CYBERCRIME AS AN ESSENTIAL IMPEDIMENT TO INTERNATIONAL TRADE[1]

Senior Research Fellow Radoslav BALTEZAREVIĆ
Institute of International Politics and Economics, Belgrade, Serbia
ORCID ID: 0000-0001-7162-3510

ABSTRACT

Cybercriminal behavior is a reflection of the many risks that came along with the introduction of new technology, which among other things greatly improved human lives and encouraged international trade and collaboration. Cybercrime encompasses a broad spectrum of illegal activities when computers and information technologies are utilized as the principal instrument or as the major object of interest. Due to the constant adaptations that cybercriminals make to existing security protocols and online behavior, the threat of cybercrime is only expected to increase. For users of digital platforms, they have the potential to inflict serious financial and emotional harm. Since the parties involved are typically located in different countries, investigating cyber fraud incidents is typically difficult without collaborating across borders. Many e-commerce businesses have been forced by this circumstance to focus on improving cyber security in order to protect both their business operations and the safety of their customers. Inadequate security measures can be costly and destroy customers' and businesses' trust when conducting online transactions. In this sense, inaction can harm an organization's reputation in the long run. Cybercrime's influence on domestic and global economies is calculated in a variety of methods, but all lead to the same conclusion: online crimes constitute a severe threat to international trade.

Keywords: New technology, International trade, Cybercrime, Cyber security

1. INTRODUCTION

The internet and the widespread use of technology have fundamentally altered how we work, live, communicate, travel, share information, and move money. Modern communications and technology are evolving quickly, which means that ideas about crime and criminality are also evolving to fit an online environment (Viano, 2017). The desire to launch a business is one of the reasons people utilize the internet, in addition to trading and gathering brand and entertainment-

[1] The paper presents findings of a study developed as a part of the research project "Serbia and challenges in international relations in 2024", financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2024.

related information (Kwiatek et al., 2021). The same technologies that have spurred business and economic expansion have also made the environment in which critical assets must be protected. The ease with which confidential information may now be stored, accessed, shared, and published, thanks to these modern technology, increases the possibility that a trade secret will be lost (Goverment of the United States, 2013).

Cybercriminals have the potential to seriously hurt digital users financially and emotionally. These actions turn into a significant issue that affects not just the states but also the general public and small and large business systems. Although there is a lot of discussion about this topic on a global scale, it seems that cybercriminals are constantly coming up with inventive ways to get around security measures and continue their illegal activity (Baltezarević & Baltezarević, 2021a). Cybercriminals come in all different kinds. They can be classified as state-sponsored actors, international cybercrime groups, or small-time scammers. Since hackers frequently target victims in several countries, cybercrime is a worldwide danger with local consequences. Cybercrime as a service has been more frequently offered by organized crime groups in recent years (Wilkinson, 2023). The primary benefit for cybercriminals employing such illicit cybermethods is that it keeps them anonymous in the online world (Baltezarević & Baltezarevic, 2023). Cybersecurity and international trade are becoming more and more entwined. International trade is changing as a result of the internet's global spread and the way that consumers and organizations use data flows globally for e-commerce, communication, and information access (Meltzer & Kerry, 2019).

Because cybercriminals are constantly adjusting to modern security measures and user behavior online, the threat of cybercrime is only going to increase. The reason why criminals are constantly one step ahead of security measures is because cybercrime is not given the proper attention it deserves (Eddolls, 2016). According to a report published by the Center for Strategic and International Studies (CSIS), cybercrime is a rapidly expanding sector that undermines innovation, trade, and competition (Reuters, 2014).

2. EFFECTS OF CYBERCRIME ON INTERNATIONAL TRADE

Cybercrime refers to a wide range of illegal activities, from electronic cracking to denial-of-service attacks, when computers or computer networks are utilized as a tool, a target, or a location for criminal conduct. It can also refer to more conventional crimes where the illegal action is made possible by the use of computers or networks (Das & Nayak, 2013). Any offense involving electronic communications or information systems can be classified as cybercrime (Tutorialspoint,

2024). The expression "cybercrime" is frequently used to refer to a variety of illegal actions involving the use of information and communication technology (ICTs). Other synonymous words like "computer crime," "virtual crime," "net-crime," and "hi-tech crime" are also frequently used (Wall, 2004).

Cybercrime includes offenses specific to computers and information systems, such as malware, denial of service attacks, and attacks against information systems, as well as traditional offenses like fraud, forgery, and identity theft. Content-related offenses include the online distribution of child pornography and the incitement of racial hatred (European Commission, 2013). Cybercrime is any illegal conduct where the target or instrument of the crime is a computer. It is classified by the US Department of Justice (DOJ) into three primary categories: a) Cyberattacks – use technology as a weapon; b) Network penetration - the act of attacking a computer or other device in an effort to enter a network without authorization; c) Computers are not the primary tool or target in crimes helped by computers, although they do play a crucial role (using a computer to store illegally downloaded files is one example) (Bluevoyant, 2022). Taking into account the broad definition of cybercrime, there are two primary categories into which it can be divided: technology as target (these are crimes involving the unlawful use of computers or mischief involving data that target computers and other information technologies), and technology as instrument (refers to criminal offenses, such as fraud, identity theft, intellectual property violations, money laundering, drug and human trafficking, organized crime, terrorism, child sexual exploitation, and cyberbullying, where the use of the Internet and information technologies is essential to the commission of the crime) (Royal Canadian Mounted Police, 2015). The primary benefit for cybercriminals employing such illicit cybermethods is that it keeps them anonymous in the online world (Baltezarević & Baltezarevic, 2023). As online grew, so did the phenomena of cybercrime, which expanded and intensified quickly (Evans & Scott, 2017).

The topic of cybercrime has not received enough attention and presents numerous challenges and issues (Griffin, 2012). Scholars claim that some forms of cybercrime go unreported because of things like small monetary loss and psychological or emotional distress resulting from a very sensitive crime. The fact that victims are unaware of where to report cybercrimes and how to do so correctly and efficiently could be another significant reason (Bidgoli & Grossklags, 2016). A few years ago, researchers examined data on cybercrime from multiple sources and calculated

that the annual damage to the world economy from cybercrime may reach up to €300 billion (McAfee & CSIS, 2014).

But each year, the harm caused by these kinds of behaviors gets worse. The cybersecurity market's "Estimated Cost of Cybercrime" global indicator was predicted to rise steadily by 5.7 trillion US dollars between 2023 and 2028 (Statista, 2023). Costs associated with cybercrime include data loss and damage, money stolen, lost productivity, intellectual property theft, financial and personal data theft, embezzlement, fraud, disruption of regular business operations following an attack, forensic investigation, data restoration and deletion, reputational damage, and more (Morgan, 2020). The study discovered that the largest economies in the world suffered the most from cybercrime, with losses to the US, China, Japan, and Germany totaling $200 billion annually (Reuters, 2014).

Inadequate cybersecurity may be expensive and erode organizations' and consumers' trust when it comes to conducting business online. Cross-border cooperation between the public and private sectors is necessary to safeguard confidence in the online environment since risks can affect individuals, companies, and governments operating on international networks (Meltzer & Kerry, 2019). Such behaviors can have long-term implications for those who are targeted, including anxiety, despair, low self-esteem, and suicidal ideation (Baltezarević et al., 2023). Economies frequently impose local data storage requirements or impose restrictions on cross-border data transfer in the name of cybersecurity or data protection. While some question data localization's efficacy in thwarting cybercrime, others view it as a valuable instrument that helps law enforcement authorities track down and apprehend offenders (Selby, 2017). Remittance is typically used to seek payments in cyberfraud cases since it is a quick method that gives victims little time to react or take action to halt the transactions. However, the victims will likely lose their best chance to hang onto their money if they don't take corrective action as soon as they learn of the possible fraud. They may also have to deal with a challenging and costly recovery process and risk suffering additional losses (Lexology, 2021). The financial industry has a long history of adhering to regulatory requirements for robust IT control settings and has been reliant on information technology for many years. Although the financial industry may be particularly vulnerable to cyberattacks, cybercriminals also face increased danger from these attacks due in part to increased attention from law enforcement (much like in the days of classic bank robberies).

Additionally, the financial industry supports law enforcement more effectively than other sectors do (Gaidosch, 2018).

Because the parties engaged in cyber fraud cases are frequently based in various nations or even different parts of the world, it is typically difficult to investigate these cases without cross-border collaboration. Cyber fraud cases typically arise in an international trade scenario. It is quite difficult to confirm the location of the scam and the identities of the perpetrators in this situation. Furthermore, recovery will be extremely difficult because the fraudsters typically move the monies as soon as they receive them (Clydeco, 2022). Traders may become victims of cybercrime either directly or indirectly. Hackers can go straight after traders by trying to access their trading accounts using passwords, from which they can move money across accounts, or they can go after the broker. The fact that brokers keep records of their clients' sensitive information can cause serious problems for those clients. Although no broker can ensure that traders won't fall prey to cyberattacks, there are a number of precautions that may be taken to increase protection when trading online. Beyond employing firewalls, anti-malware software, secure passwords, and private servers, there are further precautions that everyone accessing the internet should take to safeguard their data (Compare Forex Brokers, 2021). Cybercriminals have contributed to the decline of confidence among customers who have fulfilled their needs and desires through digital shopping by exploiting data and engaging in actions that have the potential to cause psychological and physical harm to internet users (Baltezarević & Baltezarević, 2021b).

3. CONCLUSION

Although the growth of the internet has benefited businesses and consumers everywhere, cybercrime is also becoming more and more of a threat to the health of international trade. Thankfully, corporations and governments are retaliating as they become more conscious of the dangers. Along with those efforts, the global cybersecurity business has emerged, one that is expected to grow significantly in the future.

Cybercrimes are transnational in nature, and it is difficult for developing economies to successfully respond to these threats due to weak regulatory frameworks, a lack of human capital, and limited financial resources. Given the likelihood that cybercrime will persist in the years to come, it would be beneficial to approach the threat it poses more broadly than simply as a law enforcement issue, with particular emphasis on how it could affect the stability of international relations. In order to establish a clear boundary of unacceptable activity in cyberspace and an

uncontested principle of nations' international responsibility, it is critical to make use of all available political-diplomatic resources. It can be expensive and have an effect on a company's client relationship to defend against cyberattacks. However, businesses will need to stay one step ahead of more sophisticated cybercriminals. Cybercriminal techniques used in international trade are always evolving and become more complex. Determining the veracity of pertinent information obtained from third parties can be a difficult task. While maintaining vigilance is crucial during business operations, it's also a good idea to enlist the help of outside experts (such as investigators, attorneys, or insurance providers) to reduce the likelihood of fraud, minimize losses, and, above all, increase the likelihood of recovery in the event of fraud.

REFERENCES

Baltezarević, R. & Baltezarević, I. (2021a). The Dangers and Threats that Digital Users Face in Cyberspace. IPSI *Transactions on Internet Research,* Vol. 17, No. 1, pp. 46-52.

Baltezarević, I. & Baltezarević, R. (2021b). Sajber bezbednost: izgradnja digitalnog poverenja, *Megatrend Revija*, Vol. 18 (4). pp. 269-280.

Baltezarević, R. & Baltezarevic, I. (2023). Terorizam u digitalnom okruženju. *Baština,* Vol. 33 sv. 60, pp. 173-181.

Baltezarević, V., Baltezarević, R. & Baltezarević, I. (2023). Sajber uznemiravanje dece sa posebnim osvrtom na digitalne igre, *Temida,* Volume 26, Issue 2, Pages: 261-284.

Bidgoli, M., & Grossklags, J. (2016). End user cybercrime reporting: what we know and what we can do to improve it. *Cybercrime and Computer Forensic (ICCCF)*, 1-6.

Bluevoyant (2022). Cybercrime: history, global impact, protective measures [2022]. Retrieved from: https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022 (Accessed: 22.01.2024).

Clydeco (2022). Cyber Fraud in International Trade – Precautionary Measures and Remedies. Retrieved from: https://www.clydeco.com/en/insights/2022/07/cyber-fraud-in-international-trade-precautionary-m (Accessed: 25.01.2024).

Compare Forex Brokers (2021). Preventing cybercrime in the world of forex trading. Retrieved from: https://www.itnews.com.au/feature/preventing-cybercrime-in-the-world-of-forex-trading-560555 (Accessed: 26.01.2024).

Das, S. & Nayak, T. (2013). Impact of cyber crime: issues and challenges, *International Journal of Engineering Sciences & Emerging Technologies.* vol. 6, no. 2, 142-153.

Gaidosch, T. (2018). The Industrialization of Cybercrime. Retrieved from: https://www.imf.org/en/Publications/fandd/issues/2018/06/global-cybercrime-industry-and-financial-sector-gaidosch (Accessed: 23.01.2024).

Goverment of the United States (2013). Administration Strategy on Mitigating the Theft of U.S. Trade Secrets Accessed January. Retrieved from: https://www.justice.gov/criminal-ccips/file/938321/download (Accessed: 24.01.2024).

Griffin, R. C. (2012). Cybercrime. *J. Int'l Com. L. & Tech*. 7(2)136.

Eddolls, M. (2016). Making cybercrime prevention the highest priority. Network Security, 5-8.

European Commission (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: , An Open, Safe and Secure Cyberspace, Brussels JOIN(2013) 1 final.

Evans, M., & Scott, P. (2017). Fraud and cyber crime are now the country's most common offences. Retrieved from Telegraph: https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ (Accessed: 26.01.2024).

Kwiatek, P., Papakonstantinidis, S., & Baltezarevic, R. (2021). Digital natives' entrepreneurial mindset: A comparative study in emerging markets. In: S. Rezaei, L. Jizhen, S. Ashourizadeh, V. Ramadani, & S.E. Gërguri-Rashiti, (Ed.). The Emerald Handbook of Women and Entrepreneurship in Developing Economies, Chapter 15. (pp. 295-316). Emerald Publishing Limited.

Lexology (2021). Cyber Fraud in International Trade - Precautions and Remedies. Retrieved from: https://www.lexology.com/library/detail.aspx?g=3778ec6b-0970-4ee6-991b-c1b05d402d3d (Accessed: 23.01.2024).

Meltzer, J. P. & Kerry, C. F. (2019). Cybersecurity and Digital Trade: Getting it Right. Washington, DC: The Brookings Institution.

McAfee & CSIS. (2014). Stopping Cybercrime can positively. Retrieved fromhttp://www.mcafee.com/uk/about/news/2014/q2/2014060 (Accessed: 25.01.2024).

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accessed: 26.01.2024).

Reuters, T. (2014). Cybercrime costs $445B US a year to global economy, report finds. Retrieved from: https://www.cbc.ca/news/business/cybercrime-costs-445b-us-a-year-to-global-economy-report-finds-1.2669356 (Accessed: 24.01.2024).

Royal Canadian Mounted Police. (2015). Royal Canadian Mounted Police cybercrime strategy.Retrieved from; from http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf (Accessed: 24.01.2024).

Selby, J. (2017). Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology*. 25 (3). pp. 213–232.

Statista (2023). Estimated cost of cybercrime worldwide 2017-2028. Retrieved from: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (Accessed: 24.01.2024).

Tutorialspoint (2024). Cyber Law & IT Act Overview. Retrieved from: https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm (Accessed: 26.01.2024).

Viano, E. C. (2017). Cybercrime, Organized Crime, and Societal Responses. Springer, Cham.

Wall, D. (2004). What are Cybercrimes? *Criminal Justice Matters*, 58(1), 20-21.

Wilkinson, I. (2023). What is the UN cybercrime treaty and why does it matter? Retrieved from: https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter (Accessed: 23.01.2024).