Energy Reports 7 (2021) 8176–8186

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Research paper

A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments

Yuchong Li [a,b], Qinghui Liu [c,*]

[a] College of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, Henan, China
[b] Bank of Zhengzhou, Zhengzhou 450018, Henan, China
[c] Network Center, Zaozhuang University, Zaozhuang 277160, Shandong, China

ARTICLE INFO

Article history:
Received 9 July 2021
Received in revised form 9 August 2021
Accepted 18 August 2021
Available online 3 September 2021

Keywords:
Information technology
Cyber-attacks
Cyber security
Emerging trends
Key management

ABSTRACT

At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace. Recently, many private companies and government organizations around the world are facing the problem of cyber-attacks and the danger of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are: PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors. To this end, various organizations use various solutions to prevent damage caused by cyber-attacks. Cyber security follows real-time information on the latest IT data. So far, various methods had been proposed by researchers around the world to prevent cyber-attacks or reduce the damage caused by them. Some of the methods are in the operational phase and others are in the study phase. The aim of this study is to survey and comprehensively review the standard advances presented in the field of cyber security and to investigate the challenges, weaknesses and strengths of the proposed methods. Different types of new descendant attacks are considered in details. Standard security frameworks are discussed with the history and early-generation cyber-security methods. In addition, emerging trends and recent developments of cyber security and security threats and challenges are presented. It is expected that the comprehensive review study presented for IT and cyber security researchers will be useful.

1. Introduction

For more than two decades, the Internet has played a significant role in global communication and has become increasingly integrated into the lives of people around the world. Innovations and low cost in this area have significantly increased the availability, use and performance of the Internet, thus that today the Internet has about 3 billion users worldwide (Tan et al., 2021). The Internet has created a vast global network that has generated billions of dollars annually for the global economy (Judge et al., 2021). At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace (Aghajani and Ghadimi, 2018). Vital and sensitive infrastructures and systems either form a part of cyberspace themselves or are controlled, managed and exploited through this space, and most of the vital and sensitive information is transferred to this space or basically It has been formed in this space (Akhavan-Hejazi and Mohsenian-Rad, 2018). Most media activities are transferred to this space, most financial exchanges are done through this space and a significant proportion of citizens' time and activities are spent interacting in this space (Priyadarshini et al., 2021). The share of income from cyberspace businesses in the Gross domestic product (GDP) of countries has increased significantly and among the indicators set to measure the extent of development, cyberspace indicators have a major share. A significant part of the material and spiritual capital of countries is spent on this space and a significant part of the material income and spiritual achievements of citizens are obtained or have a major impact on this space (Amir and Givargis, 2020). In other words, different aspects of citizens 'lives are literally intertwined with this space, and any instability, insecurity and challenges in this space will directly affect different aspects of citizens' lives (Li et al., 2020). Nevertheless, cyberspace

* Corresponding author.
E-mail address: lqh@uzz.edu.cn (Q. Liu).

https://doi.org/10.1016/j.egyr.2021.08.126

has posed new security challenges to governments. The low cost of entry, anonymity, uncertainty of the threatening geographical area, dramatic impact and lack of public transparency in cyberspace, have led to strong and weak actors including governments, organized and terrorist groups and even individuals in this space, and threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage (Niraja and Srinivasa Rao, 2021). This distinguishes cyber threats from traditional national security threats, which are largely transparent in nature and whose actors are governments and nations that can be identified in a specific geographical area, and it has caused national security in its traditional sense to be challenged and inefficient in this space (Sarker, 2021). For more than a decade, analysts have pondered the possible consequences of cyber-attacks (Shin et al., 2021). There are various scenarios for severe and sometimes widespread physical or economic damage, including the function of a virus that attacks the financial documents of an economic system or disrupts a country's stock market, or by sending an incorrect message, it will cause the country's power plant to stop and fail, or even by disrupting the air traffic control system, it will cause air accidents (Snehi and Bhandari, 2021; Ahmed Jamal et al., 2021). Therefore, until governments come up with a clear definition of a cyber-attack that is accepted and favored by the international community, it will certainly be very difficult for experts to address the complex and diverse dimensions and aspects of the issue and provide legal advice and analysis (Cao et al., 2021). Therefore, the question that arises is what is a cyber-attack, what are its characteristics and whether basically any attack that takes place in cyberspace can be considered a kind of attack in its traditional and classic sense or not (Gupta Bhol et al., 2021). The existence of a comprehensive definition of a cyber-attack will undoubtedly have a direct impact on the legal environment to continue and identify the consequences of this attack type (Furnell et al., 2020). There is no doubt that the lack of a clear and comprehensive definition not only obscures the leading legal path, but also leads to diversity in interpretation and practice, and ultimately to the achievement of sometimes contradictory legal conclusions (Alhayani et al., 2021). Therefore, the importance and necessity of having an acceptable definition, at least for the beginning of the topic and its explanation, adaptation and analysis is very important, and a detailed study is necessary. In the present study, first the nature of cyber-attack is explained and then the segregation and cyber-attack classification are examined and then the existing definitions are investigated and analyzed from the point of view of international experts and organizations. Finally the conclusion of the paper is presented.

2. Fundamental concepts

Cyber-attacks fall into a broader context than what is traditionally called information operations. Information operations integrated use of the main capabilities of electronic warfare, psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities and to penetration, stop, destroy or hijack human decisions and It is one of the decision-making processes of national institutions (Hart et al., 2020). Fig. 1 describes the anatomy of a cyber-attack. From the USNM Strategy for cyberspace operations, computer network operation is composed of the attack, defense, and utilization enabling (Ma et al., 2021). The latter is different from network attacks and network defense, because this type of operation focuses more on collection and analyzing information than interrupting networks, and may itself be the prelude to an attack (Alghamdie, 2021). These operations can be carried out of disseminating information and propaganda purposes (Thomson, 2015). Computer network exploitation enabling operations can also be carried out with the aim of stealing important computers data. In such a context, Trap Sniffers and Doors are beneficial tools for cyber espial (Liu et al., 2021). Trap Doors permit an external user to accessibility software at any time without the knowledge of the computer user. Sniffers are a tool to steal usernames and passwords (Karbasi and Farhadi, 2021). Table 1 describes the basic definitions and concepts of cyberspace. The consequences of cyber warfare can include the following (Khan et al., 2020; Furnell and Shah, 2020; Mehrpooya et al., 2021):

- The overthrow of the system of government or the catastrophic threat to national security; a
- Simultaneous initiation of physical warfare or groundwork and facilitate the start of physical warfare in the near future;
- Catastrophic destruction or damage to the country's image at the international level;
- Catastrophic destruction or damage to the political and economic relations of the country;
- Extensive human casualties or danger to public health and safety;
- Internal chaos;
- Widespread disruption in the administration of the country;
- Destroying public confidence or religious, national and ethnic beliefs;
- Severe damage to the national economy;
- Extensive destruction or disruption of the performance of national cyber assets.

In addition, five scenarios can be considered for cyber warfare: (1) Government-sponsored cyber espionage to gather information to plan future cyber-attacks, (2) a cyber-attack aimed at laying the groundwork for any unrest and popular uprising, (3) Cyber-attack aimed at disabling equipment and facilitating physical aggression, (4) Cyber-attack as a complement to physical aggression, and (5) Cyber-attack with the aim of widespread destruction or disruption as the ultimate goal (cyber warfare) (Alibasic et al., 2016). One type of cyber-attack is encryption. Encryption is a reversible method of encrypting data that requires a key to decrypt. Encryption can be used in conjunction with encryption, which provides another level of confidentiality (Sun et al., 2018). Encryption is the implementation and study of data encryption and decryption thus that it can only be decrypted by specific individuals. The system for encrypting and decrypting data is the encryption system (ji et al., 2021). Encryption is a powerful tool for protecting important and private information when exposed to threats from strangers and criminals, as well as for hiding unauthorized activities from law enforcement. As computers grow faster and failure methods become more secure, cryptographic algorithms require sustained consolidation to prevent insecurity (Zou et al., 2020). Note that, in general, a distinction can be made between cyber-crime, cyber-warfare, and cyber-attacks. Fig. 2 and Table 2 describes the distinction between cyber-crime, cyber-warfare, and cyber-attack that defines the conceptual distinction between them.

2.1. Definition of cyber-attack from the specialists' point of view

Various definitions of cyber-attack had been made by specialists in both legal and technical fields, the most important of which are as follows:
(1) Richard Clark: Cyber-attacks are actions taken by countries to infiltrate the computers or computer networks of a country or other countries to cause damage or disruption (Motsch et al., 2020). In the analysis and critique of this definition, it can be said that the three elements, namely the perpetrator of the attack, the purpose and intention of the attack, have been used as criteria,

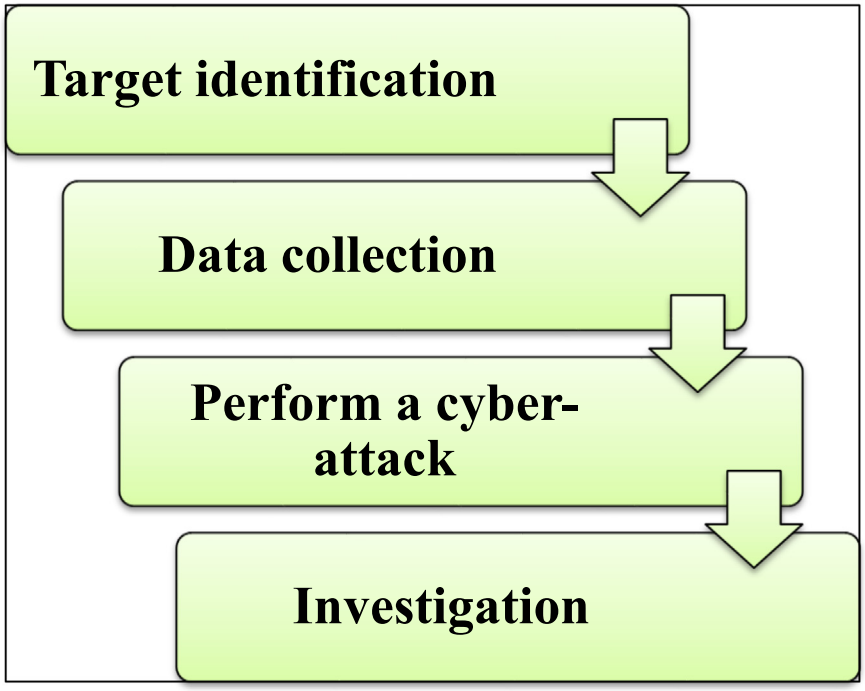

Fig. 1. Anatomy of a cyber-attack.

Table 1
Basic definitions and concepts of cyberspace (Ahmed Jamal et al., 2021; Alghamdie, 2021; Bullock et al., 2021; Ashraf et al., 2021).

Title	Definition
Cyber space	Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information.
Cyber capital	A vital (or sensitive) infrastructure of a country, a vital cyber system, a key information, or individuals belonging to a country.
Cyber vulnerability	Vulnerability refers to a weakness within an asset, security procedures or internal controls, or the implementation of that national cyber asset that can be exploited or activated by internal or external threats to conduct cyber warfare.
Cyber threats	Any event with the ability to strike a blow to missions, tasks, images, national cyber assets or personnel through an information system, through unauthorized access, destruction, disclosure, alteration of information and/or obstruction of (disruptive) service delivery.
Cyber threat level	Cyber threats are able to affect national cyber assets at the transnational, national, institutional, provincial, critical, and critical levels of infrastructure.
Probability of cyber threats	Very high (imminent), high (probable), low (unlikely) and very low (very unlikely)
Intensity of cyber threat	Very high (disaster), high (crisis), moderate (major security incident), low (security incident) and very low (security incident)
Cyber attack	Any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the said national cyber asset is called cyber-attack. Intentional use of a cyber-weapon against an information system in a manner that causes a cyber-incident is also considered cyber-attack.
Cyber weapon	A cyber weapon is a system designed and manufactured to damage the structure or operation of other cyber systems. These systems include bot networks, logic bombs, cyber vulnerability exploitation software, malware, and traffic generation systems to prevent service attacks and distributed service.
Cyber warfare	Cyber warfare is the highest level and most complex type of cyber-attack (cyber operation) that is carried out against the national cyber interests of countries and will have the most severe consequences.
Cyber warfare origin	The cyber force of the aggressor country or groups organized under the aggressor states, cyber weapons controlled or abandoned by these forces
Cyber defense	Utilization of all unarmed cyber and non-cyber facilities of a country, to create deterrence, prevention, prevention, timely detection, effective and deterrent response to any cyber attack
Cyber biome	Cyber biome refers to the formation of a native and dynamic cyber environment that is supportive for a country in various fields.
Virus	A virus is a self-replicating program that spreads to other documents and other programs by duplicating itself, and may cause programs to malfunction. A computer virus acts like a biological virus that spreads through its reproduction to cells in the host body. Some of the popular viruses are: NIMDA, SLAMMER, and SASSER.
Hacker	A person who enters a system without permission or who increases his/her access to information to browse, copy, replace, delete or destroy it.

without considering the forms of disruption (Cao et al., 2019). In addition, in terms of the perpetrator of the attack, only countries are mentioned in general, however, if an attack in the context and geographical area under the control and jurisdiction of a country (cyberspace of networks under the control of countries) by individuals and If non-governmental and private groups act against a third country, it will basically fall outside the scope of the mentioned definition and will not include them, and thus there should be a gap in the legal coverage of such attacks. Given this situation, it can be said that the mentioned definition is largely incomplete and does not include a significant part of the attacks carried out by private and non-governmental groups, and leads to a vacuum (Zhang, 2017).

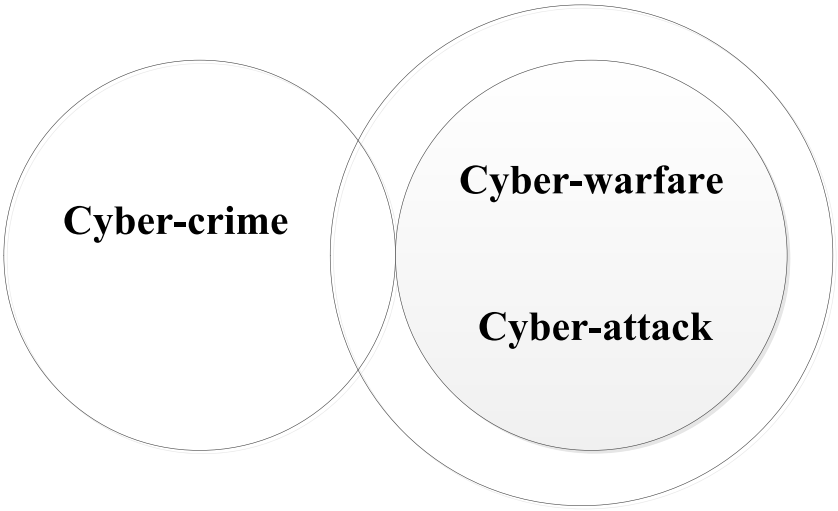

Fig. 2. Distinction between cyber-crime, cyber-warfare, and cyber-attack.

Table 2
Distinction between cyber-crime, cyber-attacks, and cyber-warfare (Zhang, 2017; Dash et al., 2021).

Type of cyber action	Nature and characteristics
Cyber-crime	Cyber actions taken only by non-governmental attackers.
Cyber-crime	The cyber action is carried out by a computer system and is merely in violation of criminal law.
Cyber-attack and cyber-warfare	The purpose of a cyber-attack is to destroy and disrupt the operation of a computer network.
Cyber-attack and cyber-warfare	The attack must have political or security purposes.
cyber-warfare	The effects of a cyber-attack are the same as an armed attack or the cyber act took place in the context of an armed attack.

(2) Michael Hayden: Any intentional attempt to disrupt or destroy another country's computer networks (Robinson et al., 2015). Obviously, this definition is also very general and does not make any distinction between cybercrime, cyber-attack and cyber warfare, and the line between their detection is in an aura of ambiguity, the lack of such a distinction will certainly affect commentators and policymakers in their actions. The broad framework of the rules of war leaves free cyberspace, which can certainly have dangerous and adverse consequences for the spread of war and belligerence of countries (Edgar and Manz, 2017). Hence, the generality of the above definition is in fact its main weakness, which leads to lack of luck. Compared to the first definition, which limited the perpetrators of the attack to government aggressors, this definition is general that it is easy to interpret and, as mentioned, can be dangerous and have negative effects and cause confusion in relations between countries and ultimately a threat to peace at the level of the international community (Nicholson et al., 2012).
(3) Martin Libicki: Digital attacks on computer systems cause the attacked computer systems to appear normal, but in fact produce and issue untrue responses (Quigley et al., 2015). This approach to defining cyber-attacks in fact excludes a wide range of potential threats to the national security of a country whose cyber infrastructure has been targeted but has not reached the level and threshold of meaningful attacks. The fact of the matter is that these threats can cause damage to the computer systems and networks of the target country. Therefore, any definition of a cyber-attack that excludes the above will necessarily be an incomplete definition that does not have the necessary comprehensiveness (Damon et al., 2014; Shamel et al., 2016).
(4) Tallinn Manual Group: A cyber-attack is an offensive or defensive cyber operation that can cause injury or death to persons or cause damage or destruction of property. The confusing point of this definition is in fact the results and effects obtained. From the point of view of the providers of this definition, a cyber-attack will be of the nature of an attack if it leads to the results stated in the definition (i.e. infliction of personal and financial injuries) (Bullock et al., 2021). Therefore, the main basis of the definition of this group is the result-oriented nature of cyber-attacks, not the attacks themselves; In this way, if this type of attack leaves the effects and consequences of violence, objective and tangible, it will be described as an attack, and it is at this stage that the rules of international law in related areas and fields (the right to appeal to coercion, the law of war and the law of international responsibility will be enforceable (Chen et al., 2021).

3. Cyber space threats

Naturally, it is the scope of the global cyberspace, which creates overlapping and overlapping areas of control for national actors with different legal and cultural approaches and different strategic interests (Iqbal and Anwar, 2020). Countries around the world have become sufficiently dependent on cyberspace for communications and control of the physical world; in a way that it is definitely impossible to separate from it. Therefore, the security tasks and functions of each country are increasingly affected by cyberspace (Zhao et al., 2020). Due to the global production of software and hardware products, it is impossible to provide guarantees in the product supply chain process. The scalability of the cyber domain makes it qualitatively different. A bomb has a limited physical range in the most extreme conditions; however cyber-threats have a very wide range of effects, therefore we have a mechanism that can control real-world operations. Like many other areas of knowledge, operations within the cyberspace are controlled by a relatively small number of individuals. Users do not have the ability to modify or control the software and hardware they use. It is no secret that a small number of people can effectively control or manage cyber warfare (Zhang et al., 2021). Despite the required concentration and specialized knowledge, the distributed nature of the cyber domain prevents a person or group of individuals from seeking complete control.

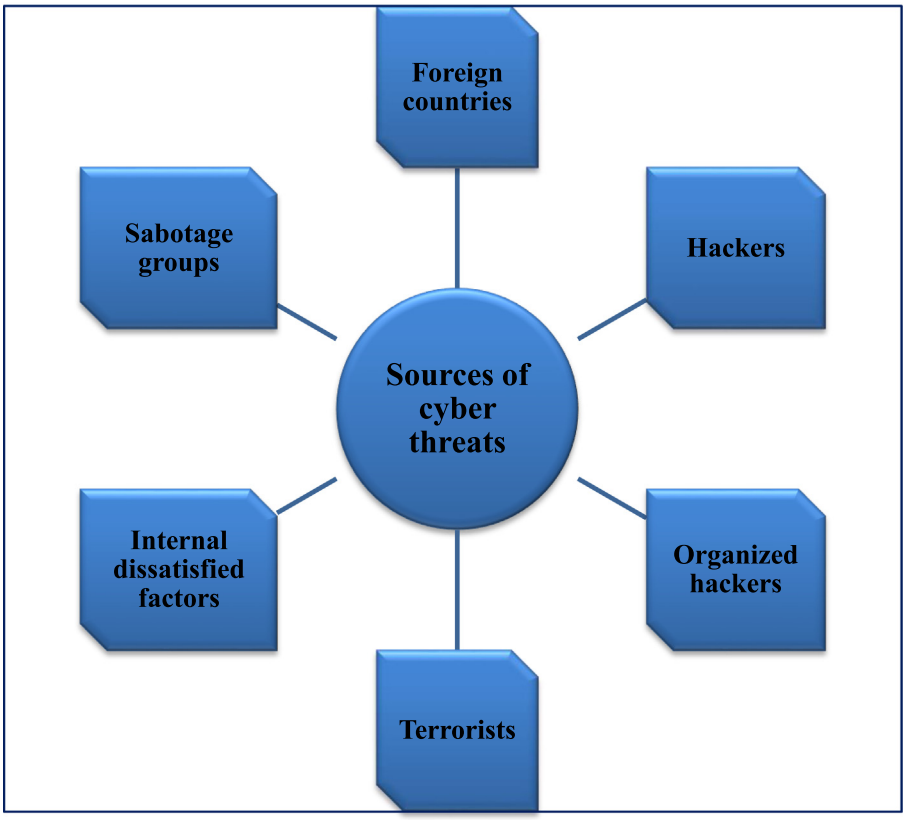

Fig. 3. Sources of cyber threats.

Changes in the field of cyber occur rapidly and are based on the constant development of computing and communication technologies. Cyber cohesion increases this acceleration. Each change creates a new era of vulnerability and response. Cyberspace is far from static and almost dynamic throughout (Varga et al., 2021). The distribution of cyber assets is widespread in all types of organizations, from closed and government-controlled systems to systems owned and managed by the private sector of society, each with different resources and facilities and different capacities and concerns are present on the scene (Zhao et al., 2021). The nature of cyberspace is such that, at present, there is no technical ability to assign activities to individuals or groups or organizations, with a high degree of confidence. The basic threats in cyberspace are: foreign threats, internal threats, threats in the supply chain of goods and services, and threats due to insufficient operational capability of local forces (Al-Ghamdi, 2021). Foreign intelligence services use cyber tools to carry out some of their intelligence gathering and espionage activities. Numerous such cases have been reported worldwide for the misuse and destruction of countries' information infrastructures, comprising the computer systems, Internet information networks, and processors and controllers embedded in vital industries. Another source of attacks is groups of people who attack cyber systems to make money, and the attacks of these groups are increasing (Beechey et al., 2021). In addition, other groups (hackers) sometimes enter the network to express themselves. In the current situation, it is possible to infiltrate networks with a minimum of knowledge and skills, by downloading the necessary programs and protocols from the Internet and using them against other sites. Meanwhile, another group (called Hacktivism) with politically motives attacks popular web pages or e-mail hosts. These groups usually impose increased loads on e-mail hosts, and by infiltrating the web sites, they announce their political messages (Solomon, 2017). On the other hand, internal dissatisfied agents operating within the organization are the main source of cybercrime, and these agents do not need to have significant knowledge of cyber-attacks; because their target system awareness mostly allows unlimited access to hit the system or steal the organization's information. Terrorists are another source of threat that seeks to destroy, disabling, or maliciously exploit vital infrastructure to menace national security, inflict heavy losses, weaken the country's economy, and undermine public mentality and trust (Saxena and Gayathri, 2021). Fig. 3 shows the sources of cyber threats.

The most important cyber-attacks methods are Denial of service, logical bomb, Abuse tools, Sniffer, Trojan horse, Virus, Worm, Send spam, and Botnet. Fig. 4 illustrates the important cyber-attacks types. In the Denial of service method, the authorized users' access to the system and vice versa is lost. In fact, the attacker from one point starts immersing the target computers in various messages and blocking the legal flow of data. This prevents any system from using the Internet or communicating with other systems (Topping et al., 2021). In another method, called widespread Denial of services, instead of launching an attack from a single source, they attack from a large number of distributed systems simultaneously. This is often done by using worms and multiplying them on multiple computers to attack the target. Abuse tools are available to the public that can detect and enter vulnerabilities in networks with different skill levels. A logic bomb is another type of attack in which a programmer enters code into a program in which, in the event of a specific event, the program automatically performs a destructive activity (Li et al., 2021; Marefati et al., 2018). Sniffer is also a program that eavesdrops on routed information and looks for specific information such as passwords by examining each packet in the data stream (Patel et al., 2021). Trojan horse hides dangerous code and commonly looks like a helpful program that the user

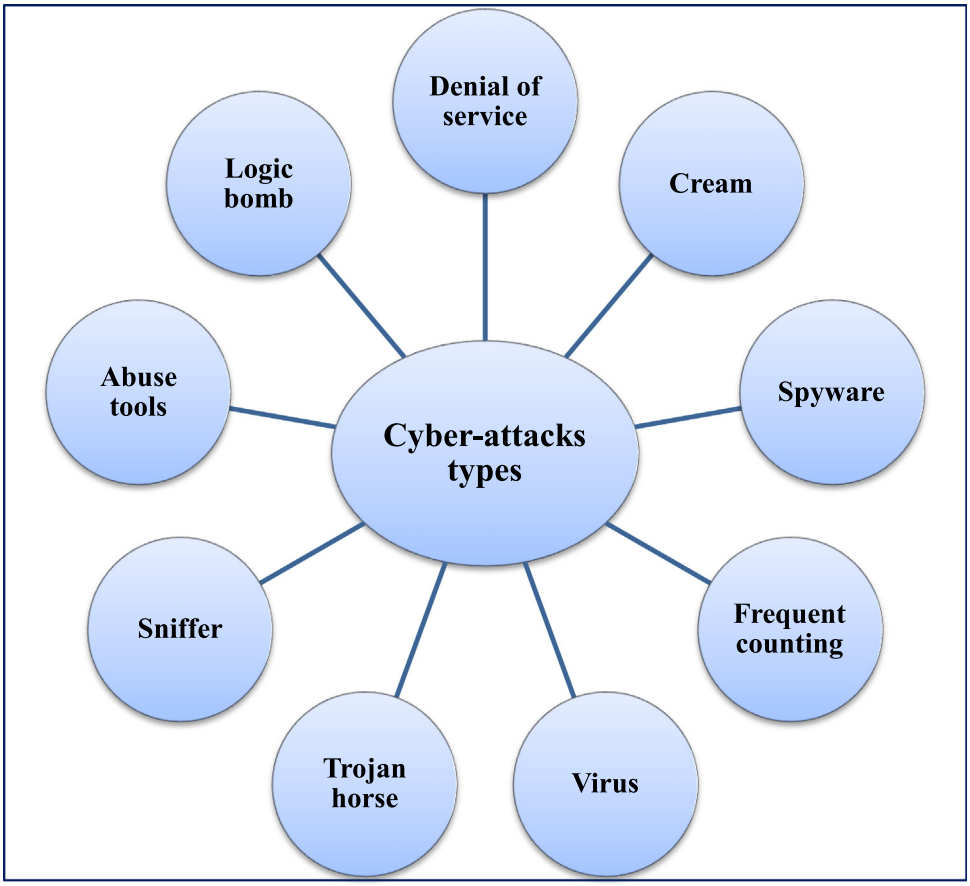

Fig. 4. Main cyber-attacks types.

is willing to run (Al Shaer et al., 2020). In addition, a virus befouls system files, which are commonly practicable programs, by inserting a copy of it into those files. By loading infected files into memory, these versions run and allow the virus to infect other files. Unlike worms, viruses require human intervention to spread. On the other hand, the worm is an autonomous system program that regenerates itself by copying from one computer to another in the network (Aziz and Amtul, 2019). Finally, Botnet is a network of infected remote control systems, which is used to distribute malware, coordinate attacks, and spam and steal messages. Botnets are usually secretly installed on the target computer, allowing the unauthorized user to remotely control the target system to achieve their malicious goals. Botnets are also referred to as electronic soldiers (Kharlamova et al., 2021).

Qiu et al. (2021) analyzed the impact and threat of cyber security in WAMS-based FFR (Fractional flow reserve) control with novel scale CNN for processing the spoofing data from two scales. They also investigated the time–frequency based cyber-security defense framework for FFR system. The result showed higher accuracy and robustness with actual synchrophasor data. Lee et al. (2021) developed a method for unified cyber-attack reply process according to a knowledge-based hidden Makrove modeling. They also examined a security state approximation method by updated HMMs. The validity of the developed method has been demonstrated via conducting a case. Zhang and Malacaria (2021) provided a cyber-security decision support system to select an optimal security portfolio to counteract multistage cyber-attacks. That system had both online and preventive optimizations supported by a LM to detect ongoing attacks. They found that the online was a Bayesian STACKELBERG game for choose the efficient solutions. Kim et al. (2020) examined the cyber-attack possibility variables for NPPs. In addition, the quantifying of the comparative significance of NPP possibility variables using AHP and FA was provided. They found that the recognition of Korean cyber security method had superior preference to be performed. Tosun (2021) showed that the cyber-attacks demonstrate sudden negative shocks to firms' popularities. In addition, financial markets respond to corporate security breaches as addition comeback decrement. Also, trading rate increased due to selling pressure and liquidity enhances. In long term, R&D and dividends drop while target firms keep compensating the CEOs.

4. Cyber-security

Cyber security is an important issue in the infrastructure of every company and organization. In short, a company or organization based on cyber security can achieve high status and countless successes, because this success is the result of the company's capability to protect private and customer data against a competitor. Organizations and competitors of customers and individuals are abusive. A company or organization must first and foremost provide this security in the best way to establish and develop itself (Rodríguez-deArriba et al., 2021). Cyber-security includes practical measures to protect information, networks and data against internal or external threats. Cyber-security professionals protect networks, servers, intranets, and computer systems. Cyber-security ensures that only authorized individuals have access to that information (Ahmed Jamal et al., 2021). For better protection, it is necessary to know the types of cyber security. Fig. 5 demonstrates the different types of cyber security. Network Security: Network security protects the computer network from disruptors, which can be malware or hacking. Network security is a set of solutions that enable organizations to

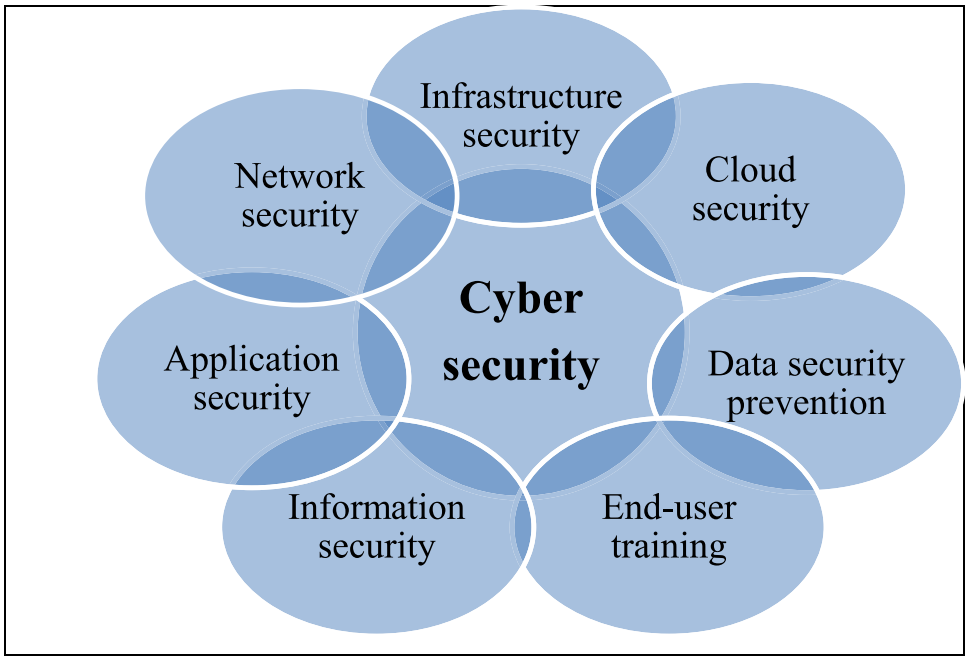

Fig. 5. Security triangle (CIA).

Fig. 6. Different types of cyber security.

keep computer networks out of the reach of hackers, organized attackers, and malware (Zhang, 2021).

Application Security: Using hardware and software (such as anti-virus programs, encryption, and firewalls) protects the system against external threats that may interfere with application development (Alkatheiri et al., 2021).

Information Security: Protects physical and digital data against unauthorized access, disclosure, misuse, unauthorized changes, and deletion (Ogbanufe, 2021).

Operational Security: Includes processes and decisions made to control and protect data. For example, user permissions when accessing the network or processes that specify when and where information may be stored or shared (Ogbanufe, 2021).

Cloud Security: Protects information in the cloud (based on the software), and monitors to remove the on-site attacks risks (Krishnasamy and Venkatachalam, 2021).

User training: Refers to unpredictable aspects of cyber-security, namely individuals. Anyone can accidentally get a virus

into the security system. Teaching the user to remove suspicious attachments in the email, not connecting to anonymous USBs, and other critical issues should be part of any company's corporate security plan (Krishnasamy and Venkatachalam, 2021).

Cybercrime is any unauthorized activity involving a system, equipment or network. Two different types of cybercrime are: Crimes that use a system as a target, and the crimes that a system unknowingly plays a role in creating. Table 3 shows the methods commonly used by cybercriminals. The security of any organization begins with three principles: confidentiality, integrity, and availability. These three principles are referred to as the security triangle, or CIA, which has served as the standard for systems security since the first computer systems (see Fig. 6) (Palmieri et al., 2021). The principle of confidentiality states that only authorized sources can access sensitive information and functions. Example: Military secrets (Confidentiality). The principles of integrity claim that only authorized individuals and resources can modify, add or remove sensitive information and functions. Example: A user enters incorrect data into a database (Integrity). Availability Principles claim that systems, functions, and data must be available on demand upon agreed parameters based on SLA service level (Availability) (Nguyen and Golman, 2021). The best cyber-security methods go outside the principles outlined mentioned. Any advanced hacker can bypass this easy defense. As a company grows, cyber-security becomes more difficult. Another limitation of cyber-security is treatment with the growing participates with the virtual and actual worlds of data exchange. An important challenge in cyber-security is the absence of eligible occupational to do the work. Many people are at the lower extremity of the vision of cyber-security with general skills. Cyberspace coverage is a broad topic. In the following article, we will review the main types of cyber security. A comprehensive strategy covers all of these aspects and does not overlook any of them (Alzubaidi, 2021). The world's major infrastructure acts as a combined cyber–physical. We get a lot of benefits from this wonderful structure. However, deploying an online system creates a new vulnerability to hacking and cyber-attacks. Organization decision-makers need to incorporate into their agenda how attacks may affect their performance. Several of the best new hackers see the security of web applications as the weakest point for attacking an organization. Application security starts with excellent encryption. Each strategy must be custom designed and implemented for each business differently. In this way, hacking information and infiltrating it is less done. Cyber-security is becoming increasingly complex. Organizations need to have a "security perspective" on how cyber-security works. As a result, you must always have high security to be one step ahead of hackers. Due to raising security ventures, investment in cyber-security systems and services is enhancing. The three companies active in this field are McAfee, Cisco, and Trend Micro (Chandra and Snowe, 2020).

4.1. Cyber-security policy

Cyber has increased the yield of the community and effectively distributed information over time. No problem what application or industry cyber is used in, increasing production has always been considered. Fast data transfer to cyberspace mostly declines the total system security. For technology professionals who improve production, security indicators are often in direct conflict with progress because prevention indicators reduce, prohibit, or delay user access, consume indicators that identify critical system resources, and respond to management attention (Katrakazas et al., 2020). The system changes to satisfactory and immediate system equipment. The conflict between the security situation and cyber performance demand along the cyber-security policy is important. The term "policy" is used in a variety of areas related to cyber-security, and refers to information distribution rules and regulations, private sector goals for data conservation, system operations strategies for technology control. However, in the works of this field, the term cyber-security policy is used for different purposes. Like the phrase "cyberspace", there is no fixed definition for cyber-security policy, but when this concept is used as an adjective in the field of policy, a common concept is intended (Tam et al., 2021).

The cyber-security policy is accepted by the regulatory framework and is officially applied lonely to the relevant areas of the regulator. Security policy components vary according to the policy spectrum (Cheng et al., 2020). The national cyber-security policy, for example, includes all citizens and perhaps foreign businessmen working in its field, but corporate cyber-security only applies to employees who are employed or have a legal contract and are expected to regulate their behavior toward the company. It is not even possible to expect resource providers who rely entirely on one customer to adhere to the customer security policy unless a formal contract is in place (Alghamdi, 2021). The content of the security policy is determined by the objectives of the relevant regulatory body. The national security objectives are very different from the corporate security objectives. The manner of interpretation and registration of the policy shall be determined by the implementing organizations and its approval shall be determined by the regulatory board and the components concerned. In government, the process by which goals become policies and the process by which policies are incorporated into law are different. But in companies, it is common to have a centralized security unit that is responsible for cyber-security policy and related standards and solutions. Standards and solutions of the security unit in companies become the guide of regulations. When security is a top priority for the organization, one can also see the cyber-security policy issued by the various internal units of the common components wing. These common components sometimes identify policy inconsistencies that occur as a result of trying to implement these issues simultaneously (Quigley et al., 2015).

The country's cyber policy is now a part of the policy of national security. Even if we consider a country's cyber-security policy in line with the State Department policy or the economic policy, these types of laws and policies are not as sovereign as the constitution. In fact, policy is created and published in reports and lectures through discussion of various points and discussions. Policies are created to guide and decide on laws and regulations. The policy itself is not related to rules and regulations. At best, laws, agreements, and rules represent a meaningful and wise policy. However, cyber-security enforcement orders, rules and regulations can be provided without creating a cyber-security policy (Sakhnini et al., 2021).

In the corporate environment, different departments are expected to follow the rules for fear of sanctions, as the sanctions will continue until the delinquent sector closes. For instance, human resource, civil, or costing policies are coded to the extent that any non-compliance with the notification rules closes the relevant section. Middle managers support processes such as hiring staff or filing expenses, and are expected to incorporate communicative policies into departmental activities and to create indicators at the departmental level to assess policy compliance. In the public sector, any type of organizational subdivision faces governance constraints (Baig et al., 2017). There are exceptions, in which different sections of the information classification are taken very seriously, but the company security policy provided by the CEO applies to the whole company, but the security policy issued by the CEO is limited to the domain. Technology staff is applicable. One of the recent changes in the organizational spectrum is the employment of a senior data security

Table 3
Methods commonly used by cybercriminals.

Method	Description	Ref.
Denial of Service	A hacker consumes all server resources, so access to the service is not possible for system users.	Alghamdie (2021)
Man-in-the-Middle	Where a hacker puts himself between the victim device and the router to eavesdrop on or change data packets.	Huang et al. (2020)
Malware	Malware is a way in which victims come in contact with worms or viruses and their devices become infected.	Edgar and Manz (2017)
Phishing	It is a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information.	Saxena and Gayathri (2021)

manager or a senior manager who is responsible for selecting different dimensions of the security situation of organizations. In addition, one of the undesirable differences between corporate cyber-security policy and human resource or legal policy is that it is left to middle managers. Cyber-security policy may require that "when the risk of disclosure of confidential information is high, information should not be provided without carefully examining the recipient's ability to maintain information security (Arend et al., 2020). This policy leaves the assessment of data risk to a manager who may want to reduce costs using outsourcing the flow of information to the office and using people outside the office to do information analysis. Maybe the same manager wants to ignore scrutiny to reduce costs. Such a situation is the result of miscalculations of information responsibilities toward a person who is not a security expert, or perhaps the culture of the organization in question bears the risk. In any case, the division of tasks is essential. These situations become more complex and difficult due to the fact that cyber-security measures have not matured as much as accounting or human resource indicators.

5. Conclusion

Cyberspace and related technologies are one of the most important sources of power in the third millennium. The characteristics of cyberspace, such as low entry prices, anonymity, vulnerability and asymmetry, have created the phenomenon of power dissipation, which means that if governments have so far divided the game of power among themselves, then it must be Other actors, such as private companies, organized terrorist and criminal groups, and individuals, although it is still governments that play an important role in this. Naturally, this phenomenon will not deprive governments of their national security. This effect can be evaluated in several ways. First is the concept of security. National security can no longer be defined in terms of military issues and internal and external borders, but today, the risk of declining quality of life of citizens is a threat to national security. The second is the disappearance of the geographical dimension of cyber threats. In the past, military threats had a specific geographical location. As a result, it was not difficult to deal with, at least in terms of identification. Third is the extent of vulnerabilities posed by cyber threats. These threats are sporadic, multidimensional, and because they are associated with sensitive networks and infrastructure, their level of damage are very high. Fourth, these threats cannot be contained by traditional means alone, such as the use of military and police force, and governments alone are not sufficient to counter them, and effective and bilateral cooperation between governments and the private sector, which has common interests in dealing with them. With such threats are, he demands. Fifth, as the previous point shows, cyber threats are not limited to governments, but individuals and companies will not be immune to the harms of these threats. Sixth, since security in the information age is not merely governmental, the various theoretical approaches in international relations whose theories are based primarily on government are easily overlooked or confusing.

CRediT authorship contribution statement

Yuchong Li: Conceptualization, Methodology, Formal analysis, Writing – original draft. **Qinghui Liu:** Supervision, Methodology, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aghajani, G., Ghadimi, N., 2018. Multi-objective energy management in a micro-grid. Energy Rep. 4, 218–225.

Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc..

Akhavan-Hejazi, H., Mohsenian-Rad, H., 2018. Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Rep. 4, 91–100.

Al-Ghamdi, M.I., 2021. Effects of knowledge of cyber security on prevention of attacks. Mater. Today: Proc..

Al Shaer, D., et al., 2020. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. Eur. J. Med. Chem. 208, 112791.

Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Mater. Today: Proc..

Alghamdie, M.I., 2021. A novel study of preventing the cyber security threats. Mater. Today: Proc..

Alhayani, B., et al., 2021. Best ways computation intelligent of face cyber attacks. Mater. Today: Proc..

Alibasic, A., et al., 2016. Cybersecurity for smart cities: A brief review. In: Nternational Workshop on Data Analytics for Renewable Energy Integration. Springer.

Alkatheiri, M.S., Chauhdary, S.H., Alqarni, M.A., 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. Sustain. Energy Technol. Assess. 45, 101219.

Alzubaidi, A., 2021. Cybercrime awareness among Saudi nationals: Dataset. Data Brief 36, 106965.

Amir, M., Givargis, T., 2020. Pareto optimal design space exploration of cyber–physical systems. Internet Things 12, 100308.

Arend, I., et al., 2020. Passive- and not active-risk tendencies predict cyber security behavior. Comput. Secur. 97, 101964.

Ashraf, J., et al., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities Soc. 72, 103041.

Aziz, A.A., Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. Pharmacol. Res. 149, 104471.

Baig, Z.A., et al., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 22, 3–13.

Beechey, M., Kyriakopoulos, K.G., Lambotharan, S., 2021. Evidential classification and feature selection for cyber-threat hunting. Knowl.-Based Syst. 226, 107120.

Bullock, J.A., Haddow, G.D., Coppola, D.P., 2021. Cybersecurity and critical infrastructure protection. In: Bullock, J.A., Haddow, G.D., Coppola, D.P. (Eds.), Introduction to Homeland Security, sixth ed. Butterworth-Heinemann, pp. 425–497 (Chapter 8).

Cao, Y., et al., 2019. A topology-aware access control model for collaborative cyber–physical spaces: Specification and verification. Comput. Secur. 87, 101478.

Cao, J., et al., 2021. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. Inform. Sci. 548, 69–84.

Chandra, A., Snowe, M.J., 2020. A taxonomy of cybercrime: Theory and design. Int. J. Account. Inf. Syst. 38, 100467.
Chen, J.-K., et al., 2021. Cyber deviance among adolescents in Taiwan: Prevalence and correlates. Child. Youth Serv. Rev. 126, 106042.
Cheng, S., et al., 2020. A new hybrid solar photovoltaic/phosphoric acid fuel cell and energy storage system; Energy and exergy performance. Int. J. Hydrogen Energy.
Damon, E., et al., 2014. Cyber security education: The merits of firewall exercises. In: Akhgar, B., Arabnia, H.R. (Eds.), Emerging Trends in ICT Security. Morgan Kaufmann, Boston, pp. 507–516 (Chapter 31).
Dash, N., Chakravarty, S., Satpathy, S., 2021. An improved harmony search based extreme learning machine for intrusion detection system. Mater. Today: Proc..
Edgar, T.W., Manz, D.O., 2017. Science and cyber security. In: Edgar, T.W., Manz, D.O. (Eds.), Research Methods for Cyber Security. Syngress, pp. 33–62 (Chapter 2).
Furnell, S., Shah, J.N., 2020. Home working and cyber security – an outbreak of unpreparedness? Comput. Fraud Secur. 2020 (8), 6–12.
Furnell, S., et al., 2020. Understanding the full cost of cyber security breaches. Comput. Fraud Secur. 2020 (12), 6–12.
Gupta Bhol, S., Mohanty, J.R., Kumar Pattnaik, P., 2021. Taxonomy of cyber security metrics to measure strength of cyber security. Mater. Today: Proc..
Hart, S., et al., 2020. Riskio: A serious game for cyber security awareness and education. Comput. Secur. 95, 101827.
Huang, J., et al., 2020. Secure remote state estimation against linear man-in-the-middle attacks using watermarking. Automatica 121, 109182.
Iqbal, Z., Anwar, Z., 2020. SCERM—A novel framework for automated management of cyber threat response activities. Future Gener. Comput. Syst. 108, 687–708.
ji, Z., et al., 2021. Harmonizing safety and security risk analysis and prevention in cyber–physical systems. Process Saf. Environ. Prot. 148, 1279–1291.
Judge, M.A., et al., 2021. Price-based demand response for household load management with interval uncertainty. Energy Rep..
Karbasi, A., Farhadi, A., 2021. A cyber–physical system for building automation and control based on a distributed MPC with an efficient method for communication. Eur. J. Control.
Katrakazas, C., et al., 2020. Cyber security and its impact on CAV safety: Overview, policy needs and challenges. In: Milakis, D., Thomopoulos, N., van Wee, B. (Eds.), Advances in Transport Policy and Planning. Academic Press, pp. 73–94 (Chapter 3).
Khan, S.K., et al., 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid. Anal. Prev. 148, 105837.
Kharlamova, N., Hashemi, S., Træholt, C., 2021. Data-driven approaches for cyber defense of battery energy storage systems. Energy AI 5, 100095.
Kim, Y.S., et al., 2020. Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP. Ann. Nucl. Energy 149, 107790.
Krishnasamy, V., Venkatachalam, S., 2021. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using index-level Boundary Pattern Convergent Encryption algorithm. Mater. Today: Proc..
Lee, C., Ho Chae, Y., Hyun Seong, P., 2021. Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs. Ann. Nucl. Energy 158, 108287.
Li, J., Sun, C., Su, Q., 2021. Analysis of cascading failures of power cyber–physical systems considering false data injection attacks. Glob. Energy Interconnect. 4 (2), 204–213.
Li, N., et al., 2020. Early validation of cyber–physical space systems via multi-concerns integration. J. Syst. Softw. 170, 110742.
Liu, X., et al., 2021. Quantitative cyber–physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. Comput. Secur. 102, 102138.
Ma, L., et al., 2021. Security control for two-time-scale cyber physical systems with multiple transmission channels under DoS attacks: The input-to-state stability. J. Franklin Inst. B.
Marefati, M., Mehrpooya, M., Shafii, M.B., 2018. Optical and thermal analysis of a parabolic trough solar collector for production of thermal energy in different climates in Iran with comparison between the conventional nanofluids. J. Cleaner Prod. 175, 294–313.
Mehrpooya, M., et al., 2021. Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device. Int. J. Energy Res..
Motsch, W., et al., 2020. Approach for dynamic price-based demand side management in cyber-physical production systems. Procedia Manuf. 51, 1748–1754.
Nguyen, D.C.L., Golman, D.W., 2021. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Comput. Law Secur. Rev. 40, 105521.
Nicholson, A., et al., 2012. SCADA security in the light of cyber-warfare. Comput. Secur. 31 (4), 418–436.
Niraja, K.S., Srinivasa Rao, S., 2021. A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security. Mater. Today: Proc..
Ogbanufe, O., 2021. Enhancing end-user roles in information security: Exploring the setting, situation, and identity. Comput. Secur. 108, 102340.
Palmieri, M., Shortland, N., McGarry, P., 2021. Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Comput. Hum. Behav. 120, 106745.
Patel, D.C., et al., 2021. Paradoxical motion on sniff test predicts greater improvement following diaphragm plication. Ann. Thorac. Surg. 111 (6), 1820–1826.
Priyadarshini, I., et al., 2021. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. Comput. Electr. Eng. 93, 107204.
Qiu, W., et al., 2021. Time-frequency based cyber security defense of wide-area control system for fast frequency reserve. Int. J. Electr. Power Energy Syst. 132, 107151.
Quigley, K., Burns, C., Stallard, K., 2015. 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Gov. Inf. Q. 32 (2), 108–117.
Robinson, M., Jones, K., Janicke, H., 2015. Cyber warfare: Issues and challenges. Comput. Secur. 49, 70–94.
Rodríguez-deArriba, M.-L., et al., 2021. Dimensions and measures of cyber dating violence in adolescents: A systematic review. Aggress. Violent Behav. 58, 101613.
Sakhnini, J., et al., 2021. Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. Phys. Commun. 47, 101394.
Sarker, I.H., 2021. Cyberlearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet Things 14, 100393.
Saxena, R., Gayathri, E., 2021. Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. Mater. Today: Proc..
Shamel, A., et al., 2016. Designing a PID controller to control a fuel cell voltage using the imperialist competitive algorithm. Adv. Sci. Technol. Res. J. 10 (30).
Shin, J., et al., 2021. Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed. Nucl. Eng. Technol..
Snehi, M., Bhandari, A., 2021. Vulnerability retrospection of security solutions for software-defined cyber–Physical system against DDoS and IoT-DDoS attacks. Comp. Sci. Rev. 40, 100371.
Solomon, R., 2017. Electronic protests: Hacktivism as a form of protest in Uganda. Comput. Law Secur. Rev. 33 (5), 718–728.
Sun, C.-C., Hahn, A., Liu, C.-C., 2018. Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56.
Tam, T., Rao, A., Hall, J., 2021. The bad and the missing: A narrative review of cyber-security implications for Australian small businesses. Comput. Secur. 102385.
Tan, S., et al., 2021. Attack detection design for dc microgrid using eigenvalue assignment approach. Energy Rep. 7, 469–476.
Thomson, J.R., 2015. Cyber security, cyber-attack and cyber-espionage. In: Thomson, J.R. (Ed.), High Integrity Systems and Safety Management in Hazardous Industries. Butterworth-Heinemann, Boston, pp. 45–53 (Chapter 3).
Topping, C., et al., 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Comput. Secur. 108, 102324.
Tosun, O.K., 2021. Cyber-attacks and stock market activity. Int. Rev. Financ. Anal. 76, 101795.
Varga, S., Brynielsson, J., Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. Comput. Secur. 105, 102239.
Zhang, T., 2017. A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law. Comput. Law Secur. Rev. 33 (1), 98–102.
Zhang, J., 2021. Distributed network security framework of energy internet based on Internet of Things. Sustain. Energy Technol. Assess. 44, 101051.
Zhang, Y., Malacaria, P., 2021. Bayesian Stackelberg games for cyber-security decision support. Decis. Support Syst. 148, 113599.
Zhang, X., et al., 2021. Ensuring confidentiality and availability of sensitive data over a network system under cyber threats. Reliab. Eng. Syst. Saf. 214, 107697.
Zhao, J., et al., 2020. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Comput. Secur. 95, 101867.
Zhao, Z.-g, et al., 2021. Control-theory based security control of cyber–physical power system under multiple cyber-attacks within unified model framework. Cogn. Robot. 1, 41–57.
Zou, T., et al., 2020. Smart grids cyber–physical security: Parameter correction model against unbalanced false data injection attacks. Electr. Power Syst. Res. 187, 106490.

Yuchong Li was born in Wugang, Henan, P.R. China, in 1980. He received the doctor's degree from National Digital Switching System Engineering & Technological Research Center, P.R. China. His research interests include information security, computational intelligence and big data analysis.

E-mail: yuchonglee@163.com.

Qinghui Liu was born in Jining Shandong, P.R. China, in 1977. He received the Master degree from Shandong University, P.R. China. Now, she works in Network Center Zaozhuang University. His research interests include Information technology and big data analysis.

E-mail: lqh@uzz.edu.cn.