Cyber Weapons Storage Mechanisms

Muhammd Mudassar Yamin, Basel Katt, Mazaher Kianpour

Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway
{muhammad.m.yamin,basel.katt,mazaher.kianpour}@ntnu.no

Abstract. In this paper, the current status of the art of cyber weapon storage methods and related processes are reviewed with particular reference to the safe guards present in storage of cyber weapons and contingency planning in case of losing controls of such weapons. Existing methods are summarized and new techniques which are currently under development are described. Some of the current limitations and challenges are also identified. To tackle these challenges, we propose a socio-technical framework, in which Cyber Ranges can play a major role.

Keywords: Cyber · Weapon · Storage · Vulnerabilities · Exploits

1 Introduction

According to the NATO CCDCOE (Cooperative Cyber Defense Center of Excellence) [1], cyber weapons are *software, firmware or hardware designed or applied to cause damage through the cyber domain*. Cyber domain provides the means of electronic information exchange by utilizing multiple information exchange technologies. The purpose of cyber weapon is to steal, tamper or disrupt the information flow in the cyber domain. Due to the rapid growth of cyber domain, usage of cyber weapon is increasing both by nation states and cyber criminals. Due to recent CIA Vault7 leaks, requirements for secure storage of cyber weapons was raised. CIA malware and hacking tools target iPhone, Android and smart TVs, and are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA. The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide. The CIA attacks systems by using undisclosed security vulnerabilities possessed by the CIA. But if the CIA can hack systems, then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from software vendors they will not be fixed, and the system will remain hackable.

These leaked exploit and vulnerability details are often used by cyber criminals for monetary gains. Two of the major ransomwares *WanaCray* and *Bad*

rabbit that affected global IT infrastructure used *EternalBlue* and *EternalRomance* exploits that were leaked from NSA Vault7 for the purpose of exploitation. Similarly, other Zero day vulnerabilities disclosure from security researcher and hacker groups affects the overall cyber security of governments and industries around the world. In this study we analyze the current state of the art of cyber vulnerabilities and exploit disclosure programs. The safe guards and contingency planning for storage of cyber vulnerabilities and exploit disclosure are examined. Usage of leaked cyber vulnerabilities and exploit in development of cyber weapons in cyber domain is highlighted, the limitation and problems present in secure cyber vulnerabilities and exploit storage are discussed, and finally the role of *Cyber Ranges* in assisting safe guards and contingency planning for leaked cyber weapons is presented.

2 Methodology

In order to understand the problem, we performed a literature review employing keyword-based research method. The researchers started with "Cyber" and" Weapon" with" Storage". They investigated the following keywords in academic databases like Google scholar, IEEE and ACM to acquire the better understanding of the given terms [2]. They also made themselves familiar with the related literature on the given topic. The researchers spotted a lot of related information but employed them in indexed research articles only.

Based upon the finding of literature review a comparative analysis [3] was performed on four key matrices (1) time to disclose the vulnerability, (2) payment for the vulnerability, (3) vulnerability information that is prone to leaking by human risk and (4) vulnerability information that is prone to technical risk of leaking. These matrices play an important role in cyber vulnerability disclosure for cyber weapon development.

Based upon the finding of the analysis, we propose a socio-technical approach to tackle these problems. As figure 1 illustrates, social component is composed of a *culture* and a *structure* elements describing a collection of values and the distribution of power in a given system, respectively. The technical component, on the other hand, is composed of methods and machines. Methods are the employed techniques, and machines are the technical artifacts that are used in different parts of a socio-technical system. These interconnecting components determine the overall security posture of the environment. A secure system maintains equilibrium among the four sub-components. Any change in one of these sub-components can change the state of the system into an insecure system [4].

3 State of Cyber Weapon Storage

The cyber weapons utilize vulnerabilities present in computer software and hardware [5]. These vulnerabilities, when weaponized, become exploits. These exploits can be used to achieve specific objectives. Tools are developed to use these exploits in an efficient manner and these tools becomes the cyber weapons. Given

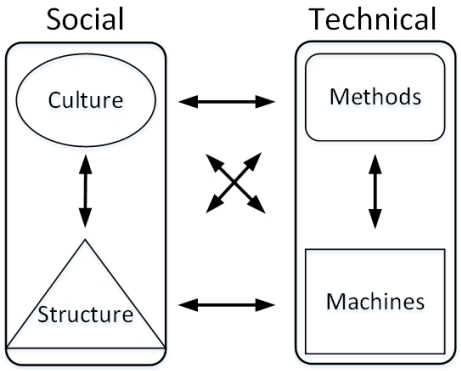

Fig. 1. The complex, dynamic socio-technical system. The interconnecting subcomponents determine the overall security posture of the system [4].

below is the vulnerabilities equities process, unclassified vulnerability databases, exploit databases and tools repositories.

3.1 Vulnerability Equities Process VEP [6]

The United States government developed the VEP (Vulnerability Equities Process) between 2008 and 2009 and publicly disclosed its existence in 2016. The VEP deals with cyber security vulnerabilities identified by United States government agencies and contractors and a decision will be made whether to disclose the vulnerability for public safety or keep it as a secret for cyber weapon development. The details of VEP process were disclosed by *White House* in late 2017, in which the VEP work flow is presented. It is a six step work-flow that runs as fallows: (1) Submission, when a government agency or a private contractor working for government identifies a vulnerability that is considered to be new, the vulnerability information is submitted to VEP with minimum vulnerability information and recommendation whether to disclose the vulnerability or not. (2) Notification, VEP executives notifies the subject matter experts within one working day after acknowledging the submission. (3) Equity and Discussion, the subject matters experts from government agencies have 5 working days to discuss the vulnerability and its impact. (4) Determination, after the vulnerability discussion, a decision is to be made whether to disclose the vulnerability or not. The decision should be made by majority of subject matters experts by voting if consensus in not reached. (5) Contested Preliminary Determinations, if one of the experts is not satisfied with the decision, then the decision can be reviewed by VEP again within 5 working days. (6) Handling and Follow-on actions, if the decision is to releases the vulnerability then the vulnerability will be released within 5 working days, if the vulnerability is not released then the vulnerability will be reviewed by VEP annually for release.

Following United States government, United Kingdom GCHQ (Government Communications Headquarters) released their VEP details in November 2018. The GCHQ VEP was developed in 2010 and was very similar to United States government VEP, compromising of six major steps i.e. (1) submission, a new vulnerability is submitted for review, (2) review, an expert meeting decide whether to retain the vulnerability or retain the vulnerability, (3) consensus, if consensus among the experts is not reached whether to retain or release the vulnerability, it is then escalated to a review board, (4) escalate, the review broad decide whether to retain the vulnerability or release the vulnerability, (5) review, after the review the review board forward its recommendation to NCSC (National Cyber Security Center) CEO to make final decision, (6) final decision, NCSC CEO decides whether to retain or release the vulnerability. In all cases where the vulnerability is retained, a review of vulnerability disclosure will be performed in twelve month. The GCHQ also have few exceptions to excludes vulnerabilities from their VEP which are:

- Vulnerabilities that are considered by similar VEP by one of the allies.
- Vulnerabilities that are identified in products that are not supported by their developers.
- Vulnerabilities that are present in products due to insecure design choice of developers which cannot be fixed.

Comparing to United States and United Kingdom, very little information is present about Chinese and Russian VEP, however, they have active vulnerability database details of which are given in section 3.5

3.2 Responsible Disclosure Programs RDP

The disclosure of United States government global surveillance program by Edward Snowden in 2013 forced major information technology companies to asses their product security. The global surveillance program exploited undisclosed vulnerabilities in major operating system and software solutions to gather intelligence data. After realizing this situation multiple private organizations started their work on identification of Zero day vulnerabilities that are not discovered or disclosed by the government. These programs are started to enhance the overall security of software products offered by multiple organizations. Two of the major efforts led by private companies are Google Project Zero and Microsoft Offensive Security Research Team. Google Project Zero is a Google's counter-surveillance initiative to identify Zero day vulnerabilities in the software product not only developed by itself but the software products that are used by its users. It was conceptualized in 2010, however, major project efforts started in 2014 after the disclosure of United States government global surveillance program. Project Zero informs the software product developer about the discovered vulnerability and waits for 90 days to release the vulnerability. In the waiting period it expects the software product developer to release the patch for the discovered vulnerability. Google Project Zero identified multiple high risk vulnerabilities in Microsoft

products and disclosed them after 90 days of reporting them to Microsoft. Microsoft argued that for complex product the 90 day disclosure window is not suitable and requested a coordinated vulnerability disclosure program. However Google insisted in quick patching of vulnerabilities. As a response, Microsoft established its Offensive Security Research Team to identify vulnerabilities in its rival products and responsibly disclose them. One of the high risk vulnerabilities that Microsoft Offensive Security Research Team discovered is a remote code execution in Google Chrome, which was responsibly disclosed to Google and patched in four days.

3.3 Exploit Acquisition Programs EAP

Private companies offer million of dollars to security researchers for selling working Zero day exploits in major IT products. The purpose of these programs are usually to develop new exploits and malware signatures of IDS/IPS, anti virus and anti malware programs. However, it can be argued that these programs can be run by government agencies to disguise their identity. Two of the major exploit acquisition programs are Trend Micro Zero Day Initiative and Zerodium Exploit Acquisition Program. Trend Micro Zero Day Initiative started in early 2005 for buying Zero day vulnerabilities discovered by independent security researchers. The purpose of this program was to gather vulnerability signatures for their intrusion detection and prevention system "Tipping Point". They offer lucrative payout to security researchers for the identification and exploitation of potential vulnerabilities present in mainstream software products. They held regular vulnerability discovery and exploitation competitions known as "Pwn2Own" in which they invite security researcher to demonstrate vulnerability discovery and exploitation. Zerodium was founded by the founder of Vupen a private company that used to independently identify Zero day vulnerabilities and sell then to private and government clients. Now, Zerodium invites independent researchers to sell their vulnerabilities exploits in major web browsers, smart phones and desktop operating systems, which it markets to private and government clients for research and development purposes.

3.4 Bug Bounties Programs BBP

Bug Bounties Programs are developed to crowd source security of a big IT infrastructure. Organizations conduct penetration tests in order to identify potential vulnerabilities in their infrastructure, however, these penetration tests are very costly and often don't cover the whole organizations infrastructure. Therefore these organizations invite independent researchers to identify vulnerability and responsibly report those vulnerabilities in order to receive a reward. This helps security researcher with extra income and organization with paying for only actual vulnerability. There are many platforms that are being used in management of these bug bounty program. Two of the major platforms that are being used actively by major organizations are given are Bugcrowd and Hackerone. Bugcrowd offers services to major information technology companies to manage

their vulnerability reward programs. It connects security researchers with companies seeking to crowd source theirs information security program. It ranks the security researchers based upon number of valid submitted reports. Hackerone helps in vulnerability information coordination and disclosure between security researchers and information technologies companies. Its platform is quite similar to Bugcrowd, however, it offers rating system of vulnerability, exploits and researchers to better results in vulnerability disclosure and coordination. The vulnerabilities and exploits that are disclosed become available to relevant vulnerability databases, details of which are given below:

3.5 Vulnerability Databases [7]

Multiple vulnerability databases exists in literature, some are maintained by governments while majority is operated by private security companies and community driven efforts. These databases contain the details about the vulnerability, the affected system and the risk of exploitation it poses. Some of the well known vulnerability databases Vulnerability Database, Common Vulnerabilities and Exposure, National Vulnerability Database, China National Vulnerability Database and Russia National Vulnerability Database. VulnDB (Vulnerability Database) is one of the oldest vulnerability database, it is being operational since 1970. It is a crowd based vulnerability database which means it is operated by people and researchers in the security field. It uses OSVDB (Open Source Vulnerability Database) format, which includes a vulnerability id, vulnerability description, possible vulnerability solution and reference to further vulnerability details. CVE (Common Vulnerabilities and Exposure) was one of the very first vulnerability database that combine vulnerability information from different sources. It was launched by MITRE organization in 1999 to overcome the problem of multiple vulnerability nomenclature used by multiple organizations. The CVE includes a vulnerability id, a brief description of the vulnerability and any references related to that vulnerability. The NVD (National Vulnerability Database) was developed by NIST (National Institute of Standards and Technology) in 2005. It uses SCAP (Security Content Automation Protocol) to manage and present vulnerability information gathered from multiple sources including CVE. The NVD database consist of vulnerability impact matrices, security check lists, security misconfigurations details, affected product names and security related flaws in software and hardware. The CNNVD (China National Vulnerability Database), CNNVD is a national-level information security vulnerability data management platform for China's *information security assessment center* to effectively perform vulnerability analysis and risk assessment functions. CNNVD combines government departments, industry users, security vendors, universities, and scientific research institutions through independent vulnerability information submission, collaborative sharing of vulnerabilities information, network attacks information collection, and technical testing of vulnerable systems. One of its main function is to provide early warning against a suspected cyber security threat. vulnerabilities in CNNVD are disclosed often early compare to other vulnerabilities databases. Russia's NVD is run by the

Federal Service for Technical and Export Control of Russia (FSTEC), a military organization with a closely defined mission to protect the state's critical infrastructure and to support counterintelligence efforts. It was established 15 years after the establishment of US NVD and roughly contains a record of 100000 vulnerabilities.

3.6 Exploit Databases

When the vulnerabilities are weaponized to compromise the security of the computer system then they become exploits. The exploits appeals nation states, cyber security companies and cyber criminals. Therefore their monetary value is quite high. Independent security researchers mostly publish these exploits free of charge, however, these exploits are also available for sale. Many of such platforms operate on TOR network, however, some of these platforms operates publicly like 0day Today, Exploit Database, Rapid7 Vulnerability and Exploit Database. 0day Today is one of the biggest crowd sourced exploit market place. Gray hat hackers can sell their exploit PoC (Proof of Concepts) in this marketplace. The platform was developed in 2008 due to increasing demand of cyber security exploits. It follows responsible disclosure guidelines and inform the software developer before releasing the exploits. It provide technical exploit information to peoples who are involved in ethical hacking activities and signature development activities for intrusion detection systems. Exploit DB (Exploit Data Base) was created by a private company "offensive security" in 2009. It also uses crowd sourcing, however, it doesn't sell exploits. All exploit available on Exploit DB are open source and free to use by anyone. The exploit database is CVE complaint and the information about the exploit is published with relevant vulnerability details. It includes remote, local, denial of service and web exploits, however, exploits targeting live websites are not published on exploit db. Rapid7, a private company, has been collecting vulnerability signatures since 2000 for the development of their vulnerability scanner. They integrated their vulnerability scanner with the metasploit exploitation framework and are now leading the metasploit exploit development. Until now they have the signature of nearly 70000 vulnerabilities and 3000 work exploits. Their vulnerability signature is CVE compliant and they follow open source exploit development techniques, however they also sell advance exploits to their customers.

3.7 Tools Repositories

Tools that automate the functionality of exploit and link multiple exploits to achieve specific objectives are considered as cyber weapons. Multiple platforms that distributes such tools are publicly available. These platforms mostly showcase tools that are publicly available and released by cyber security researchers. Some of the publicly available platforms are ToolsWatch, KitPloit,Black Arch Tools Repository. ToolsWatch is developed to distribute up to date penetration testing and security auditing tools between security professionals and researchers. It has a catalog of cyber security tools that are released by cyber secu-

rity researchers in major security conferences like Blackhat and defcon. Security researchers can submit new tools to its submission portal, which is maintained by a group of volunteers. Most of the tools available at ToolsWatch are open source and free to use while some tools have their commercial versions as well. It also has a best tools of the year competition in which security researchers votes for the best tools that are released in a year. KitPloit was launched in 2012 in order to categorize and search the exploitation tools available for relevant platforms. It hosts exploitation tools related to major operating systems like Windows, Linux, MAC, Android and IOS. Additionally, it provides tools for performing OSINT, DDOS, Malwares attacks etc. Most of the tools available at KitPloit, similar to ToolsWatch, are open source and free to use while some tools have their commercial versions as well. It accepts tools submission from security researchers and the submissions are maintained by volunteers. It also hosts the installation and usage instruction of the submitted tools. Black Arch Linux is an Arch Linux-based penetration testing distribution for penetration testers and security researchers. The repository consists of 2082 tools. These tools could be installed individually or in groups. The tools present in the repositories are compatible with other Debian based penetration testing distribution like Kali Linux and Parrot OS.

4 Analysis

In this section we will discuss and analyze the various vulnerability disclosure programs and the risks associated with the cyber weapon storage mechanisms. Afterwards, we provide a general comparison.

4.1 Cost of Leaked Cyber Weapons

As explained above vulnerabilities and exploits are in high demand by governments, security researchers and cyber criminals. Securing this valuable piece of information should be of a high priority. However, in 2017 NSA vault7 leaks exposed CIA weapons arsenals to the cyber security community. Vault7 contains information about secret CIA cyber activities collected by Wikkileaks. Its 24 parts leaks released between 7 March 2017 to 7 September 2017. Among other tools, an exploit "EternalBlue" targeting Microsoft Windows was also released. This exploit was later weaponized in "Wannacry" ransomware malware attack which had nearly 200000 victims and 300000 affected systems in 150 countries [8]. The losses caused by this single cyber attack reached 4 billion USD. Similarly, the source code of "Mirai" Botnet was released on a hacker forum. Mirai botnet in 2016 exploited Linux based IoT device to launch a DDOS (Distributed Denial of Service) attack on United Stated domain name servers to hamper its internet communication service. During the "Wanacry" attack a kill switch was developed by identifying a hard coded domain in the malware code. The kill switch was activated when the domain is registered. However, the attacker used variant of "Mirai" botnet to launch a DDOS on the domain to disable the

switch but luckily they were not successful. This indicated that new variants of cyber weapons can be used in combination of other cyber weapons to launch sophisticated cyber attacks. These cyber attacks affected health services as well, therefore, calculating the actual cost of such attacks is very difficult. Hundreds of million dollars losses in recent years are the consequence of increasing leaked cyber weapons in frequency and cost. These costs are variable across countries and industry sectors. Besides the cost of cyber incidents, understanding the different types of threats and challenges in securing cyber weapons can help to gain additional insight to counter or mitigate the impact of future incidents.

4.2 Threat Actors and Challenges in Securing Cyber Weapons

In the literature we identified multiple threat actors and challenges affecting the security of cyber weapons. These challenges are similar to challenges which are faced in securing any kind of sensitive information. Some of the major challenges, and associated threat actors, that are faced in securing cyber weapons are given below:

Human negligence Human error has been the most commonly reason of penetrated information systems. Attackers can boost their chance of success if they exploit knowledge about personal information and behavioral characteristics of targeted users. Upon the investigating of Vault7 leak's hacking tools, the United States investigation agencies are focusing on the possibility that NSA contractor or operative carelessly left the hacking tools and exploit on a remote target systems [9]. The remote target system was then exploited by "Shadow Brokers" from where they retrieved the hacking tools and exploits. There is also a possibility that the contractors or operative intentionally left the hacking tools an exploit for the "Shadow Broker" to retrieve. This leads us to next challenge in securing cyber weapons, which is Insider threat details of which are given below.

Insider threat The authorized users or employees have access to the confidential data and to the sensitive assets of an organization, so there is always a risk that employees may misuse this data access for any mischievous purpose [10]. An example of an insider case is Chelsea Manning, who was responsible for the leaking of more than 60000 U.S department of defense documents on WikiLeaks and Edward Snowden, who exposed secret NSA documents in public. These two cases are important examples of Insider threat incidents. The insiders are either motivated by financial gains in leaking sensitive information to adversaries or they are motivated by moral principals. Both motivation scenarios are exploited by states sponsor agencies, details of which are given below.

Dissatisfied gray hat hackers and security researchers Security researchers and gray hat hackers often get dissatisfied by the treatment from the system vendors, or the vulnerability disclosure program, and releases the vulnerability

information publicly. This give little time to vendors for development of security patch and provides an opportunity to cyber criminals to exploit unpatched systems

Hacktavist groups Hacktivst groups are group of hackers that hack for social and moral reasons. Multiple hacktavist groups exsist in cyber domain. The Vault7 leak was also credited to a hacktivsit group "Shadow Broker". However, the United States government argued that they are sponsored by a country as they released the hacked tools without any financial incentives. This hacktivist group also uses multiple cyber misinformation techniques to affect the public opinion as per their requirements.

State sponsored attack Intelligence operations in identifying your adversaries capabilities is a regular part of military operation. However, in cyber domain these operation further extends to obtain the information cyber weapon usage of their adversaries and identifying mitigation strategies to avoid malicious consequences of adversaries cyber weapons. This is achieved by performing offensive cyber security operation on the adversaries which include stealing of relevant information and launching misinformation campaign to demotivate the opponents work force.

4.3 Comparison

The VEP takes a minimum of 7 days to disclose a vulnerability, which it decides not to retain. The once they retain will be reviewed for release after 12 months of retention [6]. Compare to VEP, RDP release the vulnerability information after 90 days of informing the vulnerable product owner, regardless of the patch is released or not. In EAP and BBP vulnerability information disclosure solely depends upon the party which is paying for the vulnerability information therefore they have variable time for releasing the vulnerability information.

In term of monetary value of vulnerability information, no information of VEP programs is available due to their classified nature, RDP doesn't sell the vulnerability information rather than inform the affected product developers for a better secure environment for everybody. EAP business model is centered around selling the vulnerabilities to government and private clients. BBP offers security researchers payouts for identifying vulnerabilities. These programs and the associated cyber weapon storage system are also vulnerable to both technical and human risks as observed and discussed in section 4.2. Table 1 compares the various vulnerability disclosure programs.

From table 1, it can be concluded that this problem is not purely technical problem rather than a socio-technical problem [4]. RDP can be ideally used for vulnerability disclosure to avoid threat of leaked cyber weapons, however, it is not practical for governments and military purposes.

Table 1. Comparison of Different Vulnerability Disclosure Programs

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

5 Socio-Technical Framework

As we mentioned in Section 2, tackling the above described challenges in securing cyber weapons is a difficult task and requires considerations beyond software and hardware technologies. Accordingly, in this section, we present a socio-technical methodology to address the main sociological and technical components of these issues. Our proposed multidisciplinary solutions cover both components and their corresponding sub-components to protect cyber weapons from evolving cyber threats.

5.1 Culture

In a complex socio-technical system, culture is composed of beliefs, values, rules and identities of each stakeholder at different levels (e.g. individual, organization, national entities, etc.) of society. Below, we argue the role of human in cybersecurity and how it can influence the state of a secure system.

Human Moral Values Basically, human factors are known as the weakest link in cybersecurity. Understanding human factors in cybersecurity can help us to design systems and security measures more efficiently. Ethics, the moral principles governing people's behavior, is a critical part of any cybersecurity defense strategy that is highly dependent upon each individual in the ecosystem. The moral of work force which deals with development and usage of cyber weapons should be kept higher. Considering Edward Snoden NSA leaks the work force is the biggest weakness is securing cyber weapons. Cyber Weapon information security can be achieved by setting high moral and ethical standards within the organization to reduce the affects of adversaries misinformation campaigns. However it should be noted that the adversaries are not bound by such high moral and ethical values in development and usage of such weapons. While ethics can be subjective and influenced by background, culture, education, etc., good financial incentives and important meaning to assigned missions can motivate the work force to perform their duties diligently.

5.2 Structure

Understanding the underlying work structure in a system help to identify conflicts, requirements and interdependencies among the stakeholders. Digital transformation has affected the relationships among the stakeholders, their business

processes, and their performance. To maintain the system in the secure state, cooperation, as described below, and information sharing among the stakeholders is crucial.

Cooperation among the Stakeholders Interconnected digital ecosystem creates inter-dependencies among stakeholders and actors in cybersecurity. While this feature enables various the social and economic benefits to the stakeholders, it increases complexity, facilitates the propagation of threats and vulnerabilities, and increases the potential collective risk. This makes cooperation among stakeholders a necessity to encounter these risks. Cooperation is also a critical key to implement requires business and operational principles among the actors responsible for providing a secure environment. It is also essential for security and resilience measures respecting the non-technical aspects of cybersecurity, where humans have to modify their behavior and all management processes have to be adopted to support the changes due to the digital transformation in organizations.

5.3 Method

Understanding the methods and employing appropriate techniques is required not only for adopting new technologies, but also for controlling the dynamic behavior and unintended consequences of changes in other sub-components. Following, we discussed three methodological approach to secure cyber weapons against different threats.

Proactive Cyber Defense In Proactive Cyber Defense an action is taken before the attack is even happened. There are two methods to deter the cyber incidents proactively; denial and cost imposition. Denial can be defensive and offensive. It is performed to deter a cyber attack in self defense. This can be achieved by first detecting potential adversaries attack plans and then neutralizing the attack with an active cyber operation. This is done in two phases, first a defensive cyber operation is performed to identify the threat, and secondly, an active cyber operation is performed to neutralize the threat. An example of such action can be seen in darkrode incident [11] in which a website which is involved in trading of hacking services, botnets and malware was taken down by United Sates FBI (Federal Bureau of Intelligence). In the other methods, imposing relatively large costs forces the attackers to change their strategic behavior. These two strategies can together make certain attack unappealing for the attackers. Denial can reduce the chance of success, and cost imposition can make them prohibitively expensive.

Cyber Threat Hunting Cyber threat hunting is a form of active cyber defense in which it aims to proactively detect, identify and isolate threats that are not detected by security solutions. This approach is completely opposite to

traditional signature and anomalies based detection mechanism in which investigation is performed after the incident. Cyber threat hunters detect and identify new attack signatures for the identification of new threat actors. This process is mostly done manually in which security analysts have to go through information from various data sources and utilizing their experience, knowledge and understanding of network environment isolate new threats.

Cyber Security Training and Awareness Understanding the cybersecurity risks is vital when you are discussing the security of cyber weapons. Managing these risks requires appropriate skills to make responsible decisions. Training and education through practice and experience is one of the most efficient ways to acquire these skills. Therefore, the first stage of a cybersecurity risk management approach is raising awareness and acquisition of required skills to empower stakeholders. Cyber security exercises can play a key role in securing cyber weapons. Cyber security exercises are usually attack/defense exercise in which one team is involved in active attacking on a infrastructure while the other team is involved in active defenses of the infrastructure. New Cyber security exercise scenarios can be developed in which securing a hypothetical cyber security weapons can be set a task for the defenders. Similarly, an exercises scenario can be created in which the team of attackers have access to a hypothetical cyber weapons, its capabilities are public and defenders have the task to develop mitigation strategies against the known cyber weapon. This type of cyber security exercises will help in training of work force in securing cyber weapons and mitigating security issues in case of cyber weapon leakage.

5.4 Machine

The stakeholders have certain types of infrastructure and machines that they can use depending on their attitude or structure. These machines help them to achieve their desired performance and provide them with various opportunities to enhance their resources and skills. Below, we demonstrated that how cyber ranges can be employed as a platform to provide security in cyber weapons.

Cyber Range A lot of new vulnerabilities are expected to be identified in cyber ranges, due to which their responsible disclosure is a need of the day. Cooperation among the stakeholders in sharing vulnerability information for responsible disclosure will ensure a secure cyber environment. Cyber ranges can also play a vital role in testing hypothetical scenarios of leaked cyber weapons and their effects on IT infrastructure to identify the effectiveness of different methods like proactive cyber defense and cyber threat hunting. Moreover, current way of conducting cyber security exercises is quite inefficient [12], cyber ranges can assist in security exercises, training and awareness campaign of ethical and moral reasoning for enabling organizations to tackle threat of leaked cyber weapons in a efficient manner.

6 Conclusion

In this paper we first presented the current state of art for cyber weapon storage mechanisms and vulnerability equities processes. This included (1) the details of available vulnerability databases, (2) information about different exploit databases that utilize those vulnerabilities, (3) tools repositories, in which weaponized versions of those exploits are present, and (4) the responsible disclosure programs, exploit acquisition programs and bug bounty programs that are currently running for the acquisition of new vulnerabilities and exploits. After that we analyzed the data we collected in the literature review, in which we discussed (1) the costs of leaked cyber weapons, (2) the threat actors and challenges in securing information related to vulnerabilities and exploit, and finally (3) provided a comparison for the various vulnerability disclosure programs. To tackle the challenges that we identified in our analysis, we propose in section 5 a social technical framework for securing cyber weapon information.

References

1. Michael N Schmitt. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.
2. Jill Jesson, Lydia Matheson, and Fiona M Lacey. *Doing your literature review: Traditional and systematic techniques*. Sage, 2011.
3. Mark A Zschoch. Configurational comparative methods: Qualitative comparative analysis (qca) and related techniques, benoit rihoux and charles ragin, eds., thousand oaks ca: Sage publications, 2009, pp. xxv, 209. *Canadian Journal of Political Science/Revue canadienne de science politique*, 44(3):743–746, 2011.
4. Stewart Kowalski. It insecurity: A multi-disciplinary inquiry. 1996.
5. Dale Peterson. Offensive cyber weapons: construction, development, and employment. *Journal of Strategic Studies*, 36(1):120–124, 2013.
6. Ari Schwartz, Rob Knake, Belfer Center for Science, and International Affairs. *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016.
7. Anshu Tripathi and Umesh Kumar Singh. Taxonomic analysis of classification schemes in vulnerability databases. In *2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, pages 686–691. IEEE, 2011.
8. Gil Baram, Daniel Cohen, Zeev Shapira, Omri Wechsler, Nir Hight, and Isaac Ben-Israel. 2017 strategic trends in the global cyber conflict. 2018.
9. Scott Shane, Nicole Perlroth, and David E Sanger. Security breach and spilled secrets have shaken the nsa to its core. *New York Times*, 12, 2017.
10. Jason RC Nurse, Oliver Buckley, Philip A Legg, Michael Goldsmith, Sadie Creese, Gordon RT Wright, and Monica Whitty. Understanding insider threat: A framework for characterising attacks. In *2014 IEEE Security and Privacy Workshops*, pages 214–228. IEEE, 2014.
11. Peggy E Chaudhry. The looming shadow of illicit trade on the internet. *Business Horizons*, 60(1):77–89, 2017.
12. Muhammad Mudassar Yamin and Basel Katt. Inefficiencies in cyber-security exercises life-cycle: A position paper. *CEUR Workshop Proceedings*, 2269:41–43, 2018.