RETHINKING GLOBAL SECURITY USING DISRUPTIVE TECHNOLOGIES: AN ANALYSIS

[1]NAIMA ZIA, [2]IMRAN RASOOL,[3]DR.TAHIRA MUMTAZ,[4]MUNAZZAH BUKHARI,[5]NOOR UL HUDA,[6]AYESHA MARYAM,[7]SOBIA YOUNAS,

[1]Lecturer, Political Sciences
University of the Punjab
naima.zia1@gmail.com
[2]PMS Officer, Government of Punjab
ranjhaemran@gmail.com
[3]Lecturer, Political Science
Government College Women University Sialkot
tahira.mumtaz@gcwus.edu.pk
[4]Lecturer, Political science
GC Women University Sialkot
munaza.bukhari@gcwus.edu.pk
[5]Lecturer, Psychology
Forman Christian College
Noorulhuda171998@gmail.com
[6]Mphil, Department of Linguistics and Communications
University of Management and Technology
ayesha.maryam99@gmail.com
[7]Lecturer, Education
GC Women University Sialkot
sobia.younas@gcwus.edu.pk

Abstract
This paper highlights how technological innovation in the 21st century supports the decentralization of power as opposed to the technological infrastructure of the 20th century which supported the centralization of power. It builds on the assumption that amidst the current wave of technology, states need to adapt accordingly to ensure their commitment to security with their citizens. For that, this research uses a critical approach to international security and highlights different ways in which disruptive technologies such as blockchain, Internet of Things, Artificial intelligence etc. can play a decisive role. Theoretically, it is aligned with the approach of Robert Cox's critical theory through which it proposes a post-structural approach to resolving non-traditional security threats by adopting the route of digitization. It assumes that the current security infrastructure is driven by a traditional understanding of security which not only needs revision but also requires structural amendments. To keep its scope focused and manageable, this paper uses Kotler's six stages of digitization through which exponential technologies move, to reimagine security options.

Keywords: Disruptive technologies, object of referent, non-traditional security, blockchain, critical security

INTRODUCTION

As the 20-year crisis of the war on terror seems to end with the waning appetite of states to pursue it any further, a renaissance in security studies and its goals is expected. This upgrade has become inevitable both due to the crisis of COVID-19 in recent years and worldwide technological development. Fortunately, the discipline of security studies over the years has evolved into over-inclusivity regarding *objects of referent*. This has in effect halted its sole facilitation of states-centric goals(Williams, 2012). Such inclusion however created a base that initiated debates relevant to human security based on which solutions outside the traditional approaches to security

can be sought and operationalized. Not very long ago, security across the globe appeared to be compromised by the invasion of a virus that neither discriminated against any nation nor respected any borders. Shores of the Atlantic and Pacific that protected the United States given its conventional ways of combating security situations, got bypassed by a disease that is asymmetric if not an engineered threat to security (Real, 2020). While the crisis in the shape of Corona was confronted with goodwill by the states yet a bad security infrastructure from a holistic perspective, it brings us to find the answers of combating the threats in areas sidelined due to their apolitical nature or recent discovery i.e., disruptive technologies. According to Balaji Sirinavasim, a non-linear view of how security has evolved will help researchers understand how power concentration has been in a sinusoidal wave from centralised to decentralised in the last hundred years. To expand on his theory, it is apparent that in the early 20th century, traditional security and state were popular due to the technological advancement that revolved around these states and their security goals. The emergence of nuclear weapons for defense, concept of big militaries, and centralized media as well state banking systems strengthened the security norms that suited the power (Hutchcroft, 2001). In the 21st century, however, through the emergence of disruptive technologies, security norms are likely to change. These technologies include the emergence of Drones, 3D printing, virtual reality, Blockchain, IOTs(internet of Things), Robots etc. If not handled on time or aligned smartly by the states, disruptive technologies are likely to weigh in favour of decentralization and taking the power away from the centre and empowering the rest (Geiller,2022). Here is what the change looks like on the table:

Centralized - 1950s	**Decentralized - 2000s**
● Traditional Security ● State-Centered Policies ● Modern Monetization Theory ● State ● Politics ● National Liberation Movements ● Conventional War ● Centralized Electronic Media ● Nuclear Weapons ● State-owned Agencies	● Human Security ● Human-Centered Campaigns ● Cryptocurrency ● Networks ● Disruptive Technologies ● Ethnic and Religious Conflicts ● Hybrid War/terrorism ● Decentralized Social Media ● IEDs (intensively explosive devices), Bio-warfare ● Privatized Agencies

It is important here to realize that digitization in itself is nothing, only the goal-based use of digitization can bring the world closer to Human Security in terms of what it truly is and not in terms of how selectively it has been adopted. The idea is to direct technological advancement in such a way that the agency of none of the international actors is compromised, and the integrity of the centres of power is contained along with conditions that ensure it.

PROBLEM STATEMENT

The traditional approach to security which was surrounded by the proliferation of arms and building big militaries proved to be redundant when the world was confronted with a traditionally unrecognized enemy in form of COVID-19. This identified gap in the pre-placed vision of security and demanded the alternatives to the traditional concept of security. This paper uses precedents established by international actors to explore how the digital route during several phases of

digitization can facilitate nation-states in adopting a human-centered security policy using a post-structural approach.

METHODOLOGY

Theoretically, this paper is aligned with the critical approach of Robert Cox who highlighted two approaches to peace and security. In that, he gave an anti-status-quo approach which states that the traditional problem-solving approach results in providing solutions that are in the favour of the status quo. Such pro-status quo solutions put a limit on the number of possibilities that can otherwise favour peace in general (Cox, 1990). A supposed reason for such an approach is that the beneficiaries of any given system are less likely to suggest policies that can disrupt any base of power that keeps them intact. Another reason for using this particular theory for the matter under discussion is the disillusionment of policymakers with technology and their lack of interest in it (Milan, 2013). It further becomes essential when those few who are making decisions on behalf of the majority lack the technological skills to do so. The turn the world has taken after COVID-19 makes digitization no longer a choice but rather a condition that states are bound to adjust to (Amoah, 2021). According to Balajji Sirinavason "if states do not adopt the specifications of network companies, network companies are likely to adopt the specifications of states". This can be proven by the fact that companies like Tiktok, Huawei and Facebook have more variety and dimensions of data on individuals than state-owned bodies like NADRA (National Database and Registration Authority) in Pakistan or NRC(National Registration of Citizens) in India (He, 2015).

The purpose of this paper is to discuss how the disruptive nature of the newly emerging technologies can be used to amend and reconstruct the structure in a way that it can truly adhere to the needs of security in the contemporary era. Another reason why this paper departs from traditional approaches to security is that the scale at which traditional security infrastructure has been built has proved to be unsuccessful in combating a non-traditional security threat whether it is health security, environmental security or food security. This further iterates the point that solutions without the status quo carry the potential to resolve a holistic security threat that prioritizes humans.

Using the critical methodology proposed by Robert Cox, this research has leveraged the phases of Disruption, as established in the book "BOLD" (Kotler, 2015) and applied them to the given security context to illustrate the possible ways in which Disruptive technologies can be exploited to further Global Security goals and concerns considering every referent object. Robert Cox's post-status quo approach can be applied in various manners. The point this research makes is that even though a critical, outside-the-available infrastructure approach is important, it does not have to be revolutionary. It is something that can be achieved in an evolutionary manner instead of disrupting an entire system and replacing it with a new one. Changes can be functionally made within the existing systems. This creates the possibility of expanding on the idea of Kotler from a security perspective. Arguably, Kotler gave six parallel stages of technological development to which a security road map can be laid by discussing how it can happen during each stage.

The First Stage- Digitization

The most prominent of all disruptive technological infrastructure is blockchain. It has been defined as "a decentralized, distributed, and often public, digital ledger consisting of records or blocks that are used to record data across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks."(Morris, 2016) This system is famous for several reasons such as ease of access, transparency, data integrity and security. Considering the newly established notion of data to be the "new" oil (Hirsch, 2013), the first step for governments could be to create Big Data that includes digital identities of its citizens. To elaborate, it would mean digitizing manual aspects especially information sharing into a digital format. In terms of states and international organizations, it would be to build a digital infrastructure using IoT, 5G and other tools of disruption (Ebersold, 2015). It is important here to recognize how this system of data storage is different from the ones where data is already being

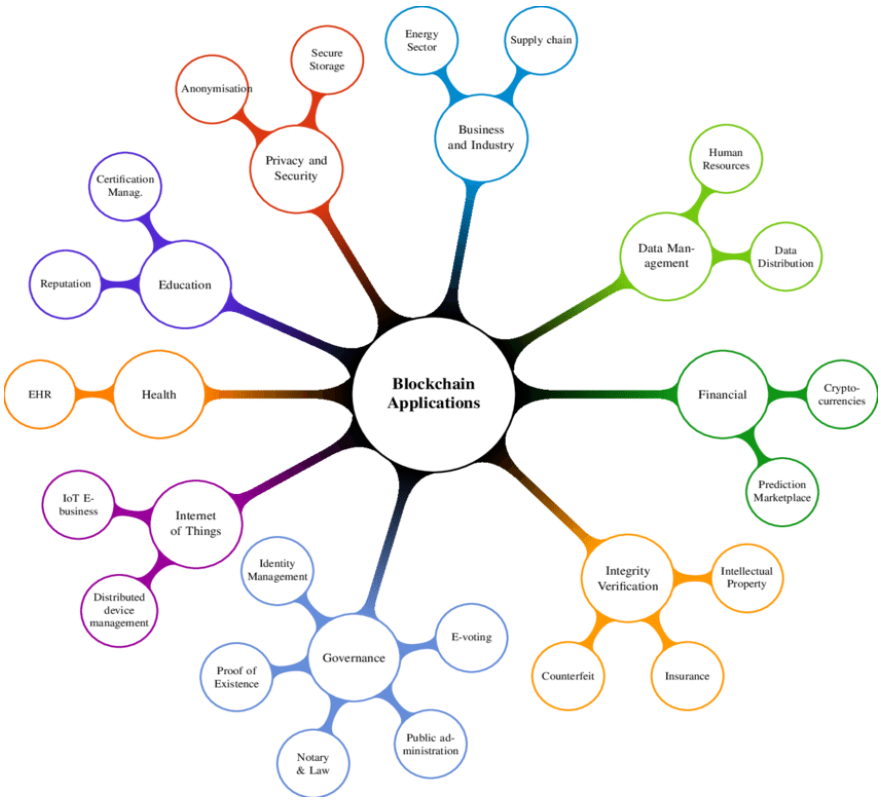
stored. Building a national or international database of identities using blockchain technology would make it more transparent and accessible where alterations are less likely to be made without the scrutiny of an exhaustive process (Li, 2015). Once the founding layer has been formed, later it will be at the discretion of security analysts, policymakers and governmental and non-governmental bodies to use it to establish further systems. Currently, regions like China, Rhode Island and Estonia have announced the use of blockchain technology to verify their citizens' identity (Kuo, 2021). Due to the immutability of data in blockchain, this technology can be efficiently used in all spheres of governmental and intergovernmental management. Different types of information can be stored in the blockchain and can be distributed among the blockchain networks. Moreover, it can also provide a sense of security to individuals by ensuring that no third party can share their personal identity against their consent. Later, this database can be applied in both centralized and decentralized ways which can further be explored in the next stages.

The Second Stage- Deception

This is the stage where a digital database is ready for establishing subsystems using a Centralized, Decentralized or Distributive Ledger Technology (DLT) system. This is called the phase of deception because digital growth is exponential. It means that initially, it might deceive one into thinking that the growth is extremely slow. However, the trends take off once they break the number barrier and the effect is multiplied instantly at this stage. It also takes time as digital transformation often faces issues of connectivity, data integrity and other challenges that might appear once the system is being run on the field. One of the major reasons why growth at initial levels is slow is because the a system always require an initial cost for its design and execution. A lot of states avoid digitization for this very fact since they assume that the initial cost would not pay them back. However, such cost can be retrieved back once the system is functional as it will be discussed in the later stages of this paper. Regardless of the initial cost, there are countries that power their systems on the Blockchain. For instance, Sierra Leone conducted a Blockchain based voting system on March 7, 2018, and became the first country in the world to do so (Zenin, 2018). It is important to note here that voting based on Blockchain is not the same as Electronic voting as in the latter, there is a lot of room available for corruption, data exploitation and other trust-related problems whereas in the former, the system is designed in such a way that need for trust is eliminated altogether. In the case of Sierra Leone, Leonardo Gammar of Agora, stored votes in an immutable distributed ledger, thereby offering instant access to the election results. Grammar has previously said, “Anonymized votes/ballots are being recorded on Agora’s blockchain, which will be publicly available for any interested party to review, count and validate” (Sharma, 2019). This certainly was an approach in which options chosen were outside the status quo but eventually led to the preservation of not only the social order but also the integrity of the contract between the state and its subjects.

From a Human Security point of view, blockchain has also been used by UNOCHA(**United Nations Office for the Coordination of Humanitarian Affairs)** to form systems through which aid and its usage can be tracked to the very end to gain confidence and trust of those investing in UNOCHA aid projects (Awan, 2020). This is because it has the potential to transform the humanitarian sector, ensuring Human security by providing cost savings and traceability of information while at the same time reducing transaction time (Verity, 2016). Although still in its nascency, at this point, several applications of disruptive technologies can be used specifically for security purposes. For instance, defense against aerosol transmission of bioterror attacks can be ensured by installing a Sentinel monitoring system and digitizing epidemiological surveillance systems to limit the chances of bioterror attacks (Lana, 2020). Same way, a Digitized military supply chain will allow for tracking the distribution of weapons to consumers. This will save the hassle of manually keeping the check on the consumer end and help identify criminal or terrorist use of military equipment. Similarly, legalizing digitized currencies will aid in tracking the transactions eliminating the possibility of money laundering, fraud and terrorist financing. From a Human Security point of view, digitized

health records will help in identifying a person with a history or present symptoms of contagious disease.



" Figure 2: Mindmap abstraction of the different types of blockchain applications. (Casino, 2019)

Digitized databases at this stage can also be imported by INGOs which can help them transfer a single message worldwide in case of a global security threat. Last, but not least, it can also be used as a tool against corruption since taxation automated by blockchain or DLT (Treiblmaier, 2020) will not leave the possibility of unchecked transactions or untracked spending. This also means reducing the workload on counter-corruption departments (Sarkar, 2021)

The Third Stage- Disruption

Once the database has been maintained, the connectivity challenge has been accomplished, the next stage that emerge is the one that allows for AI (artificial intelligence) implementation, and incorporation of extended reality as well as data exploitation into creating permissioned and open ledger systems. It is the stage when rigorous use of data begins to happen. Over here, the transition from digital paraphernalia to a full-fledged operating digital structure can be seen. Data from raw form is turned into analyzed, usable, importable and even exportable forms. Another material change that occurs at this stage is the disruption of pre-established systems and infrastructure. In terms of health security, successful efforts from regions that have been able to combat certain contagious diseases can be replicated globally to avoid re-invention of the wheel. Medium to short-term health goals might include, launching mobile applications (state-backed) that can operationalize Contact Tracing through the use of smartphones. The construction of virtual platforms that can issue e-health credentials, and digital health passports can ease the process of mobility during the outbreak of COVID-like epidemics. Selv technology launched by IOTA in collaboration with Denton is an example of issuing e-health credentials which is an appropriate example of how a digital health passport might work (Millenaar, 2020).

Additionally, the response to COVID made it visible that there is a need to incentivize the countering measures and pandemic battling by supporting new businesses that emerge (pharmaceuticals, masks, sanitizers) or social actions whether it is to do with plasma donation or mass vaccinations. Unlike how it initially seemed, the economy was not disrupted but rather reallocated in response to COVID-19. A lesson learned from such a response was that in future, most of such reallocation is going to require operational digital infrastructure. In that, the best strategy is to identify what digital gaps exist, how such gaps can be filled, and how power and politics can be managed around them. Another example of the application of AI in the Health Security context from London is Medopad Company which works in collaboration with the Chinese Tencent company. It uses AI for early diagnosis of Parkinson's disease. Medopad analyzes different types of data, computed tests, data for geographical location and movement of a person and other information to identify the Parkinson's at the early stages in an individual (Medopad, n.d.). Also in Belgium, lung diseases are being diagnosed at early stages using disruptive technology. Through the use of AI in a pilot project, researchers were able to store the results of thousands of diagnostics as a result, the machine was able to detect the diseases of lungs two times more efficiently than the pulmonologists (Topalovic, 2019).

If viewed from the perspective of the financial security of both state and their subjects, taxation is something that requires specific attention to digital disruption. Regardless of states' dependency on tax, 100% taxation has still not been ensured even in the world's leading countries. Since the beginning of the 21st century there have been 87 recorded incidents when tax resistance often leading to tax riots took place ("Tax Resistance," n.d). In most of the cases, it was the distrust of people in their governments regarding tax spending that brought people onto the streets. After the advent of disruptive technologies, systems are being organized and laws are being made to digitize the system of taxation specifically using disruptive technology. Whether it is done through permissioned or open blockchain applications, the future promises transparency to the citizens as they can monitor their tax spending till the very end (Treiblmaier, 2020). Therefore, the possibilities for this stage of disruption are many and with proper planning, systems can be inducted to increase efficiency which can ultimately lead to an environment that is secure from all possible dimensions that interact with humans.

The Fourth Stage- Demonetization

This is the state where technology becomes exponentially mature and cheaper, often to the point of being free. Although digitizing the international system in general and security in particular, can be nauseating for some in terms of the initial cost it requires, if looked at from a broader perspective, it is more of an investment. A simple way of explaining this could be, that there are two most important assets the majority would agree to, one being time and the other being money. Digitization saves both. Estonia is an example as not only did it digitized every aspect of its governance but once the system was established with several sub-systems functioning in favour of both governing and the governed, it took it to another level of demonetization. Being the pioneer in this respect, Estonia's cyber security was most vulnerable to attacks. After the 2007 cyber attacks, it upgraded its data storage using blockchain technology to ensure the integrity of data stored in government repositories and to protect its data against insider threats. As a result, it became host to the NATO Cooperative Cyber Defence Centre of Excellence and the European IT agency. As it gained more confidence, Estonia was able to digitize its Justice system, Police system as well as Legal system. For secure and speedy functioning, it developed an e-file system for the accurate exchange of information between different stakeholders such as police, prosecution offices, courts, prisons, legal aid system etc. The key takeaway from this stage is, that once the system has been established after initial investment, it is eventually going to generate profit beyond the initial costs and thus more and more can be invested into the engineering of future systems.

The Fifth Stage- Dematerialization

The Fifth stage is when systems are dematerialized. An example of that is a shift from tangible court proceedings, contracts, paper currency, votes, bills, identity cards and a lot of other aspects that require material proof. By dematerialization, not only the risk of forgery is reduced but paper dependency can also be avoided. This would not only make a document accessible from a distance but would also be an ecologically sound option. Using this approach, legal proceedings in Estonia have not only become more efficient but also are being done without physically appearing to the courts or exhausting tangible resources in drafting cases (e-Estonia, 2019). If the same system is imported by the ICJ (International Court of Justice) or courts elsewhere, the international legal process can be accelerated beyond expectations and different actors in the world can participate in the international administration of justice to ensure their security and representativeness. Such a system will enable those with limited resources, geographical constraints and authoritarian regimes to file cases and let the system do the work for them. Moreover, it also provides security to the rest where they can search for a person's criminal record while doing business with him or her and also disable the latter from getting his record removed by unlawful means. Considering its application on Environmental Security and Financial Security simultaneously, Dubai is one great example where, by digitizing governmental work that initially included tangible documentation, it reduced its paper consumption by 65%, saving $193 million USD along with more than 20,000 trees in just a few years of its practice (Teale, 2020). Estonia on the other hand introduced the e-signature program which eliminated the need and use of paperwork by creating digital identities of its citizens. As a result, it saved 2% of the country's GDP which is equivalent to Estonia's defense budget.

The Sixth Stage- Democratization

Once it is ensured that digital infrastructure is no longer a liability but an asset that is not only working to save money but also to make it, it finally reaches the point of democratization. This is the point where the idea of smart city solutions can be taken up by countries one after another after witnessing the success and popularity of the rest. Moscow by taking the example of Estonia, Singapore and others, elevated itself from zero to number one in the UN's digital e-government ranking (UN, n.d). Estonia on the other hand has established a digital asset of its own to both demonetize and democratize its digitizing experience by offering Estonian e-residency to anyone from anywhere in the world as a gateway for Non-European countries to take part in European markets (e-Estonia, 2019). It can therefore be concluded that what started with a raw data later became an entire supply chain that has its own importable products as in the case of Estonia. The end product not only favoured Estonia as a digital nation but also set a precedent for how future networking between states can take place. It is important here to notice that a single digital potential, disruptive technologies in general and blockchain in particular that was realized through the discovery of cryptocurrency has possibilities of its application in numerous fields and a number of ways. If digitization for countries that carry material infrastructure in terms of population and territory is possible, the potential it carries for International organizations is way more than that. Doing so will not only make them efficient, their services improved and their expenditures reduced but will also increase transparency, accountability, data integrity and accurate representation of actors involved in the whole process. This will ultimately ensure that all voices are heard.

Recommendations

i. Governments are advised to design independent bodies that would digitize national databases based on blockchain technology. Considering the time taken during the stage of deception, an Independent body is an integral requirement to avoid the disruption that often comes with changes in the political atmosphere.
ii. Once the digital base is placed, governments can refine the raw data into establishing systems that are designed on DLT (distributive ledger technology), a controlled version of the blockchain to ensure control on the end of system owners and transparency on the end of systems' beneficiaries.

iii. Governments should also be ready for the reallocation of the economy as manual jobs would become redundant, especially at the later stages of digitization. Those involved in the process are encouraged to draw a road map and carry out this process in an organized manner.

iv. Once the systems are designed, they can be exported elsewhere to recover the design cost. An equally relevant alternative is to import systems (such as electoral systems) from states like Estonia or El Salvador to avoid the design cost. This would not only eliminate the reinvention of the wheel but would also save resources both in terms of time and money.

v. At this point, it would also be essential to systemize the profit generation capacity of these newly formed systems and make them an official part of the economy. For instance, digitizing taxation can save cost that is being invested in ensuring the transparency of state revenues manually. Once digitized, such regulatory cost can be utilized elsewhere.

vi. Lastly, sensitization with structural amendments powered by digitization should be made part of national curricula as a long-term goal while at the same time, professional training to ensure the same can also be organized as a short-term goal.

Conclusion

Through the use of (not so) Distruptive Technologies after all, actors with objects of referent ranging from state, constitution, corporations, organizations, and ideologies to citizens can be combined to form a system based on digital networking that adheres to the concerns of all. The lesson learned from going through failed or selective modernization processes can now be remedied while going through digital transformation. The possibility of doing so would have been discouraged or given the status of normative or wishful thinking had there not been a functional example of Estonia on board along with others. The advancement is neutral and thus is likely to be taken positively by the states as well as individuals. The potential for digitization has been realized by individuals, communities and businesses, in such a scenario, states must realize its potential and direct policymakers to carve policies synchronized with digitization. It is a phenomenon that many avoided due to its interoperability challenges but in the post-COVID world, entities were being forced into opting for it. Additionally, unlike modernity, there is no cultural force taking the lead of digitization ensuring its adoption to be free of imperial burdens making it a considerable option in development. Therefore, the idea is not to disrupt the integrity of the existing status-quo at once but to replace redundant systems with efficient ones and allow for alternate instruments that can ensure sovereign integrity, economic well-being and functional abilities of actors in the international system. It is not necessary for systems to be established one at the cost of another instead promotion of co-existence of systems as diversified as actors internationally are along with their diverse referent objects is the key to harmony in attaining a globally secure world and sustaibale peace.

Reference:

1. 2018 UN E-Government Survey | Multimedia Library - United Nations Department of Economic and Social Affairs. (n.d.). Retrieved from https://www.un.org/development/desa/publications/2018-un-e-government-survey.html
2. Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of business research*, *136*, 602-611.
3. Anusuya Datta, et al. “Top Disruptive Technologies and How They Are Relevant to Geospatial.” *Geospatial World*, 8 Nov. 2019, www.geospatialworld.net/blogs/top-disruptive-technologies-relevant-geospatial/.
4. Awan, F., & Nunhuck, S. (2020). Governing blocks: building interagency consensus to coordinate humanitarian aid. *The Journal of Science Policy and Governance*, *16*(2).
5. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*, *36*, 55-81.

6. Cox, J. R. (1990). Memory, critical theory, and the argument from history. *Argumentation and Advocacy*, *27*(1), 1-13.
7. Diamandis, P. H., & Kotler, S. (2015). *Bold: How to go big, create wealth and impact the world*. Simon and Schuster.
8. Ebersold, K., & Glass, R. (2015). THE IMPACT OF DISRUPTIVE TECHNOLOGY: THE INTERNET OF THINGS. *Issues in Information Systems*, *16*(4).
9. Extending one billion lives. (n.d.). Retrieved from https://medopad.com/
10. He, W., Shen, J., Tian, X., Li, Y., Akula, V., Yan, G., & Tao, R. (2015). Gaining competitive intelligence from social media data: Evidence from two largest retail chains in the world. *Industrial management & data systems*, *115*(9), 1622-1636.
11. Hirsch, D. D. (2013). The glass house effect: Big Data, the new oil, and the power of analogy. *Me. L. Rev.*, *66*, 373.
12. Hutchcroft, P. D. (2001). Centralization and decentralization in administration and politics: assessing territorial dimensions of authority and power. *Governance*, *14*(1), 23-53 Lee-Geiller, S., & Lee, T. (2022). How does digital governance contribute to effective crisis management? A case study of Korea's response to COVID-19. *Public Performance & Management Review*, *45*(4), 860-893.
13. Justice - e-Estonia. (2019, April 11). Retrieved from https://e-estonia.com/solutions/security-and-safety/e-justice/#:~:text=KSI technology here-,e-Law,Coordination System for Draft Legislation.`
14. Kannoly, A., Arun, S., Subramanian, G., Pandey, S. K., & Arumugaselvi, M. Impact of Blockchain in the Voting System.
15. Ko, V., & Verity, A. (2016). Blockchain for the humanitarian sector: future opportunities. *Digital Humanitarian Network*.
16. Kuo, C. C., & Shyu, J. Z. (2021). A cross-national comparative policy analysis of the blockchain technology between the USA and China. *Sustainability*, *13*(12), 6893.
17. Lana, R. M., Coelho, F. C., Gomes, M. F. D. C., Cruz, O. G., Bastos, L. S., Villela, D. A. M., & Codeço, C. T. (2020). The novel coronavirus (SARS-CoV-2) emergency and the role of timely and effective national health surveillance. *Cadernos de saude publica*, *36*, e00019620.
18. Li, R., Song, T., Mei, B., Li, H., Cheng, X., & Sun, L. (2018). Blockchain for large-scale internet of things data storage and protection. *IEEE Transactions on Services Computing*, *12*(5), 762-771.
19. List of historical acts of tax resistance. (2020, June 18). Retrieved from https://en.wikipedia.org/wiki/List_of_historical_acts_of_tax_resistance
20. Milan, S., & Hintz, A. (2013). Networked collective action and the institutionalized policy debate: bringing cyberactivism to the policy arena?. *Policy & Internet*, *5*(1), 7-26.
21. Millenaar, J. (2020, May 28). Selv Demo-A Digital Health Passport. Retrieved from https://blog.iota.org/selv-demo-a-digital-health-passport-c701bb381d29
22. Morris, David Z. (15 May 2016). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". *Fortune*. Archived from the original on 21 May 2016. Retrieved 23 May 2016
23. Real Vision Finance (2020, May 18). *Tech and Future of Governance* [Video] YouTube. URL https://www.youtube.com/watch?v=Osg98jLwo7s
24. Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: an interpretive case study. *Journal of Management Information Systems*, *38*(2), 338-373.
25. Sharma, T. K. (2019, October 15). Top Countries That Conducted Elections On The Blockchain. Retrieved from https://www.blockchain-council.org/blockchain/top-countries-that-conducted-elections-on-the-blockchain/

26. Teale, C. (2020, April 27). Dubai government cuts paper use by 65%. Retrieved from https://www.smartcitiesdive.com/news/dubais-electric-water-utility-leads-city-departments-paperless-efforts/576802/
27. Topalovic, M., Das, N., Burgel, P. R., Daenen, M., Derom, E., Haenebalcke, C., ... & Ninane, V. (2019). Artificial intelligence outperforms pulmonologists in the interpretation of pulmonary function tests. *European Respiratory Journal*, *53*(4), 1801660.
28. Treiblmaier, H., & Clohessy, T. (2020). *Blockchain and Distributed Ledger Technology Use Cases*. Springer.
29. Williams, P. D. (Ed.). (2012). *Security studies: an introduction*. Routledge.
30. Zenin, S., Kuteynikov, D., Izhaev, O., & Yapryntsev, I. (2019). Applying technologies of distributed registries and blockchains in popular voting and lawmaking: Key methods and main problems. *Amazonia Investiga*, *8*(20), 330-339.