



INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 11, Issue 1 - V11I1-1366)

Available online at: <https://www.ijariit.com>

The Viability of the US Cybercrime Laws in Protecting Digital Trade Space: A Critique

Sultan Alaaya Adebayo

adebayosultanalaaya@gmail.com

American University, Washington College of Law, D.C., United States.

ABSTRACT

This paper critically examines the effectiveness and limitations of U.S. cybercrime laws in safeguarding the digital trade space. As the global economy increasingly relies on digital platforms, cybercrime poses a significant threat to online business operations, intellectual property, and personal data security. The study explores the key components of U.S. legislation, such as the Computer Fraud and Abuse Act (CFAA) and the Cybersecurity Information Sharing Act (CISA), assessing their scope, enforcement, and adaptability in responding to the ever-evolving nature of cyber threats. This critique highlights the gaps in current legal frameworks by analyzing case studies, legal challenges, and the intersection of cybercrime laws with international regulations. It offers recommendations for strengthening protections in the digital trade space. Ultimately, it seeks to provide insights into how U.S. policies can evolve to address the complexities of modern cyber threats better while balancing innovation, privacy, and global cooperation in digital commerce.

Keywords: U.S. Cybercrime Laws, Digital Trade, Cybersecurity, Computer Fraud and Abuse Act (CFAA) Cybersecurity Information Sharing Act (CISA), Digital Platforms.

INTRODUCTION

New and emerging technologies continue to transform the global economy and trade itself, giving rise to what is now commonly referred to as the digital trade space.ⁱ This encompasses all forms of trade facilitated through digital means, including e-commerce, digital services, and the transfer of digital goods.ⁱⁱ

Digital transformation of trading space has led to unprecedented reductions in the costs of engaging in international trade, changing how and what we trade, and contributing to growing competitiveness.ⁱⁱⁱ In 2020, digital trade represented around 25% of total trade of the world.^{iv} Nonetheless, with this transformation, has come an increase in cybercrimes that threaten the security and integrity of digital trade and its actors.^v

In a McKinley poll of US companies, it is reported that most executives consider[ed] digital manufacturing and design to be a critical driver of competitiveness.^{vi} However, these executives also reported feeling far from being able to capitalize on the economic potential of digital development due to a lack of industry standards and related cyber security concerns.^{vii}

Similarly, in 2021, experts estimated that cybercrimes cost the global economy \$6 trillion, a trend expected to continue annually.^{viii} This loss includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.^{ix}

Therefore, it is imperative that all actors in the trade space, including governments, businesses, and consumers, grapple with how to address this rapidly evolving, multifaceted problem specifically on the of robust legal frameworks to manage the space effectively. Thus, this paper tends to critically examine the effectiveness of the United States' cybercrime laws in protecting this vital sector of the economy.

OVERVIEW OF THE DIGITAL TRADE SPACE

While there is no single recognized and accepted definition of digital trade^x, there is a growing consensus that it encompasses digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, involving consumers, firms, and governments.^{xi} In other words, although digital technologies enable all forms of digital trade, not all digital trade is delivered digitally. For example, digital trade also encompasses digitally enabled but physically delivered transactions, such as buying a book through an online marketplace or booking an apartment stay through a matching application.^{xii}

Nonetheless, digital trade is characterized by the exchange of goods, services, and data via the internet and other digital networks, encompassing online retail, digital media, financial transactions, and various forms of digital content.^{xiii} The movement of data underpins digital trade. Data is not only a means of production but also an asset that can be traded and a means through which global value chains (GVCs) are organized and services delivered. It also supports physical trade less directly by enabling trade facilitation.^{xiv}

Additionally, data is at the core of new and rapidly growing service supply models such as cloud computing, the Internet of Things (IoT), and additive manufacturing.^{xv} The nature of digital trade transactions can occur across borders instantaneously, increasing efficiency but also exposing trade to new risks and vulnerabilities. This is further affirmed by the World Trade Organization (WTO) that digital trade has become a key driver of economic growth, yet it is also subject to diverse and evolving threats that require robust legal frameworks to manage effectively.^{xvi}

NATURE OF CYBER CRIMES IN DIGITAL TRADE SPACE IN THE UNITED STATE

Cyber-crimes are offenses committed by individuals or groups with criminal motives to intentionally inflict physical or mental harm on victims, either directly or indirectly.^{xvii} These crimes target individuals, groups, and organizations using telecommunication networks such as chat rooms, emails, notice boards, groups, and mobile phones for SMS/MMS.^{xviii} Common cyber-crimes include data breaches, identity theft, ransom ware attacks, online fraud, intellectual property theft, and cyber-espionage. These crimes significantly impact businesses that rely on online systems to deliver their goods and services.^{xix}

It is discovered that the largest economies in the world suffered the most from cybercrime, with losses to the US, China, Japan, and Germany totalling \$200 billion annually.^{xx} For instance, more than 40 per cent of the a cyber-security insights reports survey in respondents in the united states encountered authorized access to or hacking of an email or social media account.^{xxi}

Similarly, in 2021 alone, the FBI's Internet Crime Complaint Center (IC3) reported losses exceeding \$6.2 billion due to cybercrimes, with a significant portion impacting businesses engaged in digital trade.^{xxii} These crimes not only result in direct financial losses but also damage reputations and undermine consumer trust, which are critical in the digital economy.

OVERVIEW OF CYBERCRIME LAWS FOR THE PROTECTION OF THE DIGITAL TRADE SPACE IN THE UNITED STATES

The United States has established a number of frameworks of cybercrime laws aimed at safeguarding its digital trade space.^{xxiii} Key legislation such as the Computer Fraud and Abuse Act (CFAA) of 1986^{xxiv} the Cyber security Information Sharing Act (CISA) of 2015^{xxv} and the Federal Information Security Management Act (FISMA) of 2002 underpin the country's efforts to combat cybercrime.^{xxvi}

The Computer Fraud and Abuse Act (CFAA) of 1986 criminalize unauthorized access to computer systems and the theft or damage of data.^{xxvii} By so doing, it prohibits intentionally accessing a computer without authorization and obtaining information,^{xxviii} addresses fraud and related activities by prohibiting unauthorized access with the intent to defraud and obtain value whether in the form of money, property, or services^{xxix} and criminalizes actions that cause damage by transmitting harmful programs, information, codes, or commands.^{xxx}

The CFAA provides for a number of punishments for violations of its various prohibitions which subject to various criminal penalties of fines and imprisonment.^{xxxi} In the recent legal disputes, the CFAA was cited as a legal foundation to sue spammers, thus being appreciated as one of the most important, evolving, and expansive anti cybercrime statutes.^{xxxii}

Notwithstanding, it has faced criticism for its vague definitions, which can lead to overreach and misuse. It is argued that its broad language can be used to target legitimate security researchers and whistle-blowers.^{xxxiii} Furthermore, the penalties imposed by the CFAA can be disproportionately severe, deterring ethical hacking and cyber security research that could benefit the digital trade space^{xxxiv}.

Similarly, Cyber security Information Sharing Act (CISA) of 2015^{xxxv} facilitates the sharing of cyber security threat information between the federal government and private sector entities, liability protections for entities that share, and government oversight of the programs the Act establishes.^{xxxvi}

The main provisions of the Act make it easier for companies to share personal information with the government, especially in cases of cyber security threats.^{xxxvii} Without requiring such information sharing, the bill creates a system for federal agencies to receive threat information from private companies.^{xxxviii}

With respect to privacy, the Act includes provisions for preventing the sharing of personal data that is irrelevant to cyber security.^{xxxix} Any personal information that does not get removed during the sharing procedure can be used in a variety of ways. These shared cyber threat indicators can be used to prosecute cyber-crimes, but may also be used as evidence for crimes involving physical force.^{xl}

However, the Act provided that information-sharing framework is explicitly voluntary and the government cannot require an entity to provide information to the government or another third party and no liability exists “for choosing not to engage in the voluntary activities authorized in this title.”^{xli}

This Act has been criticized for potential privacy concerns. Although it includes provisions to prevent the sharing of irrelevant personal data, there are worries about the misuse of shared information and insufficient safeguards to protect individuals' privacy. Additionally, the voluntary nature of information sharing may result in inconsistent participation, limiting the effectiveness of the Act.^{xlii}

Moreover, the Federal Information Security Modernization Act of 2014 which modifies FISMA 2002 by making a number of changes to improve federal security practices in response to emerging security issues.^{xliii} These improvements result in less overall reporting, a stronger use of continuous monitoring in systems, a greater focus on agencies for compliance, and reporting that is more focused on security incident issues. FISMA 2014 also mandated that the Office of Management and Budget (OMB) amend/revise OMB Circular A130 to minimize inefficient and unnecessary reporting, as well as to reflect changes in the law and technological advancements.^{xliiv}

However, FISMA's focus on federal agencies means its impact is primarily on government systems, potentially leaving private sector entities less protected. While the updates in FISMA 2014 aimed to improve security practices, the Act still faces challenges in ensuring that all federal agencies consistently implement effective cyber security measures. Additionally, the focus on compliance and reporting can sometimes overshadow the need for proactive and adaptive security strategies.

Moreover, the Economic Espionage Act (EEA) of 1996 criminalized the theft of trade secrets by any method, including computer manipulation. Before the enactment of the EEA of 1996, corporate espionage was merely a violation of civil law. As a minimum threshold to operate criminal procedure, for a practical matter, federal district offices for the U.S. attorneys set \$100,000 in alleged losses involving the white collar crime.^{xliv} Pursuant to the EEA of 1996, corporate officials who know of spying by their employees and corporation itself may be criminally culpable separate from punishment imposed on the employees.^{xlvi}

While the EEA addresses the critical issue of trade secret theft, it may not fully account for the complexity and speed of modern cyber-espionage activities. This is because the threshold for prosecuting white-collar crimes can be a barrier to addressing smaller-scale but significant cyber thefts. Moreover, the Act's focus on criminal liability might not be sufficient to deter state-sponsored espionage activities that threaten economic interests.^{xlvii}

REGULATORY CHALLENGES OF THE DIGITAL TRADE SPACE AND US CYBERCRIME LAWS: A CRITIQUE

Despite the existence of comprehensive cybercrime laws in the United States, several regulatory challenges persist in protecting the digital trade space. One significant issue is the rapid evolution of technology, which often outpaces legislative updates. This lag makes it difficult to address emerging threats such as sophisticated ransom ware attacks and advanced persistent threats (APTs).^{xlviii}

Laws like the Electronic Communications Privacy Act (ECPA) are frequently criticized for being out-dated and insufficient in addressing modern privacy concerns. Simultaneously, the Computer Fraud and Abuse Act (CFAA) have faced critiques for potentially criminalizing benign activities and hindering legitimate cyber security research.^{xlix} Consequently, gaps in legal protections and enforcement capabilities can emerge, leaving the digital trade space vulnerable.¹

Also, the technical features of the internet enable criminals to operate anonymously, complicating the identification and prosecution of offenders in cyberspace.^{li} This anonymity coupled with the inherent difficulties in defining and determining political borders in cyberspace, presents multiple challenges in implementing cyber regulations effectively. Cybercriminals continuously adapt their techniques, making it increasingly difficult for governments and businesses to keep pace with these evolving threats.^{lii}

Similarly cybercrime often involves actors located in different countries, creating significant jurisdictional challenges for law enforcement.^{liii} The principle of state sovereignty, which underpins the current international order, implies that each nation-state has the authority to enact and enforce laws within its territorial limits. However, varying legal standards and enforcement capabilities across countries hinder the effective prosecution of transnational cybercriminals.^{liv}

Moreover, the complexity of cybercrime laws and the regulatory burden they impose can be daunting for businesses, particularly small and medium-sized enterprises (SMEs).^{lv} Ensuring compliance with multiple overlapping regulations is both challenging and costly. This regulatory complexity can strain the resources of SMEs, making them more vulnerable to cyber threats.^{lvi}

RECOMMENDATIONS AND CONCLUSION

To address the regulatory challenges facing the protection of the digital trade space under US cybercrime laws, several key recommendations are proposed. First, legislative reforms are essential. Regular updates to laws are needed to ensure they address modern privacy concerns and technological advancements. Additionally, the relevant legislations should be amended to distinguish between malicious activities and benign cyber security research, reducing the risk of criminalizing legitimate research efforts.

Also, efforts should be made to harmonize cybercrime laws and enforcement standards globally to facilitate more effective prosecution of transnational cybercriminals.

Improving mechanisms for international law enforcement cooperation, including information sharing and coordinated actions against cyber threats, is necessary for tackling the jurisdictional complexities inherent in cyberspace. Improving enforcement capabilities is another priority.^{lvii} Furthermore, increased funding and resources for law enforcement agencies are needed to enhance their ability to detect, investigate, and prosecute cybercrimes. Adopting advanced technologies, such as artificial intelligence and machine learning, can help law enforcement stay ahead of evolving cyber threats.¹ Support for small and medium-sized enterprises (SMEs) is vital in this effort. Simplifying compliance requirements can make it easier for SMEs to adhere to cybercrime laws without incurring prohibitive costs. Providing financial and technical assistance, such as grants, tax incentives, and technical support, will help SMEs strengthen their cyber security defences.

Moreover, promoting cyber security education and awareness is also essential. Developing and promoting training programs for law enforcement, legal professionals, and businesses will improve their understanding of cyber threats and the legal framework. Public awareness campaigns can educate individuals and businesses about best practices for cyber security and the importance of compliance with cybercrime laws.^{lviii}

By and large, the United States has established a robust framework of cybercrime laws to protect the digital trade space, but significant regulatory challenges remain. The rapid evolution of technology, jurisdictional complexities, and the need for continuous legislative updates highlight the dynamic nature of the cyber threat landscape. To enhance the effectiveness of these laws, legislative reforms, international cooperation, improved enforcement capabilities, and support for small and medium-sized enterprises (SMEs) are crucial. Additionally, promoting cyber security education and awareness will empower all stakeholders to better navigate and secure the digital trade environment. By addressing these challenges comprehensively, the United States can better safeguard its digital economy against the growing threat of cybercrime.

REFERENCES

- ⁱ Ezell S and Koester S., 'Transforming Global Trade and Development With Digital Technologies' (2023) available at: <https://itif.org/publications/2023/05/08/transforming-global-trade-and-development-with-digital-technologies/> accessed on 24 May 2024.
- ⁱⁱ Freehills, H S., 'Digital Trade – Definition' (2018) available at <https://globalaccesspartners.org/HSF-Digital-trade-definition.pdf> 1 accessed on 24 May 2024.
- ⁱⁱⁱ Organisation for Economic Co-operation and Development OECD (OECD), 'Digital Trade: Developing a Framework for Analysis (No. 205 OECD Trade Policy Papers, OECD Publishing, Paris). Available at: <https://dx.doi.org/10.1787/524c8c83-en> accessed on 24 May 2024
- ^{iv} Organisation for Economic Co-operation and Development OECD (OECD), 'Key issues in Digital Trade OECD Global Forum on Trade 2023 "Making Digital Trade Work for All (2023) available at: <https://www.oecd.org/trade/OECD-key-issues-in-digital-trade.pdf> 1 accessed on 24 May 2024
- ^v Chaisse J and Bauer c., 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' Vand. J. Ent. and Tech. Law, 551.
- ^{vi} Nanry, J et al., 'Digitizing the Value Chain, Mckinsey and Co' (March 2015) available at: <https://www.mckinsey.com/business-functions/operations/ourinsights/digitizing-the-value-chain> accessed on 24 May 2024
- ^{vii} *ibid*
- ^{viii} Chaisse J and Bauer c., 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' 552.
- ^{ix} Morgan S., 'Cybersecurity Ventures' (2017) 3 *Cybercrime Report* 549
- ^x Organisation for Economic Co-operation and Development OECD, 'Digital Trade' available at: <https://www.oecd.org/trade/topics/digital-trade/> accessed on 24 May 2024
- ^{xi} *ibid*
- ^{xii} Organisation for Economic Co-operation and Development (OECD), 'World Trade Organization and International Monetary Fund, 2020, Handbook on Measuring Digital Trade' available at <https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade.htm> accessed on 24 May 2024
- ^{xiii} Organisation for Economic Co-operation and Development OECD, 'Digital Trade' available at: <https://www.oecd.org/trade/topics/digital-trade/> accessed on 24 May 2024
- ^{xiv} Gonzalez L et al., 'Digital Trade: Developing a Framework for Analysis' available at: https://www.researchgate.net/publication/319667734_Digital_Trade_Developing_a_Framework_for_Analysis accessed 24 May 2024
- ^{xv} *ibid*
- ^{xvi} *ibid*
- ^{xvii} Goni O., 'The Basic Concept of Cyber Crime' (2022) *Journal of Technology Innovations and Energy*, 24. Available at: <https://doi.org/10.5281/zenodo.6499991> accessed on 24 May 2024
- ^{xviii} *ibid*

¹ Amoo O O., 'The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System' (2024) 21 (2) *World Journal of Advanced Research and Reviews*, , 205–217

- xix Kundi M H and Nawaz A., 'Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries' (2014) 4 (4) *Journal of Information Engineering and Applications*, 62
- xx Reuters, T., 'Cybercrime costs \$445B US a Year to Global Economy, Report Finds' (2014) available at: <https://www.cbc.ca/news/business/cybercrime-costs-445b-us-a-year-to-global-economy-report-finds-1.2669356> accessed 24 May 2024
- xxi The Norton Cyber Security., 'The Norton Cyber Security Insights Report Announces the Top 5 Cybercrimes in America' available at: <https://us.norton.com/blog/online-scams/top-5-cybercrimes-in-america-norton-cyber-security-insights-report> accessed on 24 May 2024
- xxii Federal Bureau of Investigation FBI, '2021 Internet Crime Report' (2021) available at: accessed
- xxiii Angle K J and McNicholas E R., 'Cyber security Laws and Regulations USA ' (2024) available at: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa> accessed on 24 May 2024
- xxiv 18 U.S.C. § 1030
- xxv (2015)
- xxvi Angle K J and McNicholas E R., 'Cyber Security Laws and Regulations USA ' (2024) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa>
- xxvii 18 U.S.C. § 1030
- xxviii Computer Fraud and Abuse Act (CFAA) of 1986, Section 1030 (a) (2)
- xxix *ibid*, Section 1030 (a) (4)
- xxx *ibid*, Section 1030 (a) (5)
- xxxi *ibid*, Section 1030(d)
- xxxii McQuade S C., *Understanding and Managing Cybercrime* (Pearson Ed. Inc. 2009) 312
- xxxiii Vilasenor J., 'Reining in overly broad interpretations of the Computer Fraud and Abuse Act' (2017) available at: <https://www.brookings.edu/articles/reining-in-overly-broad-interpretations-of-the-computer-fraud-and-abuse-act/> accessed on 25 May 2024
- xxxiv Dizon, M., *Breaking and Remaking Law and Technology: A Socio-Techno-Legal Study of Hacking* (Doctoral Thesis, Tilburg University)
- xxxv Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242
- xxxvi Cyber security Information Sharing Act (CISA) 2015, Section 103
- xxxvii *ibid*, Section 104
- xxxviii Mitchell K., 'The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress' (2014) *Harvard Law School National Security Journal*, 67.
- xxxix Andy G, 'CISA Security Bill: An F for Security But an A+ for Spying' (2015)
- xl *ibid*
- xli Cyber security Information Sharing Act (CISA) 2015, Section 108
- xlii Greene R., 'Cybersecurity Information Sharing Act of 2015 Is Cyber-Surveillance, Not Cybersecurity' (2015) available at: <https://www.newamerica.org/oti/blog/cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/> accessed 25 May 2024
- xliii Khan N and Gulati S., International Legislative Framework Of Cybercrimes- A Comparative Study Of India, Israel, And USA' (2023) 7 (1) *Journal of Positive School Psychology*, 782-800. Available at: <http://journalppw.com> accessed on 25 May 2024
- xliv Available at: <https://csrc.nist.gov/projects/riskmanagement/fisma-background> accessed on 25 May 2024
- xlv 8 U.S.C. § 1831
- xlvi 18 U.S.C. 1832 (b)
- xlvii Congressional Research Service, 'Data Protection Law: An Overview' (2019) <https://crsreports.congress.gov/product/pdf/R/R45631> accessed on 25 May 2024
- xlviii Beaman, C et al., 'Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions' (2021) *Computers & Security* 111 Available at: https://www.researchgate.net/publication/354866035_Ransomware_Recent_Advances_Analysis_Challenges_and_Future_Research_Directions accessed 25 May 2024
- xlix Electronic Frontier Foundation. "Reform the CFAA." EFF, 2021.
- ¹ U.S. Department of Justice. "Challenges in Cybercrime Investigations." DOJ, 2020.
- ^{li} Pont, G. F., 'The Criminalization of True Anonymity in Cyberspace' (2001) 7 (1) *Michigan Telecommunications and Technology Law Review*, 191-216. Available at: <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1142&context=mttlr> accessed on 25 May 2024
- ^{lii} Ajoy P.B., 'Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis Scholars International' (2022) 5 (2) *Journal of Law, Crime and Justice* 74-79
- ^{liii} Oraegbunam, I K E., 'Jurisdictional Challenges In Fighting Cybercrimes: Any Panacea from International Law' (2015) *NAUJILJ*, 57-65
- ^{liv} 3S Deb, 'What Makes Cybercrime Laws So Difficult to Enforce' (January 2014) Available at: accessed on July 24,2014
- ^{lv} Steve, V W et al., 'Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands' (2021) available at: https://www.researchgate.net/publication/351298991_Cybercrime_Reporting_Behaviors_Among_Small-and-Medium-Sized_Enterprises_in_the_Netherlands accessed 26 May 2024

^{lvi} Kianpour, M. and Raza, S., ‘More than Malware: Unmasking the Hidden risk of Cyber Security Regulations’ (2024) *5 Inter. Cybersecur. Law Review* available at: <https://doi.org/10.1365/s43439-024-00111-7> accessed 26 May 2024

^{lvii} Cerezo A I et al., *International Cooperation to Fight Transnational Cybercrime* (Centre for Applied Research in Information Systems School of Computing and Information Systems Kingston University, Kingston upon Thames, Surrey, United Kingdom 2007) 13

^{lviii} Kortjan, N., ‘ A Cyber Security Awareness and Education Framework for South Africa’ (2013) available at : <https://core.ac.uk/download/pdf/145053774.pdf> accessed 26 May 2024.