tidsförlopp; någon form av autonomi blir därmed nödvändig, och detta särskilt om en stor mängd beslut är av denna karaktär. Ytterligare en faktor är att autonoma lösningar kan kopieras, vilket gör dem kostnadseffektiva. Redan nu finns autonoma lösningar (t.ex. brandväggar och datorvirus), och även flera av de mer kvalificerade och krävande uppgifterna (t.ex. intrångsdetektion och kodtestning) är delvis automatiserade. Tänkbara konsekvenser av ytterligare automation inkluderar:

- att de med mest kraftfull automation får en allt mer dominant roll inom cyberdomänen
- att komplicerade cyberoperationer kan utföras även av små aktörer utan stora resurser, och
- att vissa yrkesroller helt kan automatiseras eller avsevärt förenklas.

Även om ökad automation i vissa fall är eftersträvansvärd finns det många hinder på vägen dit. Intrångsdetektion är ett exempel på ett cybersäkerhetsproblem där många forskningsansatser gjorts för att på olika sätt kunna ersätta mänsklig analys, men med begränsad framgång. Studien som avrapporteras i det här memot syftar till att bedöma den framtida utvecklingen inom området, och om och i vilken grad cybersäkerhetsarbete kommer att kunna automatiseras. Mer konkret svarar studien på följande delfrågor:

1. Vilka variabler påverkar hur svår en cybersäkerhetsroll är att automatisera?
2. Hur troligt är det att olika cybersäkerhetsroller som finns i dag kommer att automatiseras?
3. Vilka variabler begränsar potentialen att automatisera nuvarande cybersäkerhetsroller?

Utgångspunkten för analysen är det ramverk över cybersäkerhetsarbete som tagits fram av U.S. National Institute of Standards and Technology (NIST) som kallas för National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse, Keith, Scribner & Witte, 2017). Ramverket beskriver roller inom cybersäkerhetsområdet genom att specificera vilka uppgifter som utförs samt vilka kunskaper, förmågor och skicklighet dessa uppgifter kräver.

2 Variabler som påverkar graden av möjlig automation

Trots att automation är något som är centralt för ingenjörer, går det inte att finna någon empirisk forskning som entydigt pekat på vilka förutsättningar som gör att en uppgift är lätt eller svår att automatisera. Det går till exempel inte att finna retrospektiva studier av misslyckade automationsförsök i vilka orsakerna till resultaten identifierats. Det tidigaste försöket att skapa ett komplett bedömningskriterium som identifierats, är det som tagits fram av Frey och Osborne (2017). De utgick från variabler i U.S. Department of Labors Occupational Information Network (O*NET) som är ämnade

att beskriva krav kopplade till olika yrken. De lät vidare en panel av maskininlärningsforskare bedöma om 70 slumpvis valda yrken gick att automatisera. Panelen tittade på yrkesbeskrivningarna och svarade på frågan: ”Can the tasks of this job be sufficiently specified, conditional on the availability of big data, to be performed by state of the art computer-controlled equipment?” De använde sedan dessa bedömningar som baslinje och skapade en regressionsmodell för att skatta hur viktiga de olika O*NET-variablerna var. I arbetet identifierades följande variabler som relevanta för att kunna bedöma om ett yrke är tekniskt möjligt att automatisera givet att data finns tillgängligt (vår översättning):

- fingerfärdighet, funktionell förmåga att använda armar och händer, och förmåga att verka i trånga arbetsutrymmen eller med kroppen i besvärliga positioner
- originalitet (t.ex. kreativ problemlösning) och konstnärlighet, samt
- social uppfattningsförmåga, förhandling, övertalning, och assistans och omhändertagande av andra.

Den första punkten abstraherades till en variabel de gav namnet ”uppfattning och händighet”, den andra till ”kreativ intelligens” och den tredje till ”social intelligens”. Vissa av sambanden, t.ex. kopplingen till krav på originalitet, var olinjära.

3 Tekniska hinder och flaskhalsar för automation

Tekniska hinder och flaskhalsar för automatisering inom cybersäkerhetsområdet kan handla om:

- att det är stor variation avseende vad som ska bedömas eller göras (som i nätverkstrafiks varierade innehåll avseende olika protokoll etc.)
- att situationer kopplade till cybersäkerhet har gråskalor som är svårtolkade och svåra att beskriva distinkt (som vad som utgör en hotfull anomali i ett datornätverk eller vad som är ett rimligt mjukvarubeteende)
- att det saknas realistiska data som är strukturerade i olika klasser (som i inspelad nätverkstrafik med okända angrepp) eller att forskningen inte förmår skapa sådana data (som för sårbarhetsbedömningar), och
- att automation ibland kan ge bättre säkerhet men samtidigt medför merarbete med att instrumentera verktyg (som i fallet med formella verifieringsmetoder).

I viss utsträckning kan ovanstående problem ha att göra med att cybersäkerhetsarbete inte professionaliserats och strukturerats i lika stor utsträckning som andra yrkesområden. Inom flygledningsområdet finns exempelvis manualer på hundratals sidor som beskriver vad som kännetecknar olika situationer och anger hur flygledare ska agera. Även andra aspekter inom flygnäringen är strikt reglerade i grunden, detta för att t.ex. möjliggöra regionalt, nationellt och internationellt samarbete. Flygbranschen har ett universellt mål som alla är överens om, nämligen att minimera dödsfall och olyckor. Inom cybersäkerhet finns förvisso manualer för sådant som incidenthantering, men dessa har inte alls samma detaljeringsgrad som flygledningsmanualerna utan beskriver processer och analyssteg som bör genomföras. Inom flygledning görs också utredningar efter incidenter, och incidenter sammanställs i incidentdatabaser. Inom cybersäkerhet finns incidentdatabaser, men de täcker inte in alla incidenter som sker, eftersom vissa angrepp inte upptäcks, och har inte heller den detaljrikedom som skulle

behövas. Vidare finns det för cyberområdet inte någon global konsensus om målsättningar. Även om alla aktörer sannolikt vill säkra sina egna system, finns det ändå motsättningar då några också vill utnyttja sårbarheter i system för egen vinning.

4 Metod

I denna studie används ramverket National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse m. fl., 2017), framtaget av amerikanska U.S. National Institute of Standards and Technology (NIST), som referens för det arbete som utförs (eller bör utföras) för att åstadkomma cybersäkerhet. Det finns många tänkbara alternativ till detta ramverk som också kan användas, t.ex. standarder och handböcker över informationssäkerhet, men NICE-ramverket har flera fördelar jämfört med andra alternativ:

- det har en bred förankring då det är framtaget och utgivet av en myndighet i samverkan med industrin
- det är regelbundet uppdaterat och nyligen justerat
- det används som referens för annat arbete, som utbildningsprogram och för rekrytering, och
- det är synnerligen detaljerat och i huvudsak välstrukturerat.

Till nackdelarna hör att det är ett amerikanskt ramverk som inte nödvändigtvis passar svenska förhållanden. Det finns också enstaka kvalitetsbrister i dokumentet.

Innehållet i NICE-ramverket kan utnyttjas på flera olika sätt. Det innehåller en klassificering i sju kategorier som beskriver den högsta nivån inom vilken säkerhetsarbete genomförs, 33 specialistområden inom vilka personer kan jobba och 52 distinkta roller som personer kan ha. Varje roll är dessutom kopplad till ingående uppgifter, kunskapskrav, färdigheter och förmågor som en person som ska bemästra rollen bör ha. I den version av ramverket som används i denna studie listas totalt 1006 uppgifter, 589 kunskaper, 365 färdigheter och 176 förmågor.

I likhet med tidigare studier, se t.ex. Frey och Osborne (2017), fokuserar denna studie på de färdigheter och förmågor som är kopplade till specifika uppgifter. Det är dessa som sedan ligger till grund för bedömningar om hur lätt eller svårt det är att automatisera olika roller och specialistområden.

I tidigare forskning är man relativt överens om vilka faktorer som påverkar ifall en uppgift är enkel eller svår att automatisera (Frey & Osborne, 2017). De kriterier som används i denna studie åskådliggörs i tabell 1, och ligger också i linje med dessa faktorer. De första tre kriterierna speglar de automatiseringsbarriärer som Frey och Osborne (2017) använde, medan det fjärde kriteriet används för att gradera Frey och Osbornes antagande om datatillgänglighet. Förmågorna och färdigheternas karaktär bedömdes utifrån dessa fyra kriterier på en skala från ett (1) till fem (5), där ett (1) innebär att uppgiften är enkel att automatisera och fem (5) att uppgiften är svår att automatisera. Utöver detta bedömdes om beskrivningen av den aktuella bedömda förmågan eller färdigheten i NICE-ramverkets terminologi överhuvudtaget gick att förstå av bedömarna.

De 541 beskrivningarna (176 förmågor och 365 färdigheter) som den analyserade versionen av NICE-ramverket innehöll, extraherades och bedömdes av fyra forskare: (i) en doktor och forskningsledare inom cybersäkerhetsområdet, (ii) en docent och laborator inom beslutsstödssystem, (iii) en doktorand och officer inom cybersäkerhetsområdet med bakgrund från underrättelsedomänen, och (iv) en juris kandidat inriktad mot cyberoperationer.

Bedömningsarbetet inleddes med en kalibreringsrunda där 30 slumpvis valda beskrivningar bedömdes av de fyra forskarna oberoende av varandra. Bedömningarna

K	Förmågans eller färdighetens karaktär	Enkel att automatisera (1)	Svår att automatisera (5)
1	Krav på kreativitet	Det finns bara ett (naturligt) sätt att utföra uppgiften på som ej varierar över tid.	Uppgiften kan kräva att handlingsalternativ ingen tidigare tänkt på identifieras och tillämpas.
2	Krav på social interaktion	Kräver inte någon form av interaktion med människor.	Kräver situationsanpassad och/eller dynamisk interpersonell kommunikation med nyanser.
3	Krav på fysiskt arbete	Kan lösas helt inom en dator. Kräver inget fysiskt arbete.	Kräver varierat finmotoriskt arbete med liten tolerans för fel.
4	Existerande statistiskt underlag	Högkvalitativt underlag i tillräcklig mängd är tillgängligt. Data framtagen för att beskriva eller dokumentera arbetet finns.	Underlag finns ej, eller finns i mycket begränsad omfattning. Det finns ytterst få fall att lära sig av.

Tabell 1: Kriterier (K) använda för att gradera förmågor och färdigheter, och fall som motsvarar enkla respektive svåra automationsförutsättningar.

genomfördes på olika fysiska platser och ingen kommunikation om bedömningsarbetet förekom under denna fas. För att göra bra bedömningar fick forskarna i flera fall gå tillbaka till mer omfattande bakgrundsskrivningar i NICE-ramverket för att få förståelse för i vilken kontext de olika förmåge- och färdighetsbeskrivningarna hörde hemma. Korrelationskoefficienten mellan bedömningarna som genomfördes under kalibreringsrundan var överlag positiv (t.ex. 0,30–0,60 för kriteriet ”krav på social interaktion”), men den visade också på vissa skillnader mellan hur de fyra bedömarna tolkade och tillämpade kriterierna. Här var skillnaderna störst när det gällde kriteriet ”krav på kreativitet”. Alla upptäckta skillnader och resultatet av kalibreringsrundan i allmänhet diskuterades under ett seminarium där alla fyra bedömarna deltog.

Efter kalibreringen vidtog huvudarbetet med bedömningen av samtliga 541 beskrivningar enligt en skala som efter seminariet förfinades och preciserades. Trots diskussioner och korrigeringar under seminariet kvarstod skillnader mellan bedömarnas syn. Medelavvikelserna var i snitt 0,6 för krav på kreativitet, 0,5 för krav på social interaktion, 0,1 för krav på fysiskt arbete och 0,7 för existerande statistiskt underlag. Korrelationskoefficienterna varierade mellan 0,24 och 0,76, med ett medelvärde på 0,45. Det ska här poängteras att skillnaderna mellan bedömningarna troligen inte föranletts av en bristfällig metod, utan är en naturlig följd av att de fyra bedömarna har olika kompetens och bakgrund. Medelvärdet av de fyra bedömningarna kan antas vara en approximation av förmågans/färdighetens förutsättningar gjord utifrån flera olika sätt att se på färdigheterna och förmågorna.

Efter bedömningarna fanns för var och en av förmågorna och färdigheterna en gradering av hur stora krav de ställer på kreativitet, social interaktion och fysiskt arbete, samt hur svårt det är att skapa statistiska underlag som kan användas för att med maskininlärning (eller liknande) träna en dator att utföra uppgiften enligt bedömarna. Medelvärden användes för att erhålla ett enhetligt svar från panelen. Dessa värden ger

i sig en indikation på vad som är lätt och svårt att automatisera. Förmågan ”[a]bility to operate common network tools (e.g., ping, traceroute, nslookup)” får t.ex. lägre värden än färdigheten ”[s]kill to analyze strategic guidance for issues requiring clarification and/or additional guidance” på alla fyra kriterier, och har därmed färre hinder för automation. Medelvärdet av de olika bedömningarna kan tas som en indikation på om en förmåga eller färdighet kan utföras av en dator. Av flera skäl förtäljer inte nödvändigtvis detta medelvärde hela historien, och därför gjordes utöver medelvärdesanalysen också beräkningar enligt andra modeller. Totalt användes fem olika modeller som alla behandlar de bedömda numeriska värdena $k_1, \ldots, k_4$ för de fyra kriterierna på olika sätt enligt tabell 2.

Modell	Förklaring	Formell beskrivning
1	Effekten är enkel, additiv och linjär. Summan av de fyra kriterierna används.	$\sum_{i=1}^{4} k_i$
2	Effekten är exponentiell. Summan av exponentialfunktioner för de fyra kriterierna används.	$\sum_{i=1}^{4} 2^{k_i}$
3	Interaktioner gör det betydligt svårare om flera olika hinder behöver överkommas. Produkten av de fyra kriterierna används.	$\prod_{i=1}^{4} k_i$
4	Tillgång till statistiska data (k_4) begränsar hur mycket de andra kriterierna påverkar.	$\sum_{i=1}^{3} \min(k_i, k_4)$
5	Det högsta värdet för de olika kriterierna är avgörande/begränsande.	$\max_{i=1,\ldots,4} k_i$

Tabell 2: De fem olika modeller som användes för att bedöma automatiserbarhet.

5 Resultat

Det mest detaljerade resultatet som presenteras i detta memo återges i tabell 3, i vilken det redovisas hur automatiserbara rollerna i NICE-ramverket bedöms vara enligt de olika modellerna. Färgerna, vilka baseras på ett medelvärde av de fem modellernas resultat, visar hur lätta (gröna) och svåra (röda) de olika rollerna är att automatisera. I tabellen framgår också resultaten för de fem modellerna var för sig.

Resultatet aggregerat på specialistområden redovisas i tabell 4. Här framgår vissa mönster tydligare:

- rent tekniska uppgifter såsom databasadministration (t.ex. ”Data Administration”), nätverksadministration (t.ex. ”Cyber Defense Infrastructure Support”) och programmering (t.ex. ”Software Development”) är förhållandevis enkla att automatisera
- uppgifter som kräver teknisk kunskap men också är analytiska (t.ex. ”Systems Development”) eller som kräver koordinering med andra funktioner (t.ex. ”Cybersecurity Management”) hamnar i mitten av skalan
- områdena underrättelseinhämtning (t.ex. ”Collection Operations”) och underrättelsebearbetning (t.ex. ”Threat Analysis”) är förhållandevis svåra att automatisera
- områden som är förknippade med mycket ansvar (t.ex. ”Executive Cyber Leadership”) som regelmässigt kräver beslut där många komplexa frågor ska vägas samman (t.ex. ”Legal Advice and Advocacy”) är allra svårast att automatisera.

Roll	Medel	Modell 1	2	3	4	5
Database Administrator (OM-DTA-001)	1.00	1.00	1.00	1.00	1.00	1.00
Data Analyst (OM-DTA-002)	1.13	1.07	1.16	1.27	1.04	1.13
Network Operations Specialist (OM-NET-001)	1.27	1.10	1.21	1.82	1.07	1.16
Cyber Operator (CO-OPS-001)	1.34	1.17	1.29	1.86	1.13	1.24
Software Developer (SP-DEV-001):	1.41	1.21	1.35	1.99	1.16	1.31
Cyber Defense Infrastructure Support Specialist (PR-INF-001)	1.42	1.20	1.34	2.14	1.18	1.23
Cyber Defense Analyst (PR-CDA-001)	1.45	1.22	1.39	2.18	1.19	1.27
Secure Software Assessor (SP-DEV-002)	1.47	1.24	1.41	2.18	1.18	1.34
Cyber Defense Incident Responder (PR-CIR-001)	1.49	1.25	1.41	2.21	1.22	1.33
Cyber Defense Forensics Analyst (IN-FOR-002)	1.53	1.23	1.40	2.51	1.18	1.34
Communications Security (COMSEC) Manager (OV-MGT-002)	1.56	1.26	1.52	2.46	1.22	1.33
Forensics Analyst (IN-FOR-001)	1.57	1.24	1.42	2.63	1.19	1.35
System Administrator (OM-ADM-001)	1.59	1.25	1.46	2.72	1.21	1.30
Systems Developer (SP-SYS-002)	1.65	1.33	1.57	2.60	1.26	1.47
System Test & Evaluation Specialist (SP-TST-001)	1.68	1.33	1.56	2.81	1.28	1.44
Systems Security Analyst (OM-ANA-001)	1.72	1.35	1.66	2.83	1.27	1.49
Cyber Crime Investigator (IN-INV-001)	1.75	1.36	1.62	3.02	1.29	1.48
Exploitation Analyst (AN-EXP-001)	1.76	1.34	1.67	3.04	1.28	1.46
Vulnerability Assessment Analyst (PR-VAM-001)	1.77	1.37	1.64	3.06	1.31	1.46
Research and Development Specialist (SP-TRD-001)	1.78	1.38	1.66	3.03	1.32	1.51
Security Architect (SP-ARC-002)	1.90	1.39	1.76	3.51	1.33	1.50
Knowledge Manager (OM-KMG-001)	1.90	1.37	1.72	3.66	1.35	1.41
Information Systems Security Developer (SP-SYS-001)	1.95	1.43	1.81	3.59	1.38	1.55
Systems Requirements Planner (SP-SRP-001)	1.96	1.45	1.74	3.69	1.43	1.49
Cyber Instructor (OV-TEA-002)	1.98	1.42	1.85	3.77	1.36	1.51
Enterprise Architect (SP-ARC-001)	2.01	1.46	1.84	3.80	1.40	1.57
Product Support Manager (OV-PMA-003)	2.03	1.48	1.83	3.83	1.43	1.58
Technical Support Specialist (OM-STS-001)	2.04	1.47	1.99	3.72	1.38	1.61
Security Control Assessor (SP-RSK-002)	2.04	1.45	1.90	3.89	1.38	1.57
Target Network Analyst (AN-TGT-002)	2.06	1.46	1.97	3.89	1.40	1.57
IT Program Auditor (OV-PMA-005)	2.06	1.50	1.85	3.90	1.47	1.57
Information Systems Security Manager (OV-MGT-001)	2.08	1.46	1.93	4.01	1.42	1.57
All Source-Collection Manager (CO-CLO-001)	2.08	1.46	1.89	4.07	1.41	1.57
All Source-Collection Requirements Manager (CO-CLO-002)	2.09	1.47	1.90	4.06	1.42	1.58
Multi-Disciplined Language Analyst (AN-LNG-001)	2.10	1.45	1.92	4.14	1.39	1.58
Information Technology (IT) Project Manager (OV-PMA-002)	2.14	1.52	1.90	4.19	1.49	1.59
Program Manager (OV-PMA-001)	2.14	1.52	1.90	4.19	1.49	1.59
Cyber Workforce Developer and Manager (OV-SPP-001)	2.22	1.51	2.08	4.42	1.44	1.65
Target Developer (AN-TGT-001)	2.22	1.52	2.15	4.34	1.44	1.66
IT Investment/Portfolio Manager (OV-PMA-004)	2.32	1.58	2.02	4.82	1.56	1.63
Cyber Instructional Curriculum Developer (OV-TEA-001)	2.33	1.55	2.18	4.76	1.47	1.68
Authorizing Official (SP-RSK-001)	2.37	1.57	2.16	4.90	1.51	1.70
Threat/Warning Analyst (AN-TWA-001)	2.39	1.58	2.32	4.85	1.48	1.73
Mission Assessment Specialist (AN-ASA-002)	2.44	1.60	2.38	4.97	1.51	1.76
All-Source Analyst (AN-ASA-001)	2.47	1.60	2.40	5.05	1.51	1.77
Cyber Policy and Strategy Planner (OV-SPP-002)	2.64	1.65	2.36	5.84	1.61	1.72
Cyber Intel Planner (CO-OPL-001)	2.69	1.67	2.41	5.94	1.61	1.80
Privacy Officer/Privacy Compliance Manager (OV-LGA-002)	2.71	1.68	2.42	6.03	1.63	1.77
Cyber Ops Planner (CO-OPL-002)	2.77	1.70	2.53	6.13	1.62	1.84
Partner Integration Planner (CO-OPL-003)	2.90	1.73	2.64	6.62	1.65	1.86
Executive Cyber Leadership (OV-EXL-001)	3.06	1.78	3.03	6.82	1.69	1.96
Cyber Legal Advisor (OV-LGA-001)	3.16	1.84	2.93	7.25	1.75	2.02

Tabell 3: Roller i NICE-ramverket. Siffrorna ska läsas som ett relativt mått på hur lätt det är att automatisera specialistområdet relativt andra roller. Den roll som är enklast att automatisera inom respektive modell har index 1,0.

Dessa tendenser kan skönjas oavsett vilken modell som används.

Det finns totalt $5^4 = 625$ möjliga kombinationer av de fyra kriterierna. Var och en av dessa kombinationer kan ses som ett scenario (en hypotetisk situation) där automatiseringsmöjligheterna nått en viss nivå. Denna nivå manifesteras i dessa scenarion av vilka värden (1–5) våra fyra bedömningskriterier i tabell 1 antar. Det är exempelvis tänkbart att forskning och teknikutveckling nått eller når en sådan nivå att det blir möjligt att generellt möta:

- nivå tre på kreativitet, där flera variabler behöver vägas samman och osäkerhet behöver hanteras (t.ex. rikta reklam till rätt användare)
- nivå tre på social interaktion, vilket kan innebära att datorer kan tolka enklare kommunikation (t.ex. sammanfatta en talad konversation i text)
- nivå tre på fysiskt arbete, vilket kan visas genom maskiner som kan manövrera i utrymmen där det finns oregelbundenheter och hinder (t.ex. lagerrobotar

Roll	Medel	Modell				
		1	2	3	4	5
Data Administration (DTA)	1.00	1.00	1.00	1.00	1.00	1.00
Network Services (NET)	1.14	1.04	1.07	1.48	1.04	1.05
Cyber Operations (OPS)	1.20	1.11	1.14	1.51	1.10	1.12
Cyber Defense Infrastructure Support (INF)	1.26	1.13	1.19	1.74	1.15	1.11
Software Development (DEV)	1.28	1.16	1.22	1.68	1.14	1.20
Cyber Defense Analysis (CDA)	1.29	1.15	1.23	1.78	1.15	1.15
Incident Response (CIR)	1.32	1.19	1.25	1.80	1.18	1.20
Digital Forensics (FOR)	1.37	1.17	1.25	2.09	1.15	1.22
Systems Administration (ADM)	1.41	1.18	1.29	2.21	1.18	1.17
Test and Evaluation (TST)	1.49	1.26	1.38	2.28	1.24	1.30
Systems Analysis (ANA)	1.53	1.28	1.46	2.30	1.24	1.35
Cybersecurity Management (MGT)	1.55	1.27	1.48	2.47	1.26	1.28
Cyber Investigation (INV)	1.55	1.29	1.44	2.46	1.25	1.34
Exploitation Analysis (EXP)	1.56	1.27	1.48	2.48	1.24	1.32
Vulnerability Assessment and Management (VAM)	1.57	1.29	1.45	2.49	1.27	1.32
Technology R&D (TRD)	1.58	1.31	1.46	2.46	1.28	1.37
Systems Development (SYS)	1.63	1.32	1.52	2.62	1.29	1.38
Knowledge Management (KMG)	1.67	1.30	1.52	2.98	1.31	1.27
Systems Architecture (ARC)	1.71	1.34	1.58	2.94	1.32	1.38
Systems Requirements Planning (SRP)	1.73	1.38	1.54	3.00	1.38	1.34
Customer Service and Technical Support (STS)	1.80	1.40	1.76	3.03	1.34	1.46
Risk Management (RSK)	1.82	1.38	1.71	3.25	1.35	1.43
Collection Operations (CLO)	1.83	1.39	1.68	3.31	1.37	1.42
Training, Education, and Awareness (TEA)	1.84	1.38	1.73	3.33	1.35	1.42
Language Analysis (LNG)	1.84	1.38	1.70	3.37	1.35	1.43
Project Management/Acquisition and Program (PMA)	1.86	1.43	1.66	3.33	1.43	1.43
Targets (TGT)	1.88	1.41	1.81	3.33	1.38	1.46
Strategic Planning and Policy (SPP)	2.09	1.48	1.94	4.04	1.46	1.51
Threat Analysis (TWA)	2.10	1.49	2.05	3.95	1.44	1.56
All-Source Analysis (ASA)	2.15	1.51	2.11	4.07	1.46	1.59
Cyber Operational Planning (OPL)	2.41	1.60	2.21	5.01	1.57	1.65
Legal Advice and Advocacy (LGA)	2.41	1.61	2.19	5.02	1.59	1.63
Executive Cyber Leadership (EXL)	2.66	1.68	2.68	5.55	1.64	1.77

Tabell 4: Specialistområden i NICE-ramverket. Siffrorna ska läsas som ett relativt mått på hur lätt det är att automatisera specialistområdet relativt andra specialistområden. Den specialitet som är enklast att automatisera inom respektive modell har index 1,0.

som utöver huvuduppgiften klarar av att hantera tillfälliga, oförutsedda hinder i lagret), respektive

- nivå tre på statistiskt underlag, där åtgärder för att strukturera existerande data så att den går att använda enkelt genomförs (t.ex. klassning av stora mängder bilder).

Tabell 5 beskriver hur stor andel av uppgifterna inom respektive kategori i NICE-ramverket som är möjliga att automatisera i 21 systematiskt valda scenarion (av de 625 teoretiskt möjliga). Scenario tre (alla treor) är det scenario som beskrivs i punktlistan ovan. I detta scenario kan följaktligen 61 procent av färdigheterna och förmågorna automatiseras överlag, och hela 83 procent av de i kategorin ”Operate and Maintain”.

Tabell 5 visar förutsättningarna för automatisering givet nivåerna på de olika kriterierna i bedömningsmodellen i olika scenarion. Ur tabellen kan således utläsas vilka av de fyra bedömda kriterierna som har störst inflytande över automatiseringsmöjligheterna. Tabellen visar att kravet på fysiskt arbete är relativt betydelselöst vad gäller möjligheten att automatisera, genom att möjligheterna för automatisering är goda även om det inte finns några möjligheter att utföra fysiskt arbete (scenario 20). Det motsatta gäller för kravet på kreativitet. Det är väldigt svårt att automatisera om inte kravet på kreativitet uppfylls (scenario 18). Sammantaget visar tabellen att kreativitet spelar större roll än fysisk förmåga för möjligheterna att lösa uppgifter inom cybersäkerhets-

Scenario	Tekniken & förutsättningarna				Automatiserbarhet							
	Krav på kreativitet	Krav på social interaktion	Krav på fysiskt arbete	Tillgängligt statistiskt underlag	Totalt	Protect and Defend (PR)	Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Investigate (IN)	Analyze (AN)	Collect and Operate (CO)
1	1	1	1	1	1%	2%	0%	2%	0%	0%	2%	1%
2	2	2	2	2	19%	29%	11%	39%	12%	24%	9%	8%
3	3	3	3	3	61%	82%	62%	83%	47%	67%	49%	37%
4	4	4	4	4	96%	100%	98%	97%	91%	100%	90%	93%
5	5	5	5	5	100%	100%	100%	100%	100%	100%	100%	100%
6	1	2	2	2	2%	2%	2%	4%	1%	4%	3%	1%
7	2	1	2	2	8%	11%	4%	21%	5%	12%	3%	3%
8	2	2	1	2	18%	29%	10%	36%	12%	20%	9%	7%
9	2	2	2	1	1%	2%	0%	3%	0%	0%	2%	2%
10	1	3	3	3	2%	2%	2%	4%	1%	4%	3%	1%
11	3	1	3	3	15%	16%	12%	32%	9%	22%	8%	5%
12	3	3	1	3	54%	77%	54%	72%	46%	47%	47%	35%
13	3	3	3	1	1%	2%	0%	3%	0%	0%	2%	2%
14	1	4	4	4	3%	2%	2%	4%	1%	8%	3%	1%
15	4	1	4	4	17%	16%	13%	36%	9%	33%	8%	5%
16	4	4	1	4	82%	95%	88%	82%	89%	59%	81%	84%
17	4	4	4	1	2%	2%	0%	3%	0%	4%	2%	2%
18	1	5	5	5	3%	2%	2%	4%	1%	8%	3%	1%
19	5	1	5	5	18%	16%	13%	36%	11%	33%	10%	5%
20	5	5	1	5	87%	95%	90%	84%	97%	59%	91%	92%
21	5	5	5	1	2%	2%	0%	3%	0%	4%	2%	2%

Tabell 5: Scenarion där tekniken och förutsättningarna nått olika nivåer och därmed gör det möjligt att automatisera fler eller färre uppgifter och färdigheter. Siffrorna kan läsas som andel uppgifter och färdigheter som kan automatiseras i varje scenario.

området framgångsrikt. Det visar sig att tillgång till statistiska data och förmåga att möta krav på kreativitet är de två viktigaste kriterierna. Sedan följer krav på social interaktion. Kravet på fysiskt arbete är det minst betydelsefulla, då detta krav sällan finns överhuvudtaget.

6 Slutsatser

Nedan ges svar på de tre breda forskningsfrågor som lades fram i inledningen. Läsaren bör notera att dessa svar ges utifrån analysen som presenterats ovan och är förknippade med en betydande osäkerhet. Det ska även påpekas att svaren är av allmän natur.

Utgående från existerande modeller skapade för automatisering av arbete i allmänhet identifierades tre variabler som kan påverka hur svår en cybersäkerhetsroll är att automatisera. Inledningsvis var dessa variabler fyra till antalet: kravet på kreativitet, kravet på social interaktion, kravet på fysiskt arbete och tillgång till data kopplat till problemet. Under dessa variabler finns många dimensioner. Kreativitet kan t.ex. ses som förmåga till originalitet, som kan vara bra om tester ska genomföras, och förmåga att identifiera bra lösningar på problem, som är ett vanligare krav. Alla variabler, utom den kopplad till fysiskt arbete, är i regel ett problem för automation av cybersäkerhetsarbete. Svaret på frågan avseende *vilka variabler som påverkar hur svår en cybersäkerhetsroll är att automatisera* är därmed:

- kravet på kreativitet
- kravet på social förmåga, och
- tillgång till statistiskt underlag.

Tabellerna i avsnitt 5 visar på betydande skillnader mellan hur enkelt det verkar vara att automatisera olika roller. De visar bland annat att det är betydligt enklare att automatisera uppgifter som databasadministratörer, dataanalytiker och nätverksspecialister utför än vad det är att automatisera uppgifter som underrättelseanalytiker och högre chefer utför. Eftersom svaret på frågan om *hur troligt det är att olika cybersäkerhetsroller som finns i dag kommer att automatiseras* beror på många variabler som inte har att göra med automatiserbarhet kan denna studie inte ge ett fullödigt svar. Tabellerna i avsnitt 5 kan dock användas för vidare analyser, och de visar på relativt stora skillnader i hur lätta och svåra rollerna skulle kunna vara att automatisera.

Gällande *vilka variabler som begränsar potentialen att automatisera nuvarande cybersäkerhetsroller* så samvarierar variablerna, vilket gör det svårt att svara på frågan om vilken eller vilka variabler som är begränsande. Några saker står dock klart:

- de låga krav som finns på fysiskt arbete innebär att detta inte utgör ett betydande hinder
- krav på social interaktion utgör ett mindre hinder än kraven på kreativitet och bristen på tillgängligt statistiskt underlag, och
- kraven på kreativitet och tillgängligt statistiskt underlag samvarierar kraftigt.

Baserat på detta skulle möjligheten att kunna producera maskiner som tar fram kreativa lösningar på svåra problem vara en lösning som gör att mycket kan automatiseras.

Författarnas tack

Författarna vill tacka Erik Zouave för dennes arbete med att bedöma förmågor och färdigheter i NICE-ramverket.

Referenser

Frey, C. B. & Osborne, M. A. (2017). The future of employment: how susceptible are jobs to computerisation? *Technological Forecasting & Social Change*, *114*, 254–280. doi:10.1016/j.techfore.2016.08.019

Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST Special Publication 800-181, National Institute of Standards and Technology, U.S. Department of Commerce. doi:10.6028/NIST.SP.800-181