

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

By Muhammad Mudassar Yamin

COINS Summer School

Metochi Greece, 27th of July 2019

# 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](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

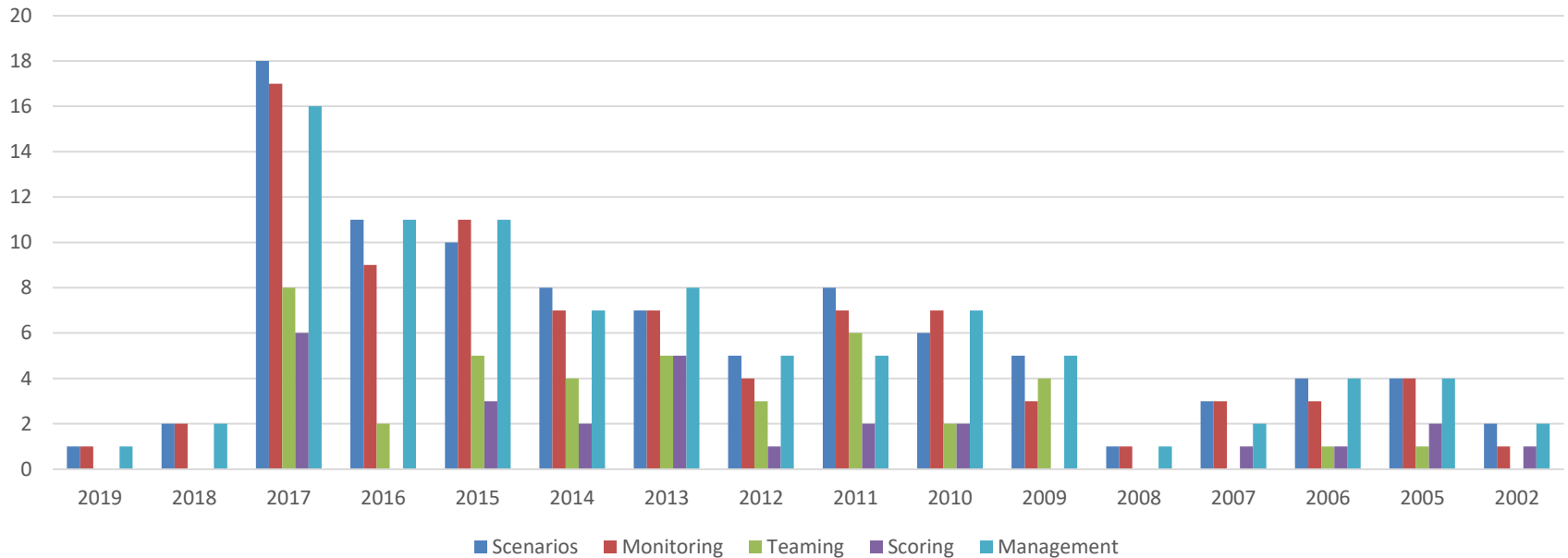
- **Round 1:** Collection of the literature was conducted in March 30th. It resulted in a total entries of 385
- **Round 2:** Elimination of duplicates was conducted in April 25th, and resulted in a total entries of 310
- **Round 3:** Back tracing additional entries from the citations of the current 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

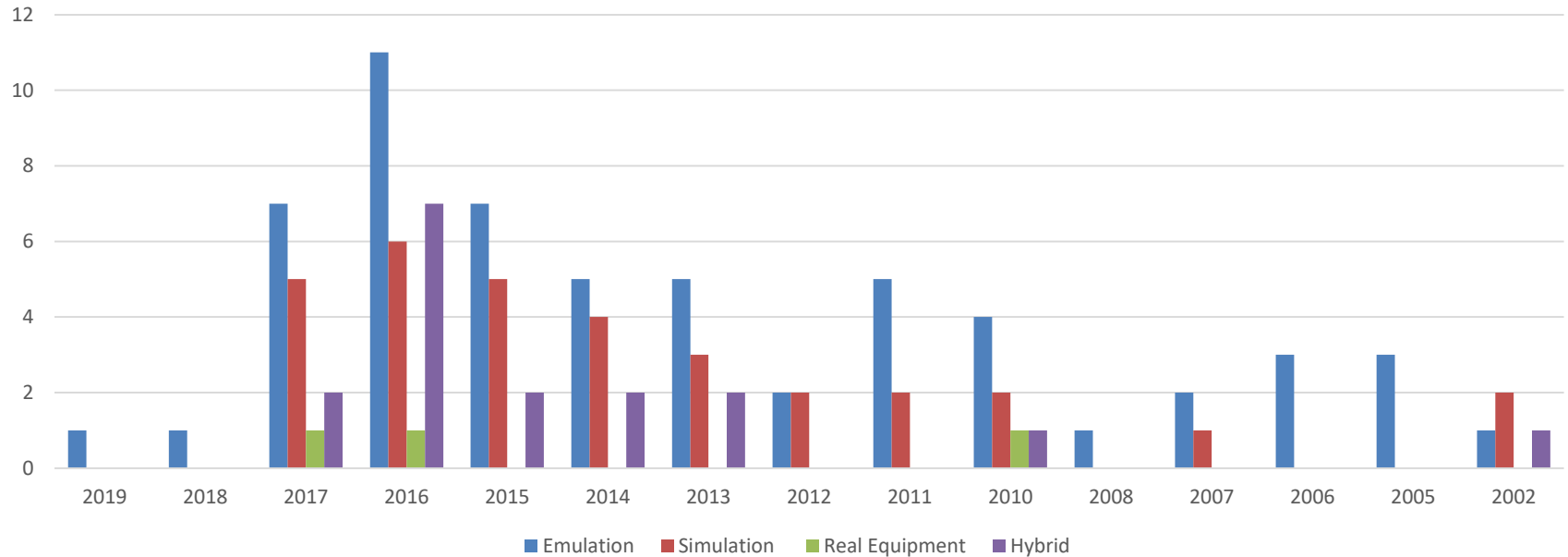
Overall Classification





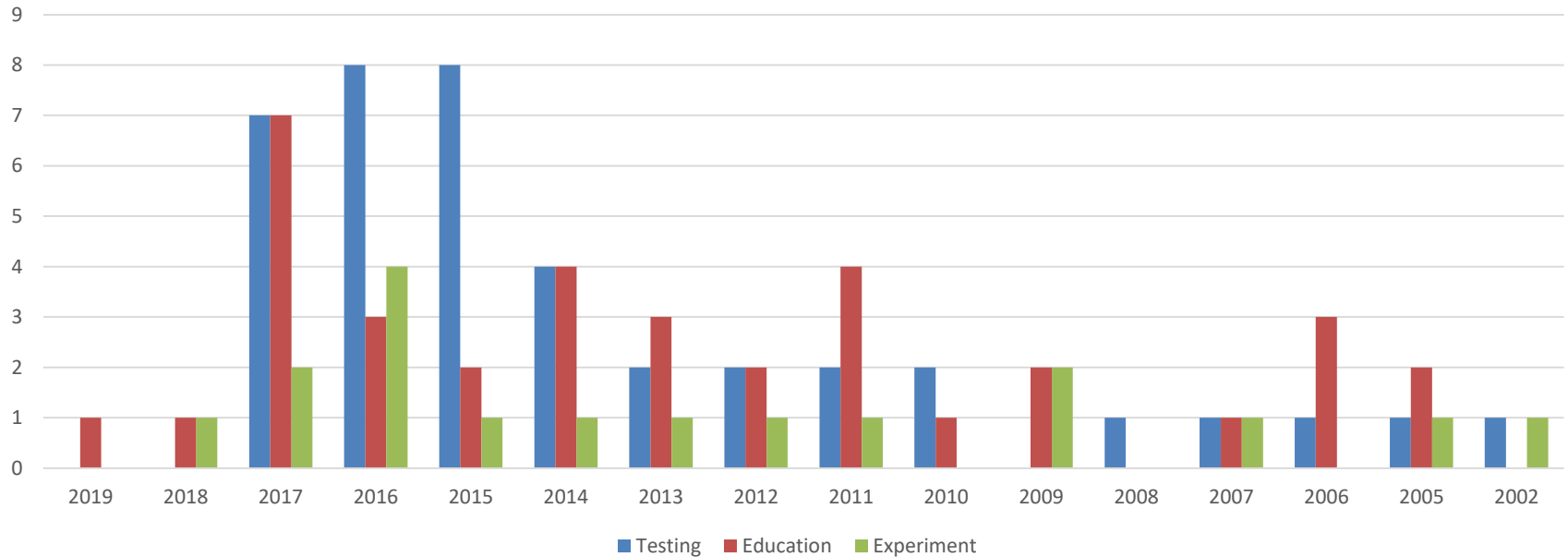
# Environment

Scenerio Execution Enviroment



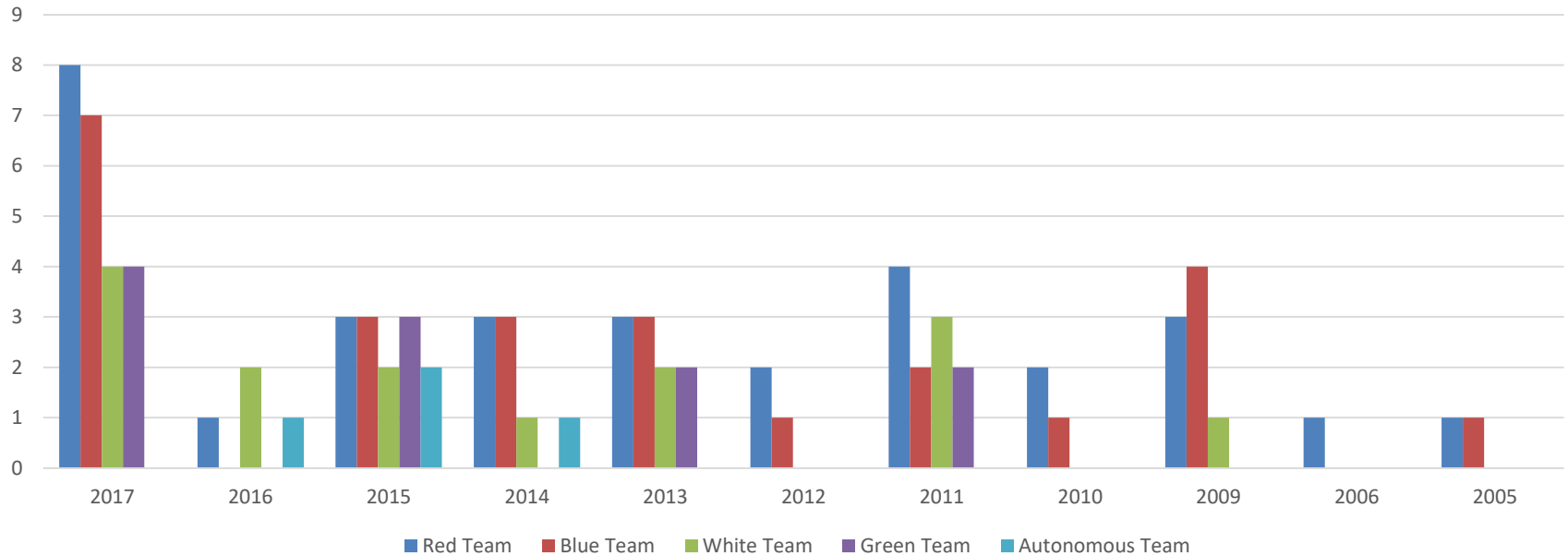
# Purpose

Scenerios Purposes



# Teams

Classification based upon teams



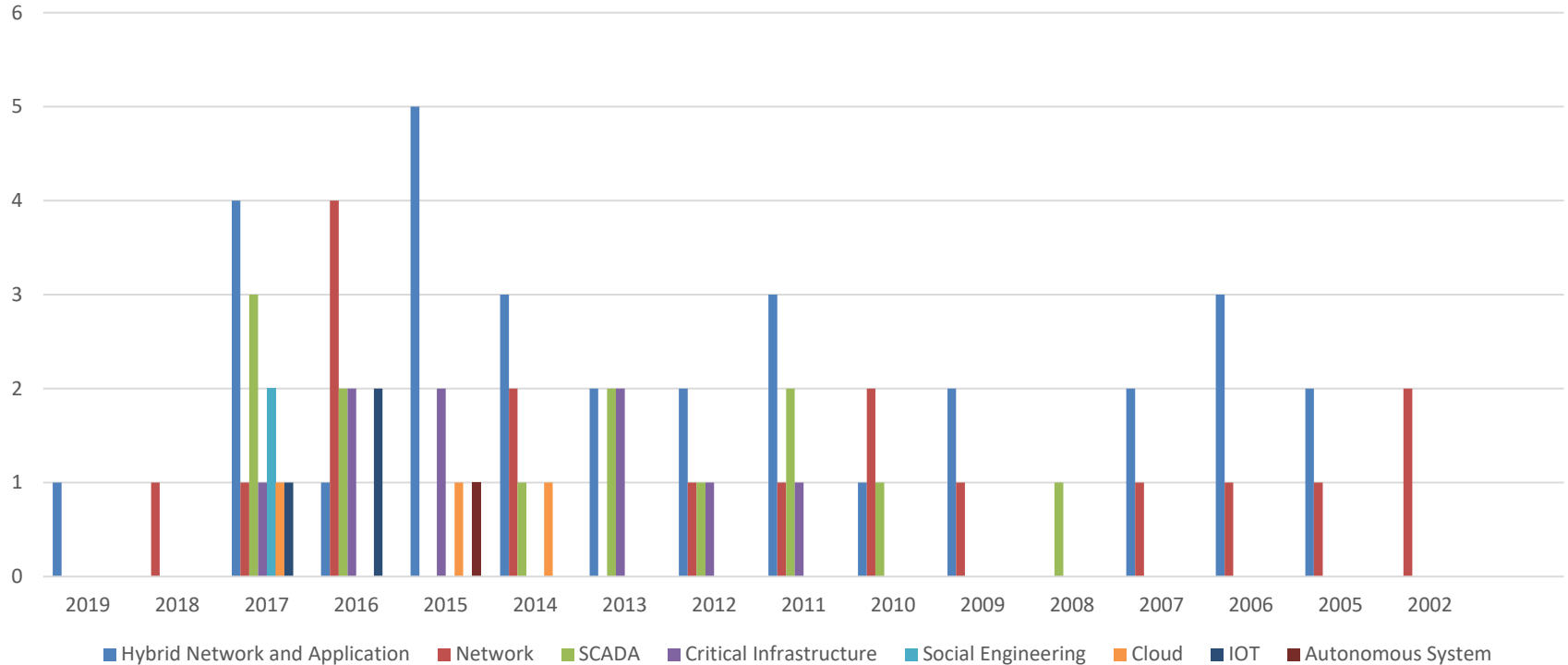
# Scoring Mechanism

classification based upon scoring mechanism



# Domains

Classification With Respect To Domain



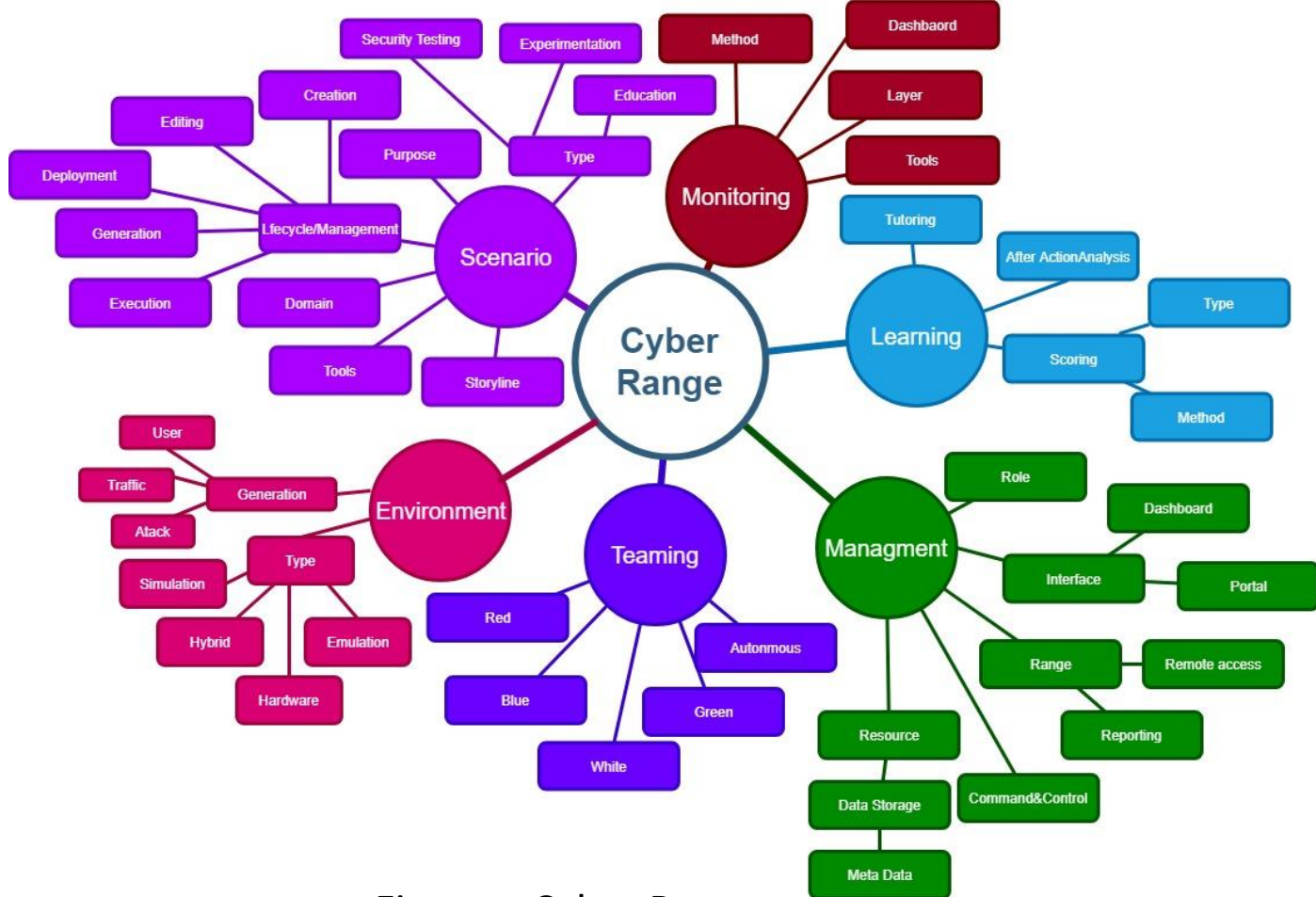


Figure : Cyber Range taxonomy

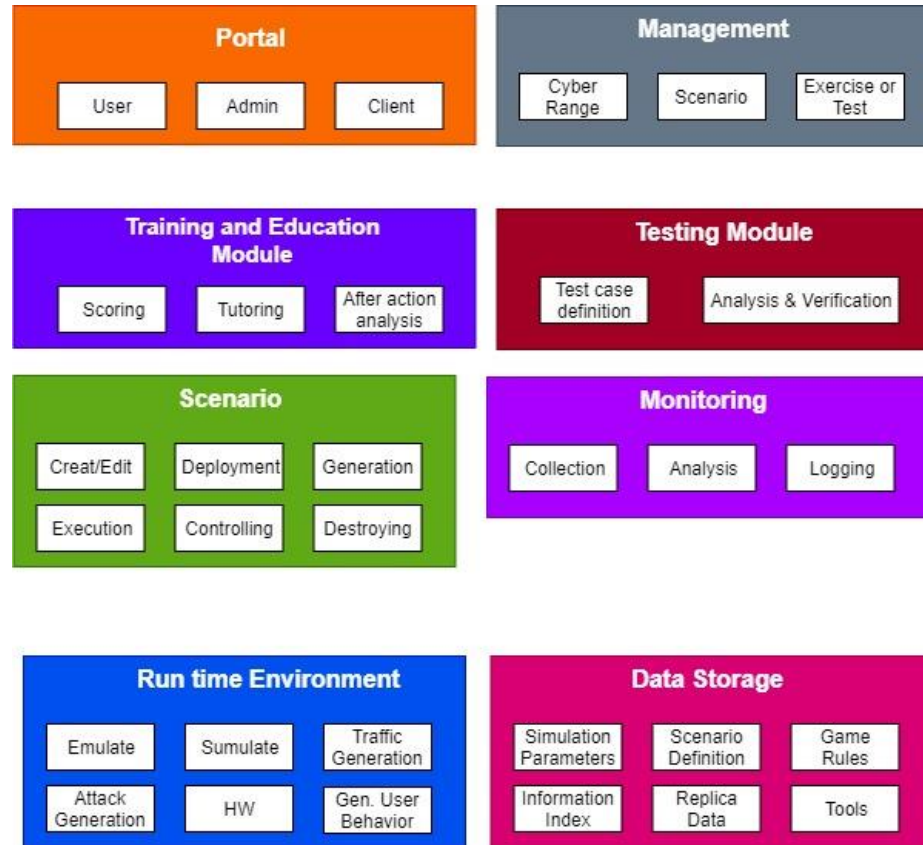


Figure : Cyber range and security testbed functional architecture

# 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.

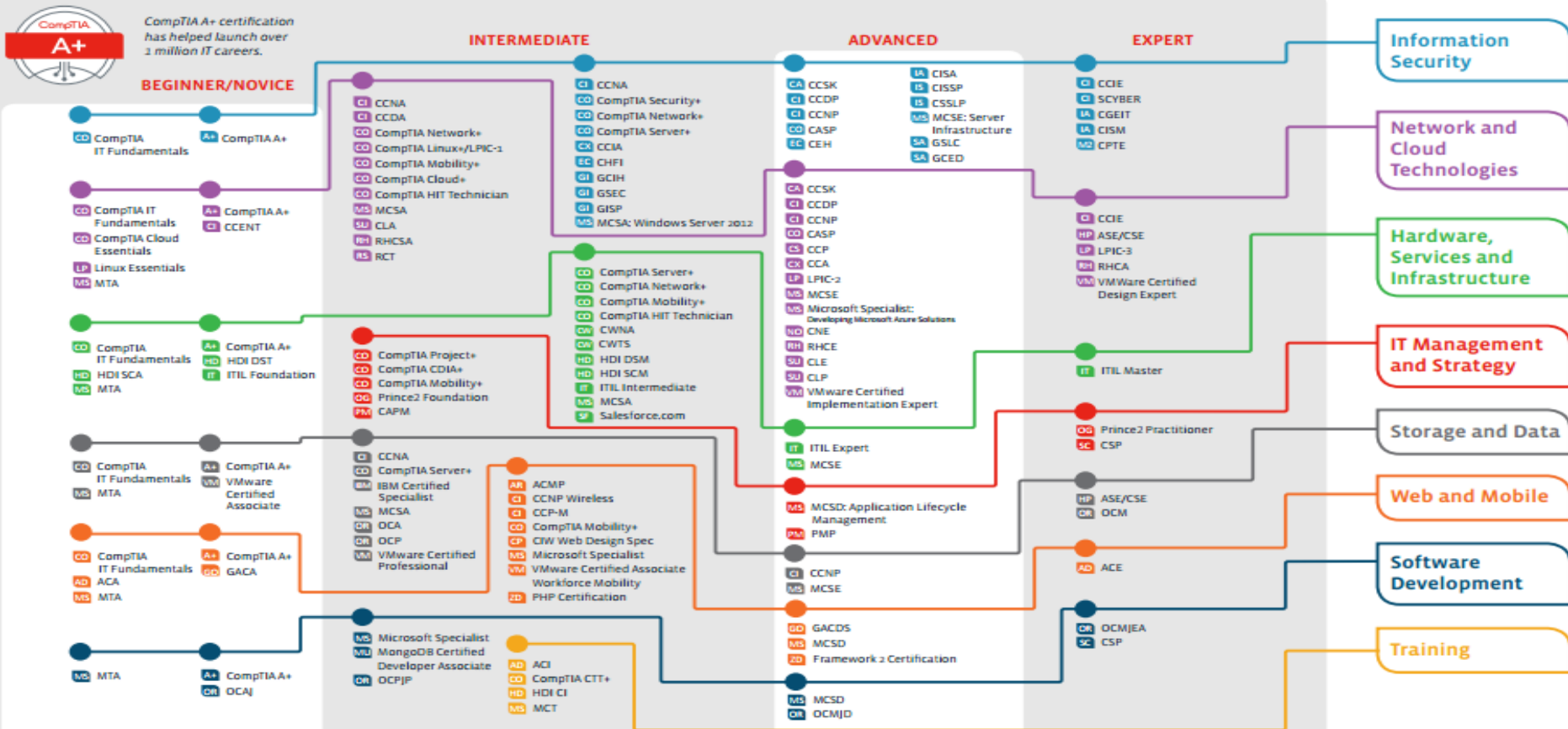


# IT Certification Roadmap

Explore the possibilities with the *CompTIA Interactive IT Roadmap at: [CompTIA.org/CertsRoadmap](http://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		
<p>IAT Level I</p> <p>A+ CE CCNA-Security Network+ CE SSCP</p>	<p>IAT Level II</p> <p>CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP</p>	<p>IAT Level III</p> <p>CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH</p>
<p>IAM Level I</p> <p>CAP GSLC Security+ CE</p>	<p>IAM Level II</p> <p>CAP CASP+ CE CISM CISSP (or Associate) GSLC CCISO</p>	<p>IAM Level III</p> <p>CISM CISSP (or Associate) GSLC CCISO</p>
<p>IASAE I</p> <p>CASP+ CE CISSP (or Associate) CSSLP</p>	<p>IASAE II</p> <p>CASP+ CE CISSP (or Associate) CSSLP</p>	<p>IASAE III</p> <p>CISSP-ISSAP CISSP-ISSEP</p>
<p>CSSP Analyst</p> <p>CEH CFR CCNA Cyber Ops CySA+ ** GCIH GICSP SCYBER</p>	<p>CSSP Infrastructure Support</p> <p>CEH CySA+ ** GICSP SSCP CFR</p>	<p>CSSP Incident Responder</p> <p>CEH CFR CCNA Cyber Ops CySA+ ** GCFA GCIH SCYBER CHFI</p>
<p>CSSP Auditor</p> <p>CEH CySA+ ** CISA GSNA CFR</p>	<p>CSSP Manager</p> <p>CISM CISSP-ISSMP CCISO</p>	

# My Experience with Certs

## RED Team Certs



## Blue Team Certs

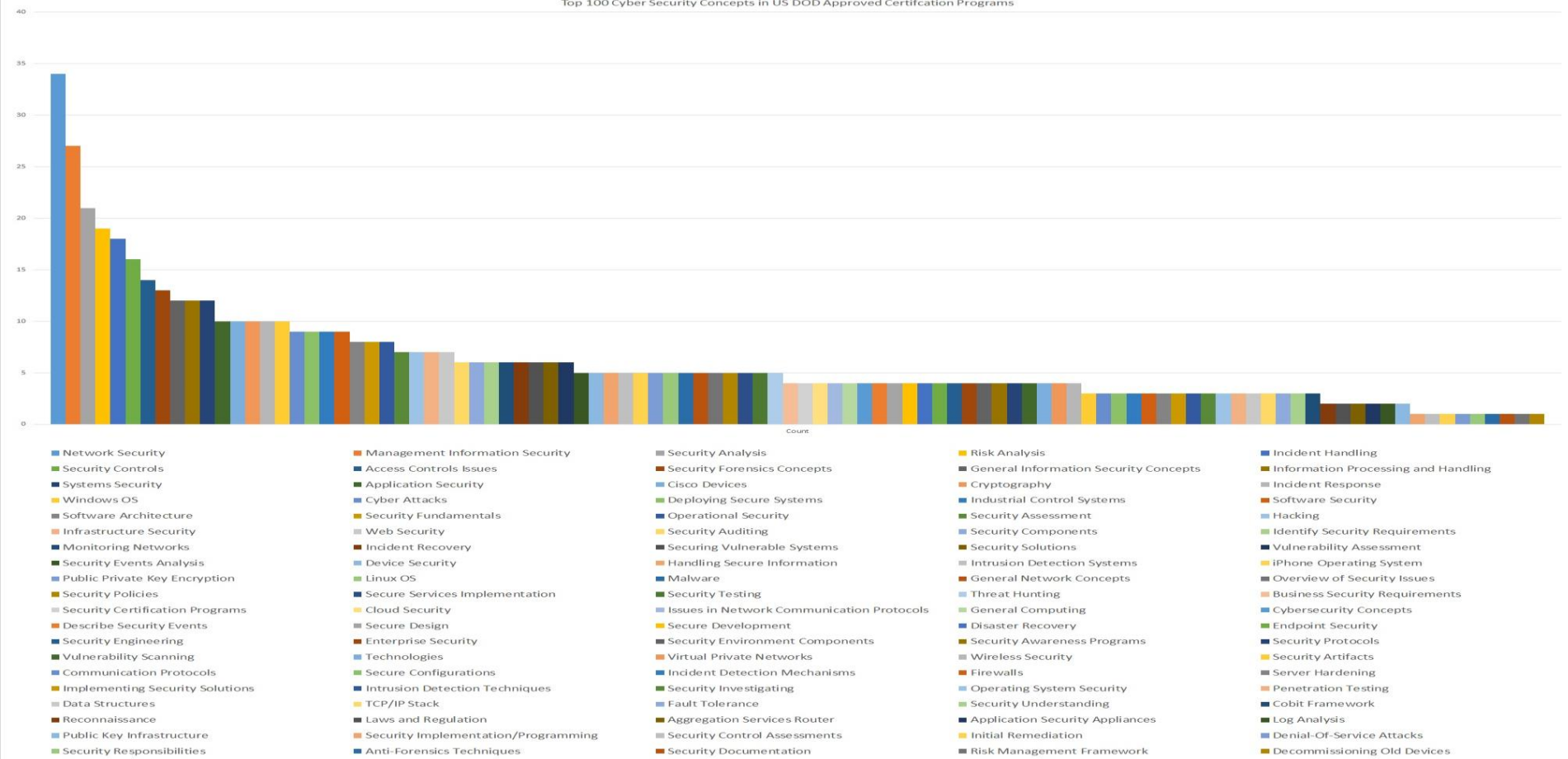


## Management

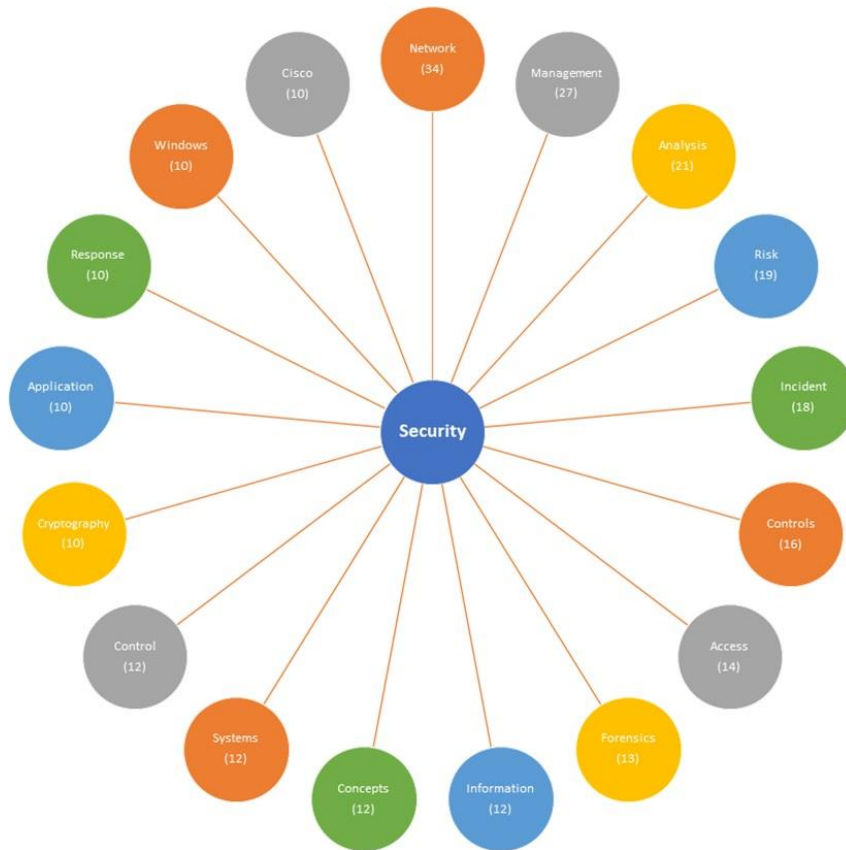


It's all for fun, but don't get me wrong -- it's about bragging rights for 364 days a year.

- 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

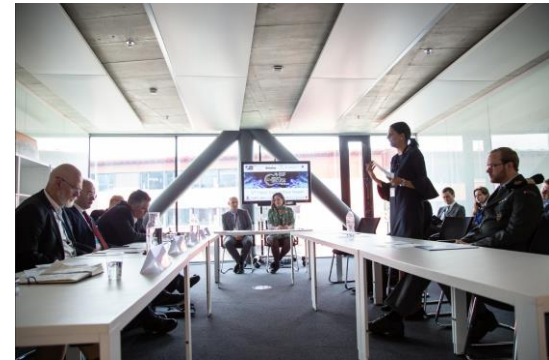
- Cyber security exercises are a very effective way of learning the practical aspects of information security<sup>[1]</sup>
- Cyber Security Exercises are broadly categorized<sup>[2]</sup>

## Operation Based



Norwegian Cyber Security Challenge 2018

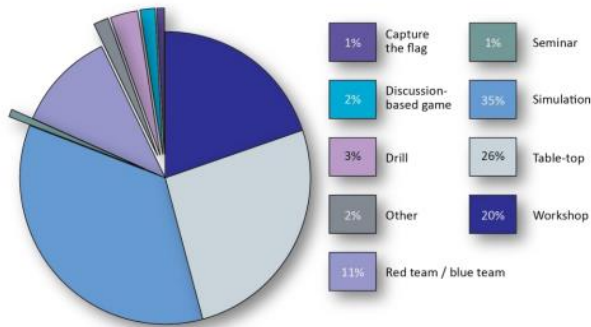
## Tabletop Based



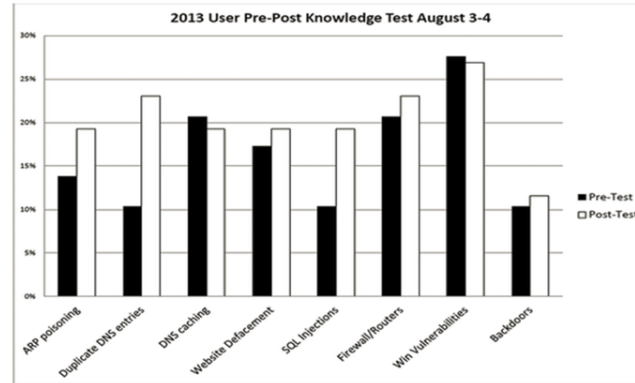
Atlantic Council Cyber 9/12 Challenge 2019

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.

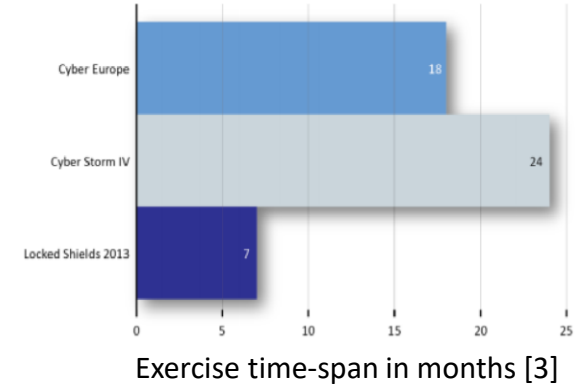
# Cyber Security Exercises



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]

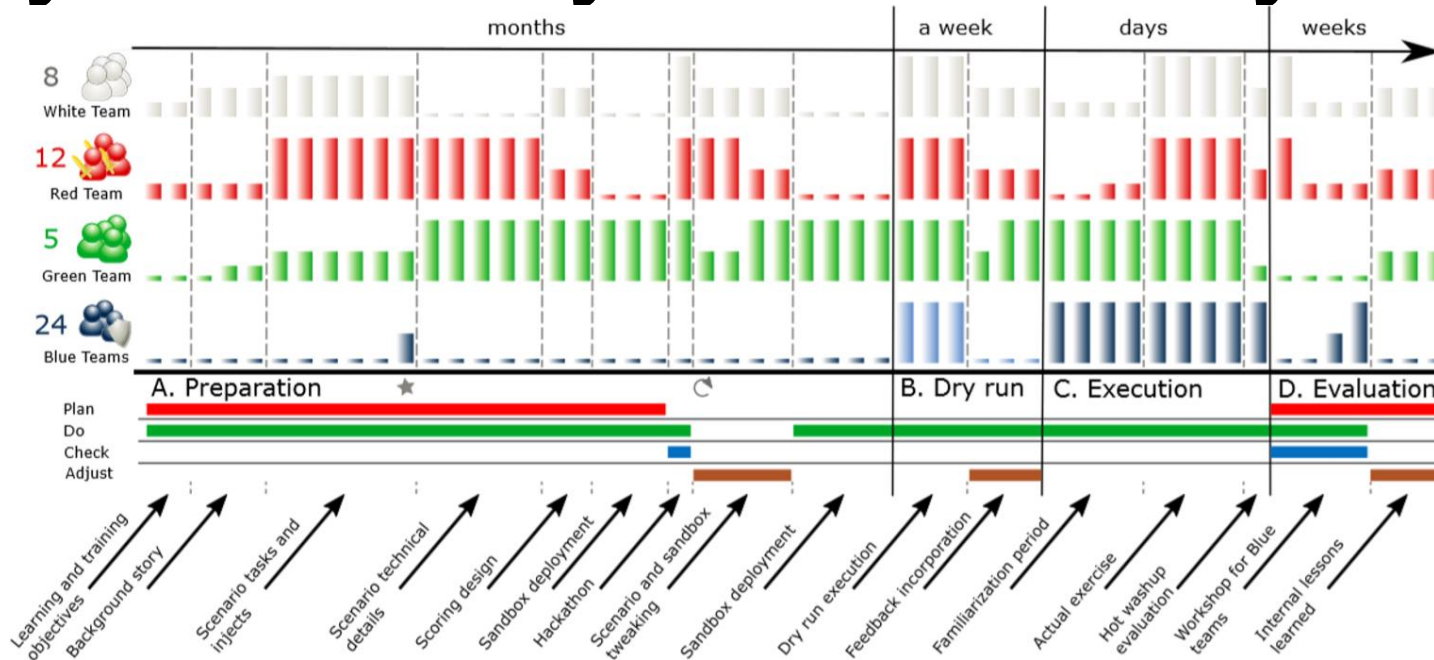


[3] B. Uckan Farnman, M. Koraeus, S. Backman, The 2015 report on national and international cyber security exercises: Survey, analysis and recommendations (2015).

[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. Vizváry, 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

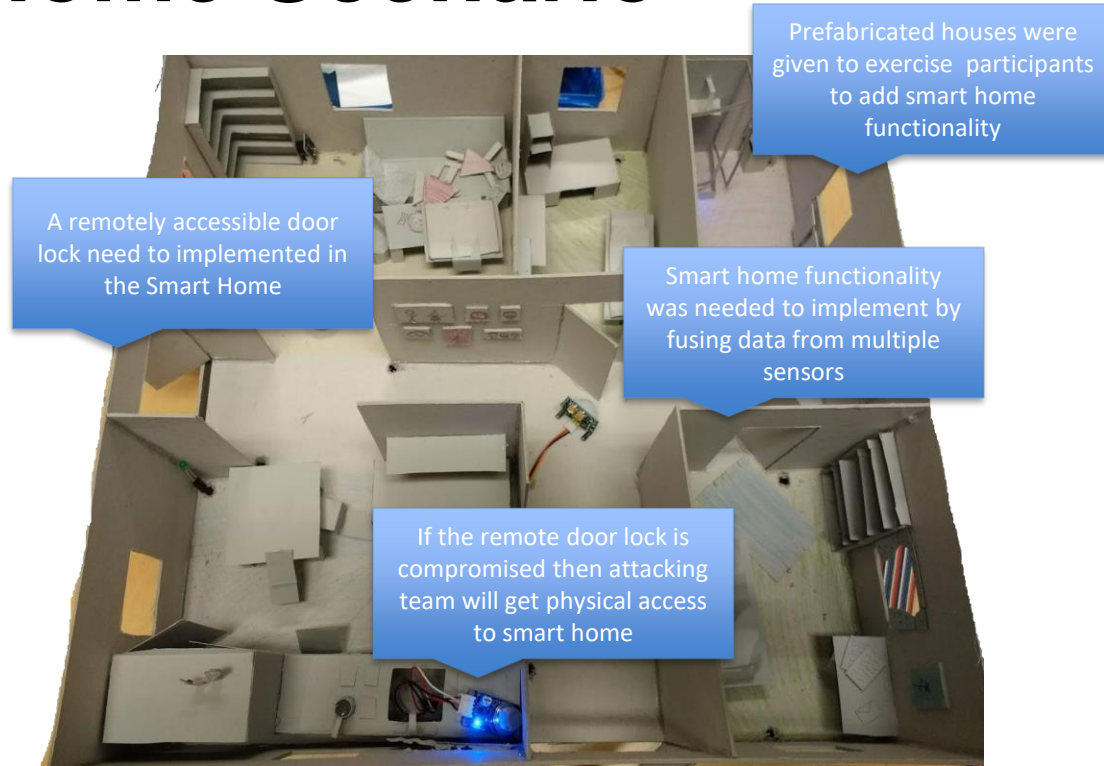
White Team	Red Team	Blue Team
Tele lab	SC2RM	VIAssist
Cyris	SVED	US ARL Cyber Agent
Secgen	Stuxnet	

[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

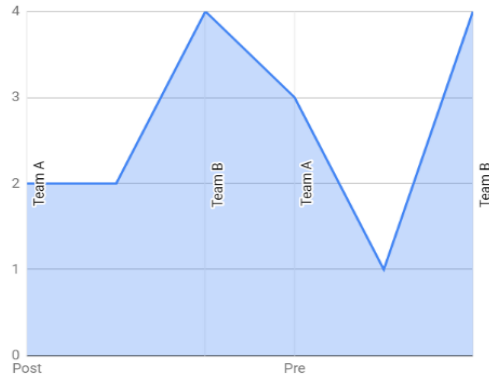
# Knowledge Improvement

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

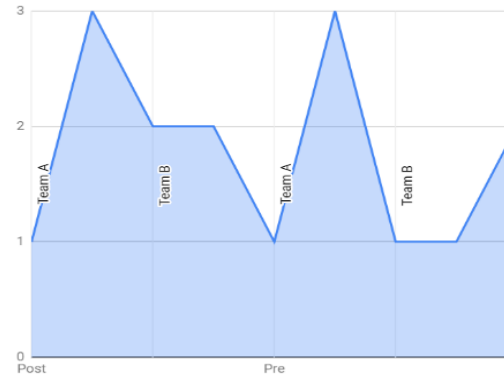
# Automation In Cyber Security Exercises[7]

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?

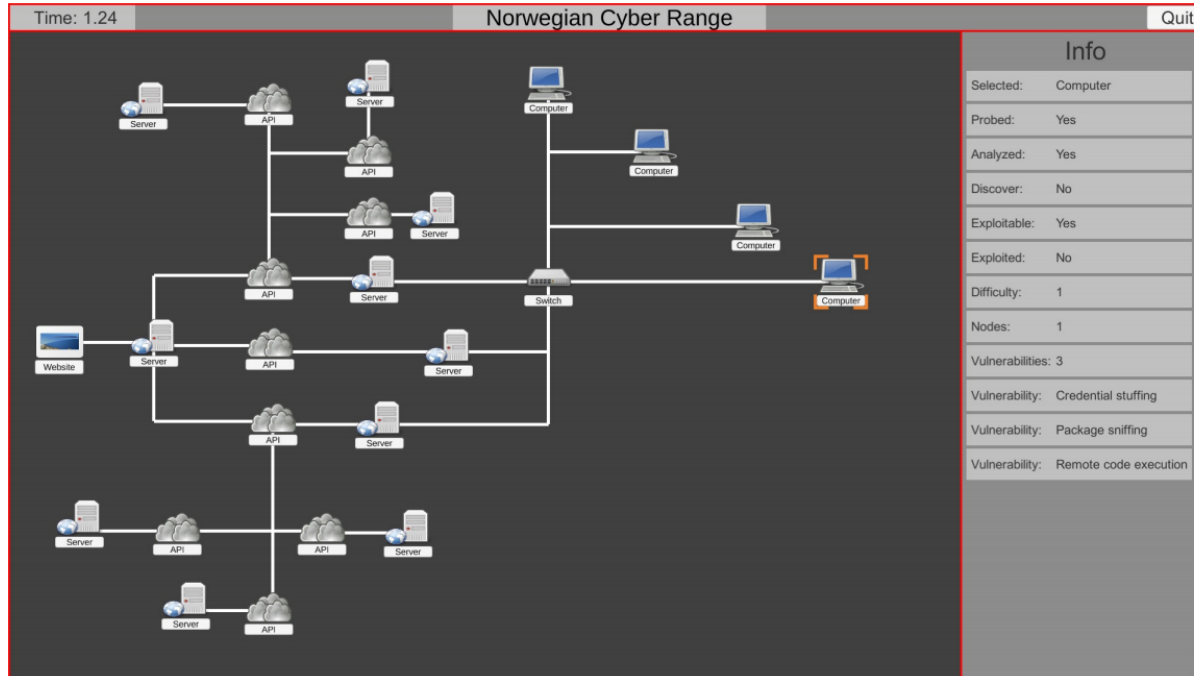


# Real Time Cyber Security Strategy Game

- 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>

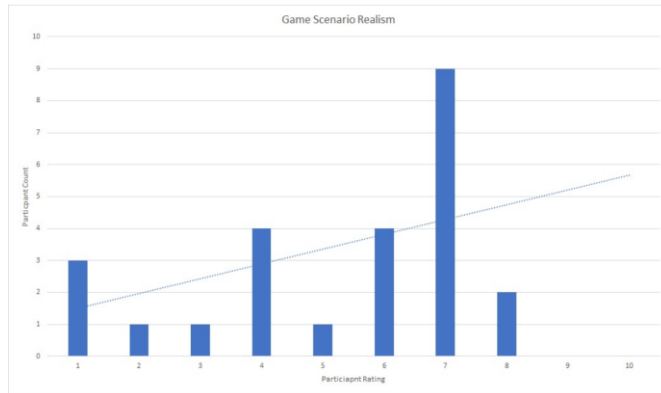


# Evaluation

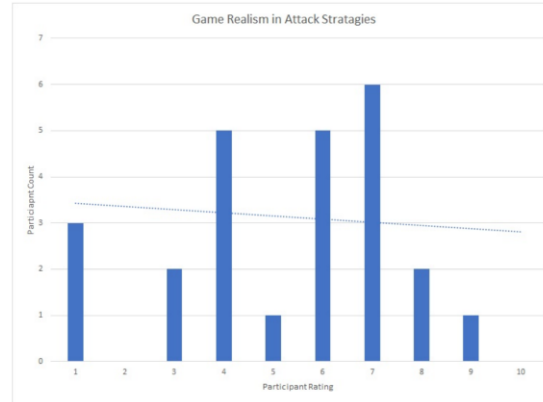


Test Subjects for Game Evaluation During Norwegian Cyber Security Challenge 2019

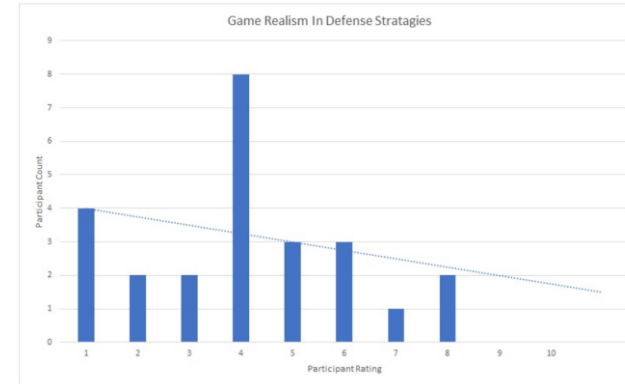
# Realistic Cyber Attack and Defense Scenario Modeling



Cyber Scenario Realism Rating

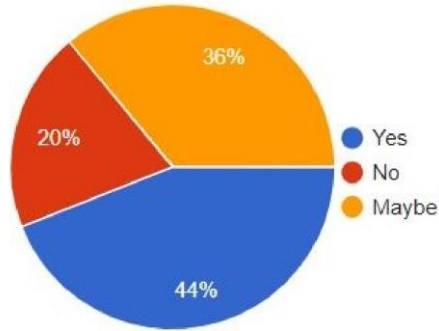


Cyber Attack Strategies Realism

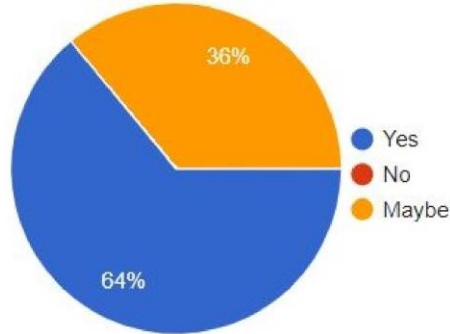


Cyber defense strategies realism

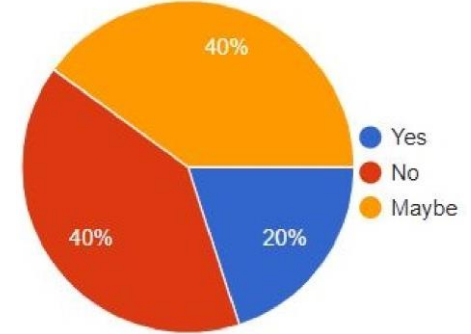
# Efficiency in Cyber Security Exercises



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



Percentage of participants who think it's 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

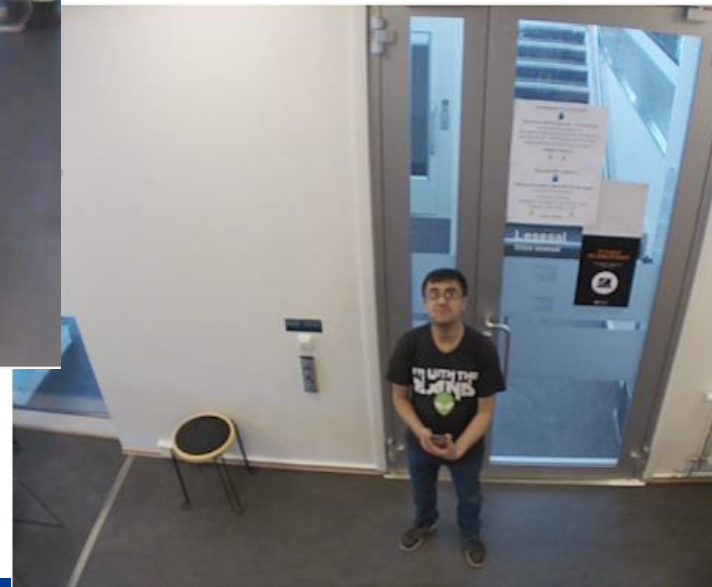
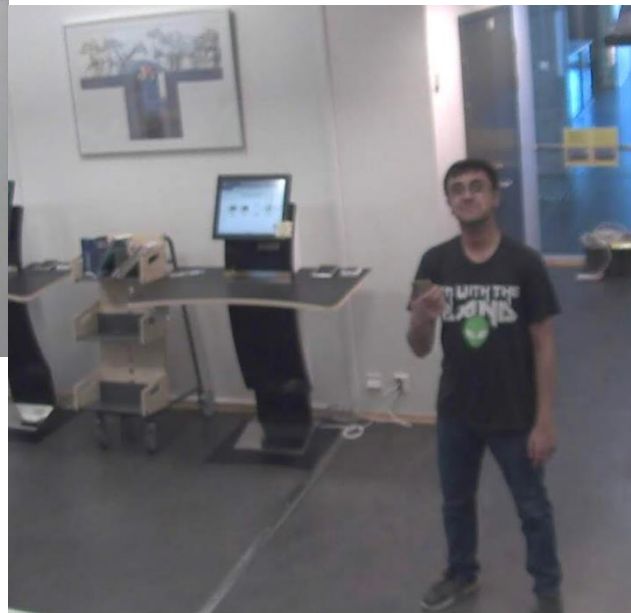
Muhammad Mudassar Yamin

With great power comes great responsibility

~Uncle Ben

To take good selfies





# 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.

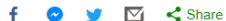
# Preferable Weapon of Choice



## Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes  
Technology reporter, BBC News

© 23 September 2010



## Ukraine power cut 'was cyber-attack'

© 11 January 2017



## Iran shows 'hacked US spy drone' video footage

© 7 February 2013



## US 'launched cyber-attack on Iran weapons systems'

© 23 June 2019



Iran-US crisis

# What if a Country Loses Control on Its Cyber Arsenal?

BBC Sign in News Sport Weather Shop Reel Travel More

**NEWS**

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

## 'NSA malware' released by Shadow Brokers hacker group

© 10 April 2017



BBC Sign in News Sport Weather Shop Reel Travel More

**NEWS**

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

## Baltimore ransomware attack: NSA faces questions

© 27 May 2019



BBC Sign in News Sport Weather Shop Reel Travel More

**NEWS**

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

## Massive ransomware infection hits computers in 99 countries

© 13 May 2017



**Forbes** Billionaires Innovation Leadership Money Consumer Indu

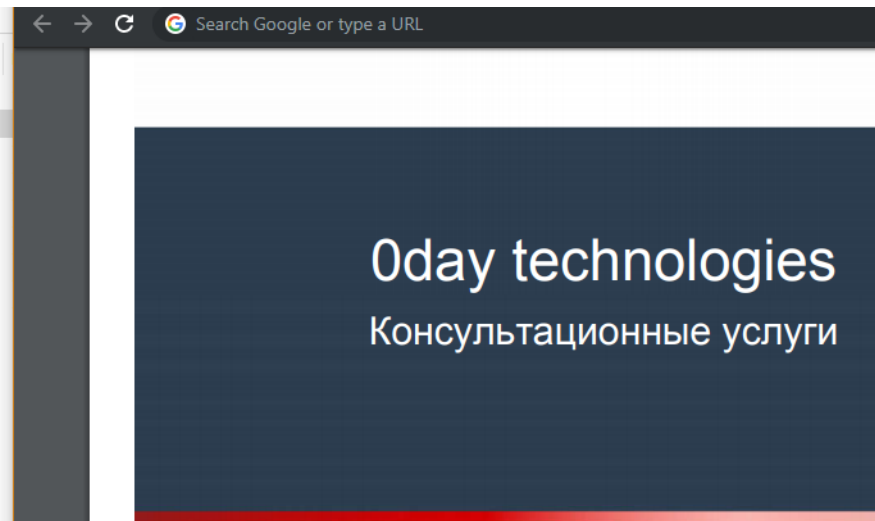
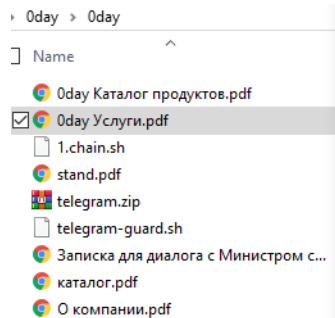
703,988 views | Jul 20, 2019, 12:39pm

## Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach In Its History'

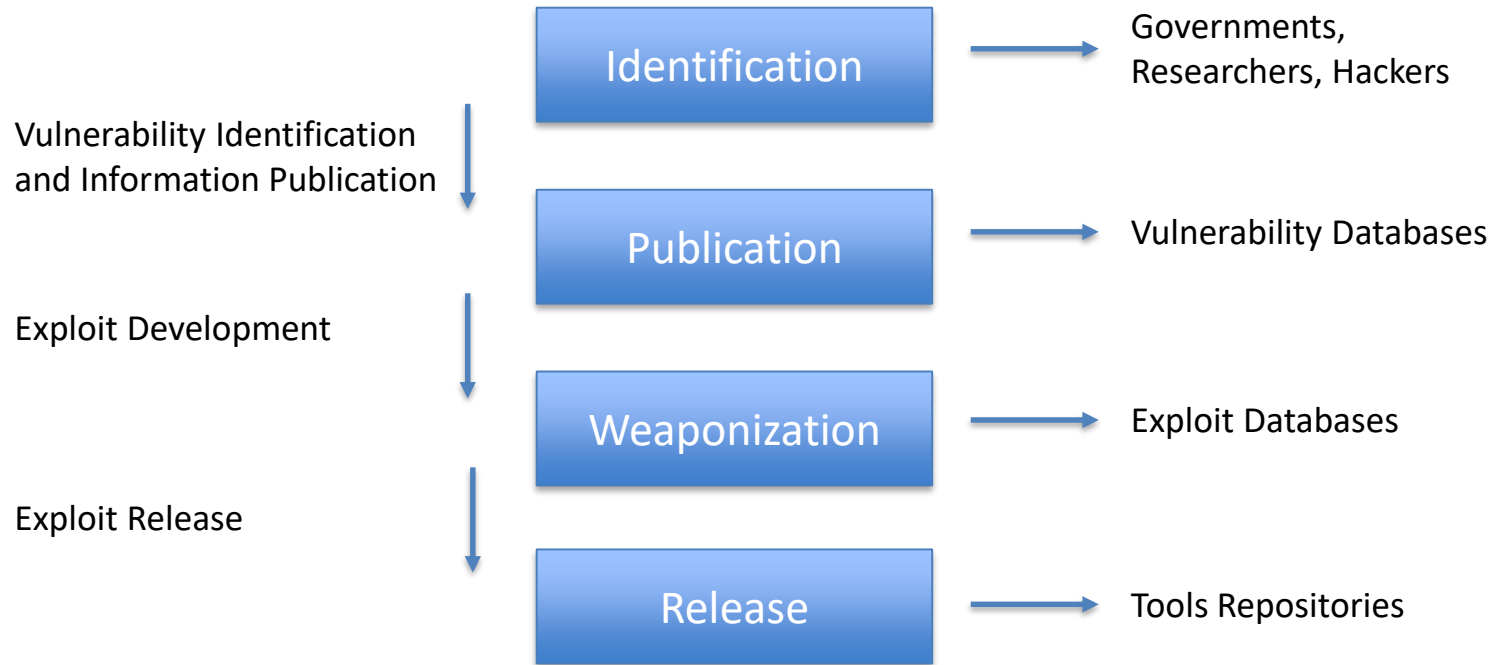
TELEGRAM PROBLEMS IN RUSSIA APR 16, 2018 12:02 Updated Apr 16, 2018 1:05 pm

## Roskomnadzor began blocking Telegram procedure

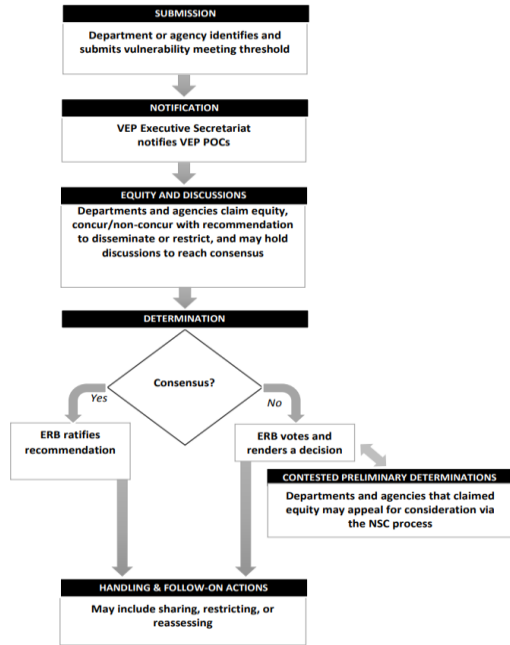
The department said they had received the relevant court decision



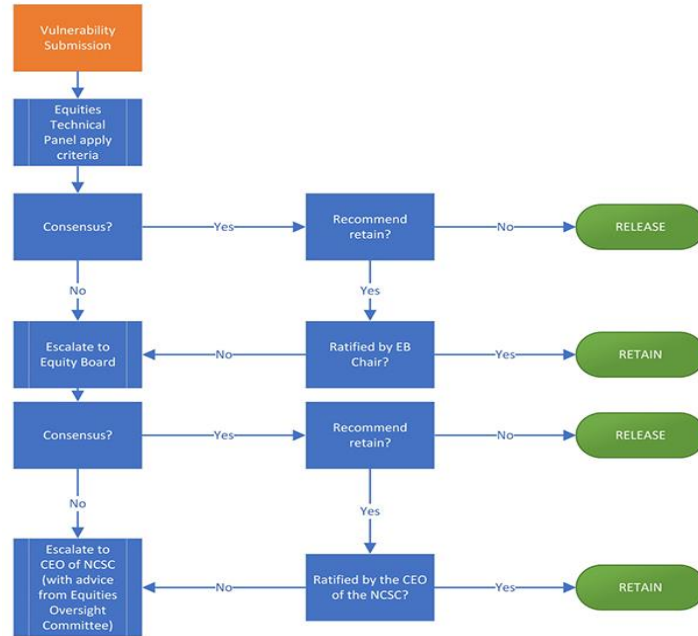
# Cyber Weapons Development Process



# 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)

Army of Hackers

Private Organizations

Report Vulnerability



Vulnerability Rewarded

# Exploit Acquisition Programs (EAP)

Army of Hackers

Intermediate Platform

Private Organizations



# Bug Bounties Programs (BBP)

Army of Hackers

Intermediate Platform

Private Organizations



# 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

**ODAY.today? TOR**

Today is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals. Our aim is to collect exploits from subdomains and various mailing lists and concentrate them in one, easy-to-navigate database. This was written solely for educational purposes. We're not responsible for any damage. (// 0073)

Today is available with TOR at <http://m0d0rdayp033n0n0n.onion>

How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

- Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
- Another way to buy exploits is to become Oday.today user, get registration. You buy it directly and anonymous and get exploit on mail. Oday.today Gold and buy required exploit in our database.

We accept: bitcoin litecoin ethereum

We accept: Crypto Currencies [Contact admin to find more]

Search:

**Today Today Exploit Market and Oday Exploits Database**

DATE	DESCRIPTION	TYPE	HITS	SCORE	LOGS
28/01-2018	Twitter reset account Private Method Oday Exploit	twitter	126/2000	★★★★★	0 0.15
07/01-2018	Instagram bypass Access Account Private Method Exploit	instagram	121/2000	★★★★★	0 0.15
31/04-2018	Hotmail.com reset account Oday Exploit	hotmail	121/5000	★★★★★	0 0.23
07/06-2018	Facebook steal Group Oday Exploit	facebook	124/5000	★★★★★	0 0.21
05/01-2019	Googlebot bypass	googlebot	118/6000	★★★★★	0 0.15
01/02-2019	Filezilla Remote File Read Vulnerability	filep	117/1000	★★★★★	0 0.66
26/01-2019	Mail_sendmailrc - 3.0 System root Privilege Escalation	mail	117/2000	★★★★★	0 0.11
08/01-2019	Facebook - disabling password access token which never expires of your accounts and pages	facebook	116/5000	★★★★★	0 0.15

https://www.exploit-db.com

EXPLOIT DATABASE

Verified  Has App

Show: 15

Date	D	A	V	Title
2019-07-07	↓	📄	×	Apache mod_ssl < 2.8.7 OpenSSL-'OpenFuckV2.c': Remote Buffer Over
2019-07-09	↓		×	Firefox 67.0.4 - Denial of Service
2019-07-08	↓	📄	×	WordPress Plugin Like Button 1.6.0 - Authentication Bypass
2019-07-08	↓		×	Karenderia Multiple Restaurant System 5.3 - SQL Injection
2019-07-05	↓		×	Microsoft Exchange 2003 - base64-MIME Remote Code Execution
2019-07-05	↓		✓	Karenderia Multiple Restaurant System 5.3 - Local File Inclusion
2019-07-03	↓		✓	Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code E
2019-07-03	↓		✓	Serv-U FTP Server - prepareInstallation Privilege Escalation (Metasploit)
2019-07-03	↓		×	Symantec DLP 15.5 MPI - Cross-Site Scripting
2019-07-02	↓		✓	Mac OS X TimeMachine - 'mdiaagnose' Command Injection Privilege Es
2019-07-02	↓		×	Centreon 19.04 - Remote Code Execution
2019-07-01	↓		×	FaceSentry Access Control System 6.4.8 - Remote SSH Root
2019-07-01	↓		×	FaceSentry Access Control System 6.4.8 - Remote Root Exploit
2019-07-01	↓		×	FaceSentry Access Control System 6.4.8 - Cross-Site Request Forgery
2019-07-01	↓		×	FaceSentry Access Control System 6.4.8 - Remote Command Injection

Showing 1 to 15 of 41,464 entries

RAPID7 Products Services Partners Research

Vulnerability & Exploit Database

## Vulnerability & Exploit Database

A curated repository of vetted computer software exploits and exploitable vulnerabilities.

Technical details for over 140,000 vulnerabilities and 3,000 exploits are available for security professionals and researchers to review. These vulnerabilities are utilized by our vulnerability management tool InsightVM. The exploits are all included in the Metasploit framework and utilized by our penetration testing tool, Metasploit Pro. Our vulnerability and exploit database is updated frequently and contains the most recent security research.

Results 01 - 20 of 147,850 in total

Ubuntu: USN-4038-3: bzip2 regression	VULNERABILITY	EXPLORE
OS X update for Messages (CVE-2019-8573)	VULNERABILITY	EXPLORE

Published: July 04, 2019 | Severity: 4

Published: July 04, 2019 | Severity: 4

# Tools Repositories

**KNPL0TT**  
THE HACKER'S TOOLS

HOME EXPLOITS WINDOWS LINUX MAC OS ANDROID IPHONE SQLI OTHERS CONTACT

Simplicity at scale

RECENT POSTS

**Riflut2 - Windows Recycle Bin Analyser**  
15 HRS AGO @ 8:07 AM

**Linux-Smart-Enumeration - Linux Enumeration Tool For Pentesting And CTFs With Verbosity Levels**  
1 DAY AGO @ 5:57 PM

**Whonix v15 - Anonymous Operating System**  
1 DAY AGO @ 8:52 AM

**toolswatch**  
HACKERS ARSENAL

News Confs Projects Best Tools & Reviews Submit a tool

NOVUS  
SUS  
VULNERABILITY

Introducing the 1st Arsenal Lab USA 2019

Introducing the 1st Arsenal Lab USA 2019  
June 29th, 2019 | by NJ Ducks

Amazing Black Hat Arsenal USA 2019 Lineup Announced  
May 23rd, 2019 | by NJ Ducks

**BLACKARCH LINUX**

Home Downloads Guide Faq Tools Community Blog Donate

Over 2200 tools

Tools

Information

Every package of the BlackArch Linux repository is listed in the following table. If you don't find your needed tool in this list simply open an [issue](#) or better do a [pull request](#) for the tool you want to be in our repository. We are fast at packaging and releasing tools.

Tool count: 2263

BlackArch Linux Complete Tools List

Name	Version	Description	Category	Website
0d1n	210.78028eb	Web security tool to make fuzzing at HTTP inputs, made in C with libCurl.	blackarch-webapp	<a href="#">🔗</a>
0trac	1.5	A hop enumeration tool	blackarch-scanner	<a href="#">🔗</a>
3proxy	0.8.12	Tiny free proxy server	blackarch-proxy	<a href="#">🔗</a>
3proxy-win32	0.8.12	Tiny free proxy server	blackarch-windows	<a href="#">🔗</a>
4zzip	42	Recursive Zip archive bomb	blackarch-dos	<a href="#">🔗</a>
a2sv	135.973ba13	Auto Scanning to SSL Vulnerability	blackarch-scanner	<a href="#">🔗</a>
abcd	4.2738609	ActionScript ByteCode Disassembler	blackarch-disassembler	<a href="#">🔗</a>

# 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

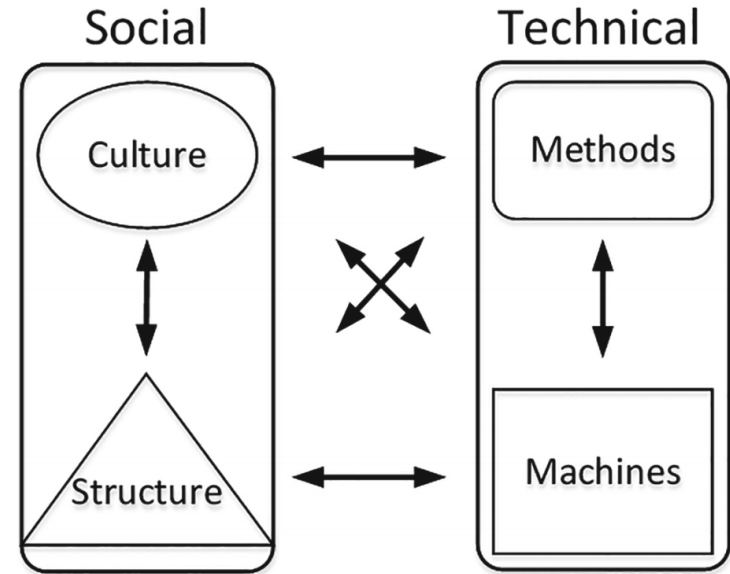


# Threat Actors and Challenges in Securing Cyber Weapons

- 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”