A Survey of Cyber Security Trends, Emerging Technologies and Threats

Anand Bhushan Pandey, Ashish Tripathi, and Prem Chand Vashist

1 Introduction

The information technology infrastructure, computer networks and digital devices have become the backbone of a society, a country and the world. The deployment of Internet in almost all walks of life has eased every task we do in our daily life but risked the security and privacy of those tasks and the information belonging to those tasks. Internet has changed the lifestyle so much that one wakes up with the start of sharing information on the Internet and goes to bed only after clicking on some links, browsing some information on the web or posting something on social media without any knowledge of how secure his shared information is? The very first thing that clicks into one's mind while discussing cyber world is cyber-crimes and cyber-attacks. The attacks have become so disastrous and frequent today that it costs billions of rupees to safeguard the cyber space from attackers [1].

For a criminal to attack someone's confidential data is much more easy and less risky than physically attacking him, and attacks can be done from anywhere in the world. The malwares that include spywares, viruses, Trojan horses and worms attack a system, and the system is compromised without any clue to the actual owner and the adversary gets the complete access to the confidential information of the legitimate owner [2].

One of the many ways in which a malware attacks the system is, whenever a USB drive is inserted into an infected system, the drive gets infected and every other device in which this infected drive is inserted subsequently gets infected. The malwares can attack any system from servers, end user systems to networking devices. The malware attacks the most vulnerable point of a system including software and hardware, and it's too difficult and expensive task to prevent a large volume of applications and

A. B. Pandey · A. Tripathi (✉) · P. C. Vashist
Department of Information Technology, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*, Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_2

data and every point of large network [2]. The easier approach to protect the network and data is to guard the network at its perimeter and using firewalls, which enquires every access to the internal network, and if the access is malicious, the firewall and the antivirus installed reject the access. In spite of emerging technologies, the advancements and sophistications in malwares enable it to exploit the flaws of the technologies and avoid detection.

As the world is heading toward a new decade, the cyber criminals may come up with new techniques and approaches, identifying and neutralizing them will be the new challenge for organizations. What may be the attack vector? Will the criminals try new technologies like Biometrics and Artificial Intelligence or rely on those old conventional methods? The answers to such questions will be of utmost importance. If they are shifting to the biometrics, the security of the information gathered and that of the network authentication token is a serious problem needing a proper solution. If the token is compromised in any circumstances, the cyber criminals may get administrative access to the network creating damage beyond imagination. The drones that are information gatherers may be used for espionage as they can perform physical damage as well as data breaches. As per a recent prediction by Goldman Sachs, more than 17 billion dollars will be spent on drone functionality itself by the businesses in the next 5 years [3].

2 Cyber Security Trends

In spite of organizations' awareness and dedicated efforts toward cyber security, the security breaches and data compromises in many organizations as well as common people's cyber space had created news headlines in 2019. The cyber security trends [4–6] that will be the area of focus in 2020 are:

- "Data breach" remains to be the biggest concern for the organizations as the organizations are very conscious about their image after the data breach is in news. The records show that the flaws in the web applications are mostly responsible for the data breaches making web application security the top priority for organizations.
- "Skill gaps" in the cyber security staff appointed by the organizations along with the shortage of staff makes two out of three organizations' cyber space vulnerable to threats. Therefore, the organizations are relying on security tools like online vulnerability management solutions that make the organization secure even with a small team of security staff.
- "Cloud security" is another very vital issue to resolve as the data are being moved to the clouds; innovative approaches are required to protect that data and the critical infrastructure.
- "Cyber security automation with integration" is required as the cyber security professionals have to do a lot with less staff. Using agile processes, the organizations are easily managing security issues.

- "Awareness of cyber security's importance" is growing speedily, and organizations have realized that maintaining cyber-hygiene is mandatory and vital.
- "Mobile devices" are at risk making the complete supply chain of the organization vulnerable to indirect attacks. Secure web infrastructures and real-time management of vulnerabilities can reduce the risk.
- "State-sponsored cyber-attacks" such as attacks of distributed denial-of-service (DDoS) are sponsored by different countries to steal political and defense secrets; spread misinformation etc. in other countries.
- "IoT devices" are booming today to create automated infrastructure but at the same time, the chances of blunders in the field of cyber security have also increased. Examples are the vulnerable web platforms, insecure wireless networks, unverified updates etc. Any IoT device if compromised will serve as the weak link of the chain and entry point for fatal attacks to the system.
- "Artificial Intelligence", on one side, is helping the cyber experts in dealing with attacks by using machine learning and deep learning technologies to detect threats, on the other side, it is being used by cyber criminals to create sophisticated attack methods and malwares.
- "Phishing threat" can be said to be evergreen threat, as it remains to be the cause of many fraudulent payments, malware spreads and credential compromises.
- "5G Technology" is the future of the cyber word. With the enhance bandwidth provided by 5G technology, the number of devices, the number of sensors and the volume of data are going the explode. The preparations and the performances of the researchers and the organizations are going to decide whether it is a boon or a bane for the society, for the country and for the world.
- "Smart devices" such as smart TV, smart speakers, smartwatches etc. are increasing at the pace more than the pace they can be provided security from cyber threats.
- "Real-time operating system vulnerabilities" were discovered and exposed to the world's cyber research community in 2019 by Armis Labs, which they named "Urgent/11" [6].
- "Butterfly effect of ransomware" may be witnessed as a consequence of the constant bombardment by the attackers. Only the first 9 months of 2019 had seen 600–700 attacks on government agencies through ransomware [3].
- "Cyber Insurance" has become very popular in spite of constant warnings by the governments. However, the effect of such cyber protection cover is contrary to its objective because the attackers are targeting the ensured organizations more frequently as the chances of getting paid are more. Insurance companies generally opt to pay the ransom if the amount of ransom is less than the cost needed to rebuild the network [3]. There are estimates that the cyber insurance market is projected to be 7 billion dollars in the USA alone [3].
- "Certified Threat Intelligence Analyst (CTIA)" program is being used by the security threat analysts to learn the skills of identifying and combating the threats. CTIA is a method-driven program, which covers every aspect from planning to create effective threat reports.

3 Emerging Technologies

The emerging technologies include smartphones, social media, cloud computing, critical infrastructure etc.

3.1 Social Media

The social networking sites that provide its users a platform to connect to people and make friend, share their views, news and events also create the cyber-attack-prone points in the same proportion. The attacker finds out the careless people from the social network and uses them to attack and send spams to the people on his friends list.

3.2 Cloud Computing

The cloud computing concept provides the users' chance to use the services of various resources without spending money and requiring any management skills for the complex infrastructure. The service of account recovery provided by Google to its Gmail users was a compromised denial of service attack [7].

3.3 Smartphone Technology

With the exponential growth in the number of smartphone users, the number of mobile malwares is also growing. The case of cyber threats to the infrastructure of electricity grids to healthcare system, communication system to banking system are also being witnessed in very high proportion.

3.4 Critical Infrastructure

The infrastructure is the backbone of all the secure operations of modern-day society and is vital to national security, business and financial activities. This infrastructure is the lifeline for security of the cyber space of the country.

3.5 Internet of Things (IoT)

The Internet of Things (IoT) is one of the growing technologies that use the Internet or Internet like network to establish a connection among various intelligent IoT devices. IoT devices include the devices for a remote dashboard, for control, for servers, for routing or bridge device, and sensors [8]. These smart IoT devices are equipped with advanced functions and features to communicate over the Internet via some wireless protocols. In recent studies, the rapid growth of IoT technology has been encountered in different domains especially in the field of smart automation and Robotics.

3.6 Embedded Systems

These are the systems used to automate mechanical and electrical machines from Mp3 players, DVD players, refrigerators to ATMs, bar code readers, power grids, railways, airways etc. most of these machines need hard real-time or soft real-time constraints to meet their target outputs and any deviation may lead to devastation results.

4 Malwares

The malwares today are used to steal the confidential information of government organizations, corporate world and that of an individual but initially, malwares were used to check and enquire the security feature and loopholes in the protection layer of an application [2]. Another area in which the malwares are frequently being used is to get control of victim's computer and display some unauthorized advertisement. For most of the attackers in cyber world, Trojans are the favorite malwares of the cyber criminals. The studies show that more than 75% of the cyber-attacks to steal information and network intrusion to take control of the network are through Trojan malwares. The malwares are spread using the following activities as vehicles for transportation.

4.1 Spams

The victim receives unwanted and inappropriate messages in his inbox without his consent, and the attacker does it all anonymously that too without any expense. The most common spams today are the email spams in which the inbox of the victim is flooded with unsolicited messages [9].

4.2 Phishing

It is a masquerading attack performed to acquire confidential information by deceiving the users into visiting malicious web pages claiming to be legitimate. The private information shared by an unsuspecting user is then used for criminal activities [10]. The phishers are using innovative techniques as the user is becoming knowledgeable and smart. The phishers send emails containing links to some fake malicious websites claiming to be legitimate organizations or use misspelled URLs to deceive the users to acquire their private information [11].

4.3 Web Downloads

The attackers use it as a speedy spread method for malwares. When user visits a website and clicks on some pop-up window, or as hidden downloads from some very popular websites, the malwares are injected into user's computer system. In most of the situations, the attacker sends spam messages to the user having links to malicious web pages and lures him to visit his malicious website, as soon as the user opens the website, the malware is automatically downloaded and installed on his machine without any clue to the user [12].

5 Emerging Threats

The emergence of new technologies has provided the cybercriminal variety of vulnerable points to attack, i.e., the emerging technologies have paved the way of emerging threats. Here, we discuss the emerging technologies and the threats to those technologies.

5.1 Social Media and Threats

Today, different social media platforms have mushroomed on the Internet, and each platform is flooded with millions of users of it. Twitter and Facebook are the most popular social media platforms with billions of active user accounts around the globe and have become the new communication platforms for new generation. The cyber attackers are using this platform to inject threats to the user's machines and as the users submit a lot of their confidential as well as personal details to these platforms, once the machine is compromised, all this information is revealed.

As per a report of Sophos, an IT security organization, most of the companies are worried that their employees share lots of their personal information with social

media platforms, and there is an alarming increase in attacks on social media websites [13]. Koobface worm [14] was the worst case of social site attack by malwares, which used its Zombie arsenal to create new fake social media accounts to be friend with unaware users. Thomos and Nicol [14] discovered the inefficiencies of the social media websites in blacklisting the malicious websites using their blacklisting services. The other malware attack is on unused accounts of Facebook and Twitter and most of the time spread malwares by clicking and following the account of clueless users. In some cases, the malwares spread when the user clicks on "trending" topic contents [15]. Social sites are new and easy targets today for a number of organizations to seek user data, some firms use these data with legitimate intentions and some for malicious purposes.

5.2 Cloud Computing and Threats

If we talk about recent times, the cloud computing is the greatest technological paradigm shift [7]. The companies whether small or large are using the IT services provided by the cloud instead of using their own IT infrastructure and resources. The cloud computing possesses different characteristics like on-demand service, location-independent resource pooling, measured service, ubiquitous network access and rapid elasticity [7]. The users can assign themselves more resources through on-demand service without any human intervention. Resource pooling means every resource is shared between multiple users needing that resource. The measured service is the characteristic of cloud computing, which facilitates the users to pay according to their consumption of different services. Rapid elasticity means the capability of locating and releasing the resources as rapidly as needed.

The services offered by cloud computing may be grouped into the following categories: Platform as a Service (PaaS), Software as a service (SaaS) and Infrastructure as a Service (IaaS) [16]. IaaS provides virtual infrastructure components like storage, operating systems and virtual machines to run applications [16]. Programming environments access additional building blocks through PaaS category of services. Application software are enabled and provided through SaaS. Through multi-tenancy feature, a query rewriter is employed by salesforce.com at database level whereas at hardware level, hypervisors are used by Amazon. As the clients use the services provided by different service providers, the most important issue is to ensure that these services are secure and well protected. The active research area in cloud computing is policy integration and trust management where cloud providers control and manage the data and services of the users. The policy integration addresses the issues of secure interoperability, policy-evolution management and semantic heterogeneity.

5.3 Smartphones and Threats

As the smartphones are carried by an individual throughout the day, its computational capability and mobility can be used to organize work and lifestyle. The exponentially growing number of smartphone users indicates the critical requirement of smartphone security measures. As people store a lot of their personal but sensitive as well as confidential information in smartphones, it has become source of risk and the smartphones have become new targets of attack for cyber criminals [17]. The design-related flaws in the infrastructure for mobile communication and management are exploited by the cyber criminals to attack and peep into the encryptions of smartphones. In most of the cases, the criminals attack the system through Wi-Fi networks to steal the personal information of the users. A worm known as Cabir spreads through Bluetooth network and is another point of concern that needs to be addressed. The mobile software is also having some flows that are exploited by criminals to spread malwares, one example is the web browser.

There are reports that special malwares have been created in last couple of years to attack the the smartphones [18]. To address this all, a centralized market place is offered by companies, which helps remove any malicious application before it is installed, for example Apple offers App Store to install application to iPhone devices, Android too offers a market place to install applications for android users and removes malicious applications from the smartphones and marketplace based on user complaints [19] Sandboxing is another approach used by companies to prevent the processes from interaction avoiding the damages done by interactions.

5.4 Critical Infrastructure and Threats

The infrastructure is the backbone for all the communications, processes and activities. The complexity of interconnection of the infrastructure makes it very hard to protect it from attacks. The nature of the infrastructure is the recent area of research, which includes self-diagnostic techniques and self-healing system that automatically responds and recovers from any attack [20]. The communication, transport, public health, finance, oil and gas etc. are the areas that are part of critical infrastructure and nowadays are facing maximum threats.

In case of wars between countries, these are the very first targets of enemies. Cyber war is the attack by a nation on other nation's cyber space, networks or computer systems to harm them or only to create disruptions. This is the most fatal attack for a county as it can damage its security and security infrastructure [21]. A country must test and update its critical infrastructure and cyber defense system for possible threats to find the loop holes and eliminate them periodically. Advanced mitigation threats are the recent fatal threats to the critical in restructure, a multi-stage Bayesian [22] concept has been proposed that uses the incompleteness of the information of the

advanced mitigation threats to counter such attacks by learning the nature of attacks and planning defensive strategies.

5.5 IoT and Threats

The attacks on sensors and embedded systems are the most fatal and sophisticated cyber threats today. Today Google, Apple and Cisco, the major ICT players take significant business decisions so as to make their position in IoT landscape [23]. The core business focus for telecom operators is machine to machine communication, and hence, the Internet of Things has shown a significant growth in the number of connected devices. The future of IoT is with other technologies like cloud computing, Big Data, Semantic technologies and Robotics. In future, the web platform of smart environments and connected devices would be integrated with the Internet of things today to make smart web of everything to support the changes in the society and the growth in economy.

Cyber security will pose a major challenge to IoT technology as with the passage of time number of IoT devices will grow to trillions. In the development of smart cities, many projects have been initiated worldwide. Likewise, the same effort has been seen in home automation. Diverse facilities and services are provided by automated homes to homeowners [24]. These services include less energy consumption, optimization of water consumption, home security service, effective use of home appliances etc. This is only possible because the smart devices are controlled by a smartphone or any other device on the network.

Recent research shows that a very high percentage of consumers have no confidence on the security mechanisms of IoT devices. The heterogeneous nature of the data as well as the devices in any IoT infrastructure is the challenge that makes it tough to provide a common security solution for any IoT deployment [25]. As the devices in IoT are connected through Internet, hence any malware threat to Internet creates a fatal threat to the devices related to healthcare, home security, business, finance and military. The solution to IoT threats includes mutual authentications and the use of new artificially intelligent machine learning tools that will detect security breaches and respond accordingly to recover [24].

5.6 Embedded Systems and Threats

Today, most of the embedded system-driven machines are on some network or on Internet itself so recent challenges to researchers include the security of the electronic devices having embedded integration circuits [26]. If the chip of such electronic devices is attacked with malicious intentions, the function of the system monitored by these devices may be affected to give fatal outcomes [27]. The Trojan malwares that are used to attack such electronic devices to alter their goals are hardware Trojans and

hence are very tough to detect and eliminate. The embedded systems are the lifeline for most of the automated mechanical and electrical machines but if the security of such systems is compromised, the damages may be beyond imagination.

Cyber security experts are of the opinion that the year 2020 is going to invite the most complex and sophisticated threats that the cyber world has ever seen. Some of the threat types that the researchers have to face in the times to come are described and compared in terms of spread methods and target systems or environments. Table 1 shows the different kinds of emerging threats.

6 Current Scenario

The research shows that today most of the organizations are capable of direct attack prevention and are focusing on the new battleground created by the indirect attacks such as the attacks on the third parties and those on the vendors in the supply chain. The cyber resilience that uses cyber security and enterprise resilience in tandem offers the capability of quick response to the posed threats, which increases customer trust.

The Accenture Third Annual State of Cyber Resilience Report, 2020 [30] says that two types of organizations are there, the first group covers 17% of the organizations that are in elite group, and they have achieved a very high level of security innovations and the cyber resilience. The other group that covers 74% of the organizations, is a group of average performing organizations. The remaining 9% are bad performers as for as their security infrastructure and security budget are concerned. While the elite group is working on the improvements, the second group is following the path shown by the leaders of elite group. Some of the observations [30] of this report are:

- In the last 3 years, the number of organizations that allocate 20% of their IT budget in technology advancements has doubled.
- A decline of 27% in security breaches and 11% in direct attacks is reported in the last 3 years of time span.
- Out of the security breaches during the last 3 years, 40% were indirect attacks that too on some weak link of the supply chain.
- Sixty-nine percent believe that an unsustainable cost is being paid for staying a step ahead of the attackers in the battle going on between the organization and the attackers.

7 Conclusions and Directions for Future Research

Analyzing every aspect of the current cyber security trends, evolutions of cyber security techniques and technological assistance to it, the past, the present and the future of the threats, the conclusions can be presented under the following points:

Table 1 Emerging threats

Serial number	Threats/Malwares	Descriptions	Target systems/Environments
1	Cloud network vulnerability [28, 29]	Cyber criminals may target public clouds and any untrained employee may trigger any number of such vulnerabilities in the network	The organizations that lack tiered security programs of access
2	Ransomware and micro ransomware [3, 29]	It is the fastest-growing attack and aims at vulnerabilities, which are different from general malwares and easy to attack The emails are the biggest vehicle for ransomware spread	It can attack the industries that use the consumer data as an asset. Ex: Healthcare, POS Systems etc.
3	IoT Botnets [6]	The legion of bots was already created in leaked Merai Code 2016 are going to expand with the expansion of IoT technology	Even the systems with machine learning capabilities can be a victim of this attack
4	Polymorphism and PowerShell [30]	PowerShell manipulation is being included in malware tool kits by APT groups. The polymorphic malwares like Qbot can change its signatures	Most of the small companies
5	Third party breach [6]	Hackers use third parties, i.e., indirect attacks to attack the target and sanitize their trail after the attack making it difficult to follow	The organizations that are doing business by sharing their digital space and security features
6	AI tools [28, 29]	AI tools may be employed by hackers to consistently scan and attack the targeted system	The companies not having the staff and security technology to ward off the attacks that change their form consistently
7	Network security risk [29]	The hackers wait for the digital and cyber space expansions by the organizations to exploit	The organizations expanding their digital ecosystem and cyber space

(continued)

Table 1 (continued)

Serial number	Threats/Malwares	Descriptions	Target systems/Environments
8	Email network security risk [29]	The organizations do not take the vulnerabilities created by wireless networks, seriously making the email vulnerability fatal	The organizations having untrained employee who clicks on phishing mail
9	Attacks on Windows subsystem for Linux (WSL) [30]	WSL is the latest technology shipped out with windows 10 and is going to be the favorite target of the attacks in 2021	Environments going for updates to Windows 10
10	Search result Hijack [5]	The search engines personalize the searching behavior of an organization and the hackers may try to hack the behavioral patterns of the organization's search results Search result tempering may lead to showing malicious site and directing to that site. Once the site is opened any security compromise may result in	Any organization big or small
11	Malwares in mobile devices [5]	These are the malwares specially developed for mobile devices to access confidential information of the user such as passwords of banking apps etc. Studies show that out of all smartphone phone users about 35% use it for financial activities	Online payment Apps Ex: Banking Apps etc

(continued)

- The reason for the flooding in cyber threats is that the attacker connected to the cyber world can be anywhere in the world geographically, while attacking the target.
- With the revolutionary developments in technology and security algorithms, the nature and techniques of the threats have also changed with same or more pace.

Table 1 (continued)

Serial number	Threats/Malwares	Descriptions	Target systems/Environments
12	Remote Code Execution (RCE) attacks[6]	It is estimated that about 20 billion IoT devices on the Internet or other similar networks are prone to remote code execution (RCE) attacks	IoT devices
13	Smishing [5, 29]	The increase in online communications and interactions, the favorite target point of the attackers may shift from e-mails to online interaction platforms	WhatsApp, LinkedIn etc
14	Latest threats [5, 29]	Generally, the organizations respond to the attacks but the industry security systems should be proactive in facing the latest threats	Any organization big or small

- The introduction of the latest technologies such as Cloud Computing, IoT, Embedded systems, Social media and many more has created new battle grounds for the researchers and the criminals.
- The new technologies like Artificial Intelligence, Machine Learning and Deep Learning are very effectively and efficiently being used by cyber criminals too.
- Going through the history of the attacks and threats, it can be concluded that the cyber criminals have focused more and more on the technologies of transportation and distribution of the malwares as compared to the malware itself.
- Safety and security of the critical infrastructure is the focus of the researchers today as it is going to be the territory for a new war, i.e., the cyber war.

Thus, the conventional security measures are not going to work in future, as the Internet and Internet-connected devices are exponentially growing. The number of IoT smart devices is going cross 75 billion as per an estimate, creating an explosive situation in terms of the number and frequency of attacks [6]. This speedy growth of the Internet requires smart and innovative approaches to curb the threats. The scale of the infrastructure and the innovations in the security attacks are the major areas of concern for future research. The introduction of 5G technology will bring the newer scopes of threats, and hence, the researchers need to focus on this aspect of the technological development as well.

The reports show that most of the reputed organizations are capable enough to prevent and safeguard their cyber space from direct attacks, i.e., the attacks made on their digital space or web space directly, so the cyber-criminals are now trying to

reach their digital space though weaker links in the supply chain of which they are part of. The researchers must try to address such indirect attacks and treat the cyber space of all the organizations, i.e., third parties in the supply chain as a cyber-village.

References

1. V. Benjamin, H. Chen, Securing cyberspace: identifying key actors in hacker communities, in *IEEE International Conference on Intelligence and Security Informatics* (2012), pp. 24–29
2. G. Cluley, Sizing up the malware threat–key malware trends for 2010. Netw. Secur. **2010**(4), 8–10 (2010)
3. Source. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020
4. Innovate for Cyber Resilience
5. Cybersecurity Trends,
6. Cybersecurity Threats
7. D. Zissis, D. Lekkas, Addressing cloud computing security issues. Futur. Gener. Comput. Syst. **28**(3), 583–592 (2012)
8. S. Madakam, V. Lake, V. Lake, V. Lake, Internet of Things (IoT): a literature review. J. Comput. Commun. **3**(05), 164 (2015)
9. Y.Y. Chen, S.P. Yong, A. Ishak, Email hoax detection system using Levenshtein distance method. JCP **9**(2), 441–446 (2014)
10. M. Khonji, Y. Iraqi, A. Jones, Phishing detection: a literature survey. IEEE Commun. Surv. Tutor. **15**(4), 2091–2121 (2013)
11. I. Qabajeh, F. Thabtah, F. Chiclana, A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Comput. Sci. Rev. **29**, 44–55 (2018)
12. L. Xu, Z. Zhan, S. Xu, K. Ye, Cross-layer detection of malicious websites, in *Proceedings of the Third ACM Conference on Data and Application Security and Privacy* (2013), pp. 141–152
13. C. Oehri, S. Teufel, Social media security culture, in *2012 Information Security for South Africa* (IEEE, 2012), pp. 1–5
14. K. Thomas, D.M. Nicol, The Koobface botnet and the rise of social malware, in *2010 5th International Conference on Malicious and Unwanted Software* (IEEE, 2010), pp. 63–70
15. Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony, A. Pentland (eds.), *Security and Privacy in Social Networks* (Springer Science & Business Media, 2012)
16. Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. **1**(1), 7–18 (2010)
17. C. Kasmi, J.L. Esteves, IEMI threats for information security: remote command injection on modern smartphones. IEEE Trans. Electromagn. Compat. **57**(6), 1752–1755 (2015)
18. D. He, S. Chan, M. Guizani, Mobile application security: malware threats and defenses. IEEE Wirel. Commun. **22**(1), 138–144 (2014)
19. Z. Fang, W. Han, Y. Li, Permission based Android security: issues and countermeasures. Comput. Secur. **43**, 205–218 (2014)
20. A. Zimba, Z. Wang, H. Chen, Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express **4**(1), 14–18 (2018)
21. C.J. Finlay, Just war, cyber war, and the concept of violence. Philos. Technol. **31**(3), 357–377 (2018)
22. L. Huang, Q. Zhu, Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. ACM SIGMETRICS Perform. Eval. Rev. **46**(2), 52–56 (2019)
23. S. Sezer, T1C: IoT security: threats, security challenges and IoT security research and technology trends, in *31st IEEE International System-on-Chip Conference (SOCC)* (IEEE, 2018), pp. 1–2

24. F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. **6**(5), 8182–8201 (2019)
25. W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. **6**(2), 1606–1616 (2018)
26. B. Yuce, P. Schaumont, M. Witteman, Fault attacks on secure embedded software: threats, design, and evaluation. J. Hardw. Syst. Secur. **2**(2), 111–130 (2018)
27. C. Paar, Hardware trojans and other threats against embedded systems, in *Proceedings of the ACM on Asia Conference on Computer and Communications Security* (2017), p. 1
28. Source. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
29. Source. https://securityintelligence.com/articles/these-cybersecurity-trends-could-get-a-boost-in-2020/
30. Source. https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET_Trends_Report_2019.pdf