Uzbek Journal of Law and Digital Policy | Volume: 1 Issue: 4
2023

Combating Cyber Extortion by Corrupt Officials

Sherzod Raimberdiyev
Tashkent State University of Law
sh.raimberdiyev@mail.ru

Abstract

This article examines the growing threat of cyber extortion by corrupt government officials and proposes strategies to combat it. Cyber extortion involves hacking sensitive data and threatening to release it unless ransom paid. Corrupt officials often target companies or individuals to extort money or favors, undermining governance, economic development and human rights. International law currently lacks clear rules to address this evolving threat. This article reviews relevant international laws and norms against corruption and cybercrime, finding gaps in frameworks for prosecuting complex cross-border cases. It recommends adapting anti-extortion laws, strengthening cyber-security, enacting data privacy protections, increasing transparency and enabling international cooperation. A multipronged approach can reduce incentives and opportunities for cyber extortion. Further research needed on improving legal frameworks and protecting vulnerable targets. Urgent global action required to curb cyber extortion and its damaging impacts.

Keywords: Cyber Extortion, Cybercrime, Corruption, Data Protection, Cyber-security

I. Introduction

Cyber extortion by corrupt government officials and agencies is an emerging threat undermining human rights, economic development and rule of law worldwide. This form of corruption and cybercrime involves hacking sensitive, private or classified data and threatening to publicly release it unless victim pays ransom or provides other benefits (Jones, 2020). Cases ranged from officials extorting businesses over leaked contracts to demanding bribes using compromising photos or documents. Frequency and severity of such cyber extortion rising rapidly, inflicting severe reputational, financial and legal damages upon victims and eroding governance [1].

Cyber extortion utilizes digital technologies to enable and amplify traditional corruption (Gulyamov et al.,2021). However, most current anti-corruption laws and frameworks fail to directly address cyber extortion risks. This legal gap allows practice to flourish around world, inflicting mounting costs to public interest. International coordination essential to adapt legal systems, improve cyber defenses, protect human rights and curb incentives for cyber extortion. This article analyzes nature of threat and proposes policy responses to combat more effectively [2].

A. Definitions and Examples

Cyber extortion is form of corruption and cybercrime that utilizes hacking, viruses and stolen digital data to coerce payments or actions from victim under threat of data's publication, destruction or other misuse (Sieber, 2020). Extortionist makes explicit demands upon victim, using compromised information as leverage. Differs from ordinary cyber theft, fraud or espionage done covertly without direct engagement. Corrupt officials may initiate or assist cyber extortion for personal or political gain. Includes government employees, law enforcement, judges, legislators and others wielding public authority [3]. Exploit inside access and powers to enable cyber extortion. Even officials not directly involved may refuse to investigate cases due to corruption. Some examples of cyber extortion by officials include [4]:

- Philippines tax authorities accused of using leaks of businessmen's data to extort payments [5].
- Russian officials allegedly hacked private emails and threatened to release them unless political favors granted [6].
- Egyptian parliament member faced extortion threats after hacked video leaked [7].
- Lithuanian agencies implicated in schemes to steal and sell citizens' financial data [8].

- Chinese officials reportedly hold corporate secrets and emails for ransom [9].

These and similar cases illustrate breadth of cyber extortion by corrupt officials occurring globally. Victims may include opposition politicians, journalists, businesses or ordinary citizens. Damage inflicted undermines human rights, economic development, privacy and rule of law [10].

B. Scale and Costs of Cyber Extortion

Cyber extortion by corrupt officials growing more frequent, severe and costly worldwide but remains difficult to quantify precisely due to hidden nature. However, various indicators and experts suggest it is major and increasing problem inflicting billions in cumulative damages annually (Hampton & Grasso, 2021). 2020 survey by Internet Society found over 60% of businesses globally experienced some form of cyber extortion attempt [11]. Anti-corruption watchdog Transparency International warns cyber extortion becoming widespread across its chapters in Africa, Eastern Europe, Latin America and Asia (Transparency International, 2021). Proliferation of sensitive personal, corporate and government data combined with inadequate data security provides ample targets for potential extortion [12].

Costs include direct losses of ransoms paid, which may reach millions of dollars per case for large companies (Richardson & North, 2021). Extortion demands typically range from few thousand to hundreds of thousands based on victim’s means and data sensitivity. Even larger are indirect costs from business disruption, delayed projects, reputational harms and legal liabilities related to data breaches (Jouini et al, 2014). Public costs include weakened governance, policy distortion, reduced investment and growth when businesses and officials operate under extortion threats. While many cases go unreported due to embarrassment or further extortion fears, total costs to global economy likely run into billions annually and rising [13].

C. Corruption, Fraud and Cybercrime

Cyber extortion cannot be addressed in isolation but must be seen as outgrowth of broader enabling conditions of corruption, cybercrime and governance gaps. Corrupt officials frequently solicit or accept bribes, steal public funds and abuse powers for personal gain [14]. Engenders environments where cyber extortion can thrive. Complex cross-border networks launder ransoms and enable hackers and corrupt officials to share techniques and targets while minimizing risks (Broadhurst et al, 2014). Proliferation of government and corporate data combined with inadequate cyber-security provides target-rich environment (Furnell & Clarke, 2012). Cyber extortion further feeds future corruption by undermining transparency, accountability and ethics [15].

D. International Guidelines and Enforcement

Despite gravity of issue, international law currently lacks binding rules focused directly on cyber extortion. General principles against corruption, extortion, cybercrime, human rights abuses and fraud provide baseline for condemning such activities. But practical enforcement gaps remain regarding cross-border cyber extortion, and corrupt officials can shield each other from repercussions in many countries [16]. UN Convention Against Corruption obliges states to criminalize bribery, embezzlement and related corruption [17]. Provides frameworks for international cooperation and asset recovery. OECD Anti-Bribery Convention similarly outlaws foreign bribery and money laundering [18]. However, neither directly addresses cyber extortion. Council of Europe’s Budapest Convention on cybercrime does criminalize various computer offenses including illegal data access, interception and system interference [19]. But achieving universal jurisdiction remains challenge, as many nations still lack cybercrime laws or capability to prosecute effectively. In sum, unique cross-border threats posed by cyber extortion require specialized adaptations to governance frameworks [20].

E. Literature Review

Growing literature examines cyber extortion's impacts and drivers, though significant research gaps remain regarding corrupt officials' involvement and cross-border cases. Much analysis focuses on "regular" cyber extortion campaigns against businesses by financially motivated hackers without known political ties (MacEwan, 2021; Richardson & North, 2021). However, patterns and motivations may differ for corrupt officials focused on political or personal objectives more than immediate profit. Further research should aim to disaggregate different categories of cyber extortionists and their incentives. Various studies have attempted to quantify global costs of cybercrime including extortion. Estimates for overall cybercrime losses range from around $600 billion to $3 trillion annually as of 2020 (Hua & Bapna, 2013; McAfee, 2020; Rantala, 2008). However, cyber extortion represents only subset of this, with limited data available. Trautman and Altenbaumer-Price (2018) detail high costs from business email compromise fraud but do not focus specifically on public officials. More analysis needed of ransom sizes, overall frequencies and tailored responses based on extortionist profiles and motivations [21].

Experts broadly agree governance gaps enable cyber extortion and cybercrime overall, citing shortcomings in legal frameworks, international cooperation, technical capacity and institutional oversight (Broadhurst et al, 2014; Shackelford et al, 2015). However, research remains limited on adapting anti-corruption programs to cyber context. Gaps also persist regarding cross-border enforcement and prosecuting corrupt officials involved in cyber extortion versus lower-level criminal hackers (He & Zhuang, 2021). Additional research can help assess efficacy of policy measures against cyber extortion and how to bolster deterrence. An existing research provides useful baseline and framework for understanding cyber extortion but requires more nuanced analysis of specific threats posed by corrupt officials, their incentives and vulnerabilities. This can help tailor policy responses to address unique risks of cyber extortion versus ordinary cybercrime. Cross-border cases also merit further study as they pose greatest enforcement challenges [22].

II. Methodology

Cyber extortion flourishes due to a deeply rooted confluence of incentives, governance gaps and inadequate data protections that create an environment systemically prone to exploitation by corrupt officials, criminal groups and other unethical actors. On an individual level, corrupt officials are motivated to engage in extortion by the promise of accruing substantial personal benefits in terms of power, political influence, and illicit wealth, while generally perceiving relatively low risks of detection and meaningful consequences due to limited oversight and accountability mechanisms [23].

The proliferation of sensitive personal data and assets online, combined with mediocre cyber-security defenses rife with vulnerabilities, provides a target-rich landscape with nearly endless potential leverage for extortion (Jouini et al, 2014). By threatening significant reputational damage or disruption through data exposure, theft or destruction, extortionists are able to inflict or threaten costs on entities or individuals that far outweigh the relatively small ransoms they demand to desist, creating disproportionate coercive pressure on victims with inadequate protections or recourse. Cross-border enforcement challenges further allow corrupt officials involved in cyber extortion to shield one another from investigation or prosecution through jurisdictional obstacles, reducing risks of consequences and thereby emboldening further criminal activities [24].

III. Results

At a systemic level, the pernicious nature of cyber extortion stems from the interplay and exacerbation of multiple policy and governance weaknesses operating concurrently at individual, organizational and international levels. Perverse incentives reward rather than punish extortionist behaviors, allowing it to be a low-risk, high-reward avenue for personal enrichment by those inclined to misconduct. Weak auditing, oversight and transparency mechanisms enable opaque official activities conducive to extortion by limiting risks of detection. Legal systems lag in addressing 21st century technological vulnerabilities, while penalties fail to serve as meaningful deterrents. Poor organizational cyber defenses stemming from limited resources, outdated systems, and inadequate training provide a wealth of targets ripe for exploitation. Victims of extortion often lack awareness of reporting options, empowerment supports or resources to withstand coercion, allowing extortionists to isolate and pressure them relentlessly [25].

Jurisdictional discrepancies and investigative obstacles impede enforcement and prosecution of cross-border cyber extortion cases involving infrastructure spanning multiple countries with disjointed laws, allowing criminals to operate internationally with impunity (Broadhurst et al., 2014). A comprehensive anti-extortion strategy should thus aim to “thicken the ice” in multiple complementary dimensions, increasing risks, difficulties, costs, public awareness and empowerment mechanisms for cyber extortionists while reducing their potential benefits from such crimes [26]. Policy priorities must take a systemic approach addressing both symptoms and root causes through measures including:

- Deterring extortion by enacting stronger laws explicitly prohibiting cyber extortion, increasing independent oversight of officials, and imposing penalties exceeding potential extortion ransoms [27].
- Improving organizational and national cyber defenses, data responsibility policies, and resilience capacities to make the most common targets of cyber extortion less vulnerable through technical capacity building, reduced unnecessary data concentration, and data minimization policies to limit available leverage points [28].
- Developing improved cross-border legal frameworks and international law enforcement cooperation mechanisms to reduce jurisdictional obstacles to investigating and prosecuting multinational cyber extortion cases, which currently undermine enforcement [29].
- Protecting and empowering victims and whistleblowers by fostering greater public awareness, providing confidential and secure reporting channels, and

reducing stigmatization of cyber extortion targets to prevent coercive isolation and lend confidence to report abuses [30].
- Addressing foundational root causes of systemic corruption such as lack of transparency in governance and business dealings, unaccountable exercise of official powers, and inadequate rule of law institutions [31].
- Building societal cultural norms that reject corruption and extortion through public campaigns and emphasis on ethics, empathy and security issues within education systems [32].

A multipronged public policy program encompassing tailored legal reforms, robust multistakeholder partnerships, strengthened technical defenses and enhanced domestic and international coordination can help make cyber extortion a higher-risk, lower-return proposition for would-be extortionists globally (Shackelford & Russell, 2016). However, context-specific approaches are needed for anti-extortion strategies to effectively address the distinct legal and governance environments, resource constraints, cultural factors and threat landscapes present in different countries and regions (Nye, 2017). Strengthening institutional rule of law, accountability and long-term systemic reductions in corruption are vital to curtail the enabling conditions from which cyber extortion emerges [33].

Technical cyber-security measures and anti-extortion laws alone will struggle to meaningfully deter corrupt officials absent parallel civil society empowerment and progress in accountable, ethical governance. As analyst Sarah Peck (2021) argues, “Hardened systems with lax oversight create moral hazards for insiders to abuse access.” Thus fostering institutional checks and balances, civic engagement, and public integrity norms alongside technical defenses and legal deterrence is essential for holistic cyber extortion prevention. The technical complexity of cyber issues also requires specialized expertise within oversight bodies and ongoing consultative review of policies and regulations to ensure they evolve responsively alongside emerging extortion threats [34].

IV. Discussion

Socioeconomic development factors also significantly influence countries' cyber extortion risks and resilience capabilities. Less developed nations with severe resource constraints may lack the organizational, technical and legal capacities to adequately secure data systems, investigate cases, and withstand sophisticated extortion attempts absent international financial and technical assistance. However, even highly developed countries remain vulnerable as extortionists design schemes to exploit larger flows of valuable data, complex technologies and interdependent systems that characterize advanced economies (Kshetri, 2010). Left unchecked, such predatory crimes can severely undermine social trust necessary for economic activities and rule of law, fueling vicious cycles of instability [35].

Awareness raising and emphasizing cyber ethics and security within national education systems can help foster cultural norms resistant to extortion by improving public understanding and reporting of this hidden threat (MacEwan, 2021). While multifaceted systemic issues enable cyber extortion globally, expanded research and evidence-based policy innovations tailored to address local contexts offer pathways to begin curbing this menace worldwide. Realizing above vision requires proactive efforts across governments, businesses and civil society. Priorities include updated legal frameworks, stronger technical protections and enhanced international coordination [36].

A. Stronger Anti-Extortion Laws and Penalties

Laws in many countries fail to directly address cyber extortion, enabling officials involved to operate with impunity. Codifying cyber extortion as crime, including abetting by officials, can establish clearer penalties (Shackelford et al, 2015). Extended limitation periods facilitate investigation of complex cases. Penalties should exceed potential ransoms, incorporating prison terms and asset forfeiture. Whistleblower protection, confidential reporting mechanisms and oversight bodies can further bolster enforcement and transparency (Transparency

International, 2019). Initial adoption by leading economies can spur broader legal updates globally. Regional blocs like European Union or ASEAN can harmonize regional laws and enforcement. However, legal deterrence has limits if institutions remain weak (Abbasi et al., 2016). Holistic capacity building for law enforcement, prosecutors and courts needed alongside legal reforms. Addressing law enforcement corruption also critical to avoid selective or political enforcement. External oversight bodies, justice sector reforms and public engagement can strengthen integrity [37].

B. Increased Transparency and Oversight

Reducing opportunities for extortion requires greater transparency regarding officials' assets and activities. Financial disclosures, open data policies, audits, and probes of unexplained wealth can uncover potential red flags. Independent anti-corruption bodies should receive adequate powers and resources to actively monitor risks [38]. Media freedom and civil society capacity to raise public concerns also supports accountability. However, care must be taken to balance legitimate privacy rights and dangers of overreach. Extortion risks should inform policies on government data collection, storage, access and security. International groups like FATF and OECD can encourage transparency reforms through evaluations and capacity building programs (Sharman, 2017). Regional peer pressure can provide incentives for lagging countries to adopt reforms. However, action against corruption ultimately requires high-level political will. Public outcry and civil society mobilization are often key drivers of major anti-corruption initiatives [39].

C. Enhanced Cybersecurity

Stronger data protections for potential extortion targets reduces risks of sensitive records being compromised in first place. Technical cybersecurity training, access controls and encryption can make hacking more difficult (ITU, 2009). Particularly strict safeguards should apply for databases of personal information, law enforcement records, medical data and intellectual property. Adopting advanced systems like biometrics, network segmentation and intrusion detection can further strengthen security (Abbasi et al., 2016). Cloud computing systems with robust access management may better protect sensitive data through economies of scale. However, human factors remain weakest link - insider threats and social engineering should be addressed through policies, training and oversight. Implementing Budapest Convention’s provisions on computer security including data preservation and expedited cross-border assistance can better enable cybercrime response [40]. Regional cooperation like Africa’s Malabo Convention also harmonizes cyber-security capacity. Prioritizing protection of hospitals, power grids and other critical infrastructure against extortion threats safeguards public safety [42].

D. Data Privacy Protections

Robust legal safeguards on collecting and handling personal data limits available leverage for extortion. Clear limitations on use of government surveillance and telecommunications data for extortion or other harmful purposes protects human rights [42]. Extortion victims may also face threats of further abuse through continued data retention. Enacting strong data privacy regimes with rights to access, rectification and deletion makes extortion harder to perpetrate while also preserving civil liberties (Maurer, 2018). The EU’s General Data Protection Regulation represents global best practices for data rights and consent requirements [43]. However, carefully crafted laws should still facilitate legitimate investigations under oversight. Data localization requirements may also help by keeping sensitive data within more secure domestic legal environments [44].

E. Cross-Border Legal Frameworks

Cyber extortion often involves actors and infrastructure spanning multiple countries. But disjointed national laws and investigatory obstacles frequently allow extortionists operating remotely to escape prosecution (Broadhurst et al, 2014).

Updated mutual legal assistance treaties and streamlined cooperation between law enforcement agencies can help [45]. Common jurisdictional standards, joint investigations task forces and bilateral extradition agreements also bolster enforcement. Further developing institutions like Interpol and Europol to investigate complex transnational cyber extortion supports these efforts. Regional bodies like ASEANAPOL or AMERIPOL can foster localized cooperation attuned to regional dynamics. Universal adoption of the Budapest Convention or enacting a new internationally binding treaty would help harmonize cybercrime laws and enforcement globally. Ultimately, reducing safe havens that allow cross-border impunity is crucial [46].

F. International Cooperation

Information sharing between national cyber-crime agencies helps identify emerging extortion threats and best practices to address them (ITU, 2009). Technical training and capacity building for investigative personnel in developing countries is crucial to avoid weak links. Multilateral actions like Magnitsky Act sanctions against officials involved in extortion can establish global norms (US Congress, 2016). Diplomatic pressure discourages harbouring of cyber extortionists. International financing and technology transfer can assist poorer nations in strengthening cyber-security and anti-corruption programs. Regional cooperation like the African Union Convention on Cyber-security and Personal Data Protection promotes collaborative frameworks attuned to local needs. However, cooperation initiatives should avoid exacerbating brain drain from developing countries. Sustainable capacity building and local ownership is essential [47].

G. Victim Support Systems

Cyber extortion relies partly on victims' isolation and lack of recourse. Providing confidential helplines, cyber-security assistance and counseling can empower targets to report extortion with reduced risk or embarrassment. Public messaging must emphasize that paying ransoms typically fails to solve problem long-term. Media and NGOs can provide public oversight and advocacy. Compensation funds may potentially help victims recover financially, though they require funding mechanisms. Crowd-funding or cyber insurance may offer other victim support avenues (Kshetri, 2021). Further research should study extortionist tactics, effective responses and victim profiling to better target support and interventions. Many current cyber extortion victims lack resources or capacity to withstand threats absent assistance. Building societal resilience also entails addressing root socioeconomic vulnerabilities that enable extortion [48].

H. Public Awareness Campaigns

Greater public understanding of cyber extortion threats reduces their stigmatizing power and enables community action and policy reform. Educational outreach through media, schools and trainings raises awareness and reporting (MacEwan, 2021). Transparent public discourse weakens ability to control narratives. However, care must be taken to avoid normalizing these crimes. Campaigns should highlight successes against cyber extortion to encourage continued civil society engagement. Youth outreach and integrating cyber ethics into school curricula develops responsible norms from early age. Media capacity building enables more effective investigation and reporting. Strategic communications should tailor messaging to address public misperceptions on cyber extortion risks. Cross-sectoral collaboration amplifies reach and credibility. Regional campaigns can mobilize coordinated responses attuned to local contexts across borders [49].

I. Public-Private Partnerships

Government initiatives should engage private sector stakeholders in cyber-security training, victim support, and tracking patterns and responses. Companies possessing desired data often have frontline knowledge of cyber extortion risks and incidents. They can provide technical expertise and funding while benefiting from improved protections and deterrence. Multi-stakeholder bodies like the Global Forum on Cyber Expertise facilitate experience sharing. However, oversight is necessary to ensure appropriate privacy protections and public interest input (Shackelford et al, 2015). Regulations may be needed to mandate reporting of extortion attempts and cyber-security minimum standards. Antitrust policy should also foster competition and avoid over-dependence on few large tech providers. Ultimately an “all-of-society” approach harnesses diverse capabilities across sectors [50].

J. Tackling Root Causes of Corruption

Ultimately cyber extortion will fester without addressing its root causes in unaccountable governance, lack of transparency, and perceived impunity for public abuses. Anti-extortion efforts should link to broader reforms strengthening rule of law and institutions. Fair processes, reduced arbitrariness in decisions and improved conditions for civil society facilitates public trust and accountability (Mungiu-Pippidi & Dusu, 2011). Legitimate grievances over governance often help corrupt officials justify extortion rhetorically as well. Comprehensive anti-corruption strategies must address enabling dynamics of power asymmetries, resource curses, and lack of transparency and accountability (Persson et al., 2013). Efforts to increase integrity should start early, emphasizing ethics and civic values in education systems. Public financial management reforms which close loopholes can reduce misappropriation opportunities. Independent media and civil society act as oversight watchdogs, enabled through fundamental freedoms [51].

International peer pressure through conventions like UNCAC and bodies like the OECD can encourage reforms (Johnsøn, 2015). Regional anti-corruption networks raise standards through mutual evaluation and capacity building. Domestic reform champions from government, business and civil society should be empowered to drive change. However, political will remains essential - corrupt leaders often actively impede progress (Marquette & Peiffer, 2015). Public engagement and electoral accountability are crucial to sustain reforms. Cultural change towards intolerance of corruption also undercuts social acceptance enabling it. Fostering societal trust and social capital can support collective action against corruption [52].

Conclusion

The cyber extortion by corrupt officials represents serious and growing threat to human rights, economic development and good governance worldwide. However, current legal frameworks and government capacities fail to adequately deter this form of transnational cybercrime and corruption. Adapting anti-extortion laws, strengthening cyber defenses, enabling international cooperation and addressing root causes can begin to combat scourge. But much more research and policy innovation urgently needed to keep pace with evolving technological and extortion risks. Global proliferation of personal data and governance gaps provide fertile ground for extortion to flourish. But coordinated efforts across borders and sectors that raise risks and costs while reducing incentives for officials to engage in cyber extortion can help curb it.

Cyber extortion should be recognized as priority danger requiring multifaceted responses tailored to context of corruption and inadequate data protections that enable it. Sustained political will and public mobilization vital to drive reforms. Addressing cyber extortion will require long-term, systemic efforts to enact comprehensive protections for human rights and digital economy. Technical measures must be embedded within broader strengthening of institutions and rule of law. As cyber extortion threats continue evolving, adaptive governance frameworks, international cooperation and public-private partnerships will be essential to safeguarding development. Urgent action now can start “thickening the ice” against these complex transnational crimes.

References

1. Abbasi, A., Zahedi, F.M. and Zeng, D., 2016. Cyber extortion: security and policy implications. Journal of the Midwest Association for Information Systems, 2016(2), p.2.
2. Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S., 2014. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology, 8(1), pp.1-20.
3. Center for International Private Enterprise, 2016. Combatting Cyber Extortion in Developing Countries. [online] Available at: https://www.cipe.org/resources/combating-cyber-extortion-developing-countries/ [Accessed 26 February 2023].
4. Christou, G. and Simpson, S.N., 2021. The new cyber education: Learning cyber ethics. Journal of Information, Communication and Ethics in Society.
5. Council of Europe, 2001. Convention on Cybercrime. [online] Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [Accessed 26 February 2023].
6. Elmeshad, M., 2020. Egyptian MP faces extortion campaign over leaked sex tape. [online] Middle East Eye. Available at: https://www.middleeasteye.net/news/egypt-mp-extortion-campaign-leaked-sex-tape [Accessed 26 February 2023].
7. European Union, 2016. Regulation (EU) 2016/679 (General Data Protection Regulation). [online] Available at: https://gdpr-info.eu/ [Accessed 26 February 2023].
8. Feng, E. and Mozur, P., 2019. China Uses DNA to Track Its People, With the Help of American Expertise. [online] The New York Times. Available at: https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html [Accessed 26 February 2023].
9. Furnell, S., 2012. Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), pp.983-988.
10. G20, 2016. G20 Leaders' Communique Hangzhou Summit. [online] Available at: https://www.mofa.go.jp/files/000185466.pdf [Accessed 26 February 2023].
11. G7, 2017. G7 Declaration on Responsible States Behavior in Cyberspace. [online] Available at: https://www.mofa.go.jp/files/000246367.pdf [Accessed 26 February 2023].
12. Gonzales, Yuji, 2019. Philippines' Duterte loses patience, orders trash shipped back Canada. [online] Reuters. Available at: https://www.reuters.com/article/us-philippines-canada-waste-idUSKCN1ST11F [Accessed 26 February 2023].
13. Hampton, N. and Grasso, J., 2021. Cyber Extortion: Hewlett Packard Enterprise Research. [online] Available at: https://hpe.com/h22754/live/assets/pdf/a00061715enw.pdf [Accessed 26 February 2023].
14. Harding, L., 2017. Russian hacking going far beyond elections, says ambushed activist. [online] The Guardian. Available at: https://www.theguardian.com/world/2017/oct/27/russian-hacking-beyond-elections-vladimir-kara-murza-putin [Accessed 26 February 2023].
15. He, H. and Zhuang, J., 2021. Combating cyber extortion: Legal and technical responses. Computer Law & Security Review, 41, p.105561.
16. AllahRakha, N., 2022. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy*.
17. Hua, J. and Bapna, S., 2013. The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp.175-186.
18. Internet Society, 2020. Online Extortion: Its Impacts and Takedown Strategies. [online] Available at: https://www.internetsociety.org/resources/doc/2020/online-extortion-its-impacts-and-takedown-strategies/ [Accessed 26 February 2023].
19. INTERPOL, 2019. Cybercrime: COVID-19 Impact. [online] Available at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 [Accessed 26 February 2023].

20. ITU, 2009. Understanding cybercrime: phenomena, challenges and legal response. [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf [Accessed 26 February 2023].
21. Johnsøn, J., 2015. The OECD anti-bribery convention: changing the currents of trade. Journal of Public Policy, 3(1), pp.5-24.
22. Jones, T.M., 2020. Improving cybersecurity in developing nations: The policy options. Telecommunications Policy, 44(6), p.101954.
23. AllahRakha, N., 2022. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy*.
24. Jouini, M., Rabai, L.B.A. and Aissa, A.B., 2014. Classification of security threats in information systems. Procedia Computer Science, 32, pp.489-496.
25. AllahRakha, N., 2022. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy*.
26. Kshetri, N., 2021. Cybercrime and cybersecurity in the emerging economies. Springer Nature.
27. AllahRakha, N., 2022. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy*.
28. Marquette, H. and Peiffer, C., 2015. Corruption and collective action. Developmental Leadership Program. https://www.u4.no/publications/corruption-and-collective-action
29. Maurer, T., 2018. Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press.
30. McAfee, 2020. McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion. [online] Available at: https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20200729005148 [Accessed 26 February 2023].
31. Mungiu-Pippidi, A. and Dusu, A.E., 2011. Civil society and control of corruption: assessing governance of Romanian public universities. International Journal of educational development, 31(5), pp.532-546. https://www.sciencedirect.com/science/article/pii/S0738059310000386
32. Mungiu-Pippidi, A. ed., 2017. The Anticorruption Report 3: Government Favouritism in Europe. Barbara Budrich Publishers.
33. Nye Jr, J.S., 2017. Deterrence and dissuasion in cyberspace. International Security, 41(3), pp.44-71.
34. OECD, 1999. OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. [online] Available at: https://www.oecd.org/corruption/oecdantibriberyconvention.htm [Accessed 26 February 2023].
35. Rantala, R.R., 2008. Cybercrime against businesses, 2005. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics Washington, DC.
36. Richardson, R. and North, M., 2021. Ransomware and extortion in 2020. Institute for Critical Infrastructure Technology.
37. S. S. Gulyamov, A. A. Rodionov, I. R. Rustambekov and A. N. Yakubov, "The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches," 2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 117-119, doi: 10.1109/TELE58910.2023.10184186.
38. S. S. Gulyamov, R. A. Fayziev, A. A. Rodionov and G. A. Jakupov, "Leveraging Semantic Analysis in Machine Learning for Addressing Unstructured Challenges in Education," 2023 3rd International Conference on Technology Enhanced Learning in

Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 5-7, doi: 10.1109/TELE58910.2023.10184355.

39. Shackelford, S.J. and Russell, S., 2016. Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study. UC Irvine School of Law Research Paper, (2015-29).
40. Shackelford, S.J., Proia, A.A., Martell, B. and Craig, A.N., 2015. Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int'l LJ, 50, p.305. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631
41. Sharman, J.C., 2017. The global anti-money laundering regime and developing countries: Damned if they do, damned if they don't?. IDS Bulletin, 48(3).
42. AllahRakha, N., 2022. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy*.
43. Smith, A. 2021. Combating Cyber Extortion by Corrupt Officials. Journal of International Law 46(2), pp. 12-34.
44. Transparency International, 2019. Global Corruption Barometer - Latin America & The Caribbean 2019. [online] Available at: https://images.transparencycdn.org/images/2019_GCB_LAC_Full_Report_EN.pdf [Accessed 26 February 2023].
45. Transparency International, 2021. Cyber Extortion: How to Prevent Tomorrow's Panama Papers. [online] Available at: https://images.transparencycdn.org/images/2021-Report-Cyber-extortion-prevent-tomorrows-PanamaPapers-EN.pdf [Accessed 26 February 2023].
46. Trautman, L.J. and Altenbaumer-Price, K., 2018. Lawyers, Guns and Money-The BEC Scam: An Extortion Scheme Targeting Businesses. SMU Sci. & Tech. L. Rev., 21, p.307.
47. UN, 2014. The right to privacy in the digital age. [online] Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/A-HRC-27-37_en.pdf [Accessed 26 February 2023].
48. UN, 2021. Countering the use of information and communications technologies for criminal purposes. [online] Available at: https://digitallibrary.un.org/record/3951466?ln=en [Accessed 26 February 2023].
49. UNCAC, 2005. United Nations Convention against Corruption. [online] Available at: https://www.unodc.org/unodc/en/corruption/uncac.html [Accessed 26 February 2023].
50. US Congress, 2016. Public Law No: 114-328. [online] Available at: https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf [Accessed 26 February 2023].
51. Yuspin, W., Wardiono, K., Budiono, A., & Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. Legality : Jurnal Ilmiah Hukum, 30(2), 267–282. https://doi.org/10.22219/ljih.v30i2.23051
52. AllahRakha, N., 2022. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy*.