Cyber Ranges, Security Exercise & ~~Everything~~ in Between

Something

By Muhammad Mudassar Yamin

COINS Summer School

Metochi Greece, 27th of July 2019

Norwegian University of Science and Technology

Test Ranges

Cyber Range

Cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing.

https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf

Purpose

1. To identify and classify the capabilities and functionalities deployed within contemporary cyber ranges and security testbeds.
2. To collect and critically evaluate existing cyber ranges and security testbeds' architectural models.
3. To identify and classify scenarios, for training or testing, applied in cyber ranges and security testbeds.
4. To identify the different roles and teams associated with the execution of an exercise in a cyber range.
5. To identify and classify hardware and software tools utilized within contemporary cyber ranges and security testbeds.
6. To identify way and methods to evaluate different cyber ranges against a standard.
7. To study the research trends and directions on the topic of cyber ranges and security testbeds.

Searching the Literature

- Examined scientific databases: ACM digital library, IEEE Xplore, Science Direct, Springer Link, and Wiley online library.
- Utilized keywords (advanced search): ”Cyber Range”, ”Security”+”Testbed”,”Security”+”Test-bed”, ”Security Exercise”.
- Publication period: 15 years (2002 - 2018).
- The total period of the literature review: April 2018 - January 2019.

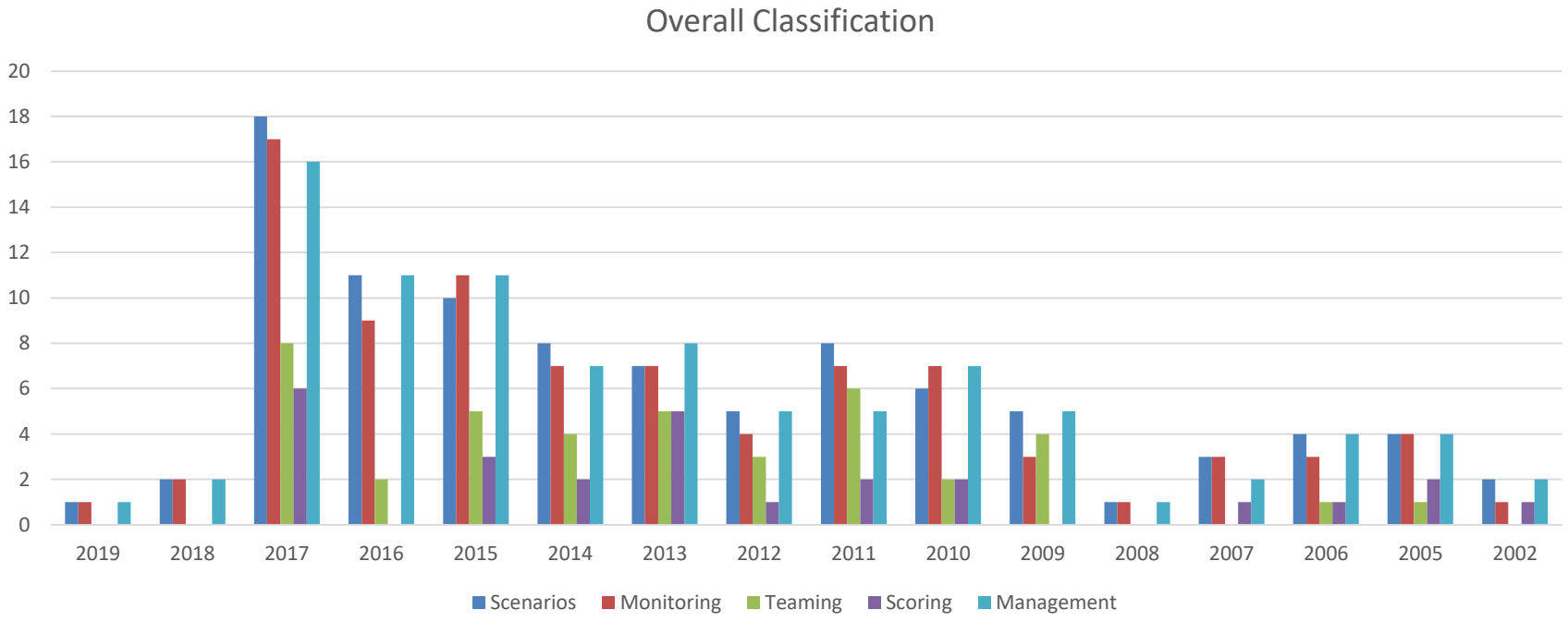
Practical Literature Screening

- **Round 1:** Collection of the literature was conducted in March 30th. It resulted in a total entries of 385
- **Round 2:** Elimination of duplicates was conducted in April 25th, and resulted in a total entries of 310
- **Round 3:** Back tracing additional entries from the citations of the current articles was conducted in June 20th. It resulted in a total number of entries 341
- **Round 4:** Quality appraisal was conducted on August 10th, and resulted in the total number of articles 100

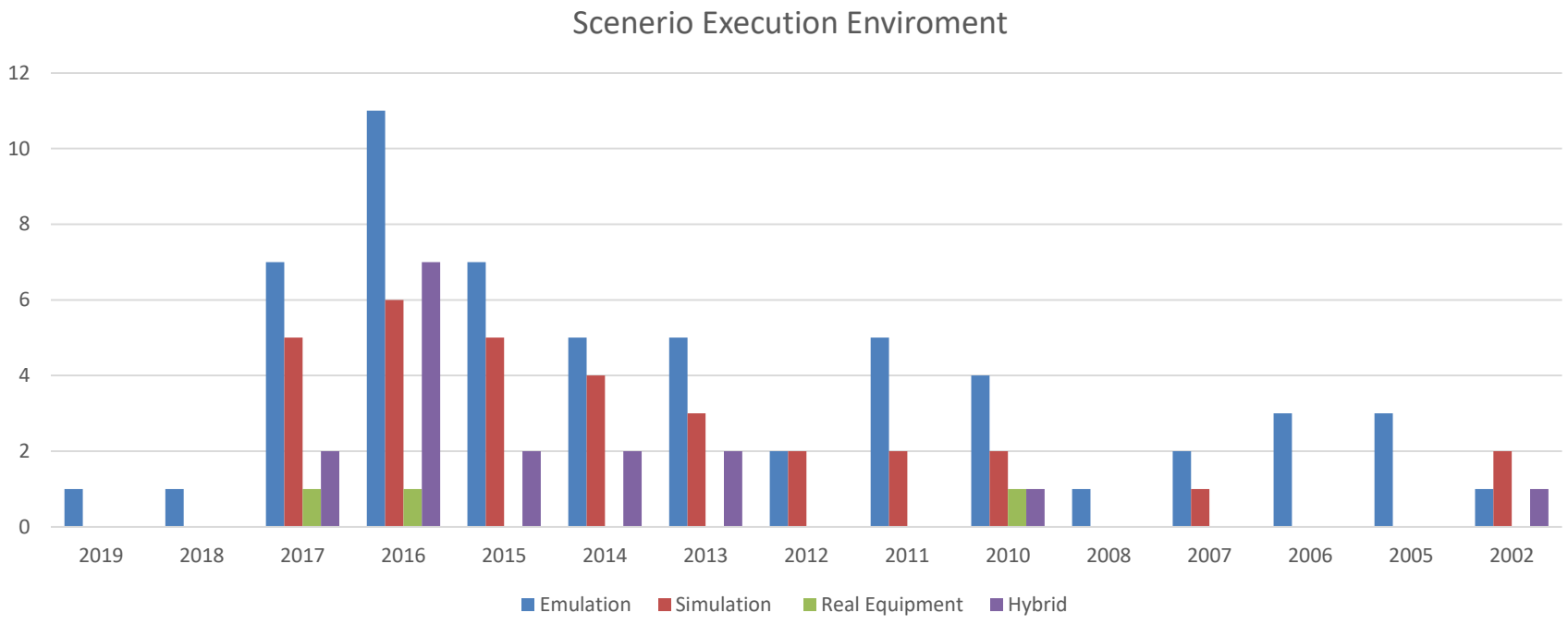
“In God we trust; all others bring data.”

~W. Edwards Deming

Overall Classification

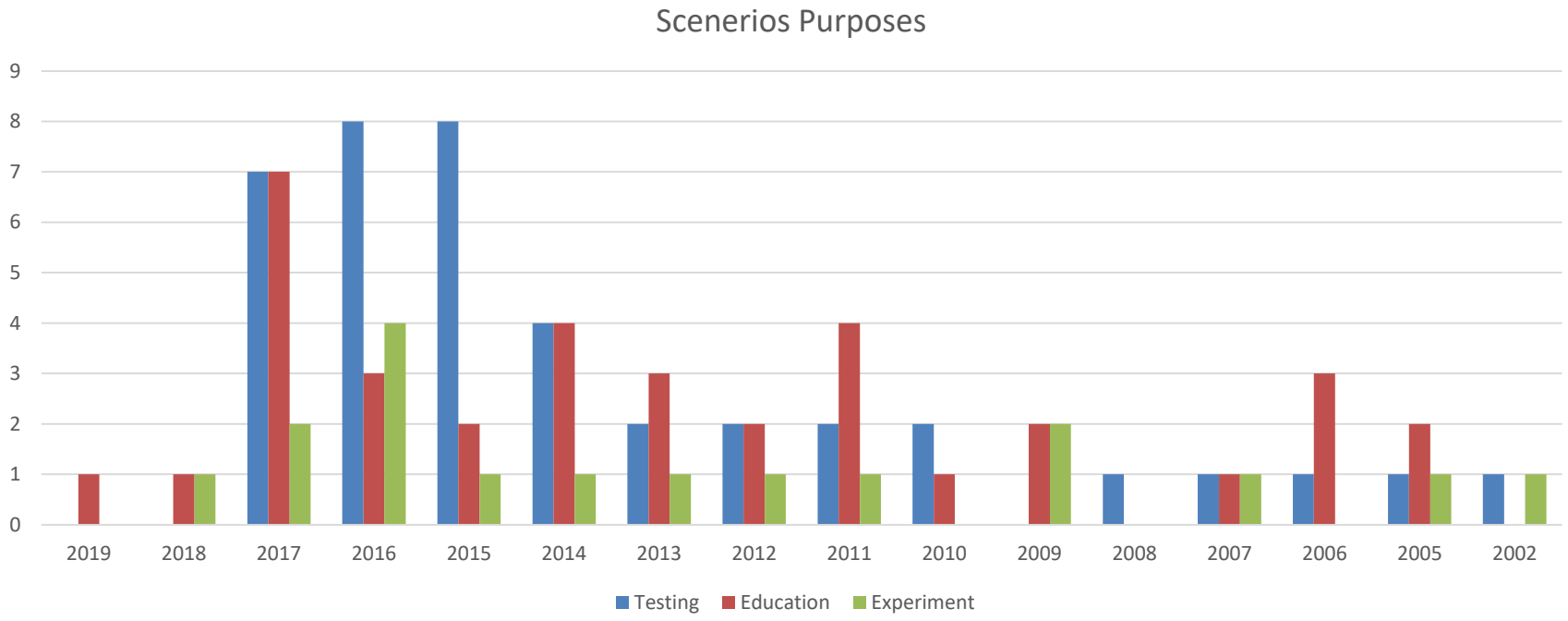


Environment



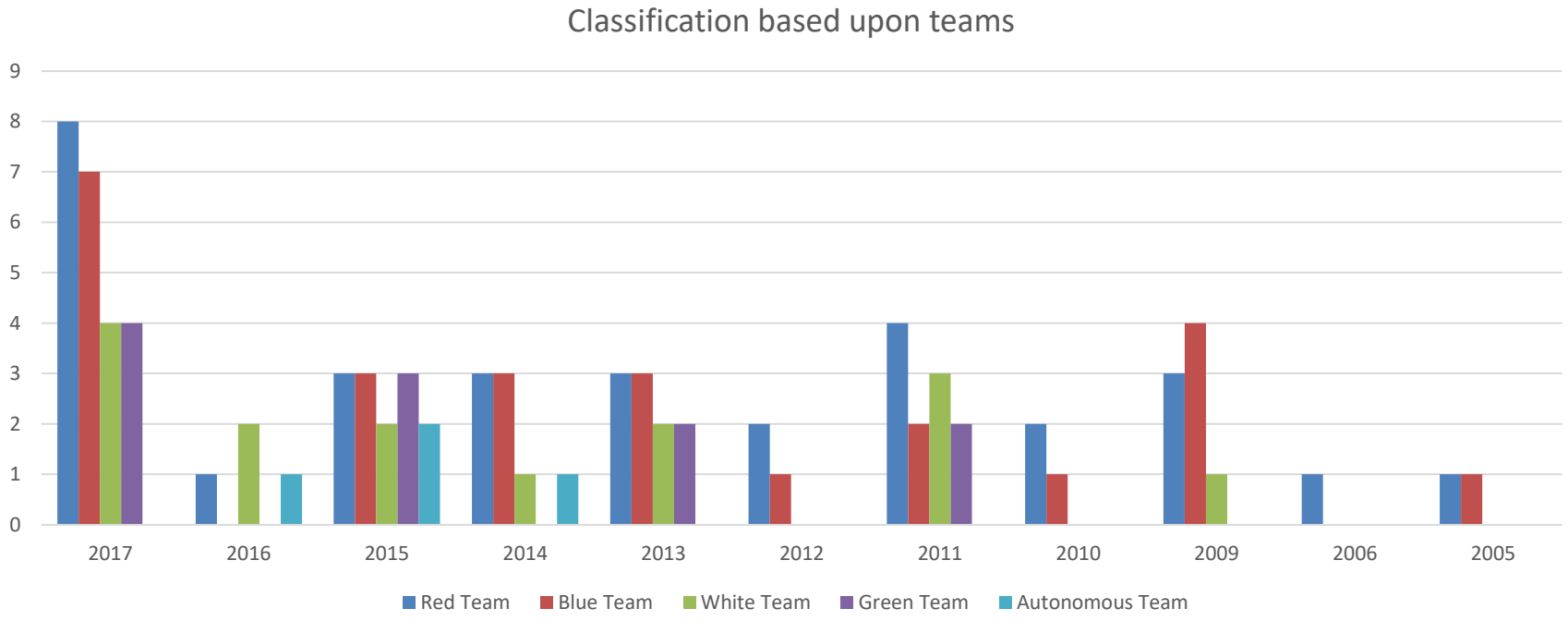
NTNU

Purpose

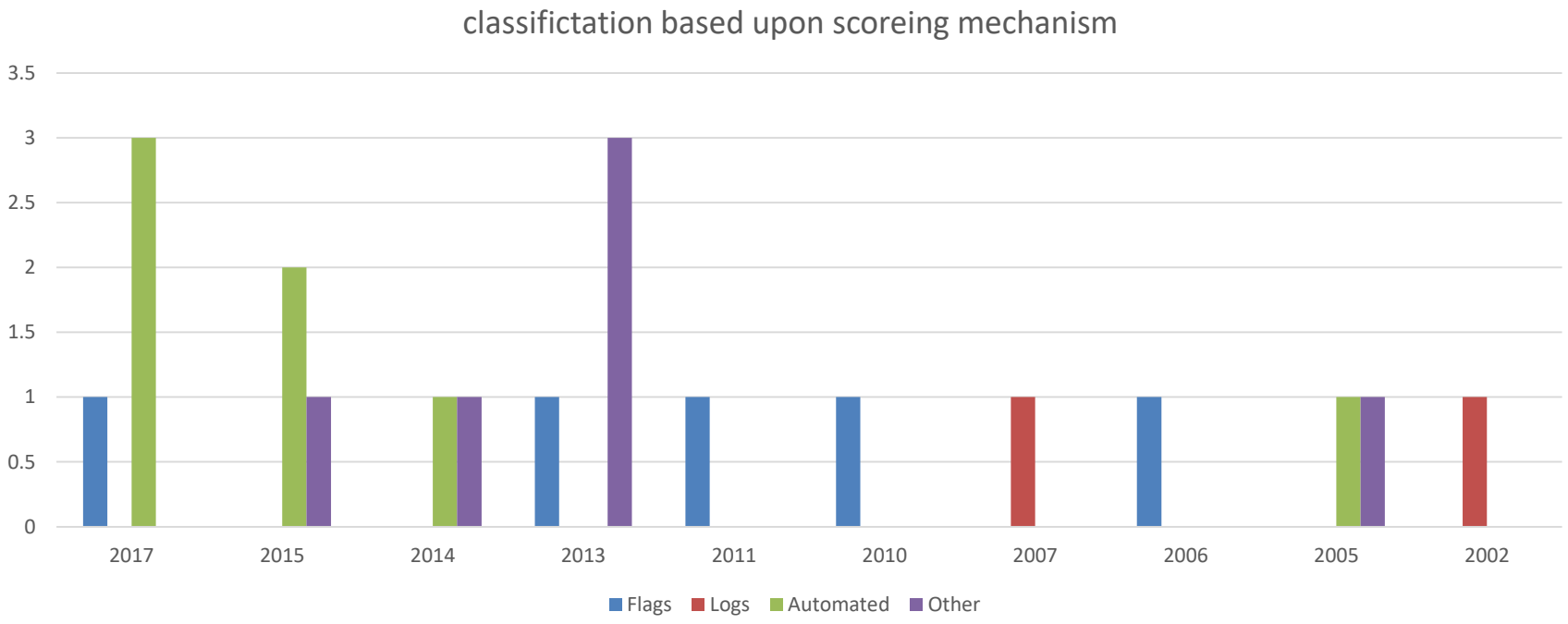


NTNU

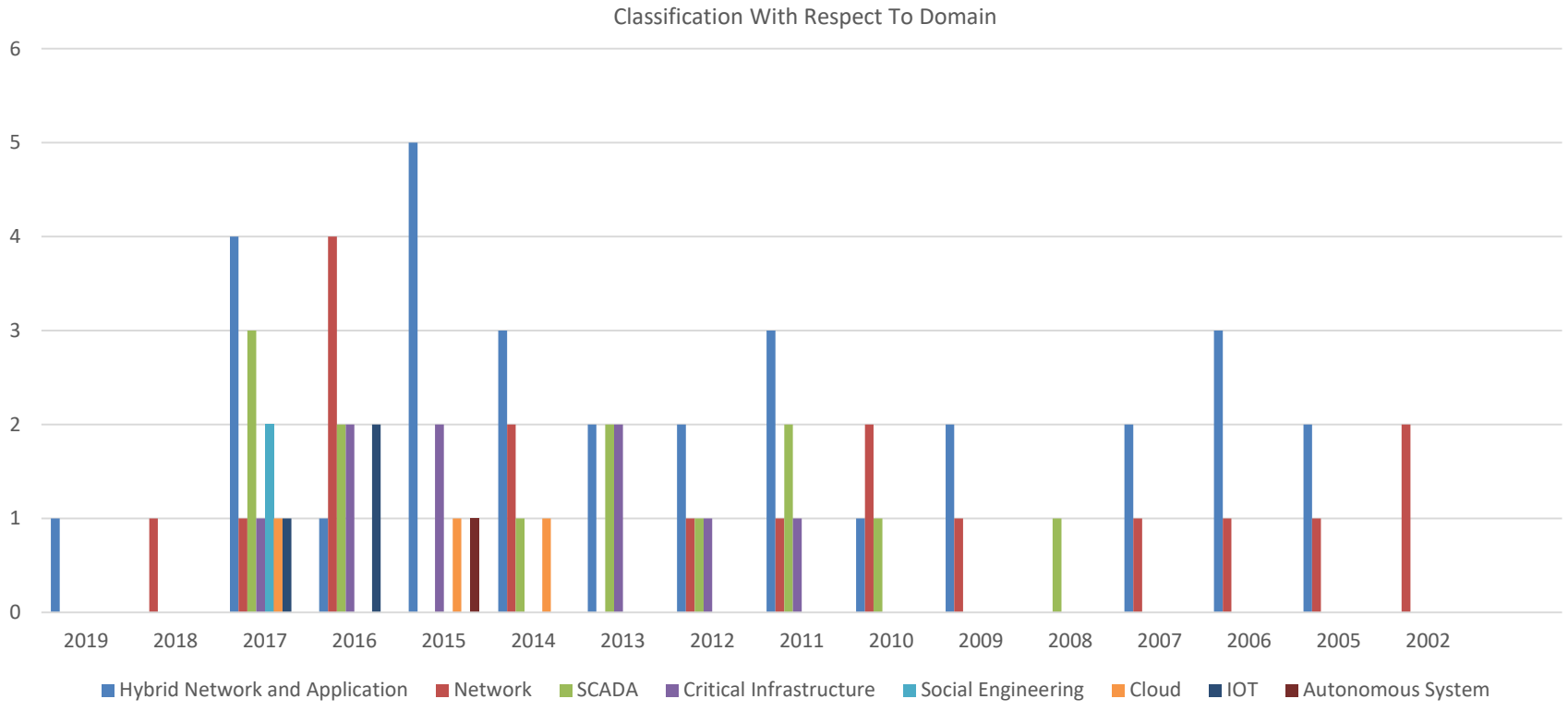
Teams


Classification based upon teams
9
8
7
6
5
4
3
2
1
0
2017
2016
2015
2014
2013
2012
2011
2010
2009
2006
2005
Red Team
Blue Team
White Team
Green Team
Autonomous Team

Scoring Mechanism



Domains



NTNU

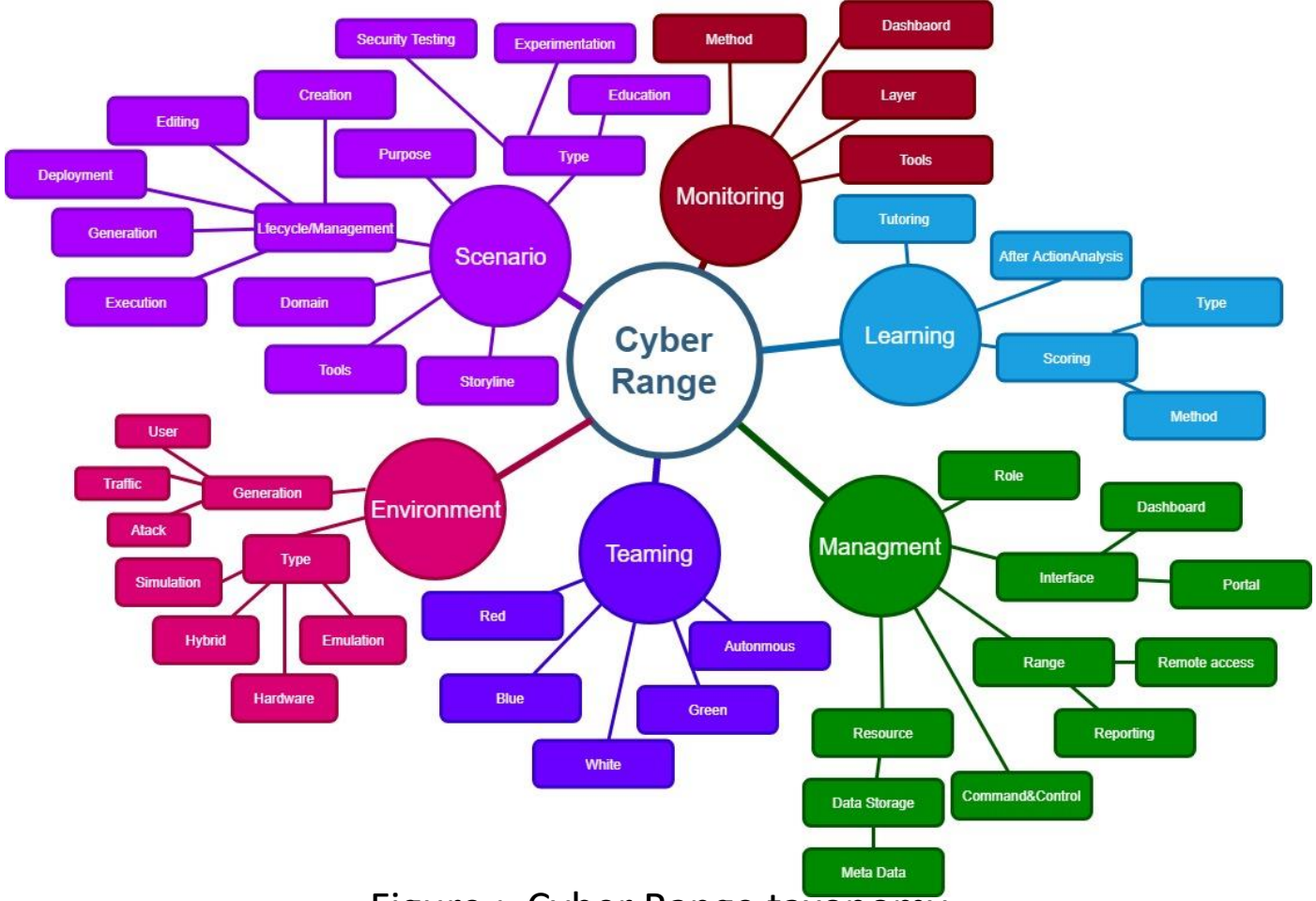


Figure : Cyber Range taxonomy

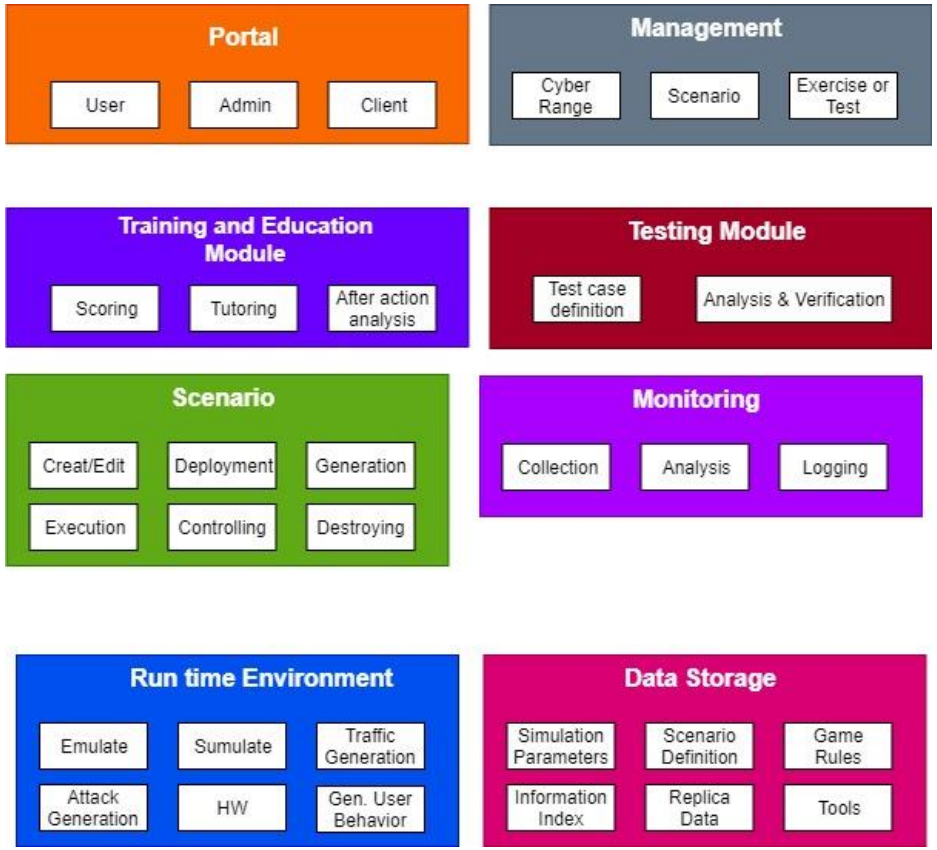


Figure : Cyber range and security testbed functional architecture

Cyber Security Certification Programs

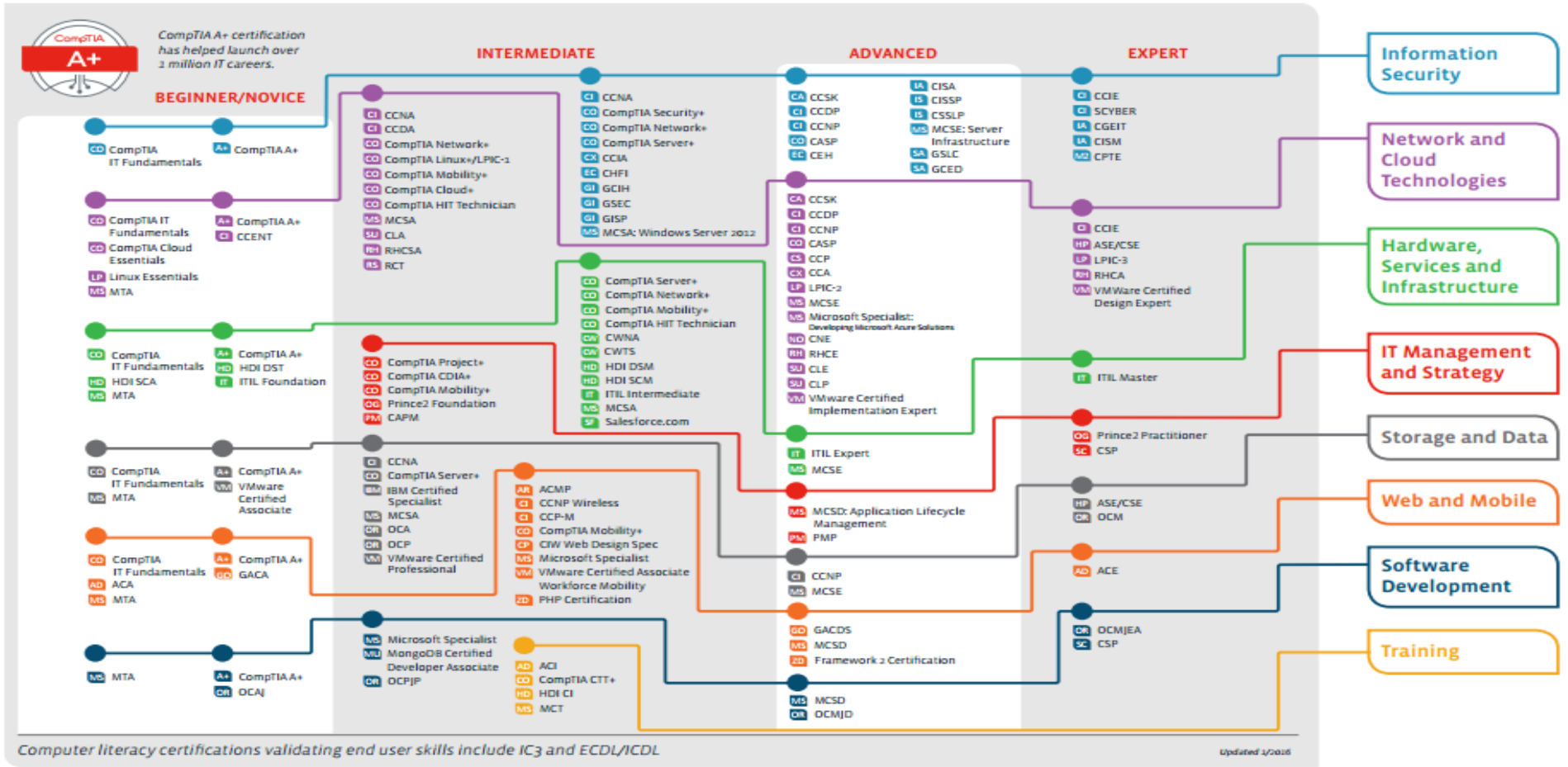
- Information Assurance Technical (IAT) IA Management (IAM) personnel must be fully trained and certified to baseline requirements to perform their IA duties.
- DoD 8570.01-M defines IAT workforce members as anyone with privileged information system access performing IA functions. IAM personnel perform management functions for DoD operational systems described in the Manual.
- The training, certification, and workforce management requirements of DoD 8570.01-M apply to all members of the DoD IA workforce including military, civilians, local nationals, Non-appropriated fund (NAF) personnel, and contractors.
- The requirements apply whether the duties are performed full-time, part-time, or as an embedded duty.

IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at: CompTIA.org/CertsRoadmap

CompTIA

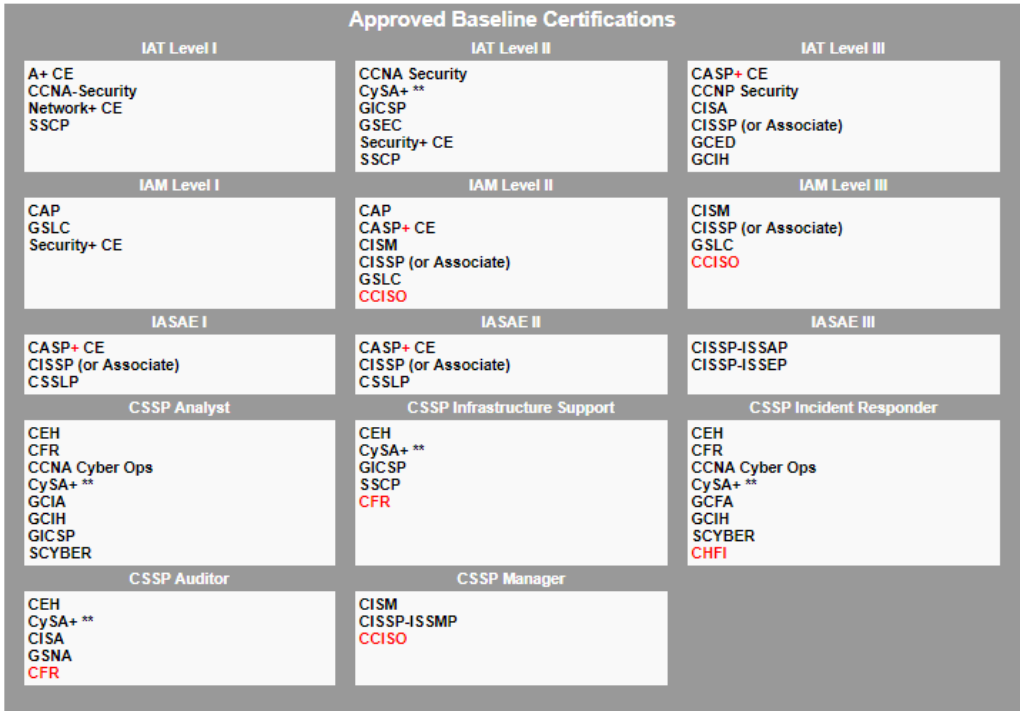
Certifications validate expertise in your chosen career.



Computer literacy certifications validating end user skills include IC3 and ECDL/ICDL

Updated 1/2016

DoD Approved 8570 Baseline Certifications



Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security Network+ CE SSCP	CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP+ CE CISM CISSP (or Associate) GSLC CCISO	CISM CISSP (or Associate) GSLC CCISO
IASAE I	**IASAE II**	**IASAE III**
CASP+ CE CISSP (or Associate) CSSLP	CASP+ CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CCNA Cyber Ops CySA+ ** GCIA GCIH GICSP SCYBER	CEH CySA+ ** GICSP SSCP CFR	CEH CFR CCNA Cyber Ops CySA+ ** GCFA GCIH SCYBER CHFI
CSSP Auditor	**CSSP Manager**	
CEH CySA+ ** CISA GSNA CFR	CISM CISSP-ISSMP CCISO	

My Experience with Certs

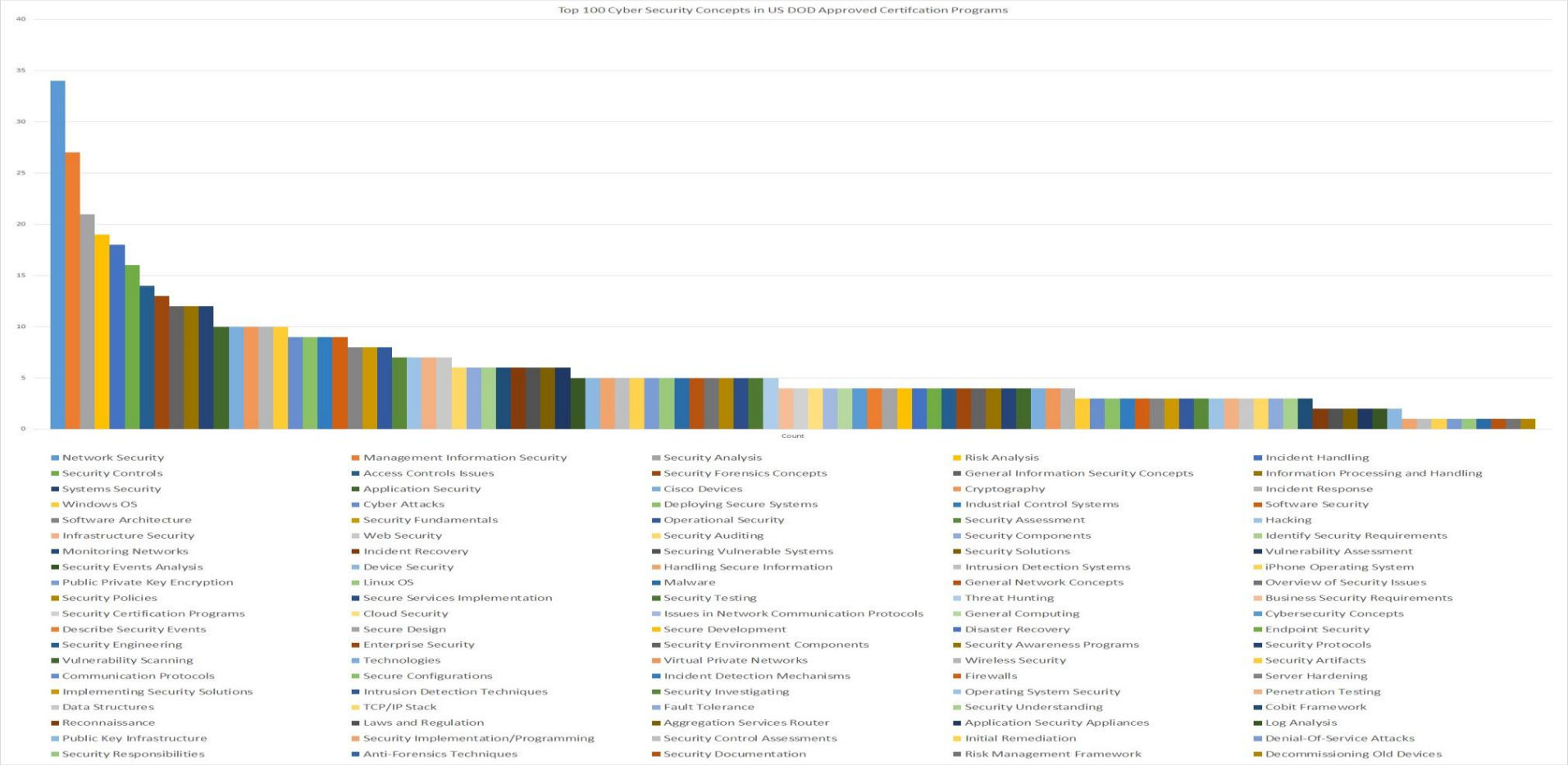
RED Team Certs

Blue Team Certs

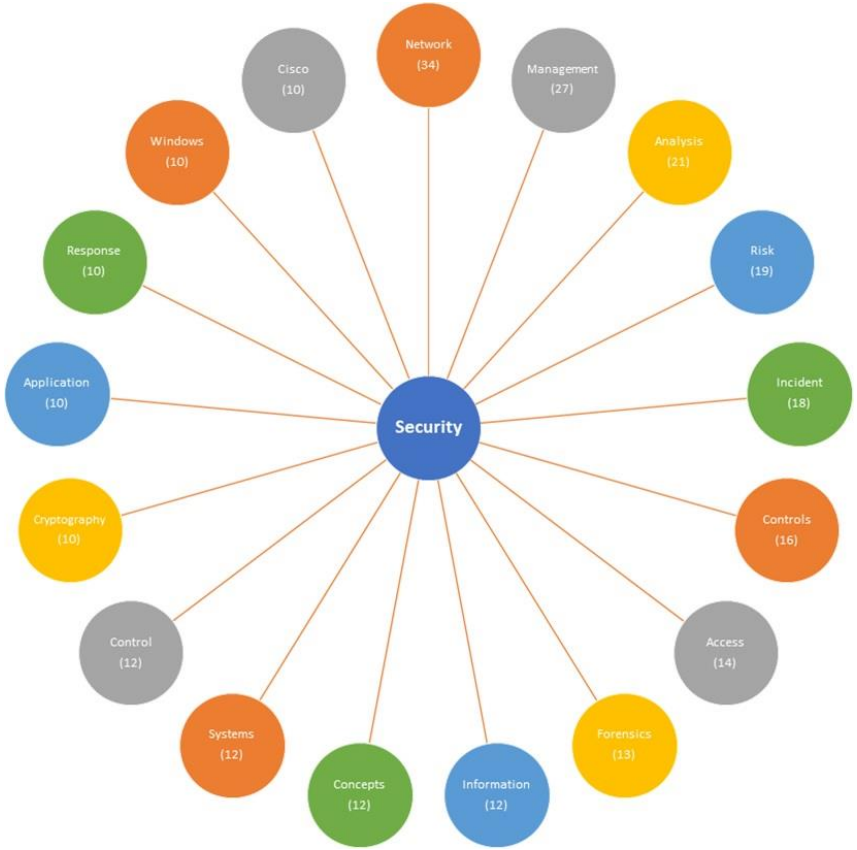
Management

It's all for fun, but don't get me wrong -- it's about bragging rights for 364 days a year.

- RANDY MOORE



30 Cyber security certification approved by US DOD were analyzed to identify overlapping concepts for cyber security skill development



30 Cyber security certification approved by US DOD were analyzed to identify overlapping concepts for cyber security skill development

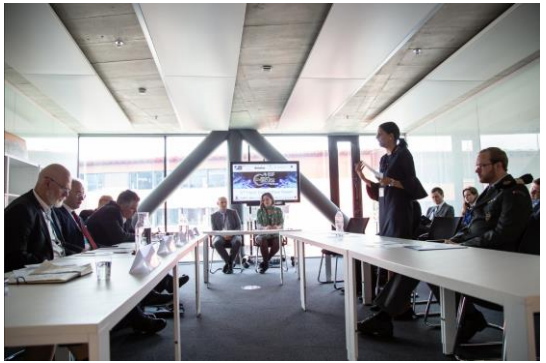
Cyber Security Exercises

- Cyber security exercises are a very effective way of learning the practical aspects of information security[1]
- Cyber Security Exercises are broadly categorized[2]

Operation Based

Norwegian Cyber Security Challenge 2018

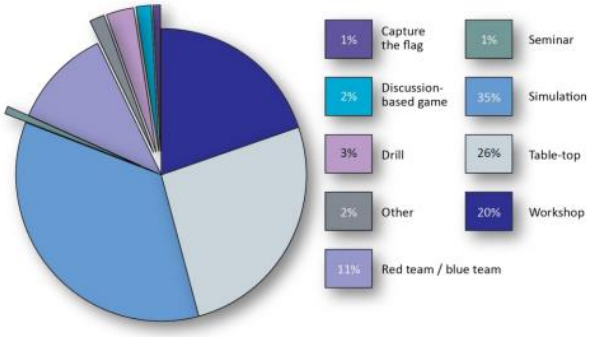
Tabletop Based



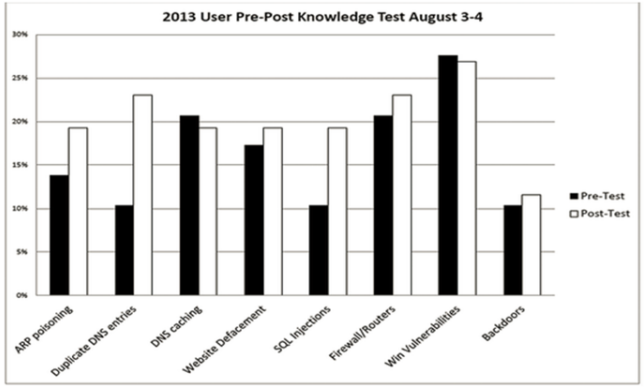
Atlantic Council Cyber 9/12 Challenge 2019

1. Patriciu, V. V., & Furtuna, A. C. (2009, December). Guide for designing cyber security exercises. In Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy (pp. 172-177). World Scientific and Engineering Academy and Society (WSEAS).
2. Gurnani, R., Pandey, K., & Rai, S. K. (2014, March). A scalable model for implementing Cyber Security Exercises. In 2014 International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 680-684). IEEE.

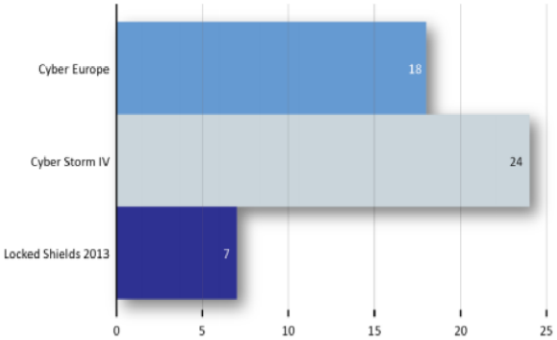
Cyber Security Exercises



Simulation, table-top and workshop, representing 81% of the total, while operation-based exercises represents 11 % of cyber security exercises conducted in 2015[3]



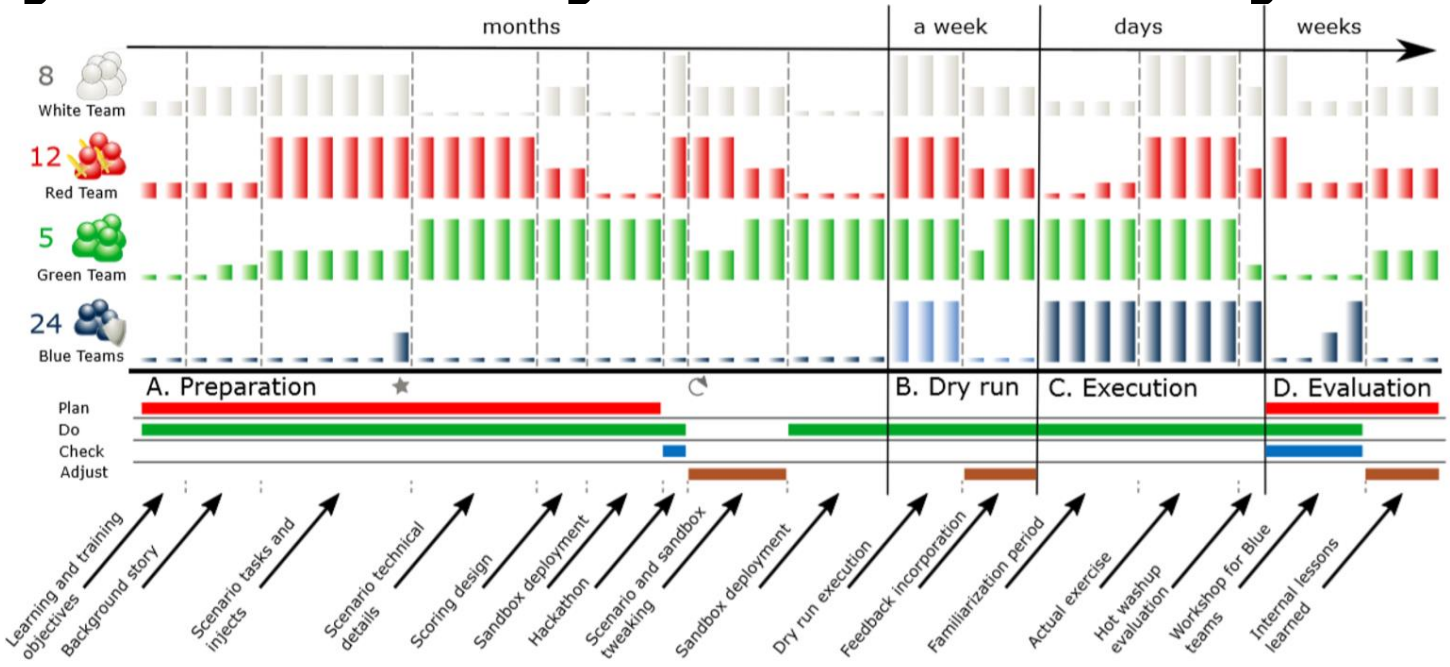
Participants knowledge test prior and after cyber-security exercise [4]



Exercise time-span in months [3]

[3] B. Uckan F¨arnman, M. Koraeus, S. Backman, The 2015 report on national and international cyber security exercises: Survey, analysis and recommendations (2015).
[4] J. Mirkovic, A. Tabor, S. Woo, P. Pusey, Engaging novices in cybersecurity competitions: A vision and lessons learned at acm tapia 2015, in: 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), 2015.

Cyber security exercise lifecycle



Cyber security exercise life cycle time requirement [5]

[5] J. Vykopal, M. Vizv´ary, R. Oslejsek, P. Celeda, D. Tovarnak, Lessons learned from complex hands-on defence exercises in a cyber range, in: Frontiers in Education Conference (FIE), IEEE, 2017, pp. 1–8.

Inefficiencies in Cyber-Security Exercises Life-Cycle[6]

- Inefficiencies in cyber-security exercise development and execution life cycle limit its ability to be widely used for cyber-security skill development.
- The roles of white, blue and red teams in a cybersecurity exercise need to be executed autonomously, which will increase the efficiency of preparation, execution and evaluation phases in cyber-security exercise life cycle .This will
  - Reduce the cost and time require for conducting cyber-security exercise,
  - Provide better training by always-available autonomous adversaries, and
  - Make cyber-exercises computationally repeatable for conducting systematic training.

Existing Research

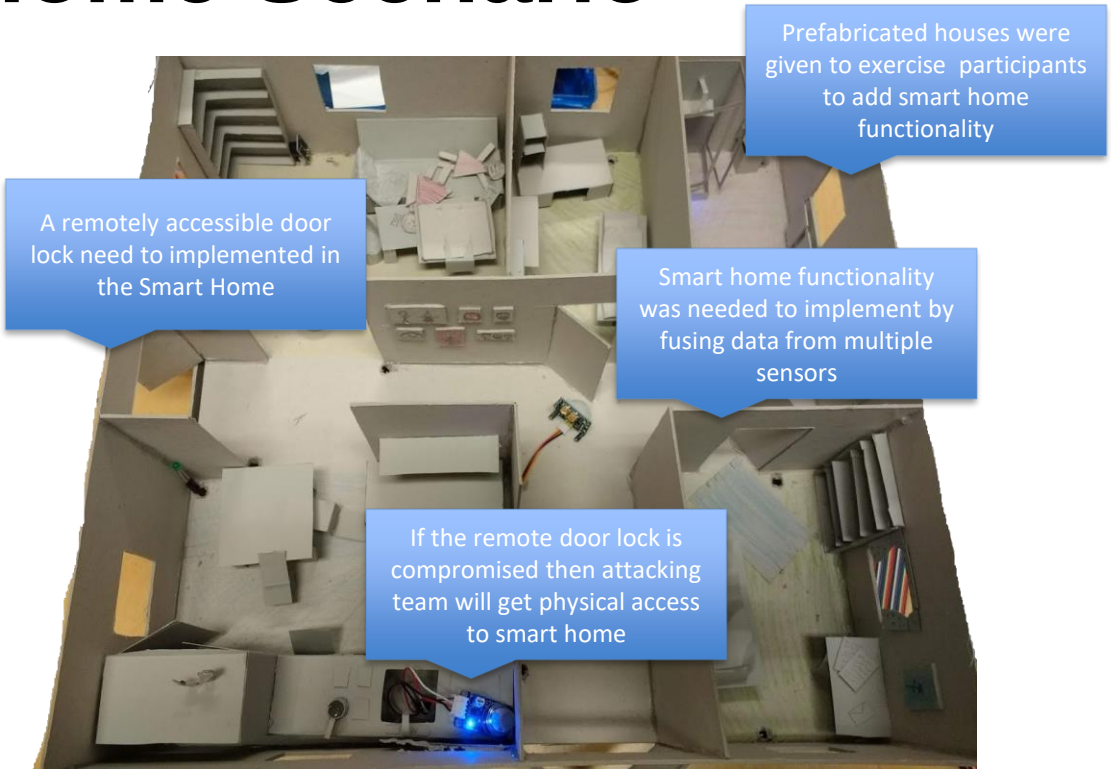
White Team	Red Team	Blue Team
Tele lab	SC2RM	VIAssist
Cyris	SVED	US ARL Cyber Agent
Secgen	Stuxnet	

[6] Yamin, M. M., & Katt, B. Inefficiencies in Cyber-Security Exercises Life-Cycle: A Position Paper.

Scenario

- An IoT based smart home scenario was created for a set of two teams A and B
- The scenario is divided in to two parts, in the first part, the teams A and B are tasked to design and build an IoT smart home from the list of given equipment
- In the second part of the scenario team A is tasked to exploit the weaknesses present in Team B’s smart home and Team B is tasked to exploit the weaknesses present in Team A’s smart home

Smart Home Scenario



Experiment Subjects

Norwegian national team for European Cyber Security Challenge 2018

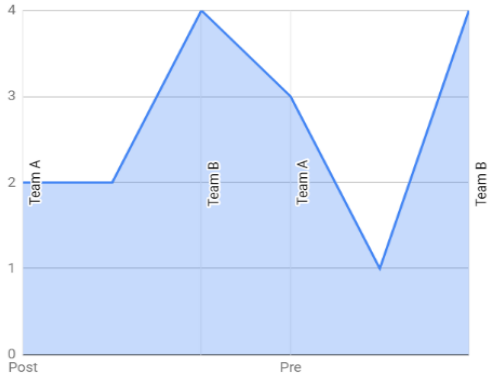
Knowledge Improvement

Phase	Team Name	knowledge in developing an IoT system?	knowledge in securing an IoT system?	knowledge in designing an IoT system?	knowledge in functional testing an IoT system?	knowledge in penetration testing an IoT system?	knowledge in interfacing between micro-controllers and sensors?	knowledge in collecting and processing IoT generated data?	knowledge in remote attacking IoT systems?	knowledge in local attacking IoT systems?
Pre	Team A	11	13	10	12	12	13	13	13	12
	Team B	11	8	10	7	5	11	10	4	7
Pre-Total		22	21	20	19	17	24	23	17	19
Post	Team A	11	14	12	14	13	14	13	16	13
	Team B	11	11	10	11	10	11	11	10	11
Post Total		22	25	22	25	23	25	24	26	24

Pre and Post exercise survey results in term of knowledge improvement

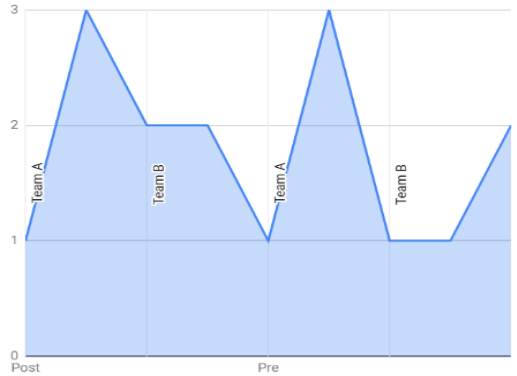
Automation In Cyber Security Exercises[7]

Do you think automation can help in planning the scenario for the test bed?



Graph 1: Pre and post exercise opinion of participants on automation of planning the scenario

Do you think automation can help in developing the test bed?



Graph 2: Pre and post exercise opinion of participants on automation in exercise testbed development

[7] Yamin, Muhammad Mudassar, et al. "Make it and Break it: An IoT Smart Home Testbed Case Study." Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control. ACM, 2018.

Serious Games as a Tool to Model Attack and Defense Scenarios for Cyber-Security Exercises

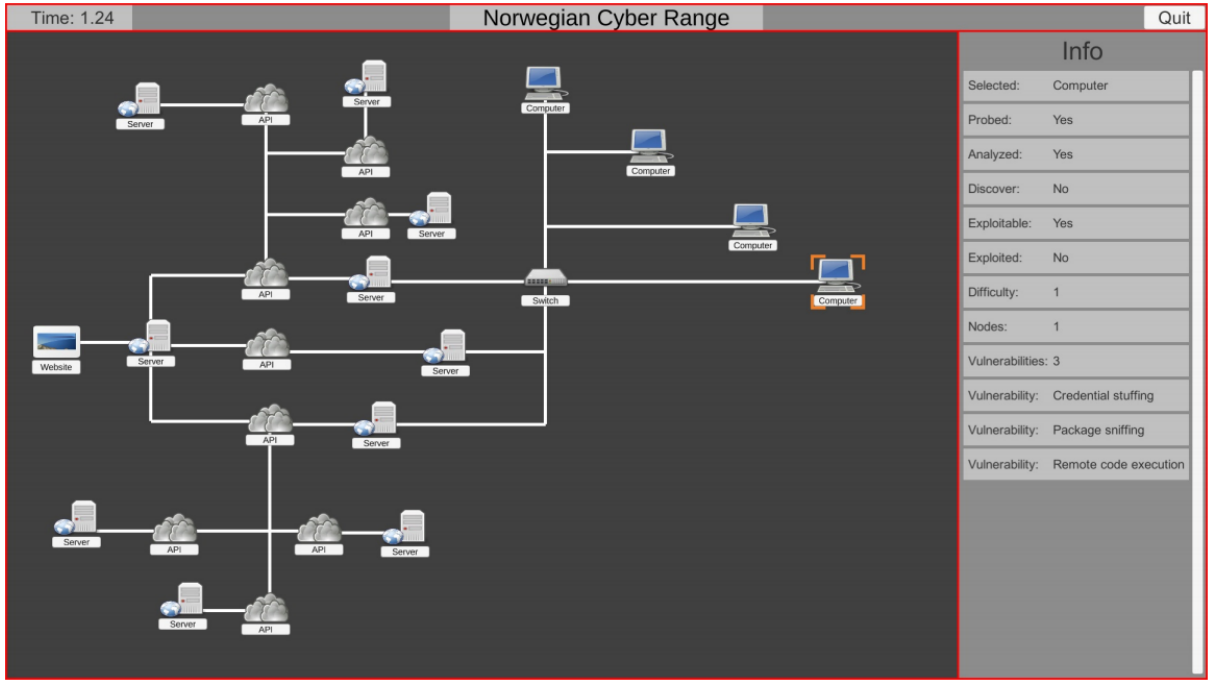
1. Use of serious games to model dynamic cyber-security exercises scenarios in a realistic manner.
2. Use of modeled cyber-security exercises in devising cyber attack and defense strategies in a realistic manner?
3. Is it efficient to conduct cyber-security exercises in a simulated modeled environment for exercise participants skill improvement?

Real Time Cyber Security Strategy Game

- Actors and functionalities
  - White Team
  - Red Team
  - Blue Team
  - Game Economy
- Methods
  - Scenario Modeling
  - Penetration Testing Methodology
  - Cyber Kill Chain

Its all about perspective

Developed Game

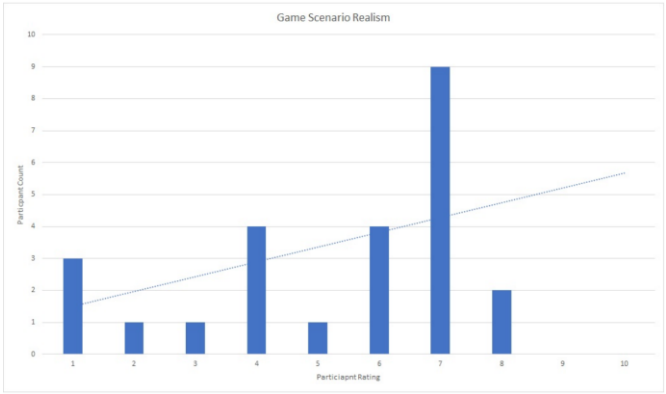


http://prod3.imt.hig.no/LordXyroz/cyber-security-simulator

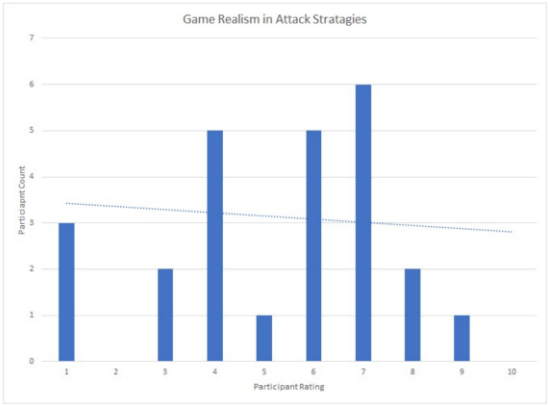
Evaluation

Test Subjects for Game Evaluation During Norwegian Cyber Security Challenge 2019

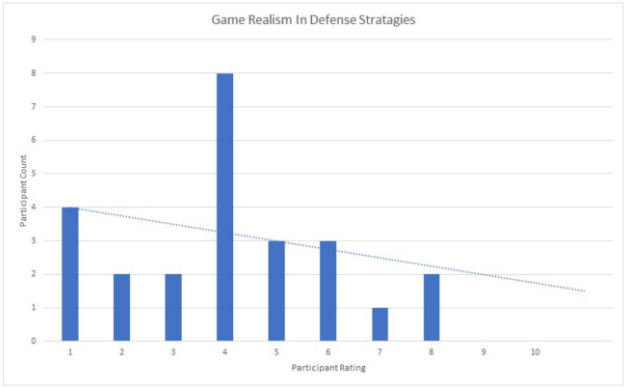
Realistic Cyber Attack and Defense Scenario Modeling



Cyber Scenario Realism Rating

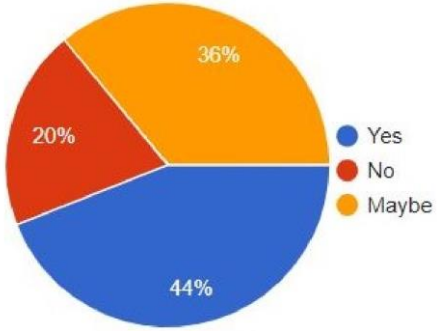


Cyber Attack Strategies Realism

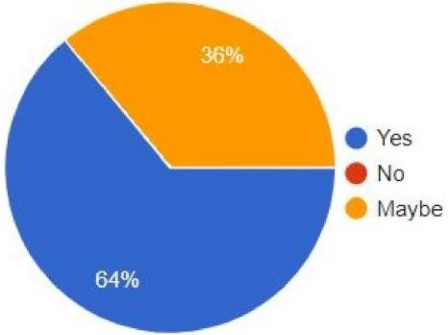


Cyber defense strategies realism

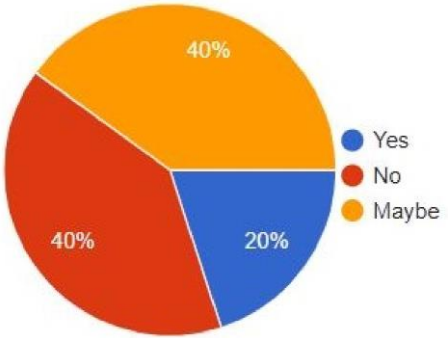
Efficiency in Cyber Security Exercises



Percentage of participants who think developed game is useful for cyber security education



Percentage of participants who think its efficient to conducting cyber-security exercises scenarios in simulated modeled environment



Percentage of operational strategy decision making skill improvement in cybersecurity exercises

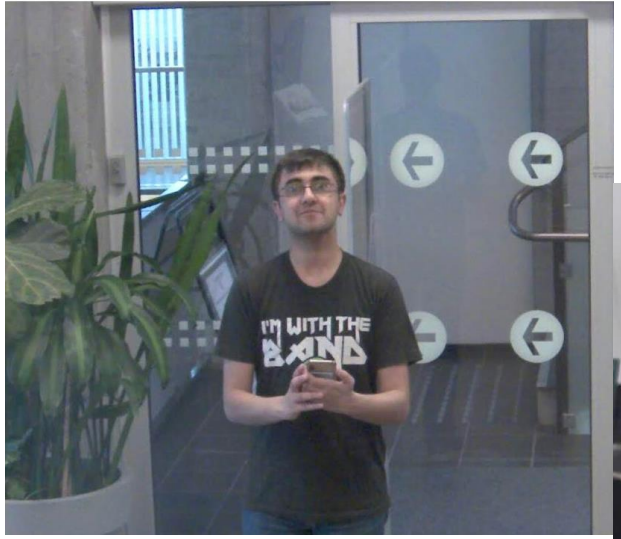
Cyber Attack Agent

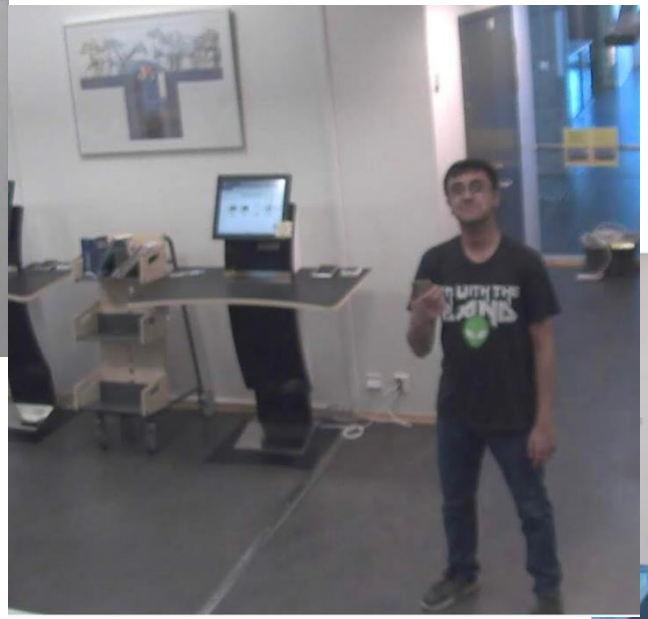
Muhammad Mudassar Yamin

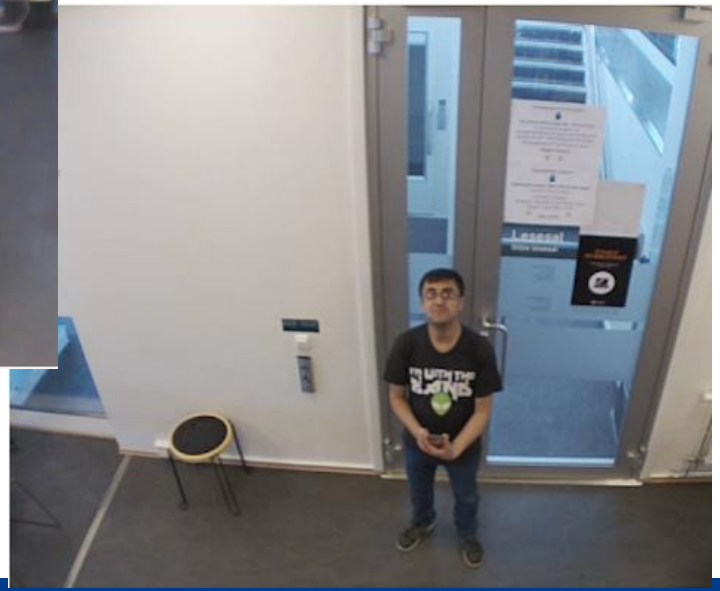
With great power comes great responsibility

~Uncle Ben

To take good selfies


I'M WITH THE
BAND





Civil Liabilities and Unintended Consequences

- Autonomous weapons system developer is responsible for unintended consequences of the autonomous system functionality*
- Autonomous weapon system user is responsible for criminal negligence*
- The consensus of international community established that the decision making of autonomous system should always be governed by human**

* Lucas Jr, G. R. (2014). Legal and ethical precepts governing emerging military technologies: Research and use. Amsterdam LF, 6, 23
** Bode, I., and Huelss, H. (2018). Autonomous weapons systems and changing norms in international

Modern Adversaries in Modern Warfare

Cyber weapons are software, firmware or hardware designed or applied to cause damage through the cyber domain*

*Michael N Schmitt. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

Preferable Weapon of Choice

NTNU

What if a Country Losses Control on Its Cyber Arsenal?

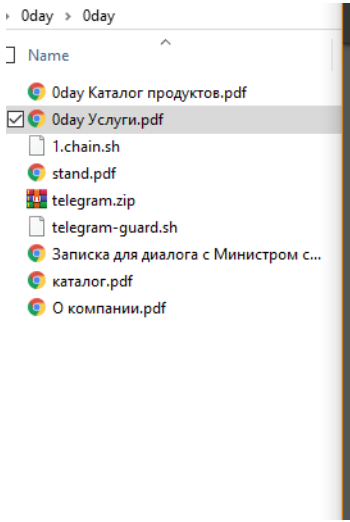
NTNU

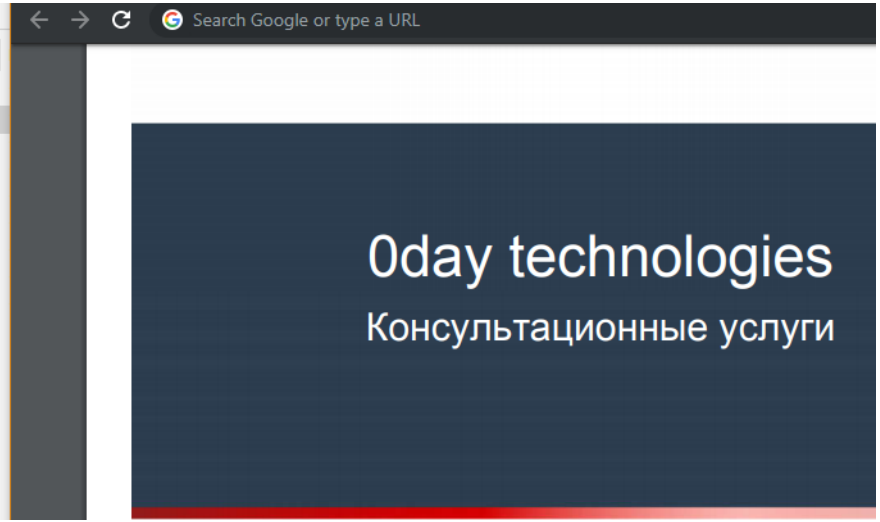
https://tass.ru/ekonomika/5129977

TELEGRAM PROBLEMS IN RUSSIA APR 16, 2018 12:02 Updated Apr 16, 2018 1:05 pm

Roskomnadzor began blocking Telegram procedure

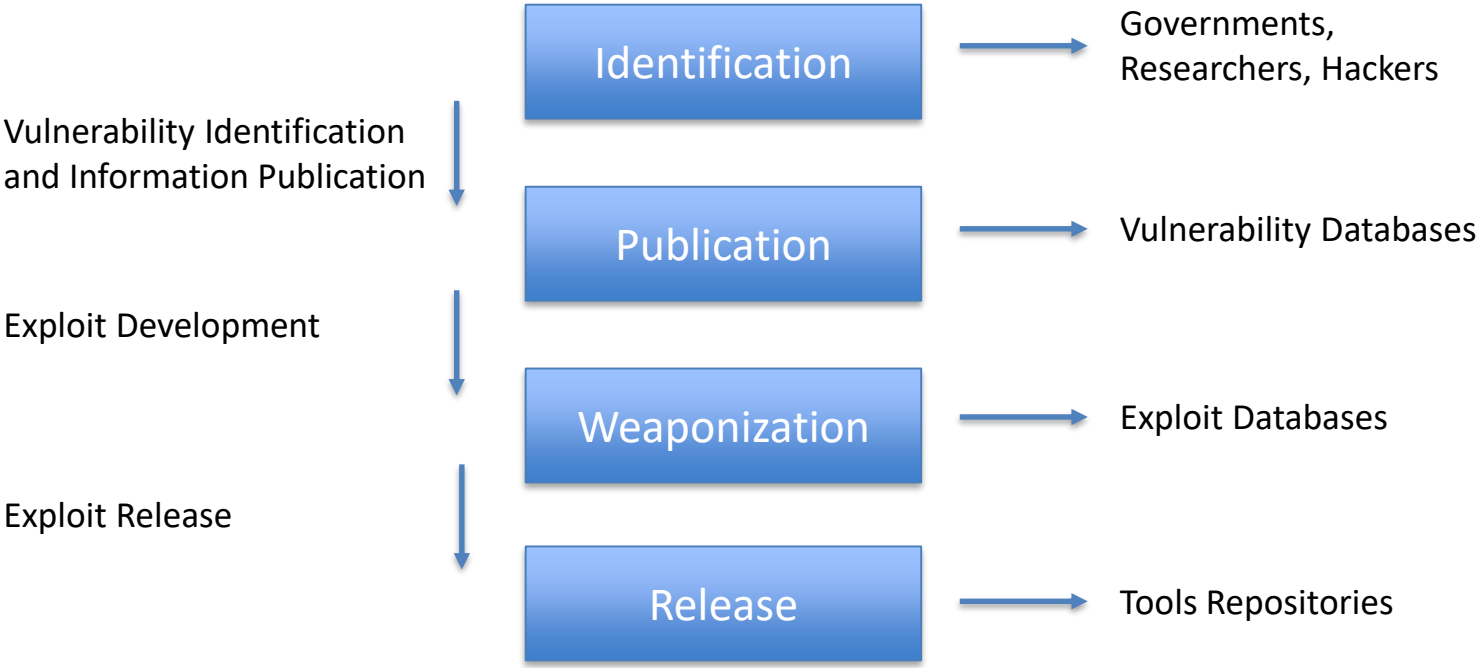
The department said they had received the relevant court decision



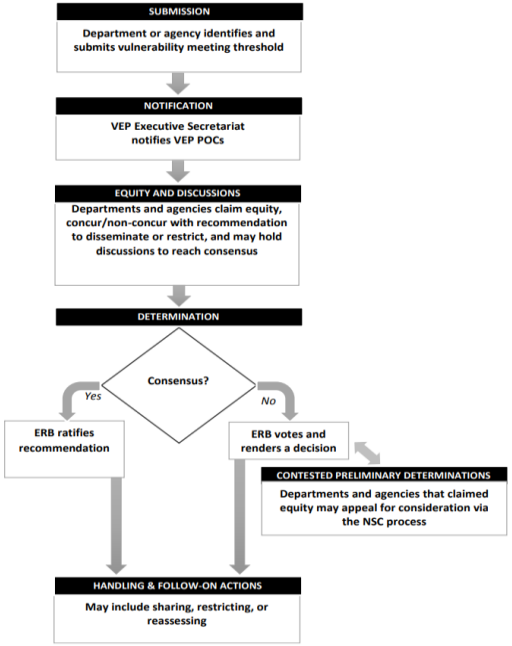


NTNU

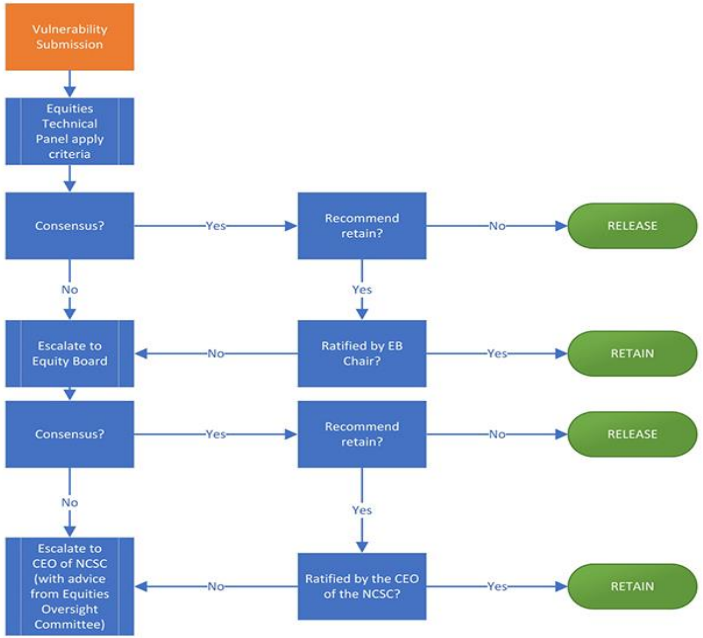
Cyber Weapons Development Process



Vulnerabilities Equities Process (VEP)



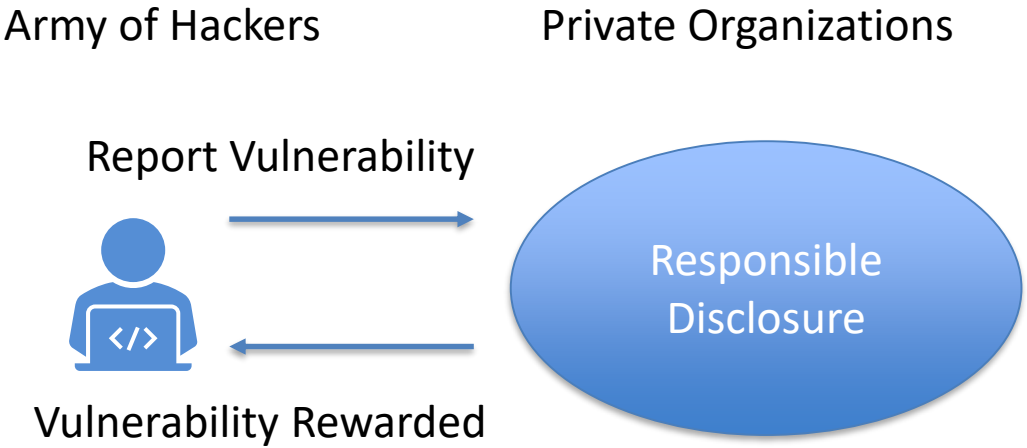
USA VEP*



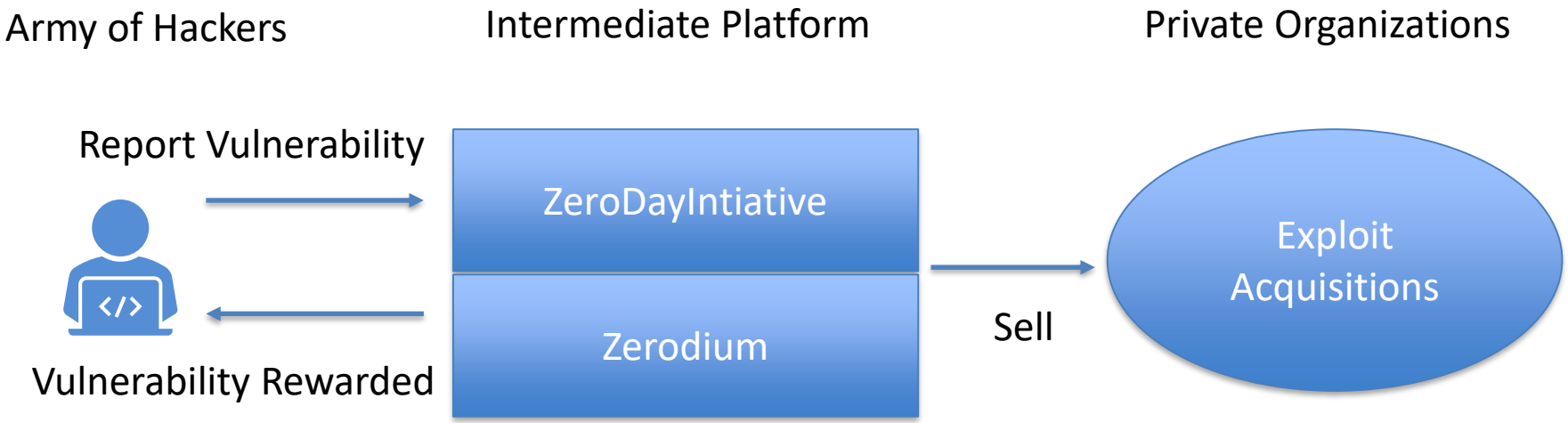
UK VEP**

https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
https://www.gchq.gov.uk/information/equities-process

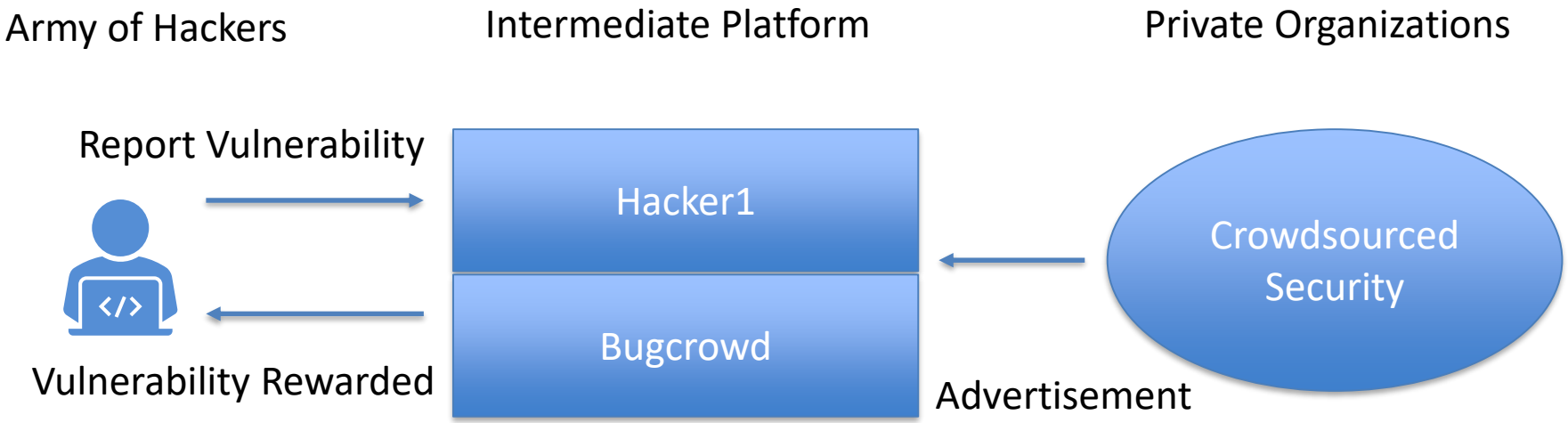
Responsible Disclosure Programs (RDP)



Exploit Acquisition Programs (EAP)



Bug Bounties Programs (BBP)



Comparison

Name	Time to Release	Payment	Technical Risk	Human Risk
VEP	>7 days	N/A	Yes	Yes
RDP	90 days	Yes	Yes	Yes
EAP	Variable	Yes	Yes	Yes
BBP	Variable	Yes	Yes	Yes

Comparison of Different Vulnerability Disclosure Programs

Vulnerability Databases

VULDB

THE CROWD-BASED VULNERABILITY DATABASE

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

CNNVD

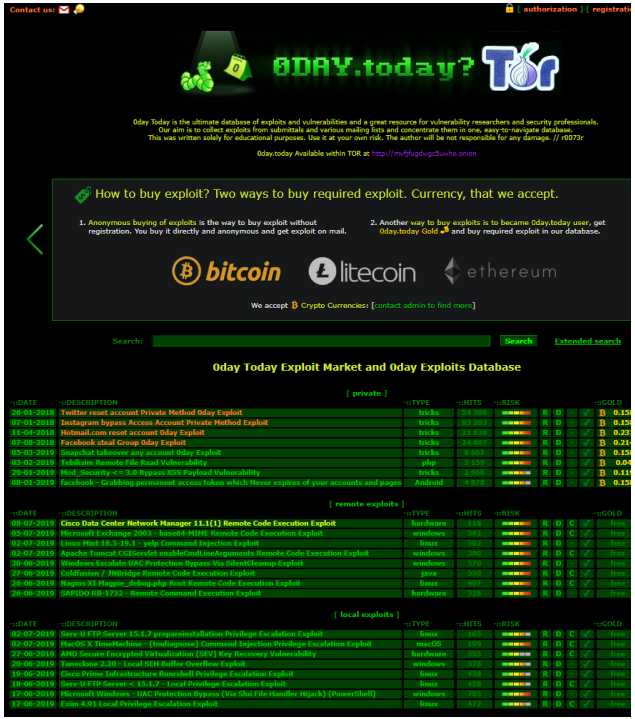
国家信息安全漏洞库

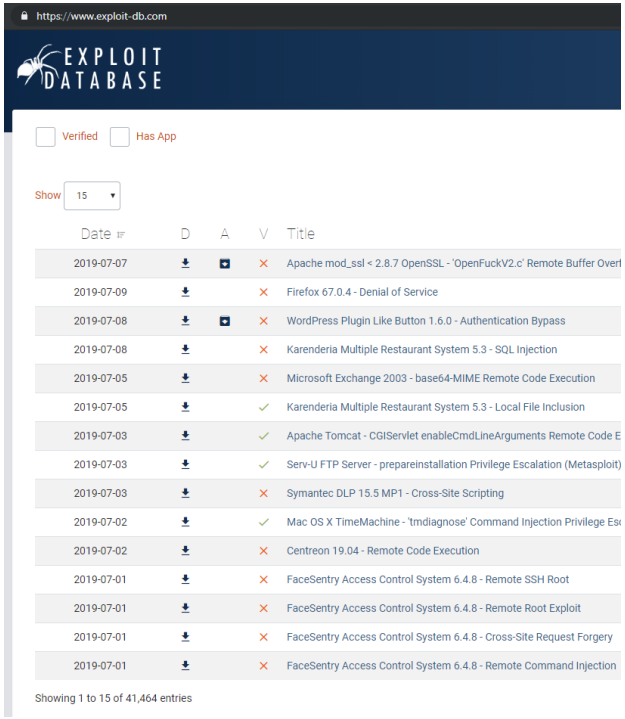
China National Vulnerability Database of Information Security

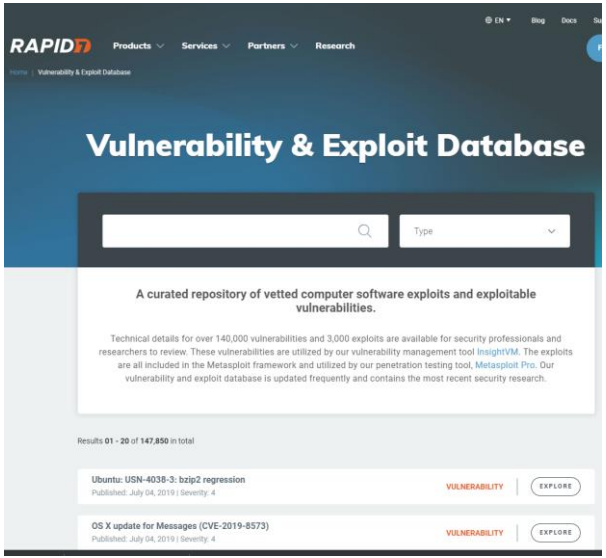
FSTEC Russia

Федеральная служба по техническому и экспортному контролю

Exploit Databases

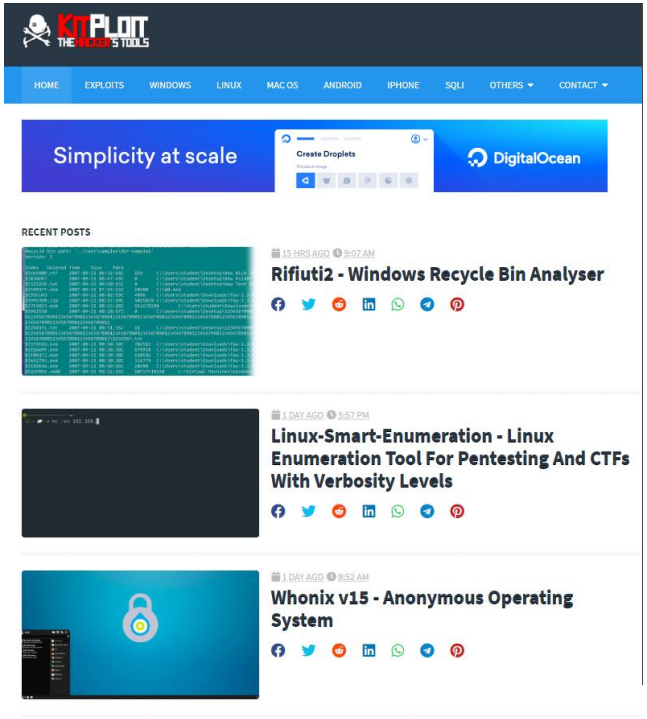


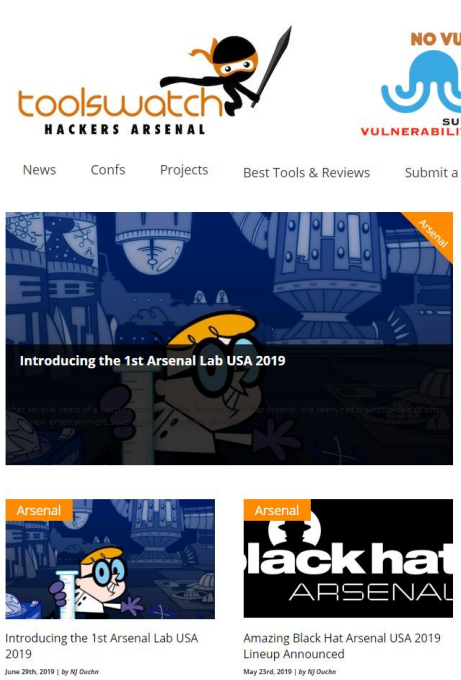


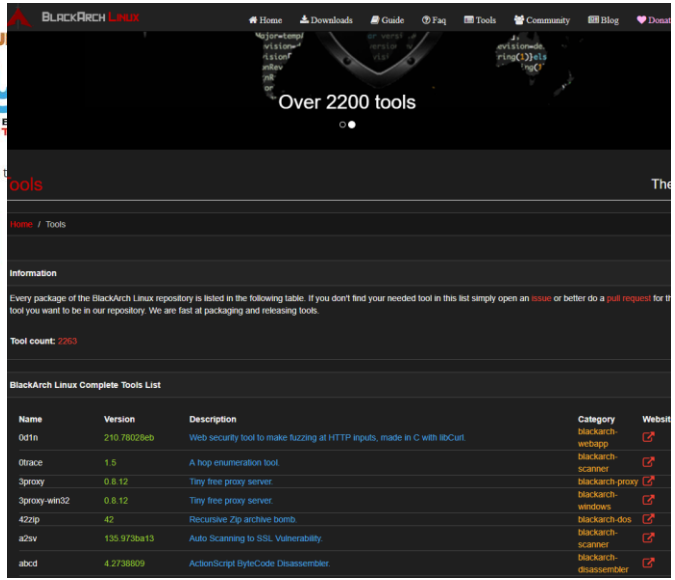


NTNU

Tools Repositories







NTNU

Cost of Leaked Cyber Weapons

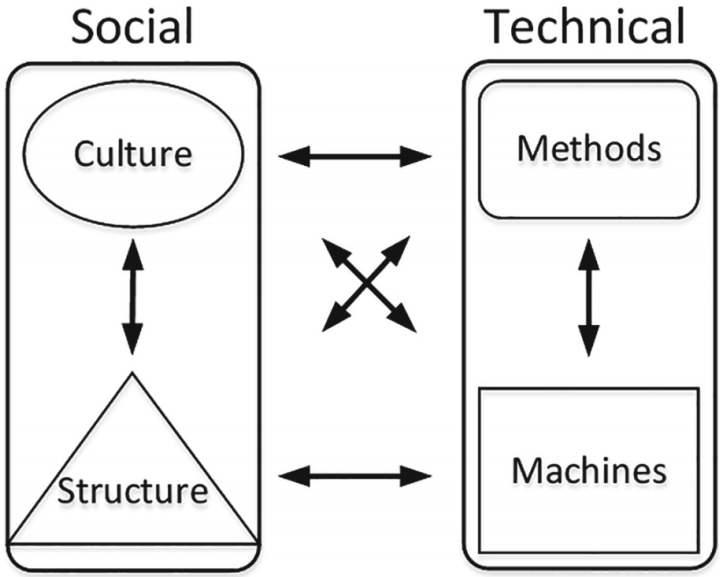
- “Wannacry” ransomware malware attack had nearly 200000 victims and 300000 affected systems in 150 countries
- The losses caused by this single cyber attack reached 4 billion
- These cyber attacks affected health services as well, therefore, calculating the actual cost of such attacks is very difficult

Threat Actors and Challenges in Securing Cyber Weapons

- Human negligence
- Insider threat
- Dissatisfied gray hat hackers and security researchers
- Hacktivist groups
- State sponsored attack

Proposed Framework

- Culture
  - Human Moral Values
- Structure
  - Cooperation among the Stakeholders
- Method
  - Proactive Cyber Defense
  - Cyber Threat Hunting
  - Cyber Security Training and Awareness
- Machine
  - Cyber Range



The complex, dynamic socio-technical system. The interconnecting subcomponents determine the overall security posture of the system

Vulnerabilities

"~~Questions~~ are guaranteed in

Patches ~~life; answers~~ aren't"