The Oscar Publishing Services
International Journal of Law And Criminology

VOLUME Vol.05 Issue11 2025
PAGE NO. 62-64
DOI 10.37547/ijlc/Volume05Issue11-10

Global Current Cyber Threats: How Attackers Operate

Nozimabonu Abdushukurova
Teacher, Andijan Institute of Agriculture and Agrotechnologies, Uzbekistan

Received: 30 September 2025; **Accepted:** 28 October 2025; **Published:** 30 November 2025

Abstract: This article reviews global cyber threats and their development. At the same time, it provides an analysis of the risks. Today, hacker attacks are increasing, which is accompanied by a rapid development of the infrastructure of international countries and the improvement of modern technologies.

Keywords: Cyber threats, attackers, infrastructure, transport, state, hacker attack, security, espionage, blackmail, raid, extortion.

Introduction: The world depends on modern technologies, and without them the functioning of state institutions, infrastructure, companies, and even ordinary people would often be impossible. However, this dependency also has a negative side — cybercriminals who constantly expose us to hacking attacks. Unfortunately, these attacks are often highly effective, leading to the theft of personal data, state and corporate secrets, and their use for harmful purposes such as espionage, blackmail, raids, extortion, and more. Throughout the history of computer networks and the Internet, numerous successful hacking attacks have occurred. Cybercriminals have targeted a wide range of entities, from government and financial institutions to pipeline operators, industrial enterprises, energy facilities, and others. In some cases, the damage caused by hackers has led to real collapse in energy, transport, and other sectors, requiring enormous human and financial resources to eliminate the consequences. We have selected several examples of such hacking attacks, and unfortunately, we must say that the overall level of electronic security in the world has not improved in recent years.

Cybercrime refers to illegal activities carried out using digital technologies and internet networks. Today, cybercrime is considered a serious threat not only to individuals or corporations but also to entire nations. Illegal activities conducted through internet networks have the potential to disrupt the economic, social, and political stability of society. Therefore, countries and international organizations around the world are paying special attention to combating cybercrime and ensuring information security. In this regard, extensive cooperation efforts are being carried out.

Yahoo breach (2013-2014): In 2016, Yahoo reported data breaches related to hacking attacks that occurred in 2013 and 2014, which had the effect of a real bombshell. As a result of the hackers’ activities, the personal information of more than 1 billion users of the platform became freely available online. However, cybersecurity experts were convinced that the real number of victims was three times higher. And that turned out to be true. A year later, the American company was forced to admit it. The global community was extremely shocked. The company’s stock price dropped sharply, and users began to abandon Yahoo’s services en masse.

Hacking of the PlayStation Network (2011): The 2011 hacker attack on the PlayStation Network went down in history due to the negligence of the company’s digital media and entertainment service security specialists. Hackers stole data from nearly 77 million accounts and caused a complete paralysis of the entire network. Worst of all, the compromised information included the actual credit card numbers of the service’s users.

OneCoin fraud (2016): This was not an ordinary hacking attack but a massive fraud scheme that for many years remained the largest scam in the history of the cryptocurrency market. Recently, the OneCoin case faded into the background amid the bankruptcy of the FTX cryptocurrency exchange. This scam was a typical Ponzi scheme—essentially a pyramid—created by the Bulgarian company OneCoin Ltd. Its founder was the Bulgarian Ruja Ignatova, who modestly called herself the "Crypto Queen." She was assisted by another fraudster, Sebastian Greenwood.

Hacking of the U.S. Department of Defense and NASA (1999): This is not only one of the oldest attacks on the list but also one of the most interesting. In 1999, a 16-year-old hacker known as cOmrade gained access to the computer network used by the U.S. Defense Threat Reduction Agency (DTRA). His backdoors allowed him to download more than 3,000 messages. This young hacker managed to obtain the login credentials of at least 19 employees. He was able to read classified documents and the internal correspondence of the agency without raising any suspicion. Interestingly, he broke in by gaining access to a router. From the router, he was able to retrieve passwords and intercept the mailboxes of DTRA staff.

Petya virus (2017): On 27 June 2017, a powerful computer virus paralyzed multiple companies across the globe. The global disruption was caused by a ransomware virus that blocked computers from functioning. The world soon learned that the malicious software originated from Russia's hacker group Sandworm. Many of you may remember this hacking attack. The Petya.A virus encrypted data on computers and then displayed a message demanding a payment of 300 dollars in Bitcoin to unlock the system. Experts stated that the virus affected only computers running the Windows operating system. The virus spread via phishing emails (phishing is a type of online fraud in which criminals impersonate well-known brands in order to obtain confidential user data). Specialists later discovered that the virus used a forged Microsoft digital signature.

Stuxnet (2010): Stuxnet is a sophisticated, autonomous industrial espionage tool designed to infiltrate the operating systems responsible for processing industrial facilities, collecting data, and providing operational dispatch control. However, unlike many similar viruses, the primary purpose of Stuxnet was not to steal information but to damage industrial automated systems. Worms of this class can remain undetected in a system in a dormant state and, at a specific moment, begin issuing commands that can shut down industrial equipment.

Uber data breach (2016): In 2016, hackers carried out a major attack on Uber's servers. Initially, it was reported that the attackers had stolen the data of 57 million platform users and drivers. Interestingly, the incident was not made public until 2022, which caused a wave of significant criticism. It later became known that the hackers had actually succeeded in stealing the personal information of nearly 77 million users and drivers.

Marriott hotel network attack (2014): In 2014, hackers breached the servers of the Marriott hotel network and stole the credit card information of seven million British customers. Even worse, they were able to decrypt the data because the decryption keys were stored on the same server, along with customers' passport numbers. A similar issue occurred in 2016 at the Starwood Hotels, which had been acquired by Marriott. However, the most alarming fact was that the data breach was only publicly disclosed in 2018, leaving hotel customers at risk of financial loss for four years.

Attack on Kaseya's global customer base: After gaining access to the servers of the SolarWinds management provider, REvil hackers created malware that spread to Kaseya's global customer base through its payment software. The malicious software was distributed by falsifying updates to VSA servers, which are used by 60 companies working with Kaseya for remote monitoring and management. This sophisticated attack, which occurred in 2021 just before the U.S. Independence Day celebrations, affected hundreds of U.S. companies that relied on Kaseya's software and services to provide internal computer network solutions.

Hackers against the Colonial Pipeline: This is one of the most recent examples on our list and also the largest attack on infrastructure in the United States. Russian hackers from the DarkSide group infected the Colonial Pipeline system, which manages an oil pipeline in the southeastern U.S., with ransomware.

The Role of Cybersecurity Experts and Their Solutions: Cybersecurity experts play a critical role in protecting systems and networks by conducting audits to assess security measures, identify areas for improvement, and test vulnerabilities. They review access control tools, ensure compliance with industry standards, and actively monitor networks and systems using intrusion detection systems, log analysis tools, and threat intelligence feeds. By participating in cybersecurity communities and collaborating with other experts, they stay informed about emerging threats, trends, and countermeasures. Organizations must evaluate the security practices of third-party vendors and suppliers, conduct security assessments, perform relevant audits, and establish contractual requirements. Additionally, implementing continuous monitoring systems such as Security Information and Event Management (SIEM) tools, threat intelligence feeds, and Security Operations Centers (SOCs) with advanced analytics helps respond to security incidents in real time. To defend against attacks, enhancing email security and training employees is crucial, especially when corporate account takeover (CATO) occurs and attackers gain access to business email accounts to initiate fraudulent transactions.[1] Warren Buffett described cybercrime as “humanity’s number one problem” and added that it “poses a real threat to humanity.” With the emergence of cybercrime, researchers have debated its exact definition and scope, and discussions continue to this day. Russian scholars V.A. Nomonkov and T.L. Tropina, in their studies, analyzed foreign annotated dictionaries describing the meaning of terms related to “cybercrime” and concluded that the term is broader than “computer crime.” According to them, “cybercrime is the set of any crimes committed in cyberspace, using or through computer systems or networks, or within the scope of computer systems and networks, including offenses against computer systems or networks.” Similarly, another group of Russian scholars, T.N. Sharipova and A.A. Sidorenko, consider the term “cybercrime” to encompass “any crime that can be committed using a computer system or network, within the scope of a computer system or network, or against a computer system or network.” Crimes can only be identified “after the fact.” Due to the large number of cybercrimes, it is practical to classify them and study them in certain groups. However, the types of cybercrimes are classified differently by various experts. For example, Kaspersky considers types such as email and internet fraud, personal data fraud (theft and misuse of personal information), theft of financial information or bank card data, corporate data theft and sale, cyberextortion, cryptojacking, and cyber espionage. They divide these into two groups: cybercrimes aimed directly at computers and cybercrimes carried out using computers. According to Tadviser, “…cybercrimes include spam, targeted phishing, PDF attacks, search engine optimization sabotage, and denial-of-service attacks.” A.Sevostyanov, head of the ITSkills project, along with authors M. Ryabukhin and R. Tyuchin, suggest that cybercrimes can include: financially motivated cybercrimes, privacy-related cybercrimes, copyright infringement-related crimes, socially and politically motivated cybercrimes, spam, cybercrimes related to incitement of hatred and harassment, terrorism, cyberbullying, illegal activities, illegal pornography, grooming, distribution of drugs and weapons. In this context, phishing, cyberextortion, and financial fraud are considered financially motivated cybercrimes. [2]

REFERENCES

1. https://root-nation.com/en/articles-en/tech-en/en-most-famous-hacker-attacks/ [1]
2. National and international standards for combating cybercrime. Tashkent–2018. N.S.Salayev, R.N.Ro`ziyev. [2]