Projektnummer/Project no
A74018

Kund/Customer
FOI

FoT-område
Operationer i cyberdomänen

Handläggare/Our reference
Henrik Karlzén

Datum/Date
2020-06-23

Memo nummer/Number
FOI Memo 7213

Omvärldsstudie om cyberanläggningar

–

1 Inledning

Detta memo beskriver en omvärldsbevakning av akademisk forskning om cyberanläggningar (eng. cyber ranges).

Genom en omvärldsbevakning kan en första bild av ett forskningsområde skapas vilket ger grundläggande ämnesmässig insikt. Vidare kan trender vid forskningsfronten upptäckas vilket gör det möjligt att identifiera vilka forskningsartiklar det vore relevant att vidareutveckla med egna forskningsinsatser. Dessutom kan möjliga samarbetspartner identifieras. Som helhet använder FOI omvärldsbevakning för att rikta in långsiktiga satsningar åt sina huvuduppdragsgivare såsom Försvarsmakten.

Ämnet för denna omvärldsbevakning, cyberanläggningar, valdes i syfte att stödja och komplettera FOI:s satsning på den egna cyberanläggningen kallad CRATE (en förkortning av Cyber Range And Training Environment) som FOI driver sedan 2008. CRATE består av hundratals nätverksanslutna servrar där IT-miljöer kan byggas upp såsom ett simulerat småskaligt internet. Med fokus på cybersäkerhet används CRATE som teknisk infrastruktur i forskning, övning och utbildning. De senaste åren har utvecklingen av CRATE gått mot att uppnå högre modularitet som gör konfigurationen enklare och som gör CRATE mer allmänt tillgänglig för externa partner i Sverige.[1]

[1] Mer information om CRATE finns på https://www.foi.se/crate

2 Metod

Vid en typisk omvärldsbevakning av akademiska forskningsartiklar tar forskare fram en söksträng (se Bilaga A för den söksträng som användes i denna omvärldsbevakning) och söker med den i en databas som innehåller metadata om akademiska forskningsartiklar. Att ta fram en lämplig söksträng är en grundläggande svårighet i arbetet. Även om inledande test på sökningar kan avgöra om de resultat som fås är relevanta så är det inte en garanti för att alla relevanta artiklar hittas.

När sökningen genomförts sorteras sökresultaten efter relevans och dylikt. Typiskt sker sökning och sortering manuellt men den här omvärldsbevakningen använder istället i huvudsak FOI:s egenutvecklade verktyg *HSTool.*[2] HSTool söker i databasen Web of Science[3] och sorterar in de hittade artiklarna i kluster baserat på titel och sammanfattning (eng. abstract). På så vis sker en automatisk indelning av sökresultaten i mindre delar. Vid indelningen ignorerar HSTool vissa vanliga (engelska) ord som exempelvis ”the”.

HSTool tar dessutom fram flera olika rankningar av artiklarna baserat på citeringsstatistik. Detta underlättar identifieringen av vilka artiklar som är mest relevanta eftersom mer populära artiklar generellt sett ses som bättre inom forskningsvärlden.

Även om HSTool har kraftfulla analysmöjligheter finns också vissa begränsningar:

- HSTool söker enbart i Web of Science. Gedigna sammanställningar av litteraturen (eng. systematic literature reviews) inom ett forskningsområde brukar söka i flera olika databaser för att få med allt eftersom en enskild databas inte indexerar all forskning. Exempelvis hade den konkurrerande databasen Scopus gett ungefär dubbelt så många träffar.[4] Samtidigt måste antalet träffar vägas mot träffarnas relevans (vilket inte utvärderades för Scopus) och analysmöjligheterna (som ges av verktyget) och då även databasernas licenskostnader för att söka med verktyget.
- HSTool saknar djupare ämneskunskap. Forskare som är experter på forskningsområdet skulle förmodligen hitta mer lämpliga kluster att sortera in sökresultaten på. Här måste dock en avvägning göras i praktiken eftersom människor i regel arbetar mycket långsammare än ett automatiserat verktyg. I denna omvärldsbevakning gjordes även viss manuell sortering.
- HSTool tar inte med författardata. Detta gör det svårt att hitta vilka forskargrupper som är mest framstående på området och därmed exempelvis vilka som är lämpliga att samarbeta med. Å andra sidan kan ett fokus på författare leda till att den som ses som framstående idag slentrianmässigt också betraktas som framstående i framtiden. Detta kan också flytta fokus från att vara på idéer (forskning) till att vara på upphovsmän (forskarna).

[2] Verktyget har fått sitt namn efter engelskans Horizon Scanning of Scientific Literature.

[3] Databasen kräver betalning och nås på https://webofscience.com/

[4] Det finns också forskning som inte alls publiceras. Exempelvis sätter företagshemligheter och försvarssekretess stopp för en del publicering och forskning där hypoteserna visade sig felaktiga publiceras sällan.

3 Resultat

Sökningen resulterade i 74 träffar (forskningsartiklar). Området är alltså ganska litet. Forskningsartiklarna har publicerats i en lång rad olika tidskrifter eller i samband med konferenser. De sju publiceringsställen där minst två artiklar publicerats återfinns i Tabell 1. Som framgår av titlarna finns (som förväntat) visst fokus på IT, säkerhet och försvar.

Tabell 1: De publiceringsställen där minst två (#) artiklar publicerats.

Tidskrift eller konferens	#
Computers & security	4
European symposium on security and privacy	4
Journal of defense modeling and simulation-applications methodology technology	3
European conference on cyber warfare and security	2
Frontiers in education conference	2
International conference on cyber warfare and security	2
Texas power and energy conference	2

Verktyget HSTool sorterade automatiskt in artiklarna i sju kluster. Dessa kluster beskrivs i Tabell 2 i form av vilka ord HSTool använde för att sortera in artiklarna i klustren.

Tabellen visar också memoförfattarens bedömning av vad varje klusters artikelsammanfattningar verkar handla om, indelat i undergrupper när så verkade lämpligt. På detta sätt kompletteras den automatiska bedömningen med en manuell bedömning som ger en mer lättförståelig beskrivning. Det bör dock noteras att denna typ av manuell bedömning inte vore praktiskt möjlig för större mängder artiklar, dels för att det tar för lång tid att läsa igenom artikelsammanfattningarna, dels för att kategorierna blir alltför många att hålla reda på.

Tre av de sju klustren (med id 113, 129 och 207) handlar inte alls om cyberanläggningar och beskrivs därför inte ytterligare i memot. Detta ger ett bortfall på 5 artiklar av totala 74 (7 procent).

De resterande fyra klustren (med id 183, 300, 306 och 401) handlar om cyberanläggningar. Referenser till dessa klusters artiklar återfinns i Bilaga A. Vissa av dessa klusters artiklar var dock inte relevanta vilket framgår på sina ställen i kolumnen längst till höger i tabellen.

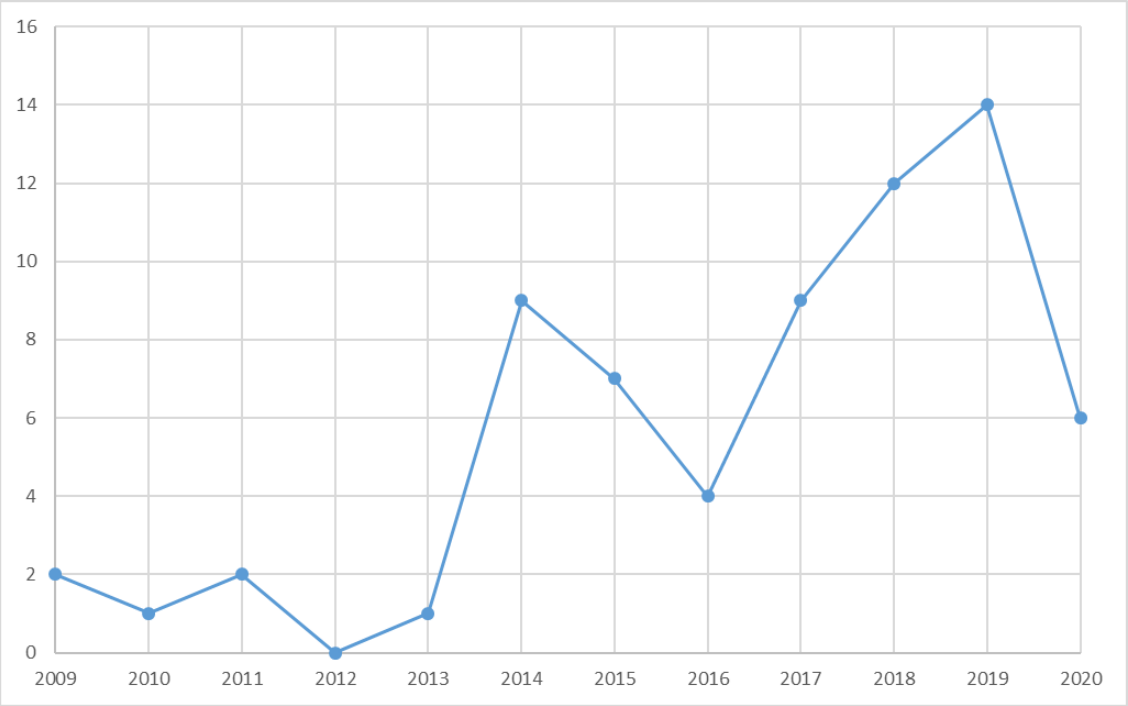
I några fall separerade den automatiska sorteringen artiklar som enligt den manuella bedömningen hade passat väl tillsammans. Dessa fall rör att använda cyberanläggningar för att studera logganalys (uppdelat på kluster 183 och 300), översikter av cyberanläggningar (kluster 300 och 401) och studierna av kognitiv belastning (kluster 300 och 401). Över huvud taget är kluster 401 och framförallt kluster 300 tämligen breda och svåra att förhålla sig till.

Tabell 2: Kluster-id (Id), HSTools klusterord (som kursiverats när de är unika för det givna klustret), antal artiklar (n) och memoförfattarens beskrivning av klustret.

Id	**HSTools klusterord**	**n**	**Beskrivning utifrån artikelsammanfattningarna**
113	*Cyberbullying, health, public, mental,* central, *science*	2	• Cybermobbning (irrelevant).
129	*Face,* science, *industry*, computer, *data, method*	2	• 3d-modeller av ansikten (irrelevant).

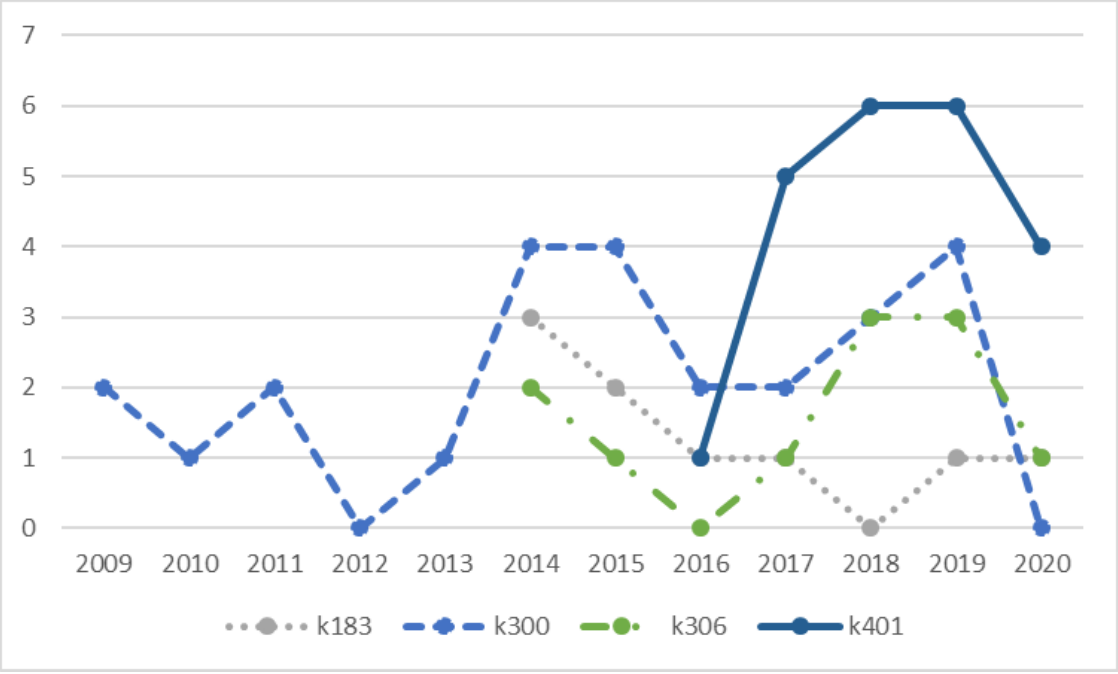
Id	HSTools klusterord	n	Beskrivning utifrån artikelsammanfattningarna
183	Science, cyber, system, *alert*, computer, *detection*, security	9	• Användning av cyberanläggningar för att studera anomalidetektion, logganalys och personers färdigheter. • (Optimering av nätverksflöden, vilket är irrelevant.)
207	Central, system, *high, risk,* science, *research, application*	1	• Tumörupptäckt (irrelevant).
300	Cyber, science, range, system, technology, computer, *attack*	25	• Översikter om cyber range-forskning och beskrivningar av specifika cyberanläggningar. • Behov, vision, modell, formalisering av cyberanläggningar. • Framtagande av sårbarheter och automatisering av angrepp mm. för cyberanläggningar. • Kognitiv belastning och lägesuppfattning vid cyberskyddssimulering. • Användning av cyberanläggningar för att studera logganalys. • (Hur datormiljöer kan saneras efter angrepp, vilket är irrelevant).
306	System, technology, security, cyber, *power, testbed, network*	12	• Cyber range som testbädd för industrin (framförallt för kraftnät och annan kritisk infrastruktur).
401	*Training*, cyber, science, *cybersecurity*, range, technology, computer	23	• Automatisering av konfiguration av cyberanläggningar samt framtagande av generella ramverk och arkitekturer. • Översikter av cyberanläggningar och capture-the-flag-övningsmiljöer. • Framtagande av specifika cyberövningsplattformar. • Hur cyberförvarsövningar bör utföras. • Hur angripare beter sig och kan simuleras i cyberförsvarsövningar. • Kognitiv belastning vid cyberövningar. • (En artikel som saknade abstract.)

Den första artikeln för de relevanta klustren publicerades år 1998 (de äldsta artiklarna av alla i databasen är från 1986) men antalet artiklar per år var länge mycket lågt. Som Figur 1 visar publicerades det fortfarande bara en eller två artiklar per år 2009–2013. Därefter har det ökat med en topp på 14 artiklar 2019. 2020 uppvisar så här långt samma takt (knappt halva året hade gått vid tiden sökningen gjordes). Noterbart är också en dipp 2015 och framförallt 2016.



Figur 1: Antal artiklar som publicerats per år (2009–2020). Notera att år 2020 löpt knappt halvvägs vid tiden för denna analys.

Figur 2 visar antal artiklar som publicerats per år och per de fyra relevanta klustren. Det bör nämnas att med så få antal artiklar går det knappast att dra några säkra slutsatser om varför ett kluster är mindre än ett annat eller hur det kommer att se ut kommande år.



Figur 2: Antal artiklar per år (2009–2020) för de fyra relevanta klustren (”k” följt av kluster-id). Notera att år 2020 löpt knappt halvvägs vid tiden för denna analys.

Trots det låga antalet artiklar kan dock vissa slutsatser dras:

- Kluster 300 dominerade i början. Detta kan förklaras av att det klustret är brett och innehåller artiklar om bland annat cyberanläggningars grunder som behov, vision och modell samt översiktliga undersökningar av vilken cyber range-forskning som skett. Studier av sådana breda och översiktliga ämnesdelar är en rimlig start på utvecklingen av ett forskningsämne.
- De senaste fem åren har ett nytt kluster (306) vuxit fram med fokus på implementationer där industrin kan använda cyberanläggningar som testbäddar. Att implementationsfokus kommit på senare år och efter den grundläggande forskningen är logiskt.
- Kluster 401 är nyast men störst. Det som tydligast utmärker detta kluster gentemot de övriga är ett ökat fokus på problemet att konfigurera en cyber range och därmed behovet av automatisering av konfigurationen. Detta är i linje med utvecklingen av FOI:s cyber range CRATE. Här finns därför onekligen anledning för FOI att både följa utvecklingen och att driva den. I klustret finns också ett ökat fokus på övningar och hur de som övas (ex. angripare) beter sig vilket också pekar på en mognad hos cyberanläggningar där fokus går mot ökad tillämpning. Det studeras också hur angripare kan automatiseras. Artiklar på detta delområde finns också i kluster 300 (exempelvis i en artikel framtagen av FOI[5]). Det verkar rimligt att anta att automatiseringen av både konfiguration och angripare kommer att få fortsatt fokus i framtiden.
- Inga slutsatser kunde dras om det minsta relevanta klustret (183).

[5] Holm, H., Sommestad, T. 2017. So Long, and Thanks for Only Using Readily Available Scripts, Information & Computer Security, 25 (1). Detta är den enda artikel i denna omvärldsbevakning som är tagits fram av FOI. Det mesta av FOI:s forskning på området publiceras istället som FOI-rapporter och FOI-memon (som det här!).

4 Slutsatser

Den nyaste och nu största delen av forskningsområdet cyberanläggningar (eng. cyber ranges) utmärks genom ett fokus på automatisk konfigurering. Detta ligger i linje med FOI:s vidareutveckling av cyberanläggningen CRATE. Här finns alltså goda möjligheter för FOI att dra nytta av utvecklingen genom att studera området djupare. Dessutom ligger FOI bra till för att vara med och driva området framåt akademiskt. Detta kräver dock ökat fokus på akademisk publicering.

Ett annat vanligt och lovande spår för automatisering är utvecklingen av verktyg för automatisering av angrepp. En av artiklarna i omvärldsbevakningen som handlar om just detta togs fram av FOI och forskningen har fortsatt sedan dess.

Denna omvärldsanalys använde FOI:s egenutvecklade verktyg HSTool för att automatisera en del av arbetet. Detta gav effektiviseringsvinster. Samtidigt skulle verktyget ge mer nytta om det var mer specialiserat för det specifika forskningsområde det för stunden används för. En möjlighet vore att låta användare av verktyget ge återkoppling på vilka ord som är alltför grundläggande i ett visst forskningsområde och som därmed inte borde användas för sortering. Det skulle också vara möjligt att inte bara sortera på enstaka ord och ha kluster-ord utan också tillåta kluster-begrepp. Det bör dock noteras att den omvärldsanalys som presenteras i detta memo är ganska liten och att verktygets sorteringsmöjligheter förmodligen är bättre vid större omvärldsanalyser.

Bilaga A – Söksträng och viktigaste sökträffar

I omvärldsbevakningen användes söksträngen:

> "Cyber* range$" OR "Cybersecurity testbed$" OR "Cyber security testbed$" OR "cyber security simulation" OR "cybersecurity simulation"

Varje sökterms ord användes även i omvänd ordning eftersom HSTool automatiskt täcker även det. Sökningen gjordes i databasen Web of science och i dess fält *title, abstract, keywords.*

Nedan ges referenser till de artiklar som ingår i de mest relevanta klustren (med id 183, 300, 306 och 401). Varje artikel har en unik identifierare i databasen Web of Science (WOS). Eftersom verktyget HSTool inte extraherar författarnamn inkluderas inte de i referenserna. Referenserna ges istället på formatet:

> *[artikeltitel].[tidskrift eller konferens].[årtal].[unik identifierare]*.

Kluster 183

A Distributed Optimization Algorithm for Attack-Resilient Wide-Area Monitoring of Power Systems: Theoretical and Experimental Methods. DECISION AND GAME THEORY FOR SECURITY, GAMESEC 2014. 2014. WOS:000345594300021.

A Framework for the Evaluation of Trainee Performance in Cyber Range Exercises. MOBILE NETWORKS & APPLICATIONS. 2020. WOS:000499972400001.

Capability Detection and Evaluation Metrics for Cyber Security lab Exercises. PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY (ICCWS 2017). 2017. WOS:000423998600049.

Detecting Anomalous Behavior in Cloud Servers by Nested-Arc Hidden SEMI-Markov Model with State Summarization. IEEE TRANSACTIONS ON BIG DATA. 2019. WOS:000484207900004.

Detection of Cyber Intrusions Using Network-Based Multicast Messages for Substation Automation. 2014 IEEE PES INNOVATIVE SMART GRID TECHNOLOGIES CONFERENCE (ISGT). 2014. WOS:000355408800008.

Entropy Clustering Approach for Improving Forecasting in DDoS Attacks. 2015 IEEE 12TH INTERNATIONAL CONFERENCE ON NETWORKING, SENSING AND CONTROL (ICNSC). 2015. WOS:000380543900056.

Intrusion alert prioritisation and attack detection using post-correlation analysis. COMPUTERS & SECURITY. 2015. WOS:000352662100001.

OutMet: A New Metric for Prioritising Intrusion Alerts using Correlation and Outlier Analysis. 2014 IEEE 39TH CONFERENCE ON LOCAL COMPUTER NETWORKS (LCN). 2014. WOS:000355285900038.

Weighted Fuzzy Clustering for Online Detection of Application DDoS Attacks in Encrypted Network Traffic. INTERNET OF THINGS, SMART SPACES, AND NEXT GENERATION NETWORKS AND SYSTEMS, NEW2AN 2016/USMART 2016. 2016. WOS:000389503600027.

Kluster 300

A Framework to Address Challenges Encountered When Designing a Cyber-Range. PROCEEDINGS OF THE 13TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY (ECCWS-2014). 2014. WOS:000361692300032.

A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. IEEE ACCESS. 2018. WOS:000439022000013.

Alfons: A Mimetic Network Environment Construction System. TESTBEDS AND RESEARCH INFRASTRUCTURES FOR THE DEVELOPMENT OF NETWORKS AND COMMUNITIES, TRIDENTCOM 2016. 2017. WOS:000401119600006.

ALPACA: Building Dynamic Cyber Ranges with Procedurally-Generated Vulnerability Lattices. PROCEEDINGS OF THE 2019 ANNUAL ACM SOUTHEAST CONFERENCE (ACMSE 2019). 2019. WOS:000490458700012.

An automated system for rapid and secure device sanitization. COMPUTERS & SECURITY. 2014. WOS:000335201000008.

Analysis of the Implementation of an Interactive Kinetic Cyber Range Component. PROCEEDINGS OF THE 14TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY (ECCWS-2015). 2015. WOS:000361690600047.

Automating Cyber Offensive Operations for Cyber Challenges. PROCEEDINGS OF THE 11TH INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY (ICCWS 2016). 2016. WOS:000391660200008.

Capturing Human Cognition in Cyber-Security Simulations with NETS. 2013 IEEE INTERNATIONAL CONFERENCE ON INTELLIGENCE AND SECURITY INFORMATICS: BIG DATA, EMERGENT THREATS, AND DECISION-MAKING IN SECURITY INFORMATICS. 2013. WOS:000327025200071.

Computational Asset Description for Cyber Experiment Support using OWL. FIFTH IEEE INTERNATIONAL CONFERENCE ON SEMANTIC COMPUTING (ICSC 2011). 2011. WOS:000410187400017.

CSRS: Cyber Survive and Recover Simulator. 2016 IEEE 17TH INTERNATIONAL SYMPOSIUM ON HIGH ASSURANCE SYSTEMS ENGINEERING (HASE). 2016. WOS:000377098300017.

CSSS: Cyber Security Simulation Service for Software Defined Tactical Networks. 2018 32ND INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING (ICOIN). 2018. WOS:000468812000103.

Current Developments in DETER Cybersecurity Testbed Technology. CATCH 2009: CYBERSECURITY APPLICATIONS AND TECHNOLOGY CONFERENCE FOR HOMELAND SECURITY, PROCEEDINGS. 2009. WOS:000265683000006.

Cyber Range CYBERIUM for Training Security Meisters to Deal with Cyber Attacks. FUJITSU SCIENTIFIC & TECHNICAL JOURNAL. 2019. WOS:000502421700011.

Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper. 2018 52ND ANNUAL IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY (ICCST). 2018. WOS:000459861200050.

Cyber Scientific Test Language. SEMANTIC WEB - ISWC 2011, PT II. 2011. WOS:000306458200007.

Cyber-attack and defense simulation framework. JOURNAL OF DEFENSE MODELING AND SIMULATION-APPLICATIONS METHODOLOGY TECHNOLOGY-JDMS. 2015. WOS:000367551100004.

Cybersecurity Experimentation at Program Scale: Guidelines and Principles for Future Testbeds. 2019 4TH IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS&PW). 2019. WOS:000485315600011.

Defining Security Primitives for Eliciting Flexible Attack Scenarios Through CAPEC Analysis. INFORMATION SECURITY APPLICATIONS, WISA 2014. 2015. WOS:000357589600029.

Fostering the Culture of Cyber Security. 2019 IST-AFRICA WEEK CONFERENCE (IST-AFRICA). 2019. WOS:000490550800054.

National Cyber Range (NCR) Automated Test Tools: Implications and Application to Network-Centric Support Tools. 2010 IEEE AUTOTESTCON. 2010. WOS:000287044100068.

National Cyber Range Overview. 2014 IEEE MILITARY COMMUNICATIONS CONFERENCE: AFFORDABLE MISSION SUCCESS: MEETING THE CHALLENGE (MILCOM 2014). 2014. WOS:000369851400020.

So long, and thanks for only using readily available scripts. INFORMATION AND COMPUTER SECURITY. 2017. WOS:000399053300003.

Technical note: exploiting problem definition study for cyber security simulations. JOURNAL OF DEFENSE MODELING AND SIMULATION-APPLICATIONS METHODOLOGY TECHNOLOGY-JDMS. 2015. WOS:000367551100002.

Techniques and research trends of network testbed. 2014 TENTH INTERNATIONAL CONFERENCE ON INTELLIGENT INFORMATION HIDING AND MULTIMEDIA SIGNAL PROCESSING (IIH-MSP 2014). 2014. WOS:000358743800133.

The Rational for Developing Larger-scale 1000+Machine Emulation-based Research Test Beds. 2009 INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS: WAINA, VOLS 1 AND 2. 2009. WOS:000271364200183.

Kluster 306

A CONCEPTURAL FRAMEWORK TO FEDERATE TESTBEDS FOR CYBERSECURITY. 2017 WINTER SIMULATION CONFERENCE (WSC). 2017. WOS:000427768600033.

Attack Scenario-based Validation of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC). 2019 IEEE TEXAS POWER AND ENERGY CONFERENCE (TPEC). 2019. WOS:000469504600041.

Awareness and readiness of Industry 4.0: The case of Turkish manufacturing industry. ADVANCES IN PRODUCTION ENGINEERING & MANAGEMENT. 2020. WOS:000524074900005.

Behavior Analysis and Anomaly Detection for a Digital Substation on Cyber-Physical System. ELECTRONICS. 2019. WOS:000464261800001.

CyberFactory#1-Securing the Industry 4.0 with cyber-ranges and digital twins. 2018 14TH IEEE INTERNATIONAL WORKSHOP ON FACTORY COMMUNICATION SYSTEMS (WFCS 2018). 2018. WOS:000490863500040.

Design and implementation of cybersecurity testbed for industrial IoT systems. JOURNAL OF SUPERCOMPUTING. 2018. WOS:000444739000020.

Development of Cyber Security Testbed for Critical Infrastructure. 2015 INTERNATIONAL CONFERENCE ON MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS (ICMCIS). 2015. WOS:000381503800020.

Distributed Specification-Based Firewalls for Power Grid Substations. 2014 IEEE PES INNOVATIVE SMART GRID TECHNOLOGIES CONFERENCE EUROPE (ISGT EUROPE). 2014. WOS:000393467600009.

ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed. 2019 IEEE TEXAS POWER AND ENERGY CONFERENCE (TPEC). 2019. WOS:000469504600060.

Multiattribute SCADA-Specific Intrusion Detection System for Power Networks. IEEE TRANSACTIONS ON POWER DELIVERY. 2014. WOS:000337137900014.

Reflections on the Construction of Cyber Security Range in Power Information System. PROCEEDINGS OF 2018 IEEE 3RD ADVANCED INFORMATION TECHNOLOGY, ELECTRONIC AND AUTOMATION CONTROL CONFERENCE (IAEAC 2018). 2018. WOS:000457576900414.

SCADA cyber security testbed development. 2006 38TH ANNUAL NORTH AMERICAN POWER SYMPOSIUM, NAPS-2006 PROCEEDINGS. 2006. WOS:000246829900066.

Kluster 401

Adversarial Reinforcement Learning in a Cyber Security Simulation. ICAART: PROCEEDINGS OF THE 9TH INTERNATIONAL CONFERENCE ON AGENTS AND ARTIFICIAL INTELLIGENCE, VOL 2. 2017. WOS:000413244200059.

An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. JOURNAL OF NETWORK AND COMPUTER APPLICATIONS. 2020. WOS:000514024000001.

Assessing the cognitive complexity of cyber range environments. JOURNAL OF DEFENSE MODELING AND SIMULATION-APPLICATIONS METHODOLOGY TECHNOLOGY-JDMS. 2020. WOS:000454881200001.

Becoming Invisible Hands of National Live-Fire Attack-Defense Cyber Exercise. 2019 4TH IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS&PW). 2019. WOS:000485315600009.

Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. COMPUTERS & SECURITY. 2020. WOS:000501392500020.

Cyber-ranger. FORBES. 1998. WOS:000076838400062.

Cyber-Ranges as a Mean of Security Culture Establishment. ERCIM NEWS. 2020. WOS:000526180300022.

Cybersecurity Education and Training Support System: CyRIS. IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS. 2018. WOS:000431772500019.

CyRIS: A Cyber Range Instantiation System for Facilitating Security Training. PROCEEDINGS OF THE SEVENTH SYMPOSIUM ON INFORMATION AND COMMUNICATION TECHNOLOGY (SOICT 2016). 2016. WOS:000403650400040.

CyTrONE: An Integrated Cybersecurity Training Framework. ICISSP: PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS SECURITY AND PRIVACY. 2017. WOS:000413241700014.

Designing Serious Games for Cyber Ranges: A Socio-technical Approach. 2019 4TH IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS&PW). 2019. WOS:000485315600010.

Evaluation of Cyber Defense Exercises Using Visual Analytics Process. 2018 IEEE FRONTIERS IN EDUCATION CONFERENCE (FIE). 2018. WOS:000468396903041.

High Impact Cybersecurity Capacity Building. NEW TECHNOLOGIES AND REDESIGNING LEARNING SPACES, VOL II. 2019. WOS:000473324400043.

Integrated framework for hands-on cybersecurity training: CyTrONE. COMPUTERS & SECURITY. 2018. WOS:000447358700004.

Interactive Cybersecurity Defense Training Inspired by Web-based Learning Theory. PROCEEDINGS OF THE 2017 IEEE 9TH INTERNATIONAL CONFERENCE ON ENGINEERING EDUCATION (IEEE ICEED 2017). 2017. WOS:000425844600018.

Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios. JOURNAL OF SYSTEMS ARCHITECTURE. 2019. WOS:000476961500011.

Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range. 2017 IEEE FRONTIERS IN EDUCATION CONFERENCE (FIE). 2017. WOS:000426974900279.

Modeling And Simulation Architecture For Training In Cyber Defence Education. PROCEEDINGS OF THE 9TH INTERNATIONAL CONFERENCE ON ELECTRONICS, COMPUTERS AND ARTIFICIAL INTELLIGENCE - ECAI 2017. 2017. WOS:000425865900012.

Predicting Adversarial Cyber-Intrusion Stages Using Autoregressive Neural Networks. IEEE INTELLIGENT SYSTEMS. 2018. WOS:000435198200004.

Realistic Cybersecurity Training via Scenario Progression Management. 2019 4TH IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS&PW). 2019. WOS:000485315600008.

Scenario Design and Validation for Next Generation Cyber Ranges. 2018 IEEE 17TH INTERNATIONAL SYMPOSIUM ON NETWORK COMPUTING AND APPLICATIONS (NCA). 2018. WOS:000469020900042.

Supporting cybersecurity education and training via LMS integration: CyLMS. EDUCATION AND INFORMATION TECHNOLOGIES. 2019. WOS:000494043600018.

Using Holistic Approach to Developing Cybersecurity Simulation Environments. ELEARNING CHALLENGES AND NEW HORIZONS, VOL 4. 2018. WOS:000468620000012.