Anno 23

ISSN 2039-6880

IL NUOVO DIRITTO DELLE SOCIETÀ

diretto da **Oreste Cagnasso e Maurizio Irrera**

Corporate governance, Sustainability, Risk Management and Reporting

8-25

In questo numero:

IUSTITIAM COLIMUS

G. Giappichelli Editore

IL NUOVO DIRITTO DELLE SOCIETÀ

diretto da Oreste Cagnasso e Maurizio Irrera

Corporate governance, Sustainability,
Risk Management and Reporting

8-2025

IL NUOVO DIRITTO DELLE SOCIETÀ

In questo numero:

G. Giappichelli Editore

IL NUOVO DIRITTO DELLE SOCIETÀ
Mensile - Iscrizione al R.O.C. n. 25223
Registrazione al Tribunale di Milano 8 novembre 2002, n. 618

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISSN 2039-6880

NDS collabora con RES Centro Studi d'Impresa, Via Crisis

Indice

Diritto dell'impresa

a cura di Oreste Cagnasso e Maurizio Irrera

Focus sull'Asia e i sistemi giuridici asiatici

a cura di Gyooho Lee

Segnalazioni

Contents

Company Law

edited by Oreste Cagnasso and Maurizio Irrera

Focus on Asia and Asian Legal Systems

by Gyooho Lee

News

Cybercorruption in Corporate Governance as a Challenge to Economic Security: Comparative Analysis of Legal Countermeasures in Leading Asian Countries as Instructive Experience for Uzbekistan

Cybercorruzione nella corporate governance come sfida alla sicurezza economica: analisi comparativa delle contromisure legali nei principali paesi asiatici come esperienza istruttiva per l'Uzbekistan

Said Gulyamov[*]

ABSTRACT

The paper discusses the rise of cybercorruption in corporate governance and its implications for economic security. It develops a comprehensive definition of cybercorruption in the corporate context and then describes ten discrete categories of illicit activity from the digital falsification of financial records to cyber-enabled money laundering. This paper examines the legal countermeasures against cybercorruption in Japan, South Korea, Singapore, and China according to their regulatory approach, enforcement mechanisms, and strategies for prevention. Based on a doctrinal legal research methodology and comparative legal research analysis, this paper examines the adequacy of different legal frameworks and their respective strategies regarding enforcement in the said countries. Later, the paper discusses the evolving cybersecurity

[*] Doctor of Law, Professor, Head of the Department of Cyber Law, Tashkent State University of Law, Tashkent, Uzbekistan, ORCID: orcid.org, e-mail: said.gulyamov1976@gmail.com.

and corporate landscape of Uzbekistan, pointing out gaps that could be filled and areas where there is room for improvement. Drawing from selected best practice examples in the reviewed Asian jurisdictions, the study makes country-specific recommendations with a view to strengthening the legal framework for Uzbekistan to address cybercorruption in corporate governance. These findings are expected to inform policy and corporate measures to help create an enabling cybersecurity environment in line with the context and path of development in Uzbekistan. The findings add to the growing literature on cybersecurity in corporate governance, thus carrying practical implications for emerging economies facing similar challenges.

Il saggio discute l'aumento della cybercorruzione nella governance aziendale e le sue implicazioni per la sicurezza economica. Elabora una definizione completa di cybercorruzione in ambito aziendale e descrive dieci diverse categorie di attività illecite, dalla falsificazione digitale dei registri finanziari al riciclaggio di denaro tramite mezzi informatici.

Il documento esamina le contromisure legali contro la cybercorruzione in Giappone, Corea del Sud, Singapore e Cina, analizzandone l'approccio normativo, i meccanismi di applicazione e le strategie di prevenzione. Basandosi su una metodologia di ricerca legale dottrinale e sull'analisi comparata del diritto, il saggio valuta l'adeguatezza dei diversi quadri normativi e delle rispettive strategie di applicazione nei Paesi in questione.

Successivamente, il saggio analizza l'evoluzione del panorama della cybersicurezza e dell'ambiente aziendale in Uzbekistan, evidenziando le lacune da colmare e le aree di miglioramento. Attingendo a una selezione di esempi di buone pratiche nelle giurisdizioni asiatiche esaminate, lo studio formula raccomandazioni specifiche per il Paese, al fine di rafforzare il quadro giuridico uzbeko per affrontare la cybercorruzione nella governance aziendale.

Si prevede che i risultati forniranno spunti per politiche e misure aziendali utili a creare un ambiente di cybersicurezza favorevole, in linea con il contesto e il percorso di sviluppo dell'Uzbekistan. I risultati contribuiscono alla crescente letteratura sulla cybersicurezza nella governance aziendale, portando implicazioni pratiche per le economie emergenti che affrontano sfide simili.

SUMMARY:

1. Introduction

The digital transition of corporate operations has brought new opportunities for efficiency and innovation. However, it also creates new forms of corruption that take advantage of the vulnerabilities of connected systems. The very potential economic consequences of cybercorruption came as a sudden awake-up call when the ransomware attack against Colonial Pipeline in 2021 paralysed fuel supplies across the southeastern United States in 2021. [1]

An interesting evolution of cybercorruption in corporate governance can be traced through seminal works in the field. Early work, such as Carr's 2003 article "IT Doesn't Matter," was skeptical of the strategic relevance of information technology in the corporate world. [2] More recent literature, such as Shackelford's "Governing the Internet of Everything," elucidates quite clearly the critical role of cybersecurity in modern corporate governance. [3] This indicates a shift in perspective driven by the sophistication of cyber threats and their threat to undermine corporate stability and economic security.

In the context of Uzbekistan, the government's "Digital Uzbekistan 2030" [4] strategy underscores the country's commitment to rapid digitalization. While this initiative promises significant economic benefits, it also exposes Uzbek corporations to heightened cybersecurity risks. The country's transition from a

[1] This incident, along with a few other highly publicized hacks-for-hire, like the 2020 Twitter bitcoin scam, epitomizes the threat of cybercorruption to economic security and corporate integrity. 2021 Colonial Pipeline Ransomware Attack. www.hsdl.org.

[2] N.G. Carr, *IT doesn't matter*, in *Harvard Business Review*, 2003, 81(5), pp. 41-49. hbr.org.

[3] S.J. Shackelford, *Governing the Internet of everything*, in *Cardozo Arts & Entertainment Law Journal*, 2014, 32(3), pp. 701-752. papers.ssrn.com.

[4] The Digital Uzbekistan 2030 strategy, adopted in October 2020, has set the course for the development of five priority areas in the country: digital infrastructure, digital economy, e-government, the national IT sector and IT education. The strategy has already contributed significantly to the development of e-government services and improved access to digital infrastructure across the country. Government of Uzbekistan. (2020). Digital Uzbekistan 2030 strategy. Retrieved from lex.uz.

centrally planned economy to a market-oriented system, coupled with its emerging digital infrastructure, creates unique vulnerabilities to cybercorruption that demand careful consideration and proactive measures.

The importance of learning from Asian countries in addressing cybercorruption cannot be overstated. As Yu argues in "A Tale of Two Development Models: East Asia Versus Latin America," the success of East Asian economies in technological advancement and governance reform offers valuable lessons for developing nations. [5] The experiences of Japan, South Korea, Singapore, and China in combating cyber corruption provide a rich tapestry of regulatory approaches and enforcement strategies that might inform the efforts of Uzbekistan to strengthen its cybersecurity framework.

This article aims to address several key research questions:

1. How can cybercorruption in corporate governance be defined and categorized?

2. What are the major legal counter-measures of leading Asian countries against cybercorruption in a corporate environment?

3. What lessons might the Uzbekistan state draw from these Asian countries to build a legal mechanism in fighting cyber corruption?

2. Methodology

The methodological approach adopted in this study is multi-faceted in analyzing the complex phenomenon of cybercorruption in corporate governance and evaluating legal countermeasures across different jurisdictions.

Hence, this study is premised on doctrinal legal research, which enables a structured approach to analyzing the primary legal sources relating to cybercorruption and corporate governance. Drawing from Hutchinson's doctrinal research approach, we consider the legislation, case law, and regulatory guidelines in the selected Asian countries to identify the main legal principles and their application in practice, as indicated. [6] In this way, one is able to develop an in-depth appreciation of the legal systems that regulate cybercorruption in corporate environments.

---

[5] P.K. YU, *A tale of two development models: East Asia versus Latin America. In Intellectual Property, Trade and Development: Strategies to Optimize Economic Development in a TRIPS-Plus Era*, Oxford, 2011, pp. 153-188, scholar.google.com.

[6] T. HUTCHINSON, *Researching and writing in law*, in *Thomson Reuters*, 2010. store.thomsonreuters.com.au.

We adopt a comparative legal analysis to juxtapose the various approaches of Japan, South Korea, Singapore, and China in the fight against cybercorruption. Based on the methodological insights of Zweigert and Kötz, we compare these legal systems, considering not only their formal rules but also their functional equivalents and socio-legal contexts. [7] This allows an insightful comparison of common trends and distinctive features of each country's efforts in fighting cybercorruption.

The typology development in cybercorruption relies on the conceptual analysis techniques. The conceptual analysis in social research guided by Neuman's framework systematic investigation of literature and legal definition to construct a comprehensive typology of cyber corruption in corporate governance. [8] This ensures our categorization to be theoretically sound and practically relevant.

The systematic literature review synthesizes knowledge on cybercorruption and identifies the gaps in current research. [9] Based on the recommendations of Okoli regarding the guidelines for a systematic review of information systems research, we critically review academic articles, policy reports, and industry publications so as to establish a sound theoretical basis for our analysis. [10]

Finally, techniques of legal interpretation are used to investigate the intent and effectiveness of the relevant laws and regulations. By adopting the principles of purposive interpretation expounded by Barak, we look at not only the letter but also the underlying aims or goals of the law and its societal context. [11] This type of interpretation, of course, furthers an in-depth understanding of how legal mechanisms address the emerging challenges related to cybercorruption at the corporate governance level.

---

[7] K. ZWEIGERT-H. KÖTZ, *An introduction to comparative law*, III ed., Oxford, 1998, www.cambridge.org.

[8] W.L. NEUMAN, *Social research methods: Qualitative and quantitative approaches*, VII ed., London, 2014, books.google.com.

[9] S.S. GULYAMOV, *International Cyber Peacekeeping: Concept and Legal Regulation*, Saarbrücken, 2023.

[10] C. OKOLI, *A guide to conducting a standalone systematic literature review*, in *Communications of the Association for Information Systems*, 37, 2015, pp. 879-910. aisel.aisnet.org.

[11] A. BARAK, *Purposive interpretation in law*, Princeton University, 2005. press.princeton.edu.

3. Results: Reconceptualising Cybercorruption in Corporate Governance

3.1. Definition of Cyber Corruption within Corporate Governance

The conceptualization of cyber corruption in corporate governance calls for deep insight into both cybercrime and corruption within the digital corporate ecosystem. Corruption is broadly defined by the United Nations Convention against Corruption, 2004, as the abuse of power entrusted for private gain (as implied in Article 19). [12] This is further complemented by the Convention on Cybercrime, 2001, drafted by the Council of Europe, which lays down a framework with which to understand offenses against the confidentiality, integrity, and availability of computer data and systems. [13] The common denominator of these ideas in the corporate world gives way to a particular kind of malfeasance that takes advantage of digital vulnerabilities for illicit purposes.

The ever-evolving face of cyber threats in organizational contexts, as assessed by Choo, presents that any comprehension of cybercorruption has to be dynamic by nature. [14] Ghosh further extends this discourse by discussing the cybersecurity threats to corporate governance structures in the digital age. [15] These scholarly standpoints highlight the multidimensional nature of cybercorruption, whereby such entities go beyond a simple technical breach in manipulating the corporate digital system for an individual or organizational gain.

In the light of these considerations, taking into account specific peculiarities provided by the digital corporate environment, we can suggest the following substantially extended definition of cybercorruption in corporate governance:

Cybercorruption within corporate governance involves the intentional act of

[12] United Nations Office on Drugs and Crime, United Nations convention against corruption, United Nations, 2004. www.unodc.org.

[13] Council of Europe, Convention on cybercrime. Council of Europe, 2001. www.coe.int.

[14] According to Choo, cybercorruption is a dynamic and constantly evolving form of corruption that exploits digital vulnerabilities in organizational systems for illicit gain. On the matter of cyber threats, he conceptualizes them as something that "continuously evolves to take advantage of the vulnerabilities within information systems to cause malicious intent on the systems", K.K.R. CHOO, *The cyber threat landscape: Challenges and future research directions*, in *Computers & Security*, 30(8), 2011, pp. 719-731. www.sciencedirect.com.

[15] Ghosh defines cybercorruption according to source, as "the exploitation of IT infrastructures and governance processes for corrupt purposes within corporate environments". Against the backdrop of cyber threats, which are constantly in evolution, he addresses a holistic IT security management. A.K. GHOSH, *Guidelines for the management of IT security. In Information Assurance*, London, 2014, pp. 1-11.

using digital systems, networks, or even data within a corporate entity to attain the ultimate goals of thwarting established mechanisms of governance, manipulating processes of decision making, or embezzling resources for personal or organizational benefit within corporate operations.

Thus, the definition of cybercorruption encompasses a combination of both technological and governance aspects of cybercorruption, as described in the OECD Corporate Governance Principles 2015 regarding integrity in corporate information systems. [16] This provides a wider overview of the identification and carrying out of analyses of different forms of cybercorruptions within a corporate setting through system exploitants who subvert governance and misappropriate resources as basic means.

3.2. Types of cybercorruption

3.2.1. Digital manipulation of financial records

Computer-mediated tampering in corporate governance involves unauthorized modification, manipulation, or destruction of financial records in electronic form with the view to misrepresent the financial position or performance of an organization. Such a form of cybercorruption goes directly against the principles in charge of presenting and making representative fair financial reporting promulgated within IFRS. [17]

Technically, it could be the use of high-level schemes involving data manipulation, making fictitious entries, and manipulating audit trails. [18]

This has deep implications for corporate governance, as digital manipulation destroys the base of transparency and accountability. The OECD Principles of Corporate Governance 2015 demonstrate an increased focus on the importance of accurate financial reporting to investor confidence and market integrity.

[16] OECD. (2015). G20/OECD principles of corporate governance. OECD Publishing. www.oecd.org.

[17] International Financial Reporting Standards Foundation. (2021). IFRS standards. IFRS Foundation. www.ifrs.org.

[18] Work by Singleton on fraud auditing and forensic accounting gives an idea of the modes of manipulations generally used; these include system vulnerability exploitation and fictitious transaction creations. Romney and Steinbart state that the growing complexity of accounting information systems on the one hand, has opened new possibilities for financial manipulation but probably provides new solutions with more effective control mechanisms too; T.W. SINGLETON-A.J. SINGLETON, *Fraud auditing and forensic accounting*, IV ed., Hoboken, 2010, onlinelibrary.wiley.com; M.B. ROMNEY-P.J. STEINBART, *Accounting information systems*, XIV ed., London, 2018, books.google.com.

Board members and executives carry a big responsibility for making sure of the integrity of digital financial records; this, in part, is something expressed by legislation such as the Sarbanes-Oxley Act of 2002 within the United States. [19]

The Wirecard scandal in 2020 was a perfect example of how really bad and destructive digital manipulation of finance could be. [20]

3.2.2. Cyber-enabled insider trading

Insider trading enabled by cyber means represents a technologically advanced version of the traditional violation under securities law. The U.S. Securities Exchange Act of 1934 explains that trading based on material, non-public information in violation of a fiduciary duty constitutes insider trading. [21] Thus, the cyber aspect adds layers of complexity to both the ways such illicit activities are executed and to their detection.

Analysis by Bharara and Copeland on "Insider Trading 2.0" throws light on the sophisticated ways insider trading is conducted with the use of cyberspace. [22] This may involve hacking into corporate networks for confidential information, deploying algorithms in high-frequency trading based on data theft, or even exploiting vulnerabilities within systems related to the transmission of financial data. Most of these methods are so technologically sophisticated that they continue to outrun conventional regulatory and compliance mechanisms.

This has big implications for corporate governance with respect to fair disclosure and integrity of the market. This practice is squarely in conflict with the emphasis the CFA Institute's Code of Ethics and Standards of Professional Conduct places on maintaining market fairness-a notion these days increasingly hard to uphold against cyber-enabled insider trading. [23] Corporate boards henceforth

---

[19] United States Congress. (2002). Sarbanes-Oxley Act of 2002. U.S. Government Publishing Office. www.congress.gov.

[20] The scheme of the German payment processor included faking electronic records and opening fictitious bank accounts, bringing down a €1.9 billion accounting fraud that brought down the company and sent shock waves through the global financial system; D. McCrum-O. Storbeck, *Wirecard's €1.9bn never entered Philippine financial system, bank governor says*, in *Financial Times*, 2020, June 18. www.ft.com.

[21] United States Congress. (1934). Securities Exchange Act of 1934. U.S. Government Publishing Office. www.law.cornell.edu.

[22] P. Bharara-R.A. Copeland, *Insider trading 2.0: When technology, social media, and the SEC collide*, in *New York University Journal of Law and Business*, 11(4), 2013, pp. 759-792. corpgov.law.harvard.edu.

[23] CFA Institute. (2014). Code of ethics and standards of professional conduct. CFA Institute. www.cfainstitute.org.

have twin issues of protection of sensitive information and detection of anomalous trading patterns that may indicate cyber-facilitated insider activities.

A striking example is the 2015 case of hackers stealing corporate press releases before their public dissemination allowed an unprecedented insider trading scheme with more than $100 million in profits resulting from illegal activity. [24]

3.2.3. Electronic voting fraud in shareholder meetings

Fraud in e-voting within the process of shareholder meetings is a serious threat to corporate democracy and integrity in governance. The Revision to the Model Business Corporation Act sets basic rights to shareholders to vote on corporation matters, which are increasingly done electronically. [25] Digitalization opened up channels for perils and risks to the shareholder decision-making processes.

Man-in-middle attacks, server manipulation and the impersonation of a voter are some of the technical modes of e-voting fraud. The integrity, confidentiality, and availability of e-voting platforms present an enormously difficult task even in a corporate environment according to a comprehensive study by Gritzalis. [26] Because of these technical deficiencies, a vote count may be altered or a lawful vote may be repressed or phantom votes may be padded and thus defeat the shareholder's will.

The implications will be far-reaching for corporate governance, as it influences shareholder rights and the principles of equitable treatment contained in the G20/OECD Principles of Corporate Governance. Fraud in electronic voting undermines basic mechanisms of corporate accountability and may lead to decisions not being reflective of the true interests of the shareholders.

While incidences of fraud in electronic voting at the corporate level are few and far between, the very prospect of such vote tampering does have people unduly worried. For instance, a disputed board election could be manipulated by rogue operators at the e-voting interface with the result being a change in the strategic control of the corporation and a loss of investor confidence.

---

[24] This case has given an example of how far back the digital information supply chain vulnerability has to be traced and also cybersecurity enhancements in corporate communications are required. United States Department of Justice. (2015). Nine people charged in largest known computer hacking and securities fraud scheme. Retrieved from www.justice.gov.

[25] American Bar Association. (2016). Model Business Corporation Act. American Bar Association. www.americanbar.org.

[26] D.A. GRITZALIS, *Principles and requirements for a secure e-voting system*, in *Computers & Security*, 21(6), 2002, pp. 539-556. www.sciencedirect.com.

3.2.4. Crypto-cyberbribery

Cyberbribery in cryptocurrencies is a new form of corruption that leverages anonymity and the decentralized nature of digital currencies in facilitating illicit payments in corporate settings. The United Nations Convention against Corruption broadly defined bribery as an act of offering, giving, receiving, or soliciting any item of value as consideration for an improper advantage relating to discharge of a public or legal duty (as outlined in Articles 15, 16, and 21). All that said, cryptocurrency adds another layer to this definition: new ways to transfer value that can elude conventional oversight mechanisms in finance.

The very nature of a cryptocurrency-based bribe exploits the features of blockchain: its pseudonymity and decentralized control. Research into Bitcoin transactional behavior by Meiklejohn et al. emphasizes the challenge in tracing and attributing cryptocurrency payments, making them an excellent tool for corrupt practices. [27] In conjunction with services relating to cryptocurrency mixing and the development of privacy-centric cryptocurrencies, detection and prevention of cyberbribery become even more complicated.

In the context of corporate governance, it is a new challenge to traditional anti-bribery and corruption compliance programs. The U.S. Foreign Corrupt Practices Act (FCPA) Resource Guide, while very substantive in its approach to combating bribery, also needs adaptation to such specifics of cryptocurrency-facilitated corruption. [28] Corporate boards and compliance officers now face the additional question of how they might monitor and regulate cryptocurrency transactions through their organizations to ensure the organization does not use cryptocurrencies in any bribery schemes.

A hypothetical example of this form of cybercorruption could be a corporation engaging in a range of cryptocurrency transactions as bribes to foreign officials for favorable treatment in contract bidding, using the untraceable nature of those payments to avoid detection by internal controls and external auditors.

3.2.5. Data theft and extortion

Data theft and extortion in a corporate setting involve unauthorized access, exfiltration, and leveraging of sensitive corporate information for financial or

---

[27] S. Meiklejohn-M. Pomarole-G. Jordan-K. Levchenko-D. McCoy-G.M. Voelker-S. Savage, *A fistful of bitcoins: Characterizing payments among men with no names*, in *Proceedings of the 2013 Conference on Internet Measurement*, 2013, pp. 127-140, ACM. dl.acm.org.

[28] United States Department of Justice & Securities and Exchange Commission. (2020). FCPA: A resource guide to the U.S. Foreign Corrupt Practices Act (II ed.). U.S. Department of Justice. www.justice.gov.

competitive gain. [29] The offenses are based on the legal frameworks that emanate from the Council of Europe's Convention on Cybercrime dated 2001 and the EU's General Data Protection Regulation (2016), [30] where there is an essence of confidentiality, integrity, and availability of data.

Technically, data theft involves various means of sophisticated cyber attack techniques, including phishing, malware injection, and exploiting insider access to information. Verizon Data Breach Investigations Report (2021) mentions these as the most common approaches to corporate data breaches, indicating a sharp increase in ransomware attacks against corporate data. [31] This sort of stolen data is usually used to extort money by threatening to make the information public or selling it to competitors.

The impact on corporate governance is huge, putting additional stress on organizations' data protection obligations and crisis management. Frameworks such as the 2018 NIST Cybersecurity Framework [32] and ISO/IEC 27001 for Information Security Management [33] provide advice to organizations on how to guard against and respond in the case of data theft and attempts at extortion. Huge responsibilities lie with the corporate boards in data security measures and response strategy formulation against the threats of extortion.

One of the most high-profile cases of theft of corporate data and ransom is the 2014 Sony Pictures hack. [34]

3.2.6. Algorithm manipulation for personal gain

Algorithm manipulation for personal gain in corporate contexts refers to the intentional modification or use of automated decision-making systems in order

[29] S.S. GULYAMOV-O.T. KHAZRATKULOV, *Digital Future & Cyber Security Necessity*, in *World Bulletin of Management and Law*, 10, 2022, pp. 31-45.

[30] European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union. eur-lex.europa.eu.

[31] VERIZON. (2021). 2021 Data breach investigations report. Verizon. www.researchgate.net.

[32] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. www.nist.gov.

[33] International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. ISO. www.iso.org.

[34] These hackers, said to be state-sponsored, stole massive volumes of sensitive data, including unreleased movies and executives' emails, with threats to publish them unless their demands were fulfilled. In this case, stolen data could seriously affect someone's reputation and cause a financial loss, which emphasized the importance of cybersecurity measures but also incident response in corporate settings; M. CIEPLY-B. BARNES, *Sony Pictures hack fuels speculation about studio's possible targets*, in *The New York Times*, 2014, December 3; www.nytimes.com.

to realize outcomes favorable to one or more persons or groups to the detriment of a corporation or its shareholders. In a critical analysis of algorithmic regulation, Yeung discussed the increasing strategic role of algorithmic systems in corporate governance and the potential for their misuse. [35]

Algorithm manipulation-technically speaking-can be an advanced practice, incorporating adversarial machine learning, data poisoning, among other practices. [36] The consequences for corporate governance are that the integrity of algorithmic decision-making systems becomes material for fairness and efficiency in corporate operations. The EU's Ethics Guidelines for Trustworthy AI [37] (2019) provide a well-known framework for the ethical development and deployment of AI systems with human oversight and accountability. The most difficult role of corporate boards involves the integrity and transparency of these increasingly complex systems.

This is not a very common scenario when high-profile cases of algorithmic manipulation for personal gains are concerned in corporate settings, but a hypothetical case could be like when a senior executive makes some slight changes in the parameters of an algorithmic trading system in his or her favor to favor his or her personal portfolio investment; exploiting insider knowledge of its operation to generate illicit profits at the expense of the company or the rest of the shareholders.

3.2.7. Cyber-enabled procurement fraud

Cyber-enabled procurement fraud in corporate governance involves the manipulation of contract awards, inflation of prices, or diversion of funds for personal benefit through exploitation of digital systems and processes at any point in the procurement cycle. The ACFE realizes that procurement fraud tends to pose one of the major risks within a corporate setting; digital technologies introduce new vectors for this kind of misconduct. [38]

---

[35] K. YEUNG, *Algorithmic regulation: A critical interrogation*, in *Regulation & Governance*, 12(4), 2018, pp. 505-523. onlinelibrary.wiley.com.

[36] Security vulnerabilities of machine learning systems were demonstrated in the work of Barreno et al., who showed how several of these systems are vulnerable to malicious inputs intended to skew their outputs. In an organizational context, this might include everything from financial forecast algorithms to risk assessment and resource allocation. M. BARRENO-B. NELSON-R. SEARS-A.D. JOSEPH-J.D. TYGAR, *Can machine learning be secure?*, in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, 2006, pp. 16-25, ACM. dl.acm.org.

[37] European Commission. (2019). Ethics guidelines for trustworthy AI. European Commission. digital-strategy.ec.europa.eu.

[38] Association of Certified Fraud Examiners. (2020). Report to the nations: 2020 global study on occupational fraud and abuse. ACFE. legacy.acfe.com.

Technically, cyber-enabled procurement fraud might take various sophisticated forms: manipulation of e-bidding systems, creation of phantom vendors in digital supplier databases, and tampering with electronic invoices. Although not procurement fraud per se, the supply chain attack on SolarWinds in 2020 exemplified how vulnerabilities in digital supply chain systems could be exploited for fraudulent purposes. [39]

Thus, the implications for corporate governance go far, as validity of supply chains and financial controls are put into question. The COSO Internal Control – Integrated Framework (2013) emphasized that any procurement process should be underpinned with a robust mechanism of control, now extended to digital systems and cyber risks. [40] Corporate boards should be responsible for the implementation of secure digital procurement processes and measures to prevent fraud.

An example of actual-life cyber-enabled procurement fraud might consist of hacking with insider collusion whereby hackers can fiddle with an e-bidding system to ensure contract awards go to preferred vendors, who will quote higher prices. It is the very digital nature of such frauds which may leave no trace to be able to detect them and, as such, would need advanced analytics coupled with continuous monitoring in the procurement system.

3.2.8. Corporate espionage through digital identity theft

Digital identity theft for corporate espionage refers to unauthorized use of digital credentials or identities to facilitate access to sensitive corporate information for a competitive advantage. The U.S. Identity Theft and Assumption Deterrence Act of 1998 provides the legal basis for understanding identity theft, which in the context of corporate espionage assumes additional dimensions of competitive intelligence and trade secret misappropriation. [41]

---

[39] One of the more sophisticated breaches in the supply chain was SolarWinds in 2020, a case where hackers inject malicious code in SolarWinds' Orion software updates but unknowingly distributed to thousands of clients, including US major government agencies and large-scale businesses. This enables attackers to seek unauthorized access to numerous organizations' networks, and there's a potential breach of sensitive data and internal systems. The attack's scope, stealth, and critical reach on valuable targets gave it all the gloss of being one of the most significant cybersecurity incidents in recent history. D.E. SANGER-N. PERLROTH-E. SCHMITT, *Scope of Russian hack becomes clear: Multiple U.S. agencies were hit*, in *The New York Times*, 2020, December 14. www.nytimes.com.

[40] Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control – Integrated framework. COSO. www.coso.org.

[41] United States Congress. (1998). Identity Theft and Assumption Deterrence Act of 1998. U.S. Government Publishing Office. www.congress.gov.

Digital identity theft can, technically, embrace complex approaches such as social engineering, credential stuffing, and APTs. The Verizon Data Breach Investigations Report summarized that the primary vector of data breaches involves credential theft, which has become prevalent in corporate espionage. [42] Once taken, these stolen identities can be used to gain entry into the entire gamut of sensitive corporate information, from general strategic plans down to very specific proprietary technologies.

The implications on corporate governance are huge, as it challenges the balance of security on one hand and collaborative, networked workspaces on the other. To this effect, the ISO/IEC 27001 standard on information security management provides an identity-based threat management framework that ensures a robust identity and access management system is at the core of any such approach. [43]

The 2010 Operation Aurora attack on Google and other companies is the most notable cases of using stolen digital identities to carry out corporate espionage. [44]

3.2.9. Manipulation of automated decision-making systems

Manipulation of automated decision-making systems in corporate governance refers to an intentional interference to develop unusual outcomes in the processes that involve AI or algorithms for particular people's or some group's benefit. [45]

These can include more sophisticated methods such as adversarial machine learning, data poisoning, and model inversion attacks in the manipulation of automated decision-making systems from a technological perspective. [46]

---

[42] VERIZON, *2021 Data breach investigations report*, Verizon, 2021. www.researchgate.net.

[43] International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. ISO. www.iso.org.

[44] The state-sponsored hackers exploited employees accounts, after the successful hacking of sensitive and secret company data such as source codes and intellectual properties through advanced exploitation techniques. In this case, however, it presented a signal call for stronger identity protection solutions and aggravated the issues of attributing and responding attacks globally, particularly in multinational business operations; K. ZETTER, *Google hack attack was ultra sophisticated, new details show*, in *Wired*, 2010, January 14. www.wired.com.

[45] Zarsky analyzes challenges linked to algorithmic decision-making in corporate settings, concerning the high possibility of this system being used in the attempt of making personal or organizational gains. journals.sagepub.com.

[46] The work by Papernot et al. has shown the vulnerability of deep learning to hostile inputs

The implications for corporate governance are severe, as increasingly core business functions are entrusted to automated decision-making systems, from credit scoring to human resource management. In this field, the EU's Guidelines on Ethics for Trustworthy AI and the OECD Principles on Artificial Intelligence [47] present a series of commitments towards integrity and fairness of AI systems in companies, based on human control and responsibility.

With poor publicity of high-profile cases of manipulation of automated decision-making systems in corporate settings, a hypothetical example would be that of several employees manipulating the input data from an AI-driven performance evaluation system to better their ratings for promotion or bonuses, hence undermining the fairness and effectiveness of a company's human resource management processes.

3.2.10. Cyber-enabled money laundering through corporate structures

Cyber-enabled money laundering through corporate structures refers to the use of digital technologies in combination with corporate entities for hiding the origin of illicitly derived funds. FATT acknowledges that "there is a growing use of digital technologies to enable money laundering, which presents new challenges in ensuring proper corporate governance and regulatory compliance". [48]

Technically, cyber-enabled money laundering could take much more complicated forms: layering through chains of digital platforms, or exploiting cryptocurrency exchanges and vulnerabilities in e-commerce systems. Each of these risks touches on money laundering concerns-a context that includes a FATF report on Virtual Assets and Virtual Asset Service Providers [49] in 2019, pointing out the developing risks coming from these new technologies. [50]

Cyber-enabled money laundering creates significant challenges for corporate governance in ensuring financial integrity and regulatory compliance. The

crafted to force systems into a particular output by demonstrating the limitations of deep learning in adversarial settings. N. PAPERNOT-P. MCDANIEL-S. JHA-M. FREDRIKSON-Z.B. CELIK-A. SWAMI, *The limitations of deep learning in adversarial settings*, in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, pp. 372-387, IEEE. arxiv.org.

[47] OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments. oecd.ai.

[48] Financial Action Task Force. (2021). Money laundering and terrorist financing in the virtual asset context. FATF. www.fatf-gafi.org.

[49] www.fatf-gafi.org.

[50] Financial Action Task Force. (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF. www.fatf-gafi.org.

Wolfsberg Anti-Money Laundering Principles for Private Banking are good but anachronistic guidance on combating money laundering, which needs adaptation to the unique risks introduced by digital technologies. [51] Boards now have to oversee the implementation of sophisticated AML compliance programs able to detect and prevent cyber-enabled laundering schemes. This is well-illustrated in the 2016 Bangladesh Bank heist, in which corporate structures were involved in cyber-enabled money laundering. [52]

3.3. Interdependencies and tendencies

The corporate governance cybercorruption landscape is highly diverse, hence very interconnected and rapidly changing. For instance, the Global Risks Report 2021 from the World Economic Forum argues that failure in cybersecurity represents one of the major risks for economic stability, hence indicating how cyber-risks within the corporate world show systemic characteristics. [53] Currently, the manifestations of cybercorruption overlap to constitute complex problems that normally fall outside typical corporate governance demarcations.

The various types of cybercorruption often blend together in complex attack vectors. For instance, digital identity theft leads on to algorithm manipulation, a means for insider trading. Cybercrime as a threat to information societies, as analyzed by Furnell, underlines how such combined attacks may lead to widespread disruption. [54]

Some emerging trends in the field of cybercorruption encompass increasing levels of utilization of artificial intelligence and machine learning-the former a tool for criminality and the latter for detection of corrupt practices. According to Brundage et al. in the work "The Malicious Use of Artificial Intelligence", there is a probability that in the near future, AI will strengthen the capabilities of cyber criminals and further complicate methods of detection and prevention. [55]

---

[51] Wolfsberg Group. (2012). Wolfsberg anti-money laundering principles for private banking. Wolfsberg Group. cbr.ru.

[52] The hackers breached the bank's system and ordered fake SWIFT transfers to try to launder close to $1 billion through several jurisdictions and corporations. Despite the blocking of most transfers, $81 million still remained unrecovered up to today, showing how complex cyber-enabled money laundering is and its influence against traditional AML frameworks; www.ft.com.

[53] World Economic Forum. (2021). The global risks report 2021 (XVI ed.). World Economic Forum. www.weforum.org.

[54] S. FURNELL, *Hackers, viruses and malicious software*, in Y. JEWKES-M. YAR (Eds.), *Handbook of Internet Crime*, London, 2010, pp. 173-193 www.semanticscholar.org.

[55] M. BRUNDAGE-S. AVIN-J. CLARK-H. TONER-P. ECKERSLEY-B. GARFINKEL-D. AMODEI,

These interrelations and tendencies create a demand for a paradigm change in methods of corporate governance. According to Deloitte's Tech Trends 2021 report, boards of directors and executive management should consider an integrated model of AI-advanced cybersecurity and governance systems that take into account the emergent landscape of cybercorruption. [56] It can include real-time monitoring systems, predictive analytics of threats, and adaptive governance models which can respond promptly and adequately to emerging cyber risks.

4. Legal Countermeasures Against Insider Trading in Leading Asian Countries: Comparative Analysis

4.1. Introduction to comparative analysis

Japan, South Korea, Singapore, and China will be discussed here because they have the leading positions in technological development and corporate governance reforms in Asia. These countries rank on high scales both in the Global Cybersecurity Index, ITU, 2020, and the Ease of Doing Business Index, World Bank, 2020. This means that the countries are leading in tackling issues of cybersecurity in sound business settings. [57]

The five major areas put into comparison from these countries include laws, means of enforcing punishment, preventive measures, and international cooperation. It is, therefore, for this reason that a comparative law approach inspired by Zweigert and Kötz will be adopted. [58] Such an approach does not only consider the formal legal structures but also their functional equivalents as well as socio-legal contexts. The added value will therefore be realized within this approach towards an effective combat strategy of cybercorruption in corporate governance.

The malicious use of artificial intelligence: Forecasting, prevention, and mitigation, 2018, arXiv preprint arXiv:1802.07228. arxiv.org.

[56] Deloitte. (2021). Tech trends 2021. Deloitte Insights. www2.deloitte.com.

[57] International Telecommunication Union. (2020). Global cybersecurity index 2020. ITU Publications. www.itu.int.

[58] K. ZWEIGERT-H. KÖTZ, *An introduction to comparative law*, III ed., Oxford, 1998, www.cambridge.org.

4.2. Country analyses

4.2.1. Japan

Japanese cybersecurity and corporate governance with an aim at a focus on technological innovation, while ensuring cooperation with the public and private sectors in particular. Basic Act on Cybersecurity (Act No. 104 of 2014) [59] forms the base of national cybersecurity strategy, while the standards of corporate practices that include overseeing cybersecurity are determined by the Corporate Governance Code of 2015 revised in 2021. [60] This legal framework is the recognition of the country's interdependence of corporate and national cybersecurity.

Laws that specifically pertain to cybercorruption include Act on the Protection of Personal Information [61] (2003). Article 2(1)(iv) of the Unfair Competition Prevention Act [62] specifically identifies trade secret misappropriation, which is particularly relevant to cyber-enabled corporate espionage. The different forms that cybercorruption takes would fall under such umbrella provisions, and Maurushat points out the specificity of Japan's focus on technological solutions as well as public-private partnerships in their cybercrime control effort. [63]

The enforcement structure is primarily an institutional structure based upon the NISC – National center of Incident readiness and Strategy for Cybersecurity, [64] which acts to coordinate national efforts on cybersecurity. One of the organizations involved in responding to cyber incidents is the Japan Computer Emergency Response Team Coordination Center, or JPCERT/CC [65] for short. Initiatives, such as the Cyber Security Alliance Japan, [66] or CSAJ for short, support collaboration between government agencies and private sector entities. This kind of multi-stakeholder approach enables rapid information sharing and allows for coordination on emerging threats.

---

[59] Basic Act on Cybersecurity (Act No. 104 of 2014) www.japaneselawtranslation.go.jp.

[60] Japan Financial Services Agency. (2021). Japan's Corporate Governance Code. FSA. www.fsa.go.jp.

[61] Act on the Protection of Personal Information (Partly unenforced). Act No. 57 of May 30, 2003. www.japaneselawtranslation.go.jp.

[62] Unfair Competition Prevention Act. Act No. 47 of May 19, 1993. www.japaneselawtranslation.go.jp.

[63] A. MAURUSHAT, *Japan's approach to cyber-crime and cyber-security*, in *University of New South Wales Law Research Series*, 2010, www.academia.edu.

[64] National center of Incident readiness and Strategy for Cybersecurity. www.nisc.go.jp.

[65] www.jpcert.or.jp.

[66] https://ajcca.net/.

The punishments for cybercorruption crimes in Japan are severe, as the response to the 2020 NTT Docomo data breach illustrates. The firm that is to suffer from heavy fines was not the only loss in terms of reputation; the firm is likely to suffer civil liabilities now. [67] The Japanese rule of law system leans toward remediation and prevention besides repressive sanctions because of a holistic approach to cybersecurity enforcement.

In Japan, the preventive measures and compliance requirements are very strict. The ISMS has been certified based on JIS Q 27001 [68] that demands corporate information security practices to a significant level. Besides that, the Japan Information Technology Security Evaluation and Certification Scheme, JISEC, [69] also provides guidelines for evaluating and certifying the IT security products. According to Japan's Corporate Governance Code, [70] the mandate of overseeing cybersecurity measures is directly put upon corporate boards as the country recognizes cybersecurity as a significant governance issue.

All this is proactive concerning international cooperation on cybersecurity matters, since it actively participates in global forums and bilateral agreements. The active state of the Japan-U.S. Cyber Dialogue and Japan's engagement in the ASEAN-Japan Cybersecurity Capacity Building Centre are exemplary in ensuring that Japan secures a leading role vis-à-vis international collaboration on cybersecurity challenges. [71] Through this international cooperation, Japan both shares its experiences and learns how to deal with cybercorruption by using best global practices.

4.2.2. South Korea

Its strong technological infrastructure, coupled with active policies from the government, characterizes South Korea's approach toward cybersecurity as well as implementing corporate governance. At the heart of South Korean cybersecurity legislation are the Act on Promotion of Information and Communications Network Utilization and Information Protection [72] of 2001, which was

[67] Kyodo News. (2020, December 25). Japan's NTT Docomo reports data breach affecting 4.5 million users. Kyodo News. english.kyodonews.net.

[68] JIS Q 27001. kikakurui.com.

[69] Information Technology Security Evaluation and Certification Scheme, JISEC. www.ipa.go.jp.

[70] Japan's Corporate Governance Code. www.fsa.go.jp.

[71] Ministry of Foreign Affairs of Japan. (2021). Japan-U.S. Cyber Dialogue. Retrieved from cybilportal.org.

[72] Act on Promotion of Information and Communications Network Utilization and Information Protection. onepark.khu.ac.kr.

last amended in 2020, while corporate practices have been guided by the Code of Best Practices for Corporate Governance of 2016. [73] This law is part of the effort of South Korea to make their country a safe digital environment for business development.

The main laws on cyber corruption are the Personal Information Protection Act [74]-the law adopted in 2011 and last amended in 2020-and the Act on the Protection of Information and Communications Infrastructure, [75] adopted in 2001 and last amended in 2013. This act requires critical infrastructure to take certain security measures based on the recognition that corporate cybersecurity is closely connected with national cybersecurity in South Korea. Choi examines cybercrime in South Korea, pointing out the country's comprehensive legislative framework dealing with a broad range of cyber offenses and considering both prevention and punishment. [76]

The leading organizations that spearhead the institutional framework for enforcement are the Korea Internet & Security Agency, [77] led by the National Cybersecurity Center of the National Intelligence Service. KrCERT/CC [78] plays a very integral role in coordinating Response to Cyber Incidents. Collaboration between government agencies and private sector entities is facilitated through the operations of initiatives like the Korea Cybersecurity Alliance. [79] This multiagency approach allows for a comprehensive and coordinated response to cybersecurity threats.

South Korea punishes and penalizes pretty seriously, as seen in the way of response towards the 2014 Korea Credit Bureau [80] data breach. There were criminal charges leveled against several senior executives, while the companies paid enormous fines due to this case. This reflects how seriously South Korea takes a stand on corporate and individual liability through cyber failures. [81] These

[73] Korea Corporate Governance Service. (2016). Code of Best Practices for Corporate Governance. KCGS. www.cgs.or.kr.

[74] Personal Information Protection Act. iapp.org.

[75] Act on the Protection of Information and Communications Infrastructure 2001 (as amended in 2013). www.dataguidance.com.

[76] K.S. CHOI, *Cybercriminology and digital investigation*, El Paso 2015, www.lfbscholarly.com.

[77] Korea Internet & Security Agency. www.krcert.or.kr.

[78] KrCERT/CC. www.cybersecurityintelligence.com.

[79] Korea Cybersecurity Alliance. thediplomat.com.

[80] Korea Credit Bureau. www.koreacb.com.

[81] C. SANG-HUN, *Theft of data fuels worries in South Korea*, in *The New York Times*, 2014, January 20, www.nytimes.com.

penalties would deter several cyber-corrupts who may indulge in this activity.

A preventive measure and requirements of compliance are comprehensive in nature in South Korea. The certification of K-ISMS [82] specifies that the best practices in corporate information security are of a high standard. The Korea Internet & Security Agency, KISA outlines detailed guidelines on information security management. The Code of Best Practices for Corporate Governance of Korea [83] explicitly charges the corporate boards to ensure measures regarding cybersecurity. This reflects integration of cybersecurity in broader corporate governance frameworks in this country.

Similarly, the country has not been passant towards international cooperation in cybersecurity-related matters. South Korea has established a series of bilateral cybersecurity agreements with several nations and actively participates in regional initiatives such as the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies. [84] This allows South Korea to engage in the sharing of its technological know-how and share in global endeavors on cybercorruption.

4.2.3. Singapore

The approach of Singapore to cybersecurity and corporate governance draws upon its status as a global financial center and on the necessity to ensure that the digital environment for doing business is secure. It is supplemented by The Cybersecurity Act 2018 [85] outlining a full legal framework for national efforts in this direction and the Singapore Code of Corporate Governance, 2018 outlining standards related to general corporate behaviour and cybersecurity oversight specifically. [86] This legislative framework demonstrates that Singapore recognizes cybersecurity as one of the ingredients required by Singapore to stay competitive in the global economy.

Key pieces of legislation that acknowledge cybercorruption include the Personal Data Protection Act 2012 (No. 26 of 2012) [87] and the Computer Misuse Act. [88] Chapter 51A of the Computer Misuse Act addresses unauthorized access

[82] Certification of K-ISMS. www.alibabacloud.com.

[83] Code of Best Practices for Corporate Governance of Korea. www.ecgi.global.

[84] ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies. aseanregionalforum.asean.org.

[85] Cybersecurity Act 2018. sso.agc.gov.sg .

[86] Singapore Code of Corporate Governance. www.sid.org.sg.

[87] Personal Data Protection Act 2012 (No. 26 of 2012). sso.agc.gov.sg.

[88] Computer Misuse Act. sso.agc.gov.sg.

to computer material, to which most types of cybercorruption relate. Chong discusses the law on cybercrime in Singapore regarding the country's active legislation in producing laws against all types of cyber threats currently in use. [89] The country is constantly updating its laws in line with technological advances.

The institutional framework of enforcement focuses on the Cyber Security Agency of Singapore [90] and the Singapore Computer Emergency Response Team. [91] These agencies are very significant in developing cybersecurity strategies at the national level and coordinating responses to incidents that arise in cyberspace. Other arrangements aim at promoting better collaboration between government agencies and private sector entities, such as the Singapore Cybersecurity Consortium. [92] This way, sharing information and making an effective response to the threats of cybersecurity can be quick.

The stance of Singapore is quite harsh when it comes to penalties and fines, as evidenced by the SingHealth data breach of 2018. [93] Preventative measures and compliance requirements are holistic and proactive in Singapore. A unique approach toward encouraging cybersecurity in the Internet of Things is the Cybersecurity Labelling Scheme of consumer smart devices. Under the Infocomm Media Development Authority, extensive information security management guidelines are present for corporations. [94] The Singapore Code of Corporate Governance [95] explicitly speaks to the mandates of corporate boards overseeing cybersecurity measures, given that cyber risks have been integrated into core business strategies.

Singapore has been proactively fostering international cooperation over matters of cybersecurity. Amongst other participation roles in international forums such as the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, [96]

---

[89] C.S. CHONG, *The law on cybercrime in Singapore*, in *Singapore Academy of Law*, 2020.

[90] Cyber Security Agency of Singapore. https://www.csa.gov.sg/.

[91] Singapore Computer Emergency Response Team. www.csa.gov.sg.

[92] Singapore Cybersecurity Consortium. www.nrf.gov.sg.

[93] The leakage of personal information concerning 1.5 million patients, with consequent major fines and an overall review of security practices in the healthcare industry, was unauthorized. In this regard, Singapore's legal system has more punitive and remedial redress for failures in cybersecurity enforcement, as if punishment and cure have equal or more weight. graphics.straitstimes.com.

[94] Infocomm Media Development Authority. (2021). Internet of Things (IoT) Cyber Security Guide. IMDA. www.imda.gov.sg.

[95] The Singapore Code of Corporate Governance. www.mas.gov.sg.

[96] United Nations Office for Disarmament Affairs. (2021). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UNODA. disarmament.unoda.org.

Singapore set up the ASEAN-Singapore Cybersecurity Centre of Excellence. [97] Initiatives like these indicate that Singapore is engaged in knowledge-sharing and participating in global activities against cybercorruption.

4.2.4. China

The Chinese approach towards cybersecurity and corporate governance has its unique internet governance model, with profound consideration for national security. The Cybersecurity Law of the People's Republic of China of 2017 [98] and the Code of Corporate Governance for Listed Companies in China of 2018 [99] formulate standards for practices at the corporate level. This constitutes the legislative framework that shapes the strategy of China to integrate cybersecurity into the national goals on security and economic development.

Key legislation that covers cybercorruption includes the Data Security Law of the People's Republic of China [100] and relevant provisions in the Criminal Law, last amended in 2020. Article 285 provides specific criminal law on illegal access into a computer information system relevant to many forms of cybercorruption. [101] Qi et al. examined cybercrime legislation in China, indicating that national security and social stability have led to the dominance of the country's theoretical conception of cybersecurity by addressing both domestic and cross-border cyber activities. [102]

The institutional framework for enforcement is led by the Cybersecurity Bureau and the National Computer Network Emergency Response Technical Team/Coordination Center of China, CNCERT/CC, [103] under the leadership of the Ministry of Public Security. The Cyberspace Administration of China has a critical role in guiding national cybersecurity strategies. The collaboration between relevant government departments and private enterprise companies is facilitated through an initiative like the China Cybersecurity Industry Alliance. [104] In this centralized system, cybersecurity policies can be implemented uniformly across sectors.

---

[97] ASEAN-Singapore Cybersecurity Centre of Excellence. www.csa.gov.sg.

[98] Cybersecurity Law of the People's Republic of China of 2017. digichina.stanford.edu.

[99] Code of Corporate Governance for Listed Companies in China. www.csrc.gov.cn.

[100] Data Security Law of the People's Republic of China. www.npc.gov.cn.

[101] Criminal Law of the People's Republic of China. Article 285. Article 285 (unodc.org).

[102] C. QI-Y. WEN-Z. QIN, *A review of cybercrime in mainland China*, in T.J. HOLT-A.M. BOSSLER (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, London, 2019, pp. 987-1007.

[103] CNCERT/CC. www.cert.org.cn.

[104] China Cybersecurity Industry Alliance. sustainablefutures.linklaters.com.

The policies for fine and penalty administration by China are extremely harsh, as evident by the examples of enforcement cases. One of the finest examples of the 2020 antitrust inquiry accompanied by cybersecurity provisions resulted in an unprecedented fine of $2.8 billion with fundamental alterations in the business conduct. [105] This case shows the will to punish firms severely for violation of cybersecurity as well as data protection regulations. Therefore, the deterrence implication of this case is more serious against corporate cybercrime.

Preventive measures and requirements for compliance in China are huge and well-regulated. The Multi-Level Protection Scheme of information system security, or MLPS 2.0, stipulates clearer standards for different types of information systems depending on the degrees to which they affect national security. [106] Normally, cybersecurity standards can be retrieved through the National Information Security Standardization Technical Committee, or TC260, [107] oftentimes compulsorily provided to enterprises in China for adoption. Explicitly, corporate boards of Chinese listed companies are doing this in light of incorporating cybersecurity into the national corporate governance framework.

This wider context of foreign policy priorities informs China's approach to international cooperation in cybersecurity. Besides the already mentioned bilateral cybersecurity dialogues with various countries, China has promoted a new international order in cyberspace by initiating proposals such as the Global Initiative on Data Security. [108] This reflects ambition on the part of China to take on at least a leadership role when it comes to shaping global cybersecurity norms and standards.

4.3. Comparative summary

Comparative analysis of Japan, South Korea, Singapore, and China by the prism of cybercorruption countermeasures draws out similarities but also a number of critical differences in approaches taken. All the four countries have passed comprehensive cybersecurity legislation and integrate cybersecurity consideration into their corporate governance framework. Specific mechanisms differ significantly, reflecting the unique socio-economic context and strategic priorities of each nation (Table 1).

---

[105] L. Wei-S. Xu, *China fines Alibaba $2.8 billion in landmark antitrust case*, in *The Wall Street Journal*. www.nytimes.com, 2021, April 10.

[106] Ministry of Public Security of the People's Republic of China. (2019). Regulations on the Multi-Level Protection Scheme of Information System Security. Retrieved from english.www.gov.cn.

[107] www.dataguidance.com.

[108] digichina.stanford.edu.

Table 1 – Comparative Analysis of Cybersecurity Approaches in Four Asian Countries

Country	Key Focus	Enforcement Approach	Distinctive Feature
Japan	Balance of innovation and security	Decentralized	Emphasis on technological solutions
South Korea	Balance of innovation and security	Decentralized	Strong public-private partnerships
Singapore	Forward-looking approach	Centralized	Focus on emerging technologies (e.g., IoT)
China	National security and social stability	Highly centralized	Integration with overall strategic objectives

As we can see from the Table above, Japan and South Korea tend to emphasize a balance of innovation and security as underlined by their firm thrust on technological solutions and public-private partnerships. Singaporean legislation stands ahead in terms of its highly forward-looking approach in dealing with the emerging technologies such as IoT. China is under the approach highly influenced by national security and social stability imperatives with cyber security laws closely related to the overall strategic objectives.

The section further discusses the enforcement mechanisms from the four countries, indicating different extents of centralization. Japan and South Korea have pursued relatively decentralized approaches to implementing cybersecurity, with several agencies in each country involved in the enforcement mechanism. The model of Singapore is more centralized, as there the CSA plays a vital role. China has the most centralized enforcement structure among the four countries, which is reflective of the broader governance model.

In general, there are harsher penalties and sanctions against cybercorruption offenses among all four nations, although with clear differences. Japan would aim at remediation, tied to penal measures, while South Korea and Singapore use sever deterrent measures, with fines that are the highest and with potential criminal charges. The penalties in China were harsh to be often associated with the general regulatory measures.

The preventive measures and requirements for compliance in all four countries are comprehensive, though with a different focus: technical standards and certifications in Japan and the Republic of Korea, innovative approaches like the Cybersecurity Labelling Scheme in Singapore, and a multi-level protection scheme with links to national security considerations in China.

International cooperation approaches are also quite different. Japan and Singapore reach out most actively to the global initiatives, sharing expertise with them. South Korea is primarily focused on regional cooperation, particularly

within ASEAN. For China, the approach is certainly more assertive, reflecting Chinese ambitions to shape global cybersecurity norms according to their strategic interests.

Though approaches vary, they all give salient insights into how other countries, such as Uzbekistan, might go about developing effective anti-cybercorruption strategies. In their fledgling experiences, the Asian leaders also show how imperative it is to contextualize cybersecurity frameworks within a country while collaborating internationally in addressing this global problem.

5. Discussion

5.1. Uzbekistan's Evolving Cybersecurity and Corporate Governance Framework

This thus places the legal landscape of Uzbekistan in an interesting comparative analytical perspective in relation to cybersecurity and corporate governance. The latest legislative attempts undertaken by Uzbekistan reflect more awareness of the challenges that cybersecurity has been posing to modern economies; at the same time, they indicate the complexity of adapting to rapidly evolving cyber threats within the framework of transitioning economies.

If LRU-764, 2022, or the Law on Cybersecurity, [109] is a landmark achievement of Uzbekistan in cybersecurity, similar foundational laws had been seen in the chain of our comparative analysis with China and South Korea. However, how effective this law would be in fighting cybercorruption in corporations is yet to come. The potential of iterative improvement afforded by LRU-964 of 2024, [110] similar to Singapore's agile approach towards regulation, could change the course.

Of great interest in this context is the Presidential Decree 'On Additional Measures for Cybersecurity of Critical Information Infrastructure' (DP-167, 2023). [111] Similar to all four analyzed countries, it places in priority the protection of critical infrastructure. Whether Uzbekistan's actual performance will live up to sophisticated sector-specific regulation in Singapore or to comprehensive compliance requirements in South Korea remains to be seen.

[109] LRU-764, 2022, or the Law on Cybersecurity of Uzbekistan. lex.uz.

[110] LRU-964 of 2024. On amendments and additions to certain legislative acts of the Republic of Uzbekistan in connection with the improvement of legislation in the field of cybersecurity. lex.uz.

[111] DP-167, 2023. On additional measures to improve the system of ensuring cybersecurity of critical information infrastructure facilities of the Republic of Uzbekistan. lex.uz.

Indirect contributors to the cybersecurity ecosystem in Uzbekistan include the Law on Payments and Payment Systems, LRU-578 of 2019, [112] and the Law on E-Government, LRU-395 of 2015. [113] These two acts may partially regulate aspects of financial cybercrime and digital security within government-business communication, respectively-areas identified in our analysis as important components of holistic cybersecurity policies. However, compared with the broad and multiagency approaches found in Japan and Singapore, the integration of these laws with more general cybersecurity and anti-corruption initiatives seems less developed.

Perhaps most poignantly, LRU-370, 2014, the Law on Joint Stock Companies and Protection of Shareholders' Rights, [114] and the Corporate Governance Code of 2015 [115] precede the explosive growth in cyber threats of the last couple of years. Such a timescale calls into question whether Uzbekistan's corporate governance framework is currently adequate to its cybersecurity needs as of today. A complete lack of clear provisions which would link corporate governance to cybersecurity stands in bold contrast to integrated approaches that were found in all four countries analyzed.

5.2. Implications for Uzbekistan

The applicability of various legal mechanisms observed in different analyzed Asian countries to the context of Uzbekistan must be assessed with due care from a number of perspectives:

a) Legal system compatibility: The legal system of Uzbekistan is partially compatible with the countries reviewed, especially China, as it is civil law-based with elements inherited from the Soviet era. In this respect, some legal mechanisms could be more easily transferred, specifically those related to centralized governance and regulation. In contrast, the implementation of more decentralized methodologies, as represented in Japan and South Korea, may require larger-scale legal reforms.

b) Institutional capacity: Uzbekistan's institutional capacity in the field of cybersecurity is still at a developing stage. Even though a State Center for Cybersecurity [116] has been established, its capabilities have not yet reached those of advanced institutions in countries analyzed. Full implementation of comprehensive

[112] LRU-578 of 2019. About payments and payment systems. lex.uz.

[113] LRU-395 of 2015. About e-government. lex.uz.

[114] LRU-370, 2014. On Amendments and Supplements to the Law of the Republic of Uzbekistan "On Joint Stock Companies and Protection of Shareholders' Rights". lex.uz.

[115] Corporate Governance Code of Uzbekistan. nrm.uz.

[116] State Center for Cybersecurity of Uzbekistan. csec.uz.

cybersecurity frameworks, as seen in Singapore or South Korea, requires substantial investment in institutional capacity building-that is, training cybersecurity professionals and creating specialized agencies.

c) Technological infrastructure in Uzbekistan, although it is developing fast, lags behind compared to analyzed countries. It is essential to point out that there is a "Digital Uzbekistan 2030" strategy; in any case, a lot more investment is required for the country to catch up with the countries analyzed. Advanced cybersecurity measures, like those found in Japan, through the ISMS certification process, or in Singapore by means of the Cybersecurity Labelling Scheme, would be difficult to implement and would be rolled out during the maturation of the technological infrastructure.

d) Corporate culture and governance practices: Uzbekistan's corporate culture is still at an evolutionary stage, shifting from being state-controlled to a more market-based approach. Corporate governance practices, specifically cybersecurity, are relatively less developed than in the analyzed countries. Extensive supervision of cybersecurity requirements for corporate boards, as introduced in all four analyzed countries, would necessitate significant transformation of corporate culture and practice.

e) Stages of economic development: Compared to Japan, South Korea, and Singapore that are at more developed stages of economic development, Uzbekistan is an emerging economy with different economic priorities and resource constraints. In the wider development context, cybersecurity may be important but probably needs to be balanced against other pressing development needs. China's approach to integrating cybersecurity into broader economic development goals may provide a relevant model for Uzbekistan.

It is given that Uzbekistan might find elements of the Chinese approach, most immediately applicable, particularly in its incorporation of cybersecurity into national development strategies and the focus on centralized control. However, as it continues to develop economically and institutionally, elements of the other countries' approaches might be integrated.

For instance, Uzbekistan might consider the adoption of a combination of the various approaches, starting with comprehensive legislation similar in nature and scope to China's Cybersecurity Law, with the goal, over the longer term, to achieve more sophisticated mechanisms, such as the sector-specific regulations of Singapore or the emphasis on international cooperation of Japan. It could also learn from South Korea about having strong enforcement mechanisms and related penalties that work as a deterrent against cybercorruption.

In the long run, Uzbekistan will have to work out an approach peculiar to its context, inexorably drawing from best practice as observable in these more advanced economies. This should focus on building institutional capacity,

developing technological infrastructure, and, where necessary and gradually, the introduction of more advanced cybersecurity measures in keeping with the development of the economy and corporate governance practices.

5.3. Challenges and Opportunities

Several problems can be seen with respect to the implementation of effective countermeasures against cybercorruption in Uzbekistan. For one, there is a problem related to the current technological condition of the infrastructure and related cybersecurity knowledge. According to Gulyamov et al, Uzbekistan "lags behind in almost all other regional countries" in its digital development, which could serve as an impetus to the failure of sophisticated cybersecurity measures. [117]

The required cultural shift to make cybersecurity a prime factor in corporate governance is another major challenge that cannot be achieved by merely regulatory changes, and education and awareness programs for corporate leadership are pursued, similar to what is done or being done for countries like South Korea.

In parallel, there is also a unique opportunity for Uzbekistan to address cybercorruption. The economic and digital transformation currently taking place in the country offers the opportunity to incorporate cybersecurity considerations, in a sense from the outset, and may thus leapfrog some of the challenges that are somewhat premature for more mature economies.

Lastly, it can also use the available literature by learning from other transition economy experiences. For instance, Estonia's successful digital transformation and strong cybersecurity framework provide valuable lessons for a country in a similar stage of development.

Another window of opportunity for Uzbekistan may also be the growing international emphasis on cybersecurity capacity building in developing countries. Against this backdrop, some programs, such as the Digital Central Asia-South Asia Project of the World Bank, [118] might provide quite substantial help for constructing the needed infrastructure and know-how.

Building on these opportunities and facing these challenges, Uzbekistan is in a position to establish a strong and functional model of fighting cybercorruption-the one responding to its context and paths of development.

---

[117] S. GULYAMOV-S. RAIMBERDIYEV, *Personal data protection as a tool to fight cyber corruption*, in *International Journal of Law and Policy*, 1(7), 2023.

[118] Digital Central Asia-South Asia Project of the World Bank. ucentralasia.org.

6. Conclusion

6.1. Summary of key results

This research has contributed a lot to the sphere with regard to an understanding of cybercorruption in corporate governance. First, this study contribution is that of formulating an overall meaningful definition of cybercorruption within the perspective of corporate studies. The second major contribution that this research made was in identifying and describing ten verbatim forms of cybercorruption, that were, in turn, elaborated on in light of their detailed typology.

The comparative review of the cybercorruption fight in Japan, South Korea, Singapore, and China showed a variety of strategies duly reflecting the specific political, economic, and technological contexts of the state. In this respect, the legislative framework, mechanisms of enforcement, preventive measures, and efforts of international cooperation have been analyzed in reviewed countries.

These understandings were used in carrying out the research on Uzbekistan by considering five decisive aspects: how best international practices may be adapted to the local context. Each of these factors serves as the base for customized recommendations for strengthening the cybersecurity framework of Uzbekistan.

The findings indicate the need for the contextualization of strategies for cybersecurity, drawing on global best practice. This study lays the foundation for developing economies in devising appropriate policy frameworks to address cybercorruption as business increasingly goes digital.

6.2. Recommendations for Uzbekistan

Recommendations and Future Directions.

Through comparative analysis, we can recommend the following building blocks of the legal framework of Uzbekistan:

Detailed Provisions Concerning Cybersecurity Risks and Cybercorruption under Corporate Governance Laws: In light of the integrated approaches of Japan and Singapore, there is a strong potential for Uzbekistan to elaborate detailed provisions relating to cybersecurity risks and cybercorruption within its corporate governance laws.

Enhance Connectivity between Cybersecurity Laws and Corporate Governance Regulations: Modification of the Corporate Governance Code should be one of the options that establish connectivity and association with the implementation of cybersecurity laws in Uzbekistan.

Build on the elaborate compliance obligations in South Korea by including more comprehensive guidelines or regulations on preventing and detecting cybercorruption in corporate settings.

Sector-specific regulations or specialized cybersecurity requirements for companies in important sectors of the economy could be considered, drawing on Singapore's experience with sector-specific regulations.

Capacity-building programs on cybersecurity and anti-corruption in the digital age for corporate executives can be designed based on successful models that have been developed from the countries analyzed.

Promote public-private partnerships in cybersecurity, building on lessons from the collaborative models that were considered in all four countries under review.

It is true that Uzbekistan has taken serious steps in the direction of responding to cybersecurity challenges, but little has been done in terms of trying to strike a blow at cybercorruption with regard to corporate governance. The experiences of Japan, South Korea, Singapore, and China offer valuable lessons and potential models for Uzbekistan as it continues to develop its legal and regulatory framework in this critical area.

The present study therefore has wider implications for the developing economies facing cybersecurity challenges in corporate governance. They do hint at the imperatives of contextualizing cybersecurity strategies within national contexts while learning from best global practices. Future research could thus focus on how different cybersecurity models function best under divergent economic and political contexts, especially in transitioning economies. Second, deeper studies are needed on the role that international cooperation may play in building cybersecurity capacity in developing nations. Other fertile areas of research are on the economic consequences of cybersecurity measures on businesses in emerging markets, which could be quite enlightening to policymakers. Finally, the studies on the interplay between artificial intelligence, blockchain technologies, and cybersecurity within the compass of corporate governance will go a long way in aiding the anticipation of future challenges and opportunities in combating cybercorruption. Such contributions would be giant areas that would go a long way in the evolution of the field of corporate governance in cybersecurity, especially within the scope of developing economies.