Cyber threats: taxonomy, impact, policies, and way forward

Annas W. Malik[1], Adnan Abid[1*], Shoaib Farooq[1], Irfan Abid[2], Naeem A. Nawaz[3], Kashif Ishaq[4]
[1] School of Systems and Technology, University of Management and Technology, Pakistan
[e-mail: S2020375001@umt.edu.pk; adnanabid7@gmail.com; Shoaib.farooq@umt.edu.pk]
[2] Military College of Engineering, National University of Science and Technology, Pakistan
[e-mail: Irfanabid78@gmail.com]
[3] Ummal Qura University, Saudi Arabia
[e-mail: nanawaz@uqu.edu.sa]
[4] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia
[e-mail: p97710@siswa.ukm.edu.my]
[*]Corresponding Author: Adnan Abid

Received November 17, 2021; revised January 17, 2022; revised March 17, 2022; accepted April 24, 2022; published July 31, 2022

Abstract

The continuous evolution and proliferation of computer technology and our increasing dependence on computer technology have created a new class of threats: "cyber threats." These threats can be defined as activities that can undermine a society's ability to maintain internal or external order while using information technology. Cyber threats can be mainly divided into two categories, namely cyber-terrorism and cyber-warfare. A variety of malware programs are often used as a primary weapon in these cyber threats. A significant amount of research work has been published covering different aspects of cyber threats, their countermeasures, and the policy-making for cyber laws. This article aims to review the research conducted in various important aspects of cyber threats and provides synthesized information regarding the fundamentals of cyber threats; discusses the countermeasures for such threats; provides relevant details of high-profile cyber-attacks; discusses the developments in global policy-making for cyber laws, and lastly presents promising future directions in this area.

Keywords: Cyber-attacks, cyber security, cyber security laws, cyber-terrorism, cyber warfare, cyber-weapons, malware, malware detection.

1. Introduction

Cyberspace is the environment in which communication over computer networks occurs, and almost everyone is connected to it in one way or another [1]. The development of the Internet or Web technologies has formed a virtual space. The Internet and Web technologies have revolutionized the computer and communications world. The infrastructure of cyberspace at the moment is pivotal to the operations of domestic and global security systems, trading networks, emergency services, basic communications, and other activities [2]. There are several security threats in cyberspace because it offers little or no regulation. These security threats are cybercrime, cyber terrorism, and cyber warfare. A wide range of critical national, military, governmental, and private infrastructures are becoming vulnerable to cyber-attacks in this cyber world. Cyber-attacks are evolving due to the availability of low-cost and effective development tools to conduct attacks and cause damages to their targets [3]. The software systems used for conducting cyber-attacks are referred to as malware. This research aims to systematically review the research work published in different important aspects of cyber threats, including some fundamental concepts related to cyber threats. Subsequently, various high-profile cyber-attacks have been discussed with relevant details. Similarly, countermeasures to mitigate cyber-attacks have also been discussed. Apart from this, policies being devised by different countries to develop cyber laws have also been presented. Lastly, future research directions have also been shared for the researchers working in this domain.

The study presented an in-depth review of most aspects of the cyber domain. The main contributions of the study are the detailed conceptual frameworks of cyberterrorism and cyberwarfare, which help to distinguish between the two. Moreover, the proposed study gives a broader spectrum of the cyber domain, which to the best of our knowledge, is not covered in other literature.

The rest of the article has been structured in the following manner. Section 2 discusses the existing relevant research work. Section 3 presents the methodology discussed to conduct this literature review. While Section 4 provides necessary fundamental details regarding cyber-threats. Important details related to the high-profile cyber-attacks in different sectors have been presented in Section 5. The countermeasures for cyber threats have been discussed in Section 6. The global efforts in policy-making for cyber laws have been discussed in Section 7. The promising research directions and open research problems in various sub-domains have been presented in Section 8. While Section 9 concludes the article.

2. Literature Review

A lot of research has been done separately on cyber terrorism, malware analysis, detection, mitigation techniques, and cyber laws. Each paper has made an appreciable contribution in the field of research. **Table 1** shows a comparison of our paper with some recent research papers in this field. Wangen [4] has explained how conventional crime differs from cybercrime, how malware has evolved over the years, and how targeted attacks have taken the shape of cyber espionage. He also has discussed some drastic malware cyber-attacks on industries and their effects in his paper. Hemsley [5], on the other hand, has explained the most dangerous malware and mentioned some of the biggest cyber malware attacks to industries from 1903 to 2017. He has categorized his work into four categories: malware, attacks on industries, groups involved, and campaigns, synthetically explaining malware attacks and their effect on industries.

Eze [6] has precisely discussed malware analysis and detection techniques explained each detection technique and analysis process synthetically and explained each technique in pictorial representation. He has also discussed various malware and malware mitigation strategies. Like Eze [6], Deka [7] has also discussed malware analysis and detection techniques in detail and also mapped malware detection techniques against each analysis technique. Sihwail [8] has discussed the malware analysis technique, successful implementation, and accuracy. Many research papers have been published on cyber laws, but D. Hagg [9] has explicitly explained Canada's cyber laws and protocols, explained which activity has to be considered terrorism, and suggested the punishment for such actions. Banks [9] explained the need for cyber laws to tackle attacks like cyber espionage, which can cause great loss to a country or an industry. He has also mapped the law-related terms with the technical terminologies and explained the cyber laws of the US. Despite this fact, all research papers have done extraordinary work in their specific field of research. But to the best of our knowledge still, there is a gap in the research, and most papers cover a single topic. We have tried our best to fill this gap, and the reader will attain detailed knowledge about several topics from this research paper.

Table 1. Comparative analysis of some related literature

Research Topics	**Cyber Weapons**	**Role of Malware**		**Counter Measures**			**Cyber Security Laws**
Research Papers		Cyber Espionage	Disruption and Destruction	Malware Analysis	Detection Techniques	Mitigation Strategies	
[5]	-	-	✓	-	-	-	-
[6]	-	-	-	✓	✓	✓	-
[7]	-	-	-	✓	✓	-	-
[10]	✓	--	-	-	-	-	-
[9]	✓	✓	-	-	-	-	✓
[4]	-	✓	✓	-	-	-	-
This paper	✓	✓	✓	✓	✓	✓	✓

2.1 Utilizing Systematic Review

Many research papers were published, focusing on Cyber Security or its subdomains separately. To the best of our knowledge, no research paper discusses all subdomains and their aspects in a single paper. This systematic review will focus on all common subdomains of Cyber Security and further extend it to the Role of Malware and countermeasures to mitigate the effect of Malware attacks.

To search for relevant papers in repositories following terms were used:

“Cyber Security,” “Cyber Security Laws,” “Malware Analysis,” “Malware Detection Techniques,” “Cyber Warfare,” “Cyber Crimes,” “Cyber Terrorism,” and “Cyber Espionage.”

An analysis of the relevant searched papers was carried out to shortlist the pertinent papers.

3. Methodology

The methodology adopted for Systematic Literature Review (SLR) step by step included: 1) Defining the Research Questions, 2) Inclusion and Exclusion Criteria, 3) Search Strategy, 4) Data Extraction, and 5) Quality Assessment. Each step is explained briefly in the subsequent parts:

3.1 Defining the research questions

As a first step of the systematic review process, the research questions were defined, which are given in **Table 2**:

Table 2. Proposed research questions and their motivation

Research Questions	Motivations
What are the fundamental cyber threats?	This question will help us with clarifying the main differences between cyber security threats.
Discuss different case-study incidents involving high severity cyber-attacks in various sectors?	This question will help us define case studies regarding various cyber malware attacks, addressing the following: How dangerous are malware attacks? How have malware attacks affected various industrial sectors?
Which countermeasures have been developed to mitigate cyber malware risk?	This question will help us compare different mitigation techniques and which one has proven to be fruitful.
What are the developments in devising policies and laws to mitigate cyber-security? Which countries have devised policies for cyber terrorism, and to what extent international cyber laws have been defined?	This question will help us discuss the following: How are countries countering cyber terrorism? What international laws and policies are defined to fight against cyber terrorism?
What are the open challenges and issues for mitigating cyber malware attacks?	This question will help us provide future directions for other researchers.

3.2 Search Strategy

Research papers were selected for the systematic review if they fulfilled the following criterion:

1. If a paper is published in a well-known venue.
2. The article focused on the following aspects: Cyber Security, Cyber Crimes, Cyber Terrorism, or Cyber Security Laws.

The following search strings were used:
((“Cyber Security”) AND (“Cyber Terrorism” OR “Malware Attacks” OR “Malware Analysis OR “Malware Detection” OR Cyber Espionage” OR “Cyber Crimes Laws” OR “Cyber Warfare”)), Intitle: “Cyber-Terrorism,” Intitle: “Malware Analysis,” Intitle: “Cyber Security,” Intitle: “Cyber Security Laws.”

An initial search was further refined through an analysis to extract precisely relevant papers. **Table 3** depicts the searched database and search strategy.

Table 3. Search queries for research databases

Database	Search Strategy
ACM Digital Library	((“Cyber Security”) AND (“Cyber Terrorism” OR “Malware Attacks” OR “Malware Analysis OR “Malware Detection” OR Cyber Espionage” OR “Cyber Crimes Laws” OR “Cyber Warfare”))
IEEE Xplore	((“Cyber Security”) AND (“Cyber Terrorism” OR “Malware Attacks” OR “Malware Analysis OR “Malware Detection” OR Cyber Espionage” OR “Cyber Crimes Laws” OR “Cyber Warfare”))
Science Direct	((“Cyber Security”) AND (“Cyber Terrorism” OR “Malware Attacks” OR “Malware Analysis OR “Malware Detection” OR Cyber Espionage” OR “Cyber Crimes Laws” OR “Cyber Warfare”))
Springer	((“Cyber Security”) AND (“Cyber Terrorism” OR “Malware Attacks” OR “Malware Analysis OR “Malware Detection” OR Cyber Espionage” OR “Cyber Crimes Laws” OR “Cyber Warfare”))
Google Scholar	((“Cyber Security”) AND (“Cyber Terrorism” OR “Malware Attacks” OR “Malware Analysis OR “Malware Detection” OR Cyber Espionage” OR “Cyber Crimes Laws” OR “Cyber Warfare”)), Intitle: “Cyber Terrorism,” Intitle: “Malware Analysis,” Intitle: “Cyber Security,” Intitle: “Cyber Security Laws,”

3.3 Data Extraction

The pertinent literature was then collated in a worksheet under the following heads:
"Title, Venue, Year, Quality rating, Domain, and Sub Domain."

The analysis of the population was made on inclusion and exclusion criteria which also included the removal of duplicates. The papers filtered through the criteria were reviewed in detail to populate the following heads in an excel worksheet. **Fig. 1** represents the data extraction process.
"Title, Venue, Year, Quality rating, Domain, Sub Domain, Citation String, Problem addressed, Proposed Solution, Results, Operating Parameters, Evaluation measures, Data set, Analysis, and Future Directions."

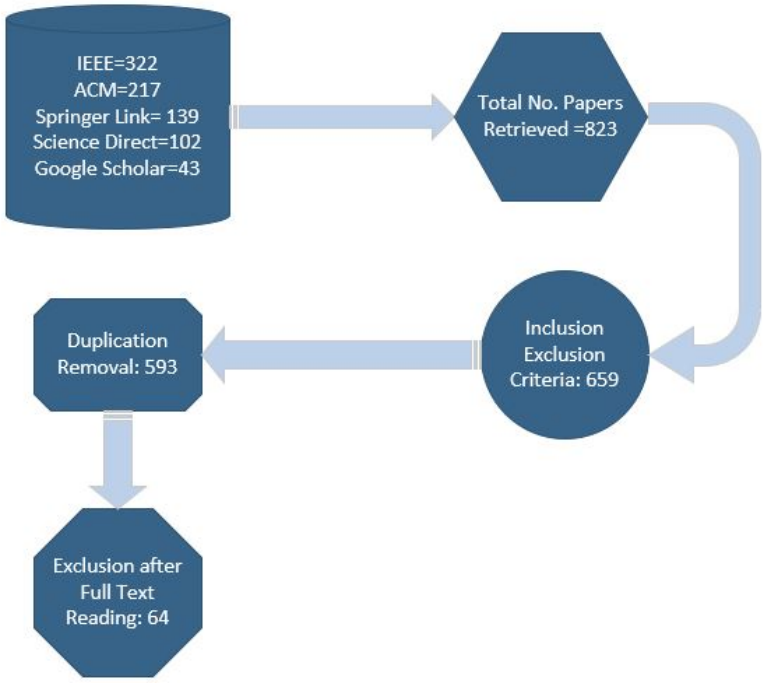


Fig. 1. Data extraction process

3.4 Quality Assessment

Quality Assessment of paper depends upon the quality ranking of Journals venues or core ranking of the Conferences. In this section, only those 64 papers are discussed, finally filtered for the evaluation/analysis process. **Table 4** shows the timeline for the publication of these papers.

Table 4. Selected Literature with Respective Publication Years.

Year	No. of Papers
2017-2020	27
2013-2016	23
2010-2012	14

A quality assessment criterion was set, making five categories as mentioned in **Table 5**, which worked on a binary system carrying either 1 or 0 marks for each category resulting in a maximum of 5 and a minimum of 0 marks for any paper under study. This criterion resulted in almost 65% of the paper in high score rank, i.e., greater than equals four, and 25% papers in average score rank, i.e., score equals three, and just 10% papers in low Score rank either 1 or 2. The low score papers were used for establishing basic concepts.

Table 5. Quality Assessment Criteria.

Sr. No.	Quality Assessment Criteria	Marks
1	Relevant to Cyber Security	
	Paper-based upon the idea of Cyber Security	1
	Paper does not base upon the idea of Cyber Security	0
2	Malware attacks and disruptions	
	The Paper discussed Malware attacks and disruptions	1
	The Paper did not discuss Malware attacks and disruptions	0
3	Papers Publications	
	Paper published in well-known Conferences/Journal	1
	Paper not published in well-known Conferences/Journal	0
4	Content Quality	
	Include Quality content and examples	1
	Does not Include Quality content and examples	0
5	Supportive Content	
	Content fully supports the Topic and domain	1
	Content does not support the Topic and domain	0
Quality Marking		
High	**Moderate**	**Low**
Score ≥ 4	Score = 3	Score ≤ 2

3.5 Results

A total of 823 records were retrieved from the five electronic databases, which after implementation of inclusion-exclusion criteria, resulted in 659 records. Sixty-six of them were excluded for duplication. Then, 529 were eliminated when reading titles and abstracts. The full text of the remaining 64 articles was retrieved for a full review to encompass the complete scope of this study.

4. What are the Fundamental Cyber Threats?

The continuous evolution in computer technologies has created a new class of threats called cyber threats. A cyber threat is a potential malignant act that seeks to sabotage a society's ability to maintain internal or external order. In this era, threat actors can operate through the Internet to initiate virtual offensives from almost anywhere on the planet. Cyber threats come in three broad categories:

4.1 Cyber-Crime

Any criminal activity committed via computers, digital devices, and networks used in the cyber domain and is facilitated through the internet medium [11]. Cybercrime knows no borders, and hence prosecuting them is no easy task. It is also exceedingly difficult to track cybercriminals as, most of the time, they are operating from across international borders. Cybercrimes are committed by a broad range of people: students, amateurs, and professionals. New advancements open new doors for criminals; however, very few unique sorts of crime. What differentiates cybercrime from conventional crime, apart from using technology, is scale, reach, and speed. These crimes can be conducted on a larger scale which may not be possible in the physical world [12]; for example, a conventional bank robber may only rob a bank or two in a go, but a cybercriminal can target hundreds of banks at once. Cybercrimes can be committed globally at machine speed; for instance, a person sitting in Russia can target a bank located in America. Some common types of cybercrime are: Carrying out frauds, trafficking in child pornography and licensed content, identity theft, violating privacy, cyberstalking, social engineering, etc. The motivations behind cybercrimes are money and information. Cybercriminals always take advantage of the vulnerability and the negligence of users where many users are not security conscious.

4.2 Cyber Terrorism

Cyber terrorism utilizes computer systems and telecommunication networks to execute ferocious actions resulting in or intimidating, loss of life, or destruction of the critical infrastructure to achieve political or ideological gains [13]. Cyber terrorism attacks are perpetrated by politically or ideologically motivated non-state actors. The main purpose behind these attacks is to create the destruction of infrastructure and disrupt the general public. These attacks are directed to specific critical systems and infrastructures. The concept of cyber terrorism can be identified by five elements, as given in **Table 6** [3]. For example, in a small town in Australia in January 2000, a man hacked into a municipal waste-management system and dumped millions of liters of raw sewage into parks, rivers, and businesses to undermine citizens' faith in the government's ability to maintain order [14]. Cyber terrorism attacks can be divided into two major classes: targeting a specific company or organization and targeting specific software or IT infrastructure [15].

Table 6. Elements of Cyber Terrorism

Elements of Cyber Terrorism	
	Motive: Religion, political, ideological, etc.
	Intention: Gain political, social, militarily, or ideological advantages.
	Means: Computer systems and communication technologies and networks.
	Target: Critical infrastructures and information systems.
	Effect: Violence, destruction, or disruption of services, physical, operational, and informational damages, and harm individuals and groups.

A common agenda gathers all the cyber terrorists and cyber-spies in the terrorist organization on the same goal. This combined action would create more chaos than the action of a solitary individual. There are many reasons why cyberspace is an alluring choice for terrorists. Using cyberspace as a medium for attacks, terrorists can inflict wider-reaching impacts on a country, community, geographic area, or ethnic group than they could by resorting to physical violence. In addition to that, cyberspace offers little or no regulation with the anonymity of communication.

Cyber espionage is another dimension of cyber-terrorism [9] [4]. It is acquiring secret information from a foe and using that information to obtain some competitive strategic, security, financial, or political advantage. Cyber espionage has become an almost constant threat. According to NATO, almost all member nations have reported cyber espionage incidents, including the United States. More than 72 companies, including 22 government offices and 13 defense contractors, were also affected through this [16].

Another dimension in cyber-terrorism is **cyber terror funding**. Cyber terrorists are shifting towards cryptocurrencies such as Bitcoin and online payment processing systems for raising and transferring finance. Most of these fundraising activities are carried out through the Dark Web [17]. The main reason behind the use of the Dark Web is anonymity. Another source of cyber-terror funding is ransomware attacks [18].

4.2.1 Cyber terrorism conceptual framework

Researchers have proposed several conceptual frameworks on cyber terrorism [19] [20] [21] and tried to outline the context in which cyber terrorism is functioning, its techniques, and object. These frameworks provide a high-level overview and serve as a basis in the domain of cyber terrorism. While researchers attempted to illustrate the effects and consequences of cyber terrorism in other literature, whereas a conceptual framework has already been developed [22], **Fig. 2** shows the proposed framework and description of the components that can be seen in **Table 7**.

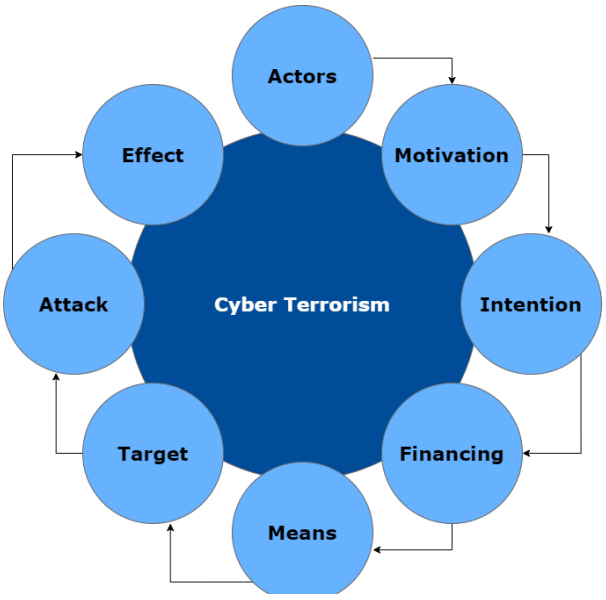


Fig. 2. Cyber terrorism conceptual framework

Actors can either be individuals or groups of politically, ideologically, or religiously motivated perpetrators. The intention is a subjective state of mind of the actors involved that represents a commitment to carrying out an attack and what outcome they have expected out of it. Terror financing itself is a topic of huge debate. Terrorist organizations have shifted to digital currencies and online payment processing systems for financing. These services usually require only a valid e-mail address to initialize an account, while the real names and locations of the actual users can be fabricated. The anonymous money transfer services provide an extremely useful tool for terrorist organizations to transfer funds with an incredibly low risk of detection. Means of attack can be a computer system, any malicious

software, or communication technologies. Potential targets can be corporations, critical infrastructures, or information systems. The attack can be divided into three types: unstructured, structured, and coordinated [23]. Unstructured attacks are mainly unfocused and can only target a single system causing the only disruption, while the structured attacks are basic and can target multiple systems, causing disruption and destruction of the data. Lastly, the coordinated attacks are complex and sophisticated, targeting various networks causing disruption and destruction of systems. The effect of these attacks can be on a massive scale.

Table 7. Cyber terrorism framework description.

Attributes	Description
Actors	Group / Individual
Motivation	Politically / Ideologically / Religious Difference
Intension	Subjective State of Mind / Forethought
Finance	Digital Currencies (Crypto-currency, Bitcoins) / Anonymous Money Transfer Services
Means	Computer Systems / Malicious Software / Communication Technologies
Target	Critical Infrastructures / Information Systems.
Attack	Unstructured / Structured / Coordinated
Effect	Violence / Destruction / Disrupt / Psychological

4.3 CYBERWARFARE

Although cyberwarfare generally refers to cyber-attacks perpetrated by one or more nation-states on another, to the best of our knowledge, there has been no agreed-upon definition of cyber warfare. The most common definition states: *Cyberwarfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information systems* [24]. It is the fifth generation of warfare and comprises cyber-space by a nation-state to achieve the same general objectives as a conventional military force. For example, the Stuxnet worm said to have been developed by the U.S. National Security Agency (NSA) and Israeli intelligence, that sabotaged Iranian nuclear centrifuges starting in 2009 [25]. Cyberwarriors are state-sponsored agents who develop capabilities and undertake cyberattacks in support of a country's strategic objectives. It should be noted that cyber warfare cannot be considered a conventional conflict, although the component of ferocity is present in cyberwarfare. The theater of operations in cyberspace is virtual and unlimited, so we cannot define a territory for cyberwarfare, unlike conventional conflict. Cyberwarfare has certain targets in war, but cyber terrorism causes fear and harm to anyone in the targeted vicinity.

Cyberespionage is also a part of the cyber warfare campaign for three reasons: deterrence through infiltrating the enemy's critical national infrastructure, military technological espionage to gain military knowledge, and industrial espionage to gain an economic advantage over enemies. In modern times, cyberwarfare capabilities are needed by a nation to attack and paralyze an enemy's military capacity or its ability to control its forces.

4.3.1 Cyberwarfare conceptual framework

Based on various literature, a conceptual framework on cyber warfare has been developed [23] [26] [27] [28]. As shown in **Fig. 3**. The most important component that differentiates cyberwarfare from cyber terrorism is the involvement of one or more nation-states. Their objective is to destroy information systems, military installments, critical infrastructures, etc.,

owned by a competitor state. The purpose is the same as that of a conventional war, i.e., destroying the enemy.

Offensive cyberwarfare attacks can be divided into three categories: destruction, disruption, or disinformation. Attacks leading to the destruction of physical assets fall into the destruction category. Disruption is the most common form of attack. This type of attack can be epitomized by website defacement, releasing computer viruses, worms, and other malicious software attacks to damage the critical data within information systems. Disinformation involves manipulating information to place the enemy in the worst public opinion possible. All attributes of the suggested conceptual framework are described in **Table 8**.

Fig. 3. Cyberwarfare conceptual framework.

Table 8. Description of cyberwarfare framework.

Attributes	Description
Nation-State	One or more nations can be involved.
Mass	Bring together all available cyber forces.
Unity of Command	Maintaining the unity of cyber forces to obtain a single objective.
Objective	Targeting an enemy's critical infrastructure or information systems.
Planning	Allocating budget, resources, etc.
Attack	Attacks can be of three types: Disinformation, Disrupt, and Destroy.
Effect	These operations can result in electrical blackouts, failure of military equipment and breaches of national security secrets, etc.

4.4 How are Cyber Weapons Different from Conventional Computer Malware Systems, and How have the Cyberweapons Evolved Over the Years?

There is no precise definition of cyberweapons or the anticipated capabilities and effects of their utilization [29], but the North Atlantic Treaty Organization (NATO) and Cooperative Cyber Defense Centre of Excellence (CCDOE) defines cyberweapons as software, firmware, or hardware designed or applied to cause damage through the cyber domain [30]. However, the definition is legally controversial, the reason being the assumption that the intended usage of software, firmware, or hardware would alter the status of a non-weapon to a weapon.

Cyberweapons are a subset of weapons, and weapons are defined as instruments designed or used with the intent of self-defense or inflicting harm. These are malicious pieces of code employed with the goal of either self-defense or inflicting harm. A state or non-state actor operates the cyberweapons against specific targets to meet objectives that would otherwise require the use of physical force. What is important is not the design or destructive capacity of a cyber-weapon but the intent with which it was employed, specifically, combining the intentions and motivations of the user of cyberweapon with its potential impact. Cyberweapons have created serious implications for the security of critical infrastructure worldwide. For example, the Stuxnet worm was used to slow down Iran's nuclear program, and it had a worldwide impact making governments and industries accelerate their efforts to enhance infrastructure security [32]. Cyberweapons can be very sophisticated, precise, and offer less costly means, offering new possibilities for achieving military objectives.

Malware is often the primary weapon in cyber conflicts, but it is important to understand that not all malware are cyber weapons [10]. Cyberweapons show high selectivity in either or both of their employment and operations. On the other hand, conventional malware is largely random and irrelevant in its operations and usually employs script kiddies or cybercriminals. A typical instance of malware may harm you through a phishing email with a malicious attachment, that is, malware disguised as a legitimate file. Once you open that file, malware attaches itself to your computer and steals all your personal information, including your passwords, bank information, etc. The following are referred to as cyberweapons by cyber-security experts [31].

- Stuxnet
- Duqu
- Wiper
- The Shamoon
- Flame
- BlackEnergy

The example of the Stuxnet worm showed us that cyberweapons are becoming more smart, precise, and sophisticated. They can operate autonomously, with commands and data wired into the code. Suppose the targeted system is not remotely accessible. In that case, it can spread across machines via USB sticks and local network links exploiting several unknown vulnerabilities and disguising themselves as legitimate software using fraudulent digital certificates. They are becoming stealthier; they can conceal themselves long enough to cause damage and afterward self-destruct themselves to remove their trace. In the future, cyber weapons may not be as restrained as their predecessors.

5. Taxonomies of Cyber-Security

After going through various literature, a taxonomy of cyber security was developed and presented in **Fig. 4**.

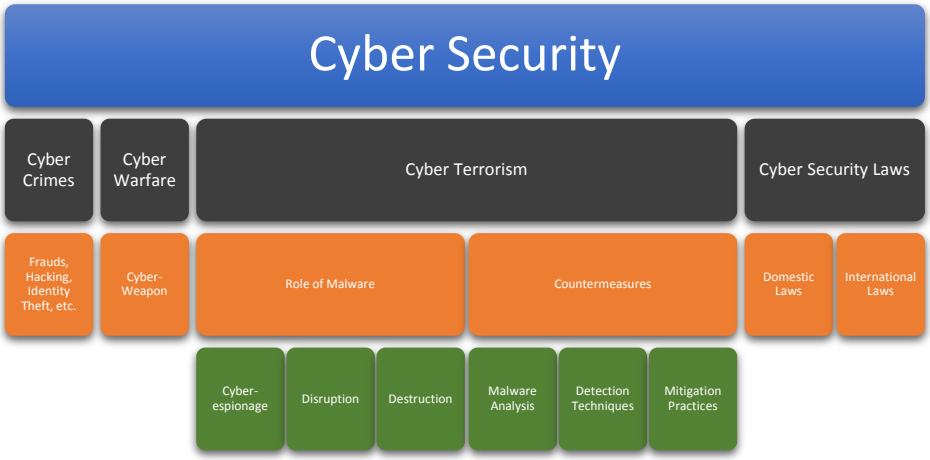


Fig. 4. Taxonomy of cyber-security

Cybersecurity is an umbrella term encompassing all the topics discussed in this study. We have classified cybersecurity threats into three (03) classes: cyber-crimes, cyber warfare, and cyber-terrorism. Cyber security laws are what help us understand, differentiate and prosecute these threats. Cyber security laws are further divided into two categories: domestic laws and international laws.

6. Discuss Different Case-Study Incidents Involving High Severity Cyber-Attacks in Various Sectors?

The previous section explained how malware has evolved and how the concept of cyber weapons came into being. State-sponsored actors or military agencies perform cyber-attacks using weaponized malware on competitor'' organizations or their enemies. In this section, some severe cyber-attack incidents using malware have been discussed in sector-wise chronological order from 2008 to 2020, as shown in **Table 9**.

6.1 AVIATION SECTOR

Shamoon Malware Attack No. 2: In November 2016 second attack of Shamoon Malware in Saudi Arabia was reported. According to the report, the Authority of Civil Aviation attacked out critical data from thousands of machines and brought operations down for several days [32].

6.2 Banking Sector

Gameover Zeus: Zeus is a botnet malware attack injected to exploit confidential information of bank accounts. According to reports, 80% of total attacks were driven by this botnet in the year 2011. However, an increase of 1.3% in financial attacks was also observed in the year 2013. This attack covers almost 65 countries globally [33]. This botnet was entitled "*King of the Underground Crimeware Toolkits*" by Symantec [34].

Target Stores attack: This attack took place on November 15, 2013. When attackers managed to get access to a stor''s HVAC (heating, ventilation, and air conditioning) control system by sending phishing emails, which installed Zeus Trojan, an attacker got access to credit card

information. After this, the attacker installed malicious credit card stealing software to access other credit card information in a chain. This attack exposed 40 million credit cards and credit card'' confidential emails. Approximately 70 million people were affected, and it was claimed to be developed in Russia [5].

6.3 Defense Sector

Stuxnet Malware: In mid of 2010, a new form of malware was discovered. This malware was found at an attack on the Iranian nuclear facility at Natanz. The purpose was to access the systems on which WinCC and PCS7 programs were running, using the default passwords. This malware affects the frequency-converter drives, which were used to manage the centrifugal speed for the concentration of uranium-235. This malware modified the frequency cycle to a speed not defined in its program, resulting in the centrifuge running higher than normal and causing huge disruption [35].
Duqu / Flame/ Gauss Malware: Duqu is a complex malware platform that uses three zero-day vulnerabilities, and this links to the PS+1 venue an event. The beauty of this malware code is it does not leave traces [36]. Flame Malware was claimed to develop by Israel and US agencies that propagate via USB port or network port by using technology "rootkit" and hides in a machine. This malware can access the audio, video skype call, activity on the network and can copy files from machine [37]. Gauss Malware was developed in 2011, and in 2012 Kaspersky Experts found this malware attack similar to flame virus based on Stuxnet programming. This malware records the browser's history and the network connection, processes, folders, and BIOS information. This malware also propagates via a USB drive [38].

6.4 Energy Sector

Turkish Pipeline Explosion: This incident took place in the Turkish oil pipeline on Aug 5, 2008, suspected of being attacked by Russia. There was a loss of around 30,000 barrels of oil, and it caused the shutdown of the pipeline for three weeks. Due to the vulnerability in the security cameras, two unauthorized persons managed to enter the facility and access the computers hosted by SCADA systems by making the pipeline over-pressurized, resulting in an explosion. They also jammed the alarm, where a resident reported the explosion [39].
Night Dragon malware: The attacker from China used this malware command and control servers situated in the USA and Netherland, targeting the global energy, oil, and petrochemical industries. This attack utilized cyber-attacks like social engineering, using vulnerabilities in MS Windows, spear phishing, MS AD vulnerabilities, and RATs (remote access Trojans) techniques to access confidential information. The attacker managed to retrieve the password and gain access to documents related to oil and gas bidding [5].
Gas Pipeline Cyber Incident Campaign: A campaign was raised in late December 2011, where different hackers sent fake emails to companies using the spear-phishing technique. The emails were composed very carefully to appear as sent by real or trusted companies. The target of this campaign was natural gas pipeline companies [5].
Shamoon Malware Attack No. 1: On Aug 15, 2010, a new form of malware was identified, attacking Saudi Arabian's oil production company "Saudi Aramco." The attackers managed to get access to a network computer and access all computers by spreading the virus with the help of this computer. Almost 30,000 computers were affected by the virus and wiped out the data from the computers, which was not recoverable. However, the attack did not stop production [40].

Dragonfly/Energetic Bear Campaign: In mid of June, Hackers launched a campaign named Dragonfly. Some reports name this campaign as the Energetic Bear Campaign because the target of this campaign was Energy sectors to gain access to the networks of target sectors. The primary tool used in this campaign was Havex malware, whereas RATs (remote access trojan) were used as a secondary tool [5].

6.5 Iron and Steel Sector

German Steel mill attack: According to the SANS report, the techniques used in this attack were spear-phishing and social engineering. The attacker gained access to the production network, failed multiple control systems, and stopped the blast furnace, using massive disruption [41].
Norsk Hydra Ransomware Incident: In March 2019, Norsk Hydra was hit by LockerGaga malware. As a result, the company had to shut down the production unit for several days. The attacker asked for ransom to decrypt all infected data [42]. The company reportedly bears the loss of $40 million [43].

6.6 Water and Power Sector

New York Dam attack: This attack took place at Bowman Dam in New York. Hackers got access to SCADA systems which connected through the cellular system to the Internet. Its details were not made public; however, the attack was attributed to the vulnerable interconnection and non-implementation of security controls [44].
Ukraine's Power Grid (Attack No. 1): This attack took place on December 23, 2015, on the Ukrainian Power grid, resulting in the power supply malfunction. According to the analysis report, workers received phishing emails that installed Black Energy malware in the systems. This malware propagated towards the network and gave a pathway to hackers to enter the network. Hackers moved towards AD (Active Directory) and gained access to user'' credentials, leading to network and subsequent access to SCADA systems. Unfortunately, the firewall policies were not configured properly. At 3:30 pm, attackers compromised SCADA systems and cut down the electrical supply for approximately 6 hours [45].
Kemuri Water Company attack: The major point of attack in KWC is using old IBM AS/400-based SCADA systems to monitor and program their PLCs. The attackers retrieved the login credentials from a front-end web server and accessed the water control software. The attackers modified some quantity of chemicals, which stopped the production, and as a result, the recovery time of the water filtration process increased [46].
Ukraine's Power Grid (Attack No. 2): On December 17, 2016, a second attack was launched on Ukraine's power grid. This time attackers using the Denial of Service (DoS) attack intruded into the network and tripped down the circuit breaker of 30 substations. As a result, approximately 225,000 customers were affected by the power cut-off [5]. It was reported the CRASH OVERRIDE Malware was used in this attack. This malware can reduce the power energy and the power gri''s substation and manipulate the circuit breakers. It can also halt the automation system by using the DoS technique [47].

6.7 Others

Crypto Locker: On Sept 05, 2013, a new form of ransomware was discovered, which encrypts files in the victi''s machine and decrypt unless the ransom was paid within 72 hours. According

to an analysis report from October 22 to November 1, 2013, approximately 22,630 machines were affected in the U.S, about 70.2% of global Crypto Locker infection [48].

APT33 Group: According to a report from FireEye, this is an Iranian hacktivist group. It was also mentioned that this works under the assistance of the Iranian Government. APT33 Group sends spear-phishing emails that appear to be legitimate emails from some recruitment companies. The target of this group is the energy sector and petrochemical industries [49].

NotPetya Malware: This is one of the most destructive and costly cyber-attack in cyber history. This malware affects the Microsoft Windows Operating System. It encrypts the hard drive, but its encryption is permanent which cannot be decrypted. The malware was claimed to be triggered by Russia. It was reported that Maersk, a Danish integrated shipping company, was affected by this malware at suddenly 80,000 employee's computers restarted abruptly, and this company lost $300 million due to this malware attack. The company had to reinstall2439approx. 4000 server and2439approx. 45000 PCs [50].

TRITON/Trisis/HatMan Malware: This malware builds its framework after intrusion into the network, exploits the industrial safety system, and causes the process shutdown. It is also given a third name HatMan Malware. This malware attack affected Schneider Electric's Triconex Safety System by adding malicious functionality that allowed the attackers to alter the contents and run their custom code that failed the safety process [5].

TSMC WannaCry Attack: Taiwan Semiconductor Manufacturing Company (TSMC) is a chip fabrication company affected by the WannaCry attack. WannaCry is a malware from the family of ransomware. It was reported that a supplier installed software without a virus scan, the virus propagated on approximately 10,000 machines. TSMC had to shut down its production, and the shutdown's impact was roughly $256 million [51].

SamSam-like attack*:* According to US-Cert Alert, this attack exploited the vulnerabilities in Windows Server and gained access to the network, and infected all available hosts. It stole the administrator's password and ran the malicious file onto the server, which infected all connected nodes with this server [52]. In November 2018, the FBI estimated that the SamSam group received approximately $6 million on ransom payments [53].

Kovter Malware: Kovter Malware, also referred to as File-less malware, hides in the registry and leaves few traces. It utilizes PowerShell to run its custom codes, after which it loses all the environmental variables [54].

EKANS Malware: EKANS malware is a new form of malware from the ransomware family. It is an obfuscated malware that was written in the Go programming language. When it runs on the system, it checks for the Mutex value, and if it is found, it will show the message "Already Encrypted" and stop the running process. Otherwise, it will start encrypting the data. The beauty of this ransom is that the system does not shut down, restart, or close any running app throughout the encryption process, and users have full access to the system [55].

Colonial Pipeline Ransomware Attack: It is an American oil pipeline system in Houston, Texas. It impacted computerized equipment managing the pipeline halting all of the pipeline's operations. Cost around $4.4 million in just a couple of hours [56].

Table 9. Malware attacks 2008 – 2020

Sectors	Year	Type	Name	Description
Aviation	2016	Attack	Shamoon Malware attack no. 2	Attack on Saudi Civil Aviation.
Banking	2011	Malware	Gameover Zeus	A botnet designed to steal bank information
	2013	Attack	Target Stores attack	Zeus malware was used to exploit credit and debit cards' information.
Defense	2010	Malware	Stuxnet Malware	Attack on Iranian nuclear facility due to modification in centrifugal speed.

	2011	Malware	Duqu/Flame/Gauss Malware	These malware programs were developed based on Stuxnet Malware.
Energy	2008	Attack	Turkish Pipeline Explosion	Attack on the Turkish oil pipeline due to vulnerability in the network.
	2010	Malware	Night Dragon Malware	Attack runs through command-and-control servers against oil, energy, and petrochemical companies.
	2012	Campaign	Gas Pipeline Cyber Incident	A spear-phishing email technique was used in this campaign.
	2012	Malware	Shamoon Malware attack no. 1	Attack on the Saudi Aramco network.
	2014	Campaign	Dragonfly/ Energetic Bear campaign	The campaign was launched to target Energy Sectors.
Iron and Steel	2014	Attack	German Steel mill attack	Attack on German Steel mill via spear-phishing and social engineering technique.
	2019	Attack	Norsk Hydra Ransomware Incident	Norsk Hydra company hit by LockerGoga malware attack.
Water and Power	2015	Attack	Ukraine power grid attack no. 1	Attackers using email phishing and black energy malware techniques gain access to the Ukrainian power grid network.
	2016	Attack	Kemuri Water Company attack	Attack due to vulnerabilities in old SCADA systems.
	2016	Attack	Ukraine power grid attack no. 2	This time attackers used CRASH OVERRIDE malware to cut the power supply down.
Others	2013	Malware	Crypto Locker	A new family of ransomware was discovered.
	2017	Group	APT33 Group	An Iranian Hacktivist group.
	2017	Attack	NotPetya malware	It encrypts the data but cannot decrypt it back.
	2017	Malware	TRITON/ Trisis. HatMan Malware	This malware targets industrial safety systems.
	2017	Attack	TSMC WannaCry Attack	The company was affected by the WannaCry ransomware attack.
	2018	Malware	SamSam-like attack	Get access to the windows server and install malware on it.
	2018	Malware	Kovter	A file-less malware.
	2020	Malware	EKANS	New malware discovers from the ransomware family.
	2021	Ransomware Attack	Colonial Pipeline	It impacted computerized equipment managing the pipeline halting all of the pipeline's operations.
	2013	Attack	New York Dam attack	Attack was made due to the vulnerable internet connection.
	2013	Malware	Crypto Locker	A new family of ransomware was discovered.

7. Which Countermeasures have been Developed to Mitigate Cyber Malware Risk?

Before mitigating any malware, we must know the kind of malware, the behavior, and the detection techniques. These techniques leave the question divided into three categories: Analysis of Malware Attacks, Detection of Malware Attacks, and Mitigation Strategies for

Malware Attacks.

7.1. Analysis of Malware Attacks

Malware Analysis itself is an incredibly challenging research topic. The malware analysis process involves different components of malware attacks, such as how they evolved, projected targets, and behavior. The malware analysis techniques are categorized into three types: Static Analysis, Dynamic Analysis, and Hybrid Analysis. The first two types of analysis are further classified as Basic static analysis, Advanced static analysis, Basic dynamic analysis, and Advanced dynamic analysis, as shown in **Fig. 5**.

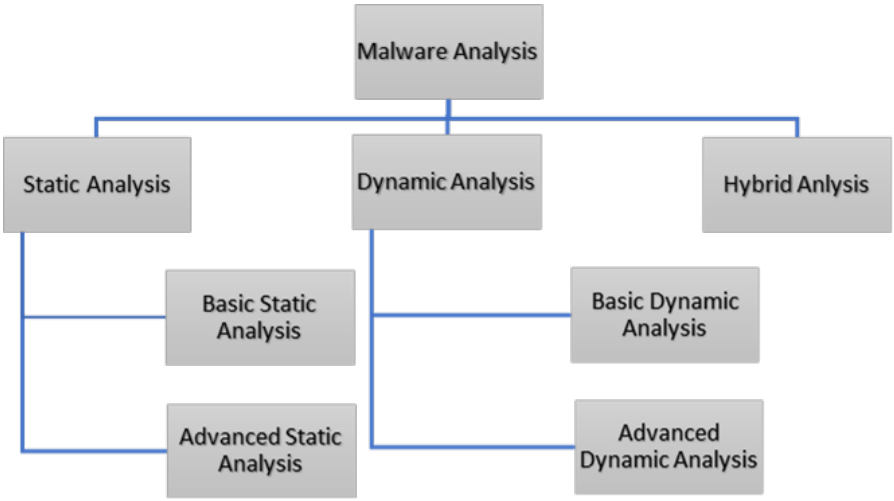


Fig. 5. Malware Analysis

Static Analysis: A process of malware analysis in which the code is analyzed without running the malicious program. The patterns used in this analysis process are string signature, byte-sequence n-grams, syntactic library call, control flow graph, operational code frequency distribution, etc.[6]. **Table 10** shows the results of research papers that applied static malware analysis.

- ***Basic Static Analysis:*** The code or structure is analyzed to determine its functionality in the static analysis technique. Moreover, the malicious code does not run in this phase.
- ***Advanced Static Analysis:*** In this technique, the malware binaries are processed, initializing malware internal content's reverse engineering process. This technique involves running the malware executable into a dissembler, examining the malware program's instruction, and giving us a proper understanding of what the malware program does [57].
-

Table 10. Research papers that applied static malware analysis

Research Paper	Static feature	Accuracy
[58]	Opcode	91.9%
[59]	API, arguments	98.5%
[60]	APIs sequence	40%
[61]	Opcode sequence	97.5%
[62]	Native APIs sequence	94.4%

Dynamic Analysis: In this process, the malicious program is executed to analyze its behavior in an emulated environment [63]. **Table 11** shows the results of research papers that applied dynamic malware analysis.

- ***Basic Dynamic Analysis:*** In this technique, further information is gathered about the purpose of code, and this technique also helps to remove the infection of a compromised system.
- ***Advanced Dynamic Analysis:*** In this analysis technique, the code runs on a debugger or emulator, which provides details of the program's internal state. It gives a clear picture of the internal state of the malware program; also, using this technique, everyone can monitor each step of malware programs easily [7].

Table 11. Research papers that applied dynamic malware analysis.

Research Paper	Dynamic feature	Accuracy
[64]	API calls	91.3%
[65]	file system, registry, network	95%
[66]	file system, registry, network	99%
[67]	APIs sequence	97.2%
[68]	APIs sequence	99.8%
[69]	User API, native API	95.9%

Hybrid Analysis: Hybrid Analysis is a combined aspect of the techniques mentioned above [7]. By using this technique, the ability to detect malicious code is increased.

7.2. Malware Detection Techniques

The techniques used for malware detection are signature, heuristic-based, and hybrid detection techniques [70]. Heuristic-based is further extended to specification-based. The taxonomy of malware detection techniques is represented in **Fig. 6**.

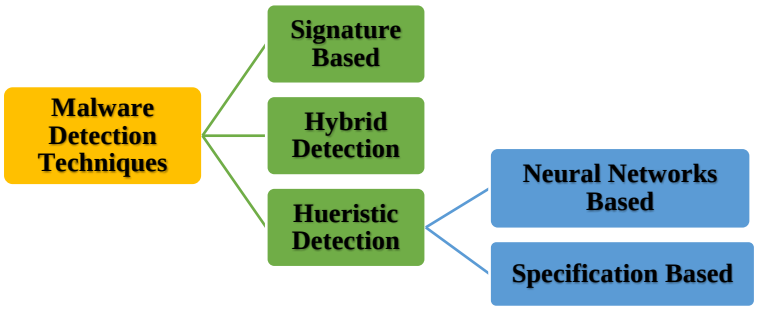


Fig. 6. Malware detection Techniques

Signature-based Detection Technique: The most popular detection technique in which a signature is a sequence of bytes, which can classify the specific type of malware. Various pattern matching schemes are available to scan signatures. Anti-virus programs should have an updated signatures repository and be regularly updated as new threats are discovered [71].

Heuristic Detection Technique: This technique is a proactive technique; it detects the difference between normal and abnormal behavior of a program. Initially, the behavior of malicious code is analyzed and maintains a record of information gathered from the analysis process, which can be checked in case of attacks. In this way, the known and unknown malware attacks are identified and thus can be fixed to help detect the malware family. Behavior detection consists of three functions: Data Collection, Interpretation, and Matching Algorithm [72]; even though it provides high accuracy to detect zero-day malware, that enables to detection of some complex malware [73].

- ***Specification Based Detection Technique:*** This technique analyzes malicious programs based on their specifications and checks against normal and abnormal behavior. The method is derived from the Heuristic technique that uses Artificial Intelligence and Machine Learning methods to analyze the malicious program [72]. **Table 12** shows the pros and cons of different malware detection techniques.
- ***Neural Networks Based Techniques:*** With advancements in AI, new and more efficient malware detection techniques based on binary visualization and self-organizing incremental neural networks were introduced. The experimental results show promising accuracy in the detection of ransomware hidden in PDF and Word files. These techniques also provide efficient detection of unknown malware in a real-time environment [74]. However, these techniques are vulnerable to adversarial samples. To resolve this shortcoming [75] proposed adversary resistant technique that stops attackers from constructing impactful adversarial samples by randomly nullifying features within data vectors.

Hybrid Detection Technique: Hybrid detection techniques are usually better in detecting malware with a low false-positive rate. [76] combined a random forest and a deep learning model using 12 hidden layers to determine malware and benign files with impressive results. [77] proposed a hybrid learning model by extract static fuzzy-hash features and dynamic behavior features of malware, then combining unsupervised clustering learning with supervised classification learning.

Table 12. Pros and cons of different malware detection techniques.

Technique	Advantages	Disadvantages
Signature Base	▪ It only detects known malware. ▪ As compared to other techniques, it uses fewer resources.	▪ It cannot detect unknown malware.
Heuristic Based	▪ Both known and unknown new malware can be detected.	▪ For new and unknown malware, the data repository must be updated. ▪ In the context of time and space, it will need more resources. ▪ The level of false positives is high.
Specification Based	▪ Both known and unknown malware can be detected. ▪ The level of false positives is low.	▪ The level of false negatives is high. ▪ For the detection of new malware, it's not much efficient. ▪ The process of specification development is time taking task.

Neural Networks Based Techniques*:*	▪ Both known and unknown malware can be detected. ▪ High level of accuracy.	▪ Can be vulnerable to adversarial samples.
Hybrid Detection Technique	▪ Both known and unknown malware can be detected. ▪ High level of accuracy. ▪ Low false positive rate.	

7.3. Mitigation Practices

On the broader level, depending on the type of malware attacks, Mitigation Practices are categorized into the following types:

7.3.1 Network environment level security

Firewall: Firewall protects from inbound or malicious and unwanted traffic. It must be configured in an environment to block suspicious traffic and only allow traffic to pass through it.

Intrusion Detection/Prevention System: Network Intruder Detection Systems (IDS) must be configured to observe traffic and alert administrators about attacks passively. It opens a way towards Intrusion Prevention Systems (IPS), which are active systems that detect and prevent intrusions.

SSL VPN: SSL VPN provides a secure connection between the branch office and trusted machines to corporate networks. [78]

Proxy Server: Proxy Server provides services by acting as an intermediate system for network connection. The front end of this server receives a request, and on behalf of the client, resolves the request. It mitigates the risk of a breach by adding an extra security layer between external traffic and corporate servers.

Security by Compartmentalization: This is a security by container approach used by Qubes Operating System. This phenomenon allows several applications to run on multiple virtual machines (VMs). If an application is running inside one compartment with malware, it will not affect other compartments, as they are not inter-linked. This phenomenon also has a concept of disposable VMs to dispose of infected machines easily [79].

Security Information and Event Management (SIEM): SIEM software works by collecting logs and event data from systems, security devices, and applications running in the environment, from antivirus to firewall logs, then sorting data based on categories and generating reports over the centralized platform. When this software identifies any threat, it generates alerts to notify administrators [80].

Sandbox Technique: Sandbox is used to monitor the environment and automate the process of dynamic analysis of emails and web content. So, it helps administrators to detect any unusual activity on network traffic, software, and applications [81].

7.3.2 End user-level security

Update OS/Patched Software: Outdated OS and unpatched software are highly vulnerable as OS must be updated. Any OS without an update will be an open door for hackers to intrude

into it, same in the case of software. Microsoft announced the end of support for Windows 7 and will not release updated patches. So, the users should upgrade from the previous version of Windows to Windows 10 or a later version.

Updated Antivirus: As discussed above, malware can be classified using a unique sequence of bytes known as Signatures. Antivirus with an updated repository of the signature database can reduce the risk of malware attacks, but it is not a complete solution to mitigate the risk of malware attacks.

End-User Training: Cyber Security awareness is a vital step to mitigate cyber-attack risk. End users are unaware of these things, and a single click will fail the whole security tools and measures. The end-user should know which email attachment to open or how to find spam emails to play his role in making the environment secure.

8. What are the Developments in Devising Policies and Laws to Mitigate Cyber-Security in Different Countries?

Technology has grown exponentially over the past few years, and our dependence on these technologies brings us the immense threat of privacy and security. Cybersecurity laws, also known as digital laws, regulate how people use technology. Some of these laws protect people from becoming victims of crime through the unethical or malicious use of technologies. In contrast, other laws create rules for how individuals and companies may use different technologies. Cybersecurity laws tend to cover the most common matters that emerge from digital threats. These matters concentrate on criminal activities, insurance matters, corporate governance, and the jurisdiction of law enforcement [82]. The three main threats that cybersecurity laws aim to mitigate are Cybercrime, Cyber-attacks, and Cyber-terrorists. In this paper, we are focusing on cybersecurity laws for mitigating cyber terrorism threats.

8.1. Cyber Terrorism Laws in Different Countries

Cyber terrorism is becoming a major threat to nations around the globe. It is a real threat to peace and has serious impacts on countries' critical infrastructure. Sensitive information of both the public and the private sectors is stored on and transmitted through sophisticated, globally interconnected computer networks, known as the *Internet*. Although the Internet offers many advantages to countries and billions of people, it has become a weapon of choice for today's cyber-terrorist. At the same time, a target for online terror attacks such as attacking crucial computer networks that can disrupt essential public services like financial systems, emergency services, hospitals, water, power, air/sea traffic control, etc. Cyber terrorists can operate from countries where cybersecurity laws barely exist, making them almost untouchable. The dangers posed by cyberterrorism require genuine attention from national security legislators and policymakers around the globe. In this regard, Governments need firmness in their attitude towards the enforcement of cybersecurity laws to fight cyber terrorism. In the wake of cyber terrorism, the five commonwealth democracies: The United Kingdom, Canada, Australia, New Zealand, and the United States of America, have passed legislation to combat cyber terrorism.

Australia: After September 11th, Australia redefined the meaning of terrorism and embedded it into Section 100.1 of the federal Criminal Code Act of 1995. The Criminal Code of Australia now penalizes a maximum of life incarceration for terrorist acts perpetrated in any jurisdiction. Subsection (2) of Section 100.1 lists the possible harm prerequisites of terrorist activity.

Although this list comprises of several possible harms, a cyber-attack would most probably fall within para (2)(f), which specifically addresses acts of terrorism against control (electronic) systems:

(2) Action falls within this subsection if it:
(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:
(i) an information system; or
(ii) a telecommunications system; or
(iii) a financial system; or
(iv) a system used for the delivery of essential government services; or
(v) a system used for, or by, an essential public utility; or
(vi) a system used for, or by, a transport system [83]

To date, no cyber-attacks have been prosecuted under section 100.1(2)(f), but the phrasing of the clause makes it very lucid that it extends to the attacks that seriously interfere with or disrupt any control (electronic) system, including nonessential ones.

United Kingdom: In the United Kingdom, the meaning of terrorism is defined in section 1 of the Terrorism Act 2000 (UK) c 11 (TA2000). Like Australian legislation, the United Kingdom's legislation penalizes maximum life incarceration for terrorist acts perpetrated in any jurisdiction. Subsection (2) lists the possible harm prerequisites of terrorist activity. If a cyber-attack were to be prosecuted as a terrorist act in the United Kingdom, it would likely fall under subsection (2)(e), which similarly criminalizes acts of terrorism against control (electronic) systems:

(2) Action falls within this subsection if it –
(e) is designed seriously to interfere with or seriously to disrupt an electronic system

This clause in United Kingdom's legislation sets a lower weight of proof. The Unitaab1234567890ed Kingdom government has stated in their National Security Strategy that cyber-attacks by state and non-state actors are one of the four, Tier-1, *highest priority* risks to national security [84].

Canada: Canadian law defines the act of terrorism within section 83.01 of the Canadian Criminal Code as amended by the Anti-Terrorism Act 2001 (ATA) [85]. The Criminal Code of Canada penalizes a maximum of life incarceration for anyone who commits an indictable offense for the benefit of or in association with a group that engages in terrorist activity. Under sub-section (b)(ii)(E), this would include cyber-attacks in Canada or any foreign country that deliberately cause genuine obstruction with or disruption to essential facilities, services, or systems, whether publicly or privately owned [86].

New Zealand: The act of terrorism is defined in clause 5 of the Terrorism Suppression Act 2002 (TSA) of New Zealand. It applies to cyber-attacks against infrastructure and penalizes a maximum of life incarceration for terror activities, which are explained as:

(1) An act is a terrorist act for this Act if
(a) the act falls within subsection (2).
(2) An act falls within this subsection if it is intended to cause, in any one or more countries, one or more of the outcomes specified in subsection (3) and is carried out to advance an

ideological, political, or religious cause, and with the following intention:
(a) to induce terror in a civilian population
(b) to unduly compel or force a government or an international organization to do or abstain from doing any act [87].

The list of possible harm prerequisites of a terror activity is defined in Subsection (3) as:

(3) The outcomes referred to in subsection (2) are –
(d) serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger life [87].

Out of each of the four definitions of commonwealth countries, New Zealand's description sets the highest standard for attacks against infrastructure by necessitating that they also are *likely to imperil life*.

United States: The United States' definition of cyber-terrorism is stated in the Patriot Act. Clause 1030 refers to it as a *federal crime of terrorism*. It is stated as:

(a) Whoever – (1) having knowingly accessed a computer without authorization or exceeding authorized access, and utilizing such conduct having obtained information that has been determined by the United States Government under an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations [or].
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and because of such conduct, intentionally causes damage without authorization to a protected computer; [and].
(b) by conduct described in clause (i). caused (or, in the case of an attempted offense, would, if completed, have caused) –
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals.
(iii) physical injury to any person.
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity to administrate further justice, national defense, or national security [88].

The United States penalizes a maximum death sentence or life incarceration for those acts resulting in death to others. In contrast, all other acts of terrorism receive lesser maximum penalties: from 35 years for maiming, 25 years for property damage, and0 years for the threat of an attack [89].

Pakistan: National Assembly of Pakistan passed a law on August 11, 2016, called the Prevention of Electronic Crimes Act (PECB), 2015-16. Later, the upper house (senate) unanimously passed the law, with several revisions [90]. It is stated as follows:
A cyber-terrorist crime is deemed to have been committed if a crime connected to critical infrastructure is carried out with the intent to commit terrorism. The punishment for such offense upon conviction is up to 14-year imprisonment or a fine of Rs5 million (about US$47,450), or both. The glorification of terrorism-related offenses hate speech, and the recruitment for or funding, and planning of terrorism "through any information system or device" are also punishable crimes under the Act. (Id. §§9, 10A, & 10B) [91].

8.2. International Cyber Terrorism Laws

During recent times, the stats have demonstrated that multilateral cooperation is the most efficacious way to respond to transnational cyber terrorism. The need for such cooperation comes to mind because different countries have different laws to govern cybercrime and cyber-attacks. Therefore, we need international laws to prevent and mitigate cyber terrorism.

United Nations (U.N.): The United Nations is the leading organization that tries to coordinate and seek cooperation in dealing with the problem of cyber-terrorism. It has established many specialized agencies and programs in this regard. The UN Office of Counterterrorism (UNOCT) has taken several initiatives to counter cyber terrorism. *In particular, the Cybersecurity and New Technologies program aims to enhance the capacities of the Member States and private organizations in preventing cyber-attacks carried out by terrorist actors against critical infrastructure. The project program also seeks to mitigate the impact and recover and restore the targeted systems should such cyber-attacks occur* [92].

The North Atlantic Treaty Organization (NATO): Cyber threats to the security of the NATO member countries are becoming more frequent, complex, destructive, and coercive. In response to these cyber threats, NATO is continuously adapting to the evolving challenges in cyberspace. NATO and its partner countries rely on strong and resilient cyber defenses to satisfy the core duty of collective protection, crisis management, and cooperative security. The alliance needs to be prepared to protect its networks and operations from the ever-growing threat of cyber-attacks.

The cyber defense was introduced into the NATO Defense Planning Process in April 2012. Relevant cyber defense requirements are identified and prioritized through the defense planning process [93]. In 2018, at the summit in Brussels, allied leaders agreed upon setting up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. The Centre was to provide situational awareness and coordination of NATO operational activity within cyberspace [93]. In February 2019, NATO defense ministers endorsed a NATO guide that sets out several tools to strengthen NATO's capacity further to respond to significant malicious cyber activities. NATO needs to utilize all the power at its disposal, including political, diplomatic, and military, to tackle the cyber threats that it faces [93].

After discussing these laws, a few questions arise: Should we consider website disfigurement an act of cyber terrorism? Would the utilization of the Internet by terrorists for activities such as fundraising, recruitment, and propaganda be considered an act of cyber terrorism? If a person commits a certain act that meets the criteria of cyber terrorism, under what law will he/she be convicted? Answers to these questions are still to be found.

9. What are the Open Challenges and Issues for Mitigating Cyber Malware Attacks?

In the present world, cybersecurity challenges have become a matter of national security. Organizations ranging from small to large enterprises, government and private institutions, energy, defense, water, and all other sectors are prone to cyber malware attacks from across the globe. Cyber malware attacks are becoming a more frequent and more damaging problem in recent years. The increasing number of new malware programs is becoming a challenging task for cybersecurity experts. According to a survey, cyber malware attacks have increased 61% from 2018 to 2019, shown in **Fig. 7** with the crime categories [94].

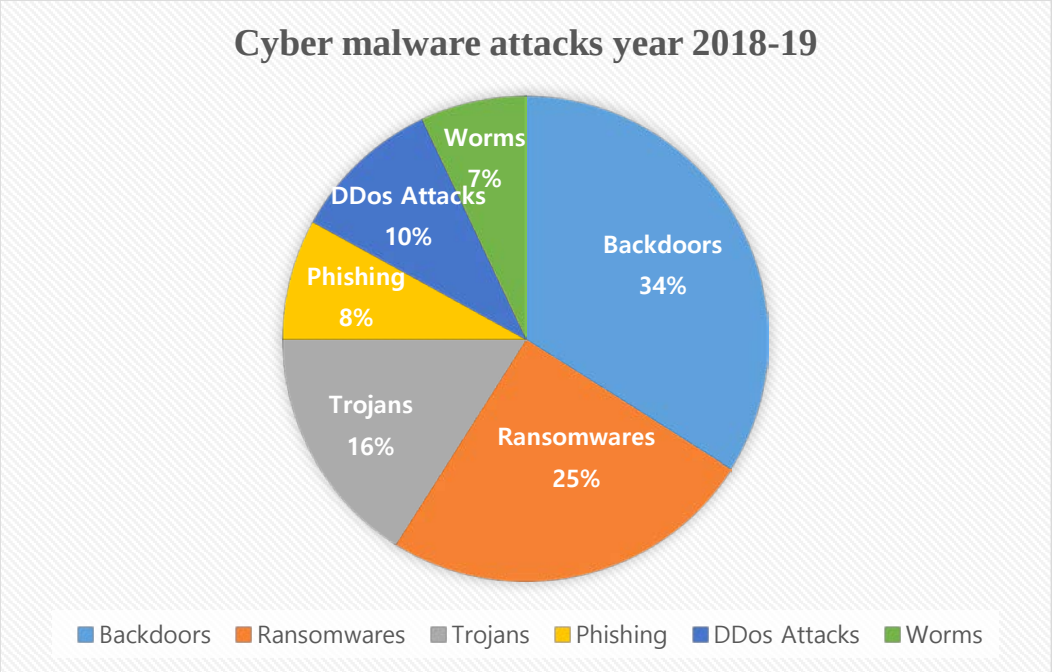


Fig. 7. Cyber malware attacks 2018-2020 [95]

9.1. Mitigation Challenges

Malware attacks are one of the major threats faced by every organization today. These programs are designed to disrupt day-to-day operations, steal valuable information, or espionage. Mitigating these attacks is a huge challenge for cybersecurity experts as these attacks are evolving with every passing day.

Exploiting the unknown faults: The first and foremost issue or challenge cybersecurity experts face for mitigating cyber malware attacks is an unknown fault in an application, a design flaw, or an implementation bug, also called vulnerabilities that threat actors can exploit to cause harm. These are called zero-day attacks. For example, Sony pictures suffered a zero-day attack in late 2014. A possible solution for this issue is that the vendors should pay bounties on finding vulnerabilities in their applications [96]. The only drawback to this can be that the application development process slows down.

The sophistication of malware attacks: Another challenge cybersecurity experts face is the complexity of attacks, which means malware programs are becoming more advanced. Their concealing property can easily be hidden in document files and go undetected by standard malware detection tools. For example, the infamous Stuxnet worm is known to have hidden its manipulation of centrifuge behavior. Cybersecurity experts foresee that the worldwide cost of malware attacks will reach $6 trillion by 2021, which will be doubled since 2015 [97].

Attacks through VoIP technologies: Cybercriminals are paying close attention to VOIP technologies for malware attacks as cell phones are becoming common tools for accessing the Internet. Attackers use them to engage in voice fraud, data theft, and other scams [95]. It is becoming a great challenge to mitigate these types of attacks.

Attacks through Social Networks: With the swift development of social networking platforms, cybercriminals begin to propagate malware more widely by utilizing various social networking platforms with large user bases, such as Facebook, LinkedIn, Twitter, Instagram, etc. [98]. Social networking platforms are used as a delivery mechanism. Studies are being done in this

field, but still, it is a great mitigation challenge for cybersecurity experts.

9.2. Digital Sigatures Validation Challenges

Another important issue that needs to be highlighted here is that the new malware programs can disguise themselves as legitimate software using fraudulent digital signatures [99]. This issue can be dealt with by tightening up validation practices, and anti-malware software should treat invalid signatures as if there is no signature.

9.3. The Broadening Skills GAP

A critical challenge of cybersecurity is the absence of qualified experts to carry out the responsibilities. The International Information System Security Certification Consortium $(ISC)^2$ estimated in 2019 that worldwide 4.07 million cyber security trained professionals are needed to fill the skill gap, which is still growing [100]. Also, cybersecurity experts who know how to protect companies from sophisticated attacks are rare to find and charge heavily, giving the extra financial burden that enterprises are not willing to pay. So, these enterprises hire individuals on the low end of the cybersecurity spectrum with basic skills [101]. These attacks create more pressure on cybersecurity teams since they do not have the talent and experience to fulfill essential security functions.

10. Future Directions

The amount and diversity of cyber threats will continue to grow year after year, but cyber security awareness is the combination of recognizing what is happening and taking action to safeguard a company's digital assets from harm. When individuals are cyber security conscious, they comprehend cyber dangers, the possible consequence of a cyber-attack on their enterprises or personal digital lives, and the procedures necessary to mitigate risk and avoid cyber-crime from penetrating their virtual workplace. In comparison, most individuals nowadays are either completely uninformed of the hazards posed by cyber intrusions or have acknowledged the potential risks of entrusting their entire life to the digital world. The media attention on identity theft, data breaches, and photo leaks has not yet slowed our propensity to save our most confidential data in the cloud. The fact is that hackers are fully aware of this and will continue to abuse our human nature regardless of the consequences. COVID-19 phishing schemes are trending in the digital world, where people provide personal information on untrusted links. There is a dire need to inform the public about cyber threats and their impact on our routine or official life through seminars, introducing undergraduate and postgraduate courses at all academic levels. So, security professionals can mitigate the risk generated by the attackers. In this era of technology, everything is connected to the internet and becomes vulnerable due to organized gangs, untrusted internet, state-sponsored attacks, decreasing international cooperation, phishing attacks. There is a need to introduce a free virtual private network (VPN) to provide end-to-end security between devices as most companies are charging a lot of money for the purpose. This solution will mitigate the risk and benefit for the people working remotely. Similarly, data storage and privacy are a great challenge in the cloud, which may be less secure and risk ransomware attacks. So, it is necessary to provide a safe environment to store data with appropriate services without charging any cost. Most companies are asking to pay an amount for extra storage and services.

11. Conclusion

The objective of this systematic review was to investigate the different cyber threats and countermeasures present in today's world. The continuous evolution in computer technologies has created a new class of threats called cyber threats. Cyber threats can be categorized into three categories: cyber-crime, cyberwarfare, and cyber-terrorism. Mostly these three threats are confused with one another, yet they are quite different. However, malware is a key weapon used in all of them. Two conceptual frames were proposed to differentiate cyber-terrorism from cyberwarfare. In this article, we investigated the evolution of malware from an ordinary computer bug to a destructive cyber-weapon and listed down history's most destructive cyber-attacks carried out in different industries. These attacks have caused billions of dollars' worth of damages over the years. To prevent such huge losses in the future, we discussed countermeasures and divided them into three categories: analysis of the threat, detection of the threat, and mitigation practices, addressed in detail. In the end, we list down cyber laws that various countries have made to fight these cyber threats. The results of this study should be seen in the light of some limitations. First, it was difficult to find in-depth details about system security breaches in various organizations as these organizations try to hide such incidents to save their reputation. Second is the presence of limited literature on different aspects of the cyber domain as a very small number of researchers work in this domain. The third is that the international laws are not well defined to prosecute cybercriminals, and LEAs are not trained enough to deal with cybercrimes. Synthesizing the existing research on cyber threats and countermeasures, the study also provided open challenges for future studies in this field.

References

[1] "COMPUTER SECURITY RESOURCE CENTER," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/cyberspace. [Accessed 11 May 2020].

[2] J. Bussell, "Cyberspace Communications," Britannica, 2013. [Online]. Available: https://www.britannica.com/topic/cyberspace. [Accessed 8 5 2020].

[3] Al Mazari, Ali and et al., "Cyber Terrorism Taxonomies: Definition, Targets, Patterns and Mitigation Strategies," *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, 2018. Article (CrossRef Link)

[4] G. Wangen, "The role of malware in reported cyber espionage: a review of the impact and mechanism," *Information*, vol. 6, no. 2, 183-211, 2015. Article (CrossRef Link)

[5] K. &. F. R. Hemsley, "A history of cyber incidents and threats involving industrial control systems," in *Proc. of nternational Conference on Critical Infrastructure Protection*, Springer, Cham, pp. 215-242, 2018. Article (CrossRef Link)

[6] A. O. &. C. C. Eze, "Malware analysis and mitigation in information preservation," *IOSR Journal of Computer Engineering*, 20(4), pp. 53-62, 2018.

[7] D. S. N. &. P. N. J. Deka, "Malware detection vectors and analysis techniques: A brief survey," in *Proc. of 2016 International Conference on Accessibility to Digital World (ICADW)*, IEEE, 2016. Article (CrossRef Link)

[8] R. K. O. a. K. A. Z. A. Sihwail, "A survey on malware analysis techniques: static, dynamic, hybrid and memory analysis," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, pp. 1662-1671, 2018. Article (CrossRef Link)

[9] W. C. Banks, "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage," vol. 66, pp 513, 2017.

[10] Herr, Trey and Paul Rosenzweig, "Cyber weapons and export control: Incorporating dual use with the prep model," *J. Nat'l Sec. L. & Pol'y*, vol. 8, p. 312, 2015.

[11] "NATIONAL RESPONSE CENTRE FOR CYBER CRIME," FIA, [Online]. Available: http://www.nr3c.gov.pk/cybercrime.html. [Accessed 17 5 2020].

[12] M. Gercke, *Understanding cybercrime: a guide for developing countries*, ITU Cybercrime Legislation Resources, 2016.
[13] Theohary, A. Catherine and J. W. Rollins, *Cyberwarfare and cyberterrorism*, brief., Washington, DC: Congressional Research Service, 2015.
[14] N. Sayfayn and S. Madnick, "Cybersafety Analysis of the Maroochy Shire Sewage Spill," *Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, MIT Management Sloan School, Working Paper CISL 9*, 2017.
[15] Matrosov, Aleksandr and et al., "Stuxnet under the microscope," *ESET LLC*, 2010.
[16] D. O. Theiler, "New threats: the cyber-dimension," *NATO Review*, 2011.
[17] Carroll, Paul and J. Windle, "Cyber as an enabler of terrorism financing, now and in the future," *Journal of Policing, Intelligence and Counter Terrorism*, vol. 13, no. 3, pp. 285-300, 2018. Article (CrossRef Link)
[18] Dion-Schwarz, Cynthia, David Manheim and Patrick, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats," *Rand Corporation*, 2019.
[19] Ahmad, Rabiah and Zahri Yunos, "A dynamic cyber terrorism framework," *International Journal of Computer Science and Information Security*, vol. 10, no. 2, 2012.
[20] R. Heickero, "Terrorism online and the change of modus operandi," *Swedish Defence Research Agency*, Stockholm, Sweden, 2007.
[21] N. Veerasamy, "Conceptual high-level framework of cyberterrorism," *researchspace.csir.co.za*, 2009.
[22] R. Ahmad and Z. Yunos, "Perception on Cyber Terrorism: A Focus Group Discussion Approach," *Journal of Information Security*, vol. 3, no. 3, 2012.
[23] T. F. O'Hara, "Cyber warfare/cyber terrorism," *ARMY WAR COLL CARLISLE BARRACKS PA*, 2004.
[24] L. Polley, "Cyber Warfare," RAND Corp., [Online]. Available: https://www.rand.org/topics/cyber-warfare.html#:~:text=Cyber%20Warfare-,Featured,denial%2Dof%2Dservice%20attacks.. [Accessed 11 7 2020].
[25] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365-404, 2013. Article (CrossRef Link)
[26] Taddeo and Mariarosaria, "An analysis for a just cyber warfare," in *Proc. of 4th international conference on cyber conflict (CYCON 2012)*, 2012.
[27] Hemanidhi, Aniwat and Sanon Chimmanee, "Military-based cyber risk assessment framework for supporting cyber warfare in Thailand," *Journal of Information and Communication Technology*, vol. 16, no. 2, 2017.
[28] Ormrod, David and Benjamin Turnbull, "The cyber conceptual framework for developing military doctrine," *Defence Studies*, vol.16, no.3, pp.270-298, 2016. Article (CrossRef Link)
[29] T. Herr, "PrEP: A Framework for Malware & Cyber Weapons," *Journal of Information Warfare*, vol. 13, no. 1, p. 95, 2014.
[30] "Cyber definitions," NATO CCDOE, 2015. [Online]. Available: https://ccdcoe.org/cyber-definitions.html. [Accessed 02 05 2020].
[31] A. Kiyuna and L. Conyers, Cyberwarfare Sourcebook, Lulu. com, 2015.
[32] S. Chan, "Cyberattacks Strike Saudi Arabia, Harming Aviation Agency," 1 12 2016. [Online]. Available: https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html. [Accessed 12 May 2020].
[33] A. M. A. a. M. A. Azab, "Machine learning based botnet identification traffic," in *Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA*, 1788-1794, 2016. Article (CrossRef Link)
[34] H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi and L. Wang, "On the analysis of the Zeus botnet crimeware toolkit," in *Proc. of 2010 Eighth International Conference on Privacy, Security and Trust*, IEEE, Ottawa, 2010. Article (CrossRef Link)

[35] B. &. R. D. Miller, “A survey SCADA of and critical infrastructure incidents,” in *Proc. of the 1st Annual conference on Research in information technology*, pp. 51-56, 2012. Article (CrossRef Link)
[36] "The Duqu 2.0 Targeted Attacks,” Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/threats/duqu-2. [Accessed 11 May 2020].
[37] N. Milosevic, “History of malware,” ArXiv.org, 2013.
[38] GReAT, “Gauss: Abnormal DIstribution,” SecureList, 9 August 2012. [Online]. Available: https://securelist.com/gauss-abnormal-distribution/36620/. [Accessed 12 May 2012].
[39] M. G. M. S. K. J. L. &. K. S. Angle, “Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems,” *IEEE Power and Energy Technology Systems Journal*, vol. 6(4), pp. 172-182, 2019. Article (CrossRef Link)
[40] S. Alshathry, “Cyber Attack on Saudi Aramco,” *International Journal of Management and Information Technology*, vol. 11, pp. 3037-3039, 2016.
[41] M. J. A. a. T. C. Robert M. Lee, “German Steel Mill Cyber Attack- ICS Defense Use Case,” *SANS*, Bethesda, Maryland, 2014.
[42] A. A. C. a. T. S. Adamov, “An Analysis of LockerGoga Ransomware,” in *Proc. of 2019 IEEE East-West Design & Test Symposium (EWDTS)*, 2019. Article (CrossRef Link)
[43] C. Cimpanu, “Norsk Hydro ransomware incident losses reach $40 million after one week,” ZDnet, 26 3 2019. [Online]. Available: https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/. [Accessed 13 May 2020].
[44] T. K. a. S. M. Shimon Prokupecz, “Former official: Iranians hacked into New York dam,” CNN, 22 December 2015. [Online]. Available: https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html. [Accessed 12 May 2020].
[45] K. O. D. G. a. J. S. David E. Whitehead, “Ukraine Cyber-Induced Power Outage: Analysis and practical mitigation strategies,” in *Proc. of 2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, 2017. Article (CrossRef Link)
[46] T. V. C. a. S. Z. Alladi, “Industrial Control Systems: Cyberattack trends and countermeasures,” *Jounrnal of Computer Communications*, vol. 155, pp. 1-8, 2020. Article (CrossRef Link)
[47] M. A. H. a. S. L. Touhiduzzaman, “An Distributed Cyberattack Diagnosis Scheme for Malicious Protection Operation based on IEC 61850,” in *Proc. of the Fifth Annual Industrial Control System Security (ICSS) Workshop*, pp. 21-29, 2019. Article (CrossRef Link)
[48] K. Z. Z. A. D. a. G.-J. A. Liao, “Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin,” in *Proc. of 2016 APWG Symposium on Electronic Crime Research (eCrime)*, 2016. Article (CrossRef Link)
[49] J. K. K. V. a. N. F. Jacqueline O’Leary, “Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware,” FireEye, 20 9 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html. [Accessed 13 May 2020].
[50] C. Osborne, “NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs,” ZDNet, 26 1 2018. [Online]. Available: https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/. [Accessed 12 May 2020].
[51] M. Kumar, “TSMC Chip Maker Blames WannaCry Malware for Production Halt,” The Hacker News, 7 8 2018. [Online]. Available: https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html. [Accessed 12 May 2020].
[52] "SamSam Ransomware,” 3 12 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/AA18-337A. [Accessed 12 5 2020].
[53] K. E. Hoffman, “True crime: SamSam ransomware I am,” SC Media, 1 2 2019. [Online]. Available: https://www.scmagazine.com/home/security-news/true-crime-samsam-ransomware-i-am/. [Accessed 13 May 2020].
[54] S. Kumar, “An emerging threat Fileless malware: a survey and research challenges,” *Cybersecurity*, Springer, vol. 3, pp. 1-12, 2020. Article (CrossRef Link)

[55] "EKANS Ransomware and ICS Operations," DRAGOS, 3 2 2020. [Online]. Available: https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/. [Accessed 13 May 2020].
[56] Christopher and S. Kelly, *Colonial Pipeline Ransomware Attack*, Houston: Reuters. Archived, 2021.
[57] S. N. T. S. K. D. Om Prakash Samantray, "A Theoretical Feature-wise Study of Malware Detection Techniques," *International Journal of Computer Sciences and Engineering*, 6(12), pp. 879-887, 2018.
[58] H. &. H. A. Hashemi, "Visual malware detection using local malicious pattern," *Journal of Computer Virology and Hacking Techniques*, 15(1), pp. 1-14, 2019. Article (CrossRef Link)
[59] Z. S. A. &. G. M. Salehi, "Using feature generation from API calls for malware detection," *Computer Fraud & Security*, vol. 2014, no. 9, pp. 9-18, 2014. Article (CrossRef Link)
[60] K. S. K. I. K. &. I. E. G. Han, "Malware classification methods using API sequence characteristics," in *Proc. of the International Conference on IT Convergence and Security 2011*, Springer, Dordrecht, pp. 613-626, 2012. Article (CrossRef Link)
[61] I. B. F. U.-P. X. &. B. P. G. Santos, "Opcode sequences as representation of executables for data-mining-based unknown malware detection," *Information Sciences*, vol. 231, pp. 64-82, 2013. Article (CrossRef Link)
[62] Y. F. W. H. W. &. A. J. Cheng, "A shellcode detection method based on full native api sequence and support vector machine," in *Proc. of IOP Conference Series: Materials Science and Engineering*, 2017.
[63] N. K. a. A. K. Bindal, "A complete dynamic malware analysis," *International Journal of Computer Applications*, 135.4, pp. 20-25, 2016.
[64] G. P. J. &. D. C. Liang, "A behavior-based malware variant classification technique," *International Journal of Information and Education Technology*, vol. 6(4), pp. 291-295, 2016. Article (CrossRef Link)
[65] A. &. A. O. Mohaisen, "Unveiling zeus: automated classification of malware samples," in in *Proc. of the 22nd International Conference on World Wide Web*, pp. 829-832, 2013. Article (CrossRef Link)
[66] A. A. O. &. M. M. Mohaisen, "Amal: High-fidelity, behavior-based automated malware analysis and classification," *computers & security*, vol. 52, pp. 251-266, 2015. Article (CrossRef Link)
[67] H. S. M. Y. B. &. A. M. A. Galal, "Behavior-based features model for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 12(2), pp. 59-67, 2016. Article (CrossRef Link)
[68] Y. K. E. &. K. H. K. Ki, "A novel approach to detect malware based on API call sequence analysis," *International Journal of Distributed Sensor Networks*, vol. 11(6), p. 659101, 2015. Article (CrossRef Link)
[69] C. I. H. H. W. C. C. H. &. T. Y. F. Fan, "Malware detection systems based on API log data mining," in *Proc. of IEEE 39th annual computer software and applications conference*, 2015. Article (CrossRef Link)
[70] M. S. K. S. a. H. R. Sewak, "Comparison of deep learning and the classical machine learning algorithm for the malware detection," in *Proc. of 2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2018. Article (CrossRef Link)
[71] A. D. T. F. V. C. A. A. T. H. &. S. M. Damodaran, "A comparison of static, dynamic, and hybrid analysis for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 13(1), pp. 1-12, 2017. Article (CrossRef Link)
[72] R. Tahir, "A study on malware and malware detection techniques," *International Journal of Education and Management Engineering*, vol. 8, no. 2, pp. 20-30, 2018. Article (CrossRef Link)
[73] Ö. A. Aslan &. S. R. Aslan, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249-6271, 2020. Article (CrossRef Link)

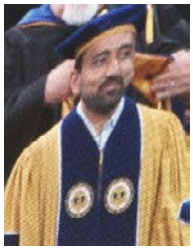
[74] I. S. S. a. N. K. Baptista, "A novel malware detection system based on machine learning and binary visualization," in *Proc. of 2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019. Article (CrossRef Link)
[75] Q. G. W. Z. K. O. A. G. X. X. L. X. &. G. C. L. Wang, "Adversary resistant deep neural networks with an application to malware detection," in *Proc. of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1145-1153, 2017. Article (CrossRef Link)
[76] S. K. S. K. S. &. K. B. B. Yoo, "AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification," *Information Sciences*, vol. 546, pp. 420-435, 2021. Article (CrossRef Link)
[77] G. H. B. L. P. J. M. S. Z. Y. F. &. Z. L. LIANG, *A Malware Detection Method Based on Hybrid Learning*, ACTA ELECTONICA SINICA, 2021.
[78] L. Phifer, "Search Networking," TechTarget, [Online]. Available: https://searchnetworking.techtarget.com/tip/Securing-the-new-network-architecture-Security-for-distributed-dynamic-networks. [Accessed 5 May 2020].
[79] S. S. S. D. &. V. V. Chakkaravarthy, "A survey on malware analysis and mitigation techniques," *Computer Science Review*, vol. 32, pp. 1-23, 2019. Article (CrossRef Link)
[80] "What is SIEM," Forcepoint, [Online]. Available: https://www.forcepoint.com/cyber-edu/siem. [Accessed 5 May 2020].
[81] A. Chowdhury, "Recent cyber security attacks and their mitigation approaches–an overview," in *Proc. of International conference on applications and techniques in information security*, Singapore, pp. 54-65, 2016. Article (CrossRef Link)
[82] O. Nelson, "Cybersecurity Laws – A Complete Overview," cyberexperts, [Online]. Available: https://cyberexperts.com/cybersecurity-laws/. [Accessed 07 05 2020].
[83] K. Hardy, "Cyber-attacks against infrastructure in domestic anti-terror laws," *Computer Law & Security Review*, vol. 27, no. 2, 2011.
[84] U. K. Government, "The national security strategy - a strong Britain in an age of uncertainty," Cabinet Office and National security and intelligence, 18 10 2010. [Online]. Available: https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty. [Accessed 8 5 2020].
[85] "Justice Laws Website," Canadian Government, [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/c-46/. [Accessed 8 5 2020].
[86] M. Nesbitt and D. Hagg, "Terrorism Prosecutions in Canada: Elucidating the Elements of the Offences," *Alberta Law Review, Forthcoming*, 2019.
[87] "Terrorism Suppression Act 2002," New Zealand Government , [Online]. Available: http://www.legislation.govt.nz/act/public/2002/0034/55.0/DLM151491.html. [Accessed 8 5 2020].
[88] "18 U.S. Code § 2332b.Acts of terrorism transcending national boundaries," Legal Information Institute, [Online]. Available: https://www.law.cornell.edu/uscode/text/18/2332b. [Accessed 8 5 2020].
[89] "18 U.S. Code § 2332b.Acts of terrorism transcending national boundaries," Legal Information Institute, [Online]. Available: https://www.law.cornell.edu/uscode/text/18/2332b. [Accessed 8 5 2020].
[90] R. Khan, "Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried," DAWN News, 11 8 2016. [Online]. Available: https://www.dawn.com/news/1276662. [Accessed 9 6 2020].
[91] "National Assembly of Pakistan," 2016. [Online]. Available: http://www.na.gov.pk/uploads/documents/1470910659_707.pdf. [Accessed 9 6 2020].
[92] "Office of Counter-Terrorism," U.N., [Online]. Available: https://www.un.org/counterterrorism/cybersecurity. [Accessed 8 5 2020].
[93] "Cyber defence," North Atlantic Treaty Organization (NATO), 17 3 2020. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_78170.htm?. [Accessed 8 5 2020].

[94] "Top 10 Malware January 2019," Center for Internet Security, 2019. [Online]. Available: https://www.cisecurity.org/blog/top-10-malware-january-2019/. [Accessed 11 5 2020].
[95] Pandey and A. Kumar, "Trends in Malware Attacks: Identification and Mitigation Strategies," *Critical Concepts, Standards, and Techniques in Cyber Forensics*, pp. 47-60, 2020. Article (CrossRef Link)
[96] L. Ablon and A. Bogart, "Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits," *Rand Corporation*, 2017.
[97] S. Morgan, "Cybercrime Magazine," 7 12 2018. [Online]. Available: https://cybersecurityventures.com/annual-cybercrime-report-2019/. [Accessed 27 10 2020].
[98] C. M. L. a. P. L. Xu, "Bifurcation of a Fractional-Order Delayed Malware Propagation Model in Social Networks," *Discrete Dynamics in Nature and Society*, 2019. Article (CrossRef Link)
[99] P. Wood, "Internet Security Threat Report," *Symantec*, 2016.
[100] B. Alberti, "(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide," *(ISC)²*, 2019.
[101] M. MANGAT, "What is Cyber Security? Challenges and Threats Organizations Face," PhoenixNAP, [Online]. Available: https://phoenixnap.com/blog/what-is-cyber-security. [Accessed 9 6 2019].
[102] M. N. a. D. Hagg, "Terrorism Prosecutions in Canada: Elucidating the Elements of the Offences," *Alberta Law Review, Forthcoming*, 2019.
[103] Denning and E. Dorothy, "Stuxnet: What has changed?," *Future Internet*, vol. 4, no. 3, pp. 672-687, 2012. Article (CrossRef Link)
[104] A. D. T. F. V. C. A. A. T. H. &. S. M. Damodaran, "A comparison of static, dynamic, and hybrid analysis for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 13(1), pp. 1-12, 2017. Article (CrossRef Link)
[105] T. T. W. a. M. S. Vaidya, "Whisper: A unilateral defense against voip traffic re-identification attacks," in *Proc. of the 35th Annual Computer Security Applications Conference*, pp. 286-296, 2019. Article (CrossRef Link)
[106] "malware," Malwarebytes, [Online]. Available: https://www.malwarebytes.com/malware/. [Accessed 18 5 2020].
[107] G. Wangen, "The role of malware in reported cyber espionage: a review of the impact and mechanism," *Information*, vol. 6, no. 2, pp. 183-211, 2015. Article (CrossRef Link)
[108] NortonLifeLock employee, "What is a computer virus?," Norton, [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html. [Accessed 6 6 2020].
[109] "What's the Difference between a Virus and a Worm?," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms. [Accessed 6 6 2020].
[110] J. Regan, "What is a Trojan Horse? Is it Malware or Virus?," AVG, 10 12 2019. [Online]. Available: https://www.avg.com/en/signal/what-is-a-trojan. [Accessed 6 6 2020].
[111] "Ransomware," The Cybersecurity and Infrastructure Security Agency (CISA), [Online]. Available: https://www.us-cert.gov/Ransomware#:~:text=Ransomware%20is%20a%20type%20of,an%20individual%20or%20an%20organization.. [Accessed 6 6 2020].
[112] "Backdoor," Malwarebytes, [Online]. Available: https://www.malwarebytes.com/backdoor/. [Accessed 6 6 2020].
[113] K. Ishaq, N.A.M. Zin, F. Rosdi, M. Jehanghir, S. Ishaq, & A. Abid, "Mobile-assisted and gamification-based language learning: A systematic literature review," *PeerJ Computer Science*, vol. 7(e496), 1–57, 2021. Article (CrossRef Link)

Annas Malik is a researcher, whose areas of interest are chaos and cryptography, and computer forensics. His skill are in the field of Information Security, IT Security, Computer Security, Cyber Security Cryptography, Internet Security, Information Systems Security, Wireless Security, Computer Security and IT Forensics.

ADNAN ABID (Member, IEEE) was born in Gujranwala, Pakistan, in 1979. He received the B.S. degree from the National University of Computer and Emerging Science, Pakistan, in 2001, the M.S. degree in information technology from the National University of Science and Technology, Pakistan, in 2007, and the Ph.D. degree in computer science from the Politecnico Di Milano, Italy, in 2012. He spent one year in EPFL, Switzerland, to complete his M.S. thesis. He is currently an Associate Professor with the Department of Computer Science, University of Management and Technology, Pakistan. He has almost 70 publications in different international journals and conferences. He has served as a reviewer in many international conferences and journals. His research interests include computer science education, information retrieval, and data management. He is a member of the IEEE Education Society and the IEEE Education Society. He is also an Associate Editor of IEEE ACCESS journal.

Muhammad Shoaib Farooq is working as Professor of Computer Science at University of Management and Technology, Lahore. He was the affiliate member of George Mason University, USA. He possesses more than 26 years of teaching experience in the field of Computer Science. He has published many peer-reviewed international journal and conference papers. His research interests include Theory of Programming Languages, Big Data, IOT, Internet of Vehicles, Machine Learning, Blockchain and Education.



Irfan Abid has more than 21 years of professional experience in academia, industry, and research institutes. He is working as Project Director at Frontier Works Organization (FWO), also working as Adjunct faculty member in School of Civil and Environmental Engineering at National University of Science and Technology (NUST), Pakistan, Risalpur Campus.

NAEEM A. NAWAZ received the B.Sc. degree from the University of Punjab, Pakistan, in 1997, the M.Sc. degree in computer sciences from Hamdard University, Pakistan, in 2000, the M.S. degree in computer engineering from Mid Sweden University, Sweden, in 2008, and the Ph.D. degree from International Islamic University Malaysia, in 2018. He received different diploma (DCS) and certifications. He is currently a Lecturer with the Department of Computer Science, Umm Al-Qura University, Makkah Al-Mukarmah. He has published research articles in renowned journals and conferences. He is also serving as a reviewer for many journals, conferences, and books. His teaching and research interests include WSN, the IoT, crowd management, computer networks, and programing language.

KASHIF ISHAQ is born in Sheikhupura, Pakistan. He has completed his Ph.D. from Universiti Kebangsaan Malaysia in 2022. He received his Master's in Information Technology from Department of Computer Science, University of Management and Technology, Pakistan. He has published many peer-reviewed journal and conference papers. His research interests include Serious Games, MALL, Usability, and E-learning technology.