 DOI: 10.5281/zenodo.10371066

PROTECTION OF ONLINE AGREEMENTS IN CYBER CRIME

BY *DIVYANSHI GUPTA*[1]

ABSTRACT

Rapid digitalization of transactions and agreements has transformed company processes, but it has also introduced new concerns, notably in the area of cybersecurity. This in-depth investigation digs into the complex world of internet agreements and their weaknesses in the face of criminality. This research gives a detailed knowledge of the challenges posed by cybercriminals and the methods necessary to defend digital agreements efficiently, from analysing the complexities of various online agreement forms to investigating the latest cybersecurity technology. The research looks at essential factors including encryption mechanisms and user education & awareness emphasizing their importance in strengthening online agreements. It also digs at upcoming technologies including as artificial intelligence & machine learning and virtual reality & augmented reality, highlighting their potential to revolutionize online agreement protection. The study also examines notable cybercrime instances affecting online agreements, using insights from real-world case studies. Furthermore, the research examines the legal environment, exploring national regulations governing online agreements, and emphasizing the need for compliance in the digital age. Finally, this research not only summarises major findings but also offers practical establish a resilient ecosystem where online agreements are secured against cyber threats, and cyber thefts, maintaining confidence, security and dependability in the digital era by adopting new technology, increasing user awareness and remaining up to date on legislative changes.

Keywords: Cyber Crime, Cyber Law, Internet, Agreements, Privacy, Online, Security

[1] Author is a student at Lloyd School of Law, Greater Noida

1. Introduction

The internet or 'Cyberspace' has made it simpler and more effective to transfer data or any information between various networks. In the age of digitalization, the internet becomes the important tool from online dealing to online transaction. When it comes to doing business, collaborating and transferring information internet plays a major role. The majority of users have been using the computers for years, either for their personal or professional benefits. Security related issues are now of great concern for administrators. As a result, Cyber Crime was born. This had resulted in illegal societal activities. We can define the 'Cyber Crime' which means any crime which is done by using computer or involvement of any computer activities which is illegal and it usually take place over the cyberspace i.e. internet. Now the term 'Cyber Law' which means the law that governs the cyberspace. Cyber law comprises the legal principles and laws that regulate internet usage and online activity. It is crucial in dealing with legal concern that develop in the digital environment, such as online privacy violation, hacking, digital fraud, copyright infringement and other internet-related offences. It also covers the laws of electronic contracts, digital signatures and online transactions.

The Information Technology Act, 2000 (IT Act, 2000) is a legislative framework in India that was created to solve the issues of the digital era. The IT Act, 2000 is instrument in safeguarding individual, businesses and government entities from the variety of cybercrime. The Act play a major role in protecting cybercrime victims by defining offences and prescribed punishments for unauthorized access, data theft, online fraud and cyber terrorism. It also defined the criteria for digital signature and ensuring the legitimacy of electronic documents.

2. Online Agreements

Online agreements are also known as digital agreements or e-agreements. Online agreements are legally binding arrangements that can be done by using several electronic devices and signed electronically. These agreements given the same legal status as traditional agreements which involves papers and these agreements can be done by using variety of devices.

2.1. **Types of online agreements**

2.1.1. Shrink-Wrap Agreements

"Shrink-wrap agreements are basically licensing agreements for software. In these types of agreements, the terms and conditions to access to such software products shall be enforce by the person purchasing it, with the beginning of the software product's packaging." These days licensing agreements are frequently not sent with the software, but rather appear before installing it.

As we will see, shrink wrap agreements have a distinct benefit over other types of electronic agreements in that their acceptance can be revoked by returning the merchandise.

2.1.2. Click-Wrap Agreements

Click wrap agreements is common and mostly found as a part of software. The users have only 2 choices either agree and use the software or disagree with the terms and conditions provided and not to use that particular software.

2.1.3. Browse-Wrap Agreements

"Browse-wrap agreements are contracts to which you agree simply by continuing to use the service or browsing the web page, which is where the term originates." A browse-wrap agreements is typically found on a website or in a downloadable product. These contracts are published on a specific webpage, and users must navigate to that webpage to find these terms and conditions. These contracts are typically secret.

3. Cyber Crime: A Growing Threat

Cyber Crime is the crime in which the computer is used as the object of the crime or utilized for committing the crime or any illegal activity is done via electronic devices in cyberspace i.e. internet. A cybercriminal may exploit a device to get access to a user's personal information, confidential corporate information, government data or to deactivate a device. There are major 3 categories of cybercrime assault: individual, organization and government.

Before discussing about cybercrimes one should know the target of such online attacks. People think that cybercrime have little impact on them because they do not have any confidential information. But in this technological era, when bank accounts are accessible over the internet, everyone possesses a lot of information whose loss will result in a very big trouble.

3.1. **Types of Cyber Crime**

3.1.1. Phishing

In phishing, "hackers send malicious email attachments or URLs to victims in order to obtain access to their accounts or computers." The purpose of this conduct is to obtain personal information from the consumers or organization by duping them. The cybercriminal may not physically destroy the equipment but he may cause financial loss to the user as a consequence of credential supplied, data loss as a result of website access that results in identity theft.

3.1.2. Identity theft

The term itself define identity theft occurs when some other person impersonates the original user. The cyber theft steals the personal information of the users for fraudulent purpose. They can also open the phone or internet account in users name and organize a criminal activity in user identity. They may accomplish this by stealing into user accounts or obtaining personal information from social media

3.1.3. Denial of service (DoS)

In DoS cyberattacks, attackers sending a large number of requests to a service or computer network and fill the e-mail box with spam mails. This type of attack is intended to crash the network by flooding it with worthless traffic. A Distributed Denial of Service (DDoS) attack is another variation on a normal denial of service attack in which the attackers are numerous and geographically dispersed.

3.1.4. Malware attacks

Malware is the short form of 'malicious software' which means programs designed to cause harm. Ransomware is one kind of malware attack. Like, malware includes viruses, worms, spyware and adware. Malware as opposed to other types of cybercrime such as theft or fraud, is intended to inflict damage and harm to a computer system or the data it contains.

3.1.5. Cyberstalking

"Cyberstalking is used in stalking a person online, such as by sending them unwanted messages or tracking their position over the internet." In order to stalk the person, some cyberstalkers utilize spyware to get access to digital speakers.

3.2. **Case Analysis: Prominent Cybercrime Incidents Having an Impact on Online Agreements.**

3.2.1. Capital One Cyber Incident (2019)

Incident: "An unauthorized access was achieved by an outsider who got various kinds of personal information about Capital One credit card customers and persons who had applied for the credit card product."

Impact on Online Agreements: The leak most certainly breached Capital One's data protection terms of service. Capital One faced legal consequences, inquiries, and financial costs as a result of its failure to comply with its online agreements.

3.2.2. Marriott International Cyber Incident (2018)

Incident: "The attack compromised over 300 million visitors credit card information, passport numbers and birthdates kept in the brand's global guest reservation database. It is one of the biggest data breaches in the history."

Impact on Online Agreements: Marrott's internet agreements most certainly included provisions for protecting consumer data. The violation prompted inquiries and legal action, which could affect Marriott's compliance with its terms of service.

4. Legal Framework for Online Agreements

4.1. National Cybersecurity and Data Protection Regulation.

- The procedures used to secure a computer or computer system from an unauthorized access by a hacker are referred to as Cybersecurity. A strong cybersecurity policy safeguards secure, critical or sensitive data and keeps it out of the hands of harmful third parties. They can also mandate for organizations to deploy security measures, report breaches and safeguard vital infrastructure.

  The effect on online agreements is that the rules frequently require online services providers to comply to specified cybersecurity requirements. Compliance with these criteria may be noted in the terms of service, assuring customers that the platform has proper cybersecurity protections in place.
- Data protection refers to a systematic structure of laws, regulations, standards and rules developed by the government and regulatory bodies to protect individuals' privacy and avoid data manipulation caused by malpractice such as unconsented and unauthorized data storage and dissemination. Personal data collection, processing, storage and sharing are all governed by data protection regulations. They frequently include provision addressing user permission, data security and individuals' rights to personal information.

  The effect on Online agreements are particularly privacy rules, must adhere to national data protection legislation. These rules govern how firms gather, use and secure user data and they require clear disclosure of data practices in online contracts.

4.2. Contract Law and Online Agreements

Contract law established the rules and principles that regulate the formation, validity and enforceability of contracts, including those entered into online agreements.

4.2.1. Offer and Acceptance

E-contracts with an offer and acceptance are legally binding contracts. The parties exchanging e-mails or accepting a terms and conditions, or downloading can also suggest a contract is a valid contract. Email, internet forms and EULA (end user licence agreements) are the options for making electronic or online agreements.

4.2.2. Intention to create a legal relationship

It states that only agreements between two parties where they had an intention to enter into the legal relationship, shall be deemed a contract under contract law. In context of online agreements, conditions of service, sales agreements and subscription conditions are all designed to establish legal relationships. Users that transact online except these agreements to be legally binding.

4.2.3. Consideration

According to the Indian Contract Act, 1872 "*Consideration is something done at the desire of promisor. As consideration, the promisor may ask the promise or any other person to do or abstain from doing something. This act of abstinence from it is known as the consideration to the contract.*"

Consideration in online agreements mostly involves payments for goods or services. Users pay for goods, services and so on in exchange for promises made in online agreements.

4.2.4. Competency of contract

The Indian Contract Act, 1872 lays down the qualifications which unable a person to enter into a contract. "A person should have attend the age of majority, should be of sound mind at the time of entering into a contract and a person should not be disqualified by law."

The issue arises with online contract is that both parties are unaware of each other's existence. The party supplying the service or commodities has no knowledge of whether the other party is legally competent to contract or not. Like if a minor under the age of 16 orders something from any online retailer.

5. Technological Solutions

5.1. Protocols for Encryption and Secure Communication

5.1.1. Encryption

Encryption is a type of data security that converts information to ciphertext. Only authorized individuals with the key can decrypt the code and access the original plaintext data. Encryption not only secure data or message confidentiality, but it also provides authentication and integrity, demonstrating that the underlying data or messages have not been altered in any way from their original condition.

Encryption is used to protect data sent between users and online platforms. This includes login credentials, personal information, financial information and any other sensitive information shared via online agreements. It ensures that even if intercepted, the data looks as gibberish in the absence of the encryption key.

Types of Encryptions:

- Symmetric Encryption

  It is the most basic type of encryption. The same key is used for encryption and decryption in symmetric encryption. When encrypting data-in-motion, the key is generated and sent to both the sender and the recipient of the message.

- Asymmetric Encryption

  Asymmetric encryption makes use of the concept of a kay pair, in which a distinct key is used for encryption and decryption. One key is kept private, while the other is made public. The public key is used to encrypt data and the private key is used to decrypt it.

5.1.2. Secure Communication

It is a method of preventing unauthorized parties from accessing data. It entails utilizing encryption and other security measures to enable secure data transmission between two or more parties.

To protect user data during transmission, secure communication protocols are used in a variety of online services such as websites, email services and messaging apps.

They ensure that data sent between the user's device and the servers is encrypted and secure against interception or alteration.

Types of Internet Security Protocols

- SSL Protocols

  "SSL (Secure Sockets Layers) protocol is an encryption-based Internet security protocol that protects data confidentiality and integrity." SSL is used to protect the privacy and authenticity of data transmitted over the internet.

- TLS Protocols

  "TLS (Transport Layer Security) is widely used for privacy and security over the internet. It generates the master secret, which is a key used for encryption between the protocol client and protocol server, using pseudo-random technique. It is mostly used to encrypt communication between online servers, such as when a web browser loads a web page from an online server."

- SHTT Protocol

  "SHTTP (Secure Hyper Text Transfer Protocol) is a collection of security methods aimed to secure internet communication such as creating strong passwords, installing a firewall, considering antivirus protection and so on. It includes data entry forms for entering data previously collected into a database as well as online transaction."

5.2. AI- driven Fraud Detection and Prevention

Artificial intelligence can help in fraud management by detecting and preventing fraudulent actions. AI plays a very important role in fraud management. AI technology, such as machine learning algorithms, can analyze massive volumes of data and finf trends and abnormalities that may suggest fraudulent activity. AI-powered fraud management systems can detect and prevent numerous sorts of fraud, including as financial fraud identity theft and phishing attempts. They can also adapt to and learn from new fraud patterns and trends, boosting their detection over time. AI-based solutions can also be integrated with other security systems to provide a more holistic approach to fraud prevention.

Fraud is an imminent threat to online transactions, causing both businesses and individuals to lose money. Fraudsters employ a variety of ways to steal identities, modify data and circumvent security measures. In this, we will look at how artificial intelligence can help with fraud detection and prevention.

5.2.1. Anomaly detection

It is the process of discovering patterns or behaviours in a dataset that depart from the usual or anticipated. For example, if a customer makes a substantial purchase from a foreign country all of a sudden, this could be an anomaly indicating fraud. Machine learning algorithms that learn from historical data and flag questionable transactions in real time can assist AI discover anomalies in online transactions. Deep learning techniques, such as neural networks, can also be used by AI to process complicated and high-dimensional data, such as photos, videos or audio and find abnormalities that humans cannot see.

5.2.2. Natural Language Processing (NLP)

NLP is the use of artificial intelligence (AI) to analyze and generate human language, such as text or speech. For example, if a client writes a review, sends an email, or makes a phone call that information might be analyzed using NLP to detect fraud. AI can assist in the usage of NLP in online transaction by extracting meaning, emotion or essential information from the language through semantic or sentiment analysis. AI can also employ generative models, such as GPT-3 to generate realistic and coherent language that can confuse or defraud fraudsters.

5.2.3. Biometric Authentication

The method of authenticating a person's identification based on physical or behavioural traits such as fingerprints, face or voice is known as biometric authentication. Like if a customer checks in to an online account, biometric authentication might be used to prevent fraud. AI can assist in the usage of biometric authentication in online transactions by capturing and comparing the person's biometric traits using computer vision, speech recognition, or behavioural analysis. AI may also leverage adversarial learning techniques, such as generative adversarial networks to generate synthetic biometric data that can be used to improve or challenge authentication.

6. Effective Practices for Ensuring the Security of Online Agreements

6.1. User Education and Awareness

User education is an important process that equips people with the information and skills they need to recognize and manage cybersecurity threats. It provides consumers with the resources they need to make educated decisions and take proactive steps to secure their digital assets. End users are frequently the first line in defence against cyberattacks. End-user education aids in raising knowledge of potential cyber dangers and their consequences. Many people are ignorant of the many forms of cyber dangers, such as phishing, malware and ransomware, and how they may damage their personal and professional life. End-user education can assist organization enhance their overall security posture. Human mistake is the root cause of many cyberattacks, such as using weak passwords, reading unexpected emails or files and accessing insecure websites. End-users become more informed about how to safeguard themselves and the organization by being educated on recommended practices such as using strong passwords, avoiding strange emails, and avoiding risky websites.

6.2. Regular Security Audits and Updates

Regular security audits and updates are critical practices for ensuring the security and integrity of online contracts, user data and digital infrastructure. Security audits aid in the identification of vulnerabilities, the evaluation of the efficacy of current security measures, and the compliance with industry norms and laws.

Importance of Security Audits

- Vulnerabilities Identifications

  Regular security audits assist firms in identifying possible vulnerabilities in their systems and networks. These audits might uncover flaws in a company's cybersecurity procedures, such as obsolete software or insufficient password policies.

- Ensuring Compliance

  Many businesses are governed by legislation and compliance standards. Regular security audits can help a company achieve these obligations and avoid any fines or penalties.

- Protecting Reputation

  A cyber assault may harm a company's reputation and diminish consumer trust. Regular security audits may assist firms in identifying and correcting weaknesses before they are exploited by hackers, therefore safeguarding their reputation and guaranteeing consumer loyalty.

- Financial Savings

Cyber assaults can result in considerable financial losses for a company. Regular security audits can help discover possible security problems before they do financial harm.

7. Challenges and Future Trends

7.1. Emerging Cyber Threats

Cyber incidents in cyberspace changes with time, taking advantages of new tactics. Most of the time, cybercriminals will change existing malware signatures in order to exploit holes in new technology. In other circumstances, they just investigate the specific qualities of new technology in order to uncover gaps via which malware might be injected. Cyber thieves exploit modern Internet technologies, which have millions and billions of active users, to reach out to a large number of victims swiftly and efficiently. Some emerging technological advancements are as follow:

- Social Media

  Social media platforms play a vital part in cyber security and personal cyber-attacks. Because the majority of employees use social media or social networking sites on a daily basis, it has become a big arena for cyber criminals to hack private information and steal valuable information. Because of social media, people are more likely to reveal sensitive information, which hackers might exploit. As a result, users must take reasonable precautions to avoid the abuse and loss of their information via social media.

- Cloud Computing

  It is a new technology that poses a significant challenge to cyber security as traffic can go around traditional points of inspection. Furthermore, as the number of cloud-based apps rises, policy controls for web applications and cloud services will need to adapt in order to prevent the loss of vital data. Even while cloud offers several advantages, it should be emphasized that as the cloud evolves the security issue increases.

- Mobile Networks

  The advancement of wireless technology has resulted in an increasingly powerful computer and communication device that people carry with them throughout the day. The confluence of increased processing power, customization and mobility makes them an appealing way if planning and organizing individuals' professional and private lives. We must continuously consider the security of these mobile networks. Furthermore, because mobile networks are so vulnerable to cybercrime, extreme caution must be exercised in the event of a security breach.

7.2. Future Technological Trends in Online Agreement Protection

The subject of online agreement security is constantly evolving as a result of technology breakthroughs and the ever-changing panorama of cybersecurity threats. A number of upcoming technology change are predicted to influence how online agreements are protected and safeguarded. Here are some crucial trends are as follows:

- Artificial Intelligence and Machine Learning

  AI is intended to provide computers with the full responsiveness of the human mind. This is the field under which many other disciplines fall, such as machine learning and deep learning.

  Machine learning employes pre-existing behavioural patterns to make decisions based on previous data and findings. Some modifications still require human involvement. To date, machine learning is certainly the most relevant AI cybersecurity discipline.

  Its advantage includes proactive threat detection, real-time reaction, increased accuracy in detecting fraudulent actions and fewer false positives.

- Virtual Reality and Augmented Reality

  Virtual reality and augmented reality achieve various things in different ways. Whereas virtual reality replaces your view, augmented reality enhances it. The discrepancies are due to the instruments used and the experience itself:

  AR employs real-world surroundings whereas VR is purely virtual.

  AR users may control their presence in the actual world but VR users are controlled by the technology.

  AR can be accessed with only a smartphone whereas VR requires a headgear device.

  They both are strong technologies that have yet to make an impact on most people's lives. They have the potential to completely change the way we use computers in the future. Its advantages include secure virtual interactions, prevention of virtual property fraud and better security for VR based online agreements.

8. Conclusion

Protecting internet agreements is critical in the world of cybercrime. The need of encryption, safe communication protocols, user education and continual security audits is highlighted by key results, which emphasis the complexity of online agreements, the growing nature of cyber threats, and the importance of online agreements. Emerging technologies like a blockchain, AI, sophisticated biometrics and so on are altering the future of online agreement protection.

The amount and severity of cybercrime attacks are projected to rise as technology develops, resulting in severe financial and reputational losses. We must take action to combat cybercrime by raising awareness and implementing preventative measures. Individuals should follow best practices in cybersecurity and purchase cyber insurance. To combat cybercrime, business must prioritise cybersecurity and purchase cyber insurance. Government may enact rules that hold culprits responsible and encourage best practices in cybersecurity.

In short, preventing cybercrime necessitates a collaborative effort on the part of individuals, corporation and governments. We can lower the risk of cybercrime and protect ourselves from its disastrous repercussions by working together and adopting preventive actions.

The convergence of upcoming technologies such as quantum-safe encryption, decentralized identity solutions and augmented reality with online agreement security should be the focus of future study. Researching user behaviour in the context of online agreements and creating AI-driven fraud detection tools targeted to specific businesses are two more areas of interest. Furthermore, politicians and legal professionals will need o comprehend the legal and ethical consequences of modern technology in online agreements.

Cybercriminal techniques evolve in pace with technological advancement. Businesses, researchers and governments must work together to create proactive adaptable policies. A safer digital environment may be established by embracing breakthrough technology, encouraging user education and staying ahead of developing risks. The protection of online agreements is not just an obligation but also a must for a safe and trustworthy digital future.

References

- Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah, *A brief study on Cyber Crime and Cyber Law's of India,* 4 IRJET 1633, 1633-1636 (2017).
- Zhang, Yanping & Xiao, Yang & Ghaboosi, Kaveh & Zhang, Jingyuan & Deng, Hongmei, *A survey of cyber crime,* 5 SCN 422, 423-425 (2012).
- Wpadmin, *Cyber Laws in India and Information Technology Act*, Proind, https://www.proind.in/blog/cyber-laws-in-india-and-information-technology-act-all-you-need-to-know/
- Shresth Goel, *Enforceability of E-Contracts in India,* 9 IJCMS 9, 10 (2022), https://www.internationaljournalssrg.org/IJCMS/2022/Volume9-Issue2/IJCMS-V9I2P102.pdf
- SignDesk, https://signdesk.com/in/esign/what-are-the-different-types-of-electronic-contracts (last visited Oct. 10, 2023)
- Legal PaathShala Online Contracts under Indian Contract Act, 1872 - Legal PaathShala (last visited Oct 15)
- Dennis, Michael Aaron, Cybercrime, Encyclopedia Britannica, 30 Oct. 2023, https://www.britannica.com/topic/cybercrime
- Vidhikarya, https://www.vidhikarya.com/legal-blog/types-of-cyber-crime-and-prevention (last visited Oct 17)
- Jain, Neelesh and Shrivastava, Vibhash and Professor, and Professor, Assistant, *CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY,* 4 IJCA 76, 79-80 (2014)
- CapitalOne https://www.capitalone.com/digital/facts2019/
- Paquet-Clouston, Masarah and Décary-Hétu, David and Bilodeau, Olivier, *cybercrime is whose responsibility? A case study of an online behaviour system in crime,* 19 GC 1, 8-9 (2018).
- Jordan Hollander, *Marriott Data Breach FAQ: What Really Happened?* HotelTechReport https://hoteltechreport.com/news/marriott-data-breach
- https://www.dfa.ie/our-role-policies/international-priorities/international-law/how-international-law-works/
- AmTrust Financial https://amtrustfinancial.com/blog/small-business/cybersecurity-vs-data-privacy
- King Stubb & Kasiva, *Data Protection and Privacy – Cyber Security Laws in India,* Ksandk, https://ksandk.com/information-technology/cyber-security-laws-in-india/
- Donal Nolan, *Offer and Acceptance in the Electronic Age,* SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082505

- Jasmeen Choudhary And Amulya Nigam, *Legal issues involved in electronic contracts under Indian law,* LawBhoomi, https://lawbhoomi.com/legal-issues-involved-in-electronic-contracts-under-indian-law/
- FORTINET, https://www.fortinet.com/resources/cyberglossary/encryption
- Riley Dickens, *What are Encryption Protocols and How Do They Work?,* Encryption Consulting, https://www.encryptionconsulting.com/what-are-encryption-protocols-and-how-do-they-work/
- National Cyber Security Centre, https://www.ncsc.gov.uk/guidance/secure-communication-principles
- PrivacySense.net, https://www.privacysense.net/terms/secure-communication/
- GeeksforGeeks, https://www.geeksforgeeks.org/types-of-internet-security-protocols/
- SEON, https://seon.io/resources/fraud-detection-with-machine-learning/
- COINTELEGRAPH, https://cointelegraph.com/explained/how-is-artificial-intelligence-used-in-fraud-detection
- Security Awareness Program Special Interest Group PCI Security Standards Council, *Security Awareness Program Special Interest Group PCI Security Standards Council,* PCI DSS 1, 1-2 (2014), https://listings.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf
- Aldheleai, Hassan and Bokhari, Mohammad and S. A. Hamatta, Hatem*, User Security in e-Learning System,* CSNT 767, 767 (2015).
- AUDITBOARD, https://www.auditboard.com/blog/what-is-security-audit/
- Soliman, Rony, *The nature of cyber threats has changed dramatically over the past three decades,* (2022).
- Gade, Nikhita Reddy and Reddy, Ugander, *Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies,* (2014).
- Rajasekharaiah, K. and Dule, Chhaya and Sudarshan, Dr, Cyber Security Challenges and its Emerging Trends on Latest Technologies, 981 IOP Conference Series: Materials Science and Engineering 022062, (2020).
- Kaspersky, https://www.kaspersky.com/resource-center/definitions/ai-cybersecurity