eISSN 2656-8209 | pISSN 2656-1565
JURNAL INOVASI ILMU SOSIAL DAN POLITIK (JISoP)
Vol. 6, No. 2 (2024) pp. 104-115
Accreditation S3 – Decree No. 177/E/KPT/2024
https://riset.unisma.ac.id/index.php/JISoP/article/view/21574
DOI: 10.33474/jisop.v6i2.21574

The clarifying lawful overseas use of data (CLOUD Act): Counter-terrorism effort or reproduction of United States' hegemony in cyberspace?

Rizki Puji Gustian
Universitas Indonesia, Depok, Indonesia, email: rizki.puji@ui.ac.id

Article Info

Article history:
Submission: **2024-03-11**
Accepted: **2024-11-20**
Published: **2024-11-25**

ABSTRACT

Besides the emergence of new technology since the inception of technology industry 4.0, cyberspace has also emerged as a new spatial dimension apart from land, sea and air. Cyber security is not only tied to one region or country but has become a global issue. As a non-traditional security concern, cyberspace threats vary from state and non-state actors. The United States (US) responded to this threat by issuing the Clarifying Lawful Overseas Use of Data (CLOUD Act) policy. The CLOUD Act aims to give the US the legitimacy to gain access to data related to terrorism, violent crime, child exploitation, and cybercrime abroad that is stored with digital service providers from the US. This research tries to question why the United States uses the issue of terrorism in CLOUD Act. This research uses a non-traditional security perspective, namely, cyber security and human security in cyber space. Using qualitative methods with deductive approach utilizing the perspectives of Non-Traditional Security (NTS), this research sees the formation of the CLOUD Act as an exceptional US step involving the issue of terrorism, like other steps after the 9/11 tragedy. This article argues that the U.S. CLOUD Act strategically uses concerns about terrorism and cybercrime to legitimize exceptional measures for accessing data from U.S.-based digital platforms, reinforcing US hegemony in cyberspace. It highlights how this policy enables the US to exert global influence over digital infrastructures, often at the expense of privacy and multilateralism.

Keywords:
CLOUD Act; cybercrime; United States; hegemony

Please cite this article in APA style as:
Gustian, R. P. (2024). The clarifying lawful overseas use of data (CLOUD Act): Counter-terrorism effort or reproduction of United States' hegemony in cyberspace? *Jurnal Inovasi Ilmu Sosial dan Politik (JISoP)*, *6*(2), 104–115. https://doi.org/10.33474/jisop.v6i2.21574

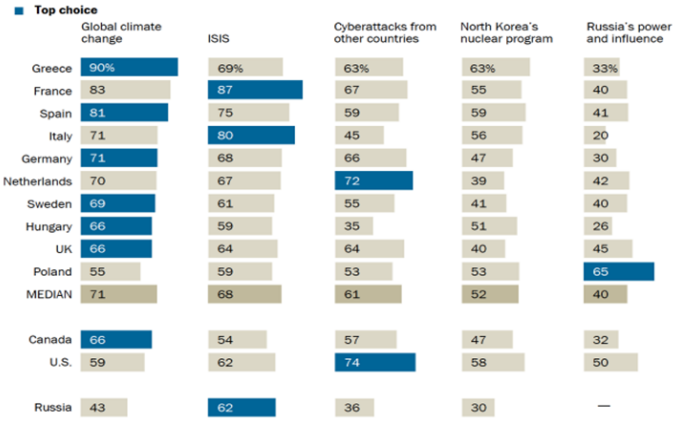
INTRODUCTION

The existence of cybertechnology cannot be separated from our lives. The emergence of cyber technology in various aspects of human and political activities has increased in the last two decades after the emergence of the COVID-19 pandemic. Cyber technology has been

adapted in various sectors and can eliminate physical boundaries so that people can connect with other people transnationally. A new wave of digitalization and the rise of platforms have occurred since 2008, facilitating the rapid transnationalisation of digital-based services. In addition, the COVID-19 pandemic has accelerated digital restructuring and a massive expansion of digital services. These services include remote work, drone delivery, cash-free payments, financial technology, tracking and surveillance technology, medical and legal services, remote teaching, and remote recording technology. The digital revolution 4.0 is different from the 3.0 revolution, where the 4.0 revolution creates a combination of new technologies and blurs the boundaries between the physical, digital and biological worlds. (Lupovici, 2023; Robinson, 2020).

Cybertechnology gives rise to a new spatial dimension, namely cyberspace. The classification of cyberspace as a new space after the Industrial Revolution 4.0 causes countries to face new challenges. Cyberspace is the fifth war domain after air, space, land and sea (Greiman, 2015). Adamson (2016) explained that cyberspace is a new political space created through technological innovation. This space is a place that allows users to be involved in activities carried out through an electronic field with a territorial domain that is able to go beyond traditional regional, governmental, social, and economic boundaries.

Based on a survey conducted by the Pew Research Center, Europe and North America view climate change as a major concern, but so do ISIS and cyber attacks. (Poushter & Huang, 2019). Cyber attacks are the top concern in the US, with threat perception at 74%, ISIS at 62%, and climate change at 59%. In 2018, there was an increase to 61% of respondents who saw cyber threats as a serious problem from previously only 54%.



Picture 1. Threat perception in 2018
Source: (Poushter & Huang, 2019)

Schwartz (2018) stated that the U.S. law enforcement is concerned about the potential of "going dark," a state in which they are unable to gain access to both stored and transmitted data. Thus, to respond to the emergence of violence in cyberspace, the United States Department of Justice (DOJ) in March 2018 enacted the Clarifying Lawful Overseas Use of Data Act or CLOUD Act, intending to accelerate efforts to gain access to electronic information from global digital platforms based in the US to be used in special criminal investigation efforts ranging from terrorism and violent crimes to sexual exploitation of children and cyber crimes (The Department of Justice United States, n.d.-a). According to Abraha (2019), the CLOUD Act is a response to the challenges US domestic and foreign law enforcement authorities face in accessing electronic evidence stored outside their territorial jurisdiction. Additionally, the CLOUD Act has 4 primary objectives. Those objectives are to enable US authorities to gain timely access to data stored outside the US, to allow foreign

governments to gain expeditious access to data stored in the US, to avoid potential conflicts of legal obligations, and to provide substantive and procedural protections.

This act provides permission for US foreign partners who prioritize the protection of privacy and civil liberties to be able to use law enforcement officers from partner countries to access electronic evidence to combat serious crime and terrorism (The Department of Justice United States, n.d.-b). The cooperation within the scope of the CLOUD Act is currently underway between the US and the UK. According to Rutherford (2019), This agreement or cooperation between the US and the UK is carried out within the scope of the UK's interests in carrying out digital data-sharing efforts to deal with terrorism issues and other serious actions. However, according to Rutherford, this raises new problems, considering the possibility of a public perception that the country's policies are becoming more conservative in data protection. Britain could be seen as more concerned with diplomatic relations with the US than prioritizing its people.

This cooperation between the US and the UK is considered a reform of the Mutual Legal Assistance Treaties (MLAT), which is considered inefficient (Abraha, 2019; Cochrane, 2021; Rutherford, 2019). In the MLAT process, requests for access require time and a complicated process through the country's legal system, not through the foreign government directly to the private entity that stores the data. With the CLOUD Act, law enforcement in foreign countries can directly convey their demands to companies in the US (Rutherford, 2019). However, Schwartz (2018) and Abraha (2019) criticized that the CLOUD Act could threaten countries with data localization policies who fear that their privacy, trade information and data sovereignty are threatened due to the US's business model and surveillance actions.

Criticism was also conveyed by the European Data Protection Board (EDPB) of the European Union (EU). European Data Protection Board (2019) stated that the CLOUD Act is not in line with the General Data Protection Regulation (GDPR) Article 49 regarding transferring personal data as stated in the US CLOUD Act. According to the EDPB, these requests require strict consideration and are difficult to fulfil. In addition, some EU member states have national laws that prevent digital service providers in the EU from disclosing information to third-party countries.

The issue of US interests in becoming a hegemon in cyberspace is also an interesting thing to discuss. Rovner dan Moore (2017) discuss the position of the US as the hegemon of the internet. Rovner and Moore also criticized Hegemonic Stability Theory (HST) in cyberspace, the internet, and the US position. They stated that cyber security as a "global public good" does not always require a hegemon. Apart from that, Rovner and Moore also discussed the decline in international cooperation regarding the internet with the US after the revelation of US involvement in the Stuxnet case in 2012 and the Snowden case.

The US effort to use the issue of terrorism in the CLOUD Act is an interesting thing to discuss further. Despite several rejections and criticisms, the US continues to campaign for its interests in gaining access to digital data in cyberspace produced by US digital platform providers operating abroad. This research seeks to offer novelty considering that some previous literature related to the CLOUD Act (Abraha, 2019; Cochrane, 2021; Rutherford, 2019) has not discussed the CLOUD Act from a non-traditional security or cyber security perspective. Literature on cyber security that has discussed the use of cloud computing, namely Skillicorn et al. (2016), has not discussed the relationship between the CLOUD Act and efforts to prevent terrorism.

METHOD

This article uses qualitative research methods with deductive approach. Qualitative research uses research strategies with an emphasis on words rather than counting or quantification in data

collection and analysis (Bryman, 2012; Neuman, 2014). This research uses CLOUD Act documents published by the US DOJ Criminal Division (Congress of the United States, 2018; The Department of Justice United States, n.d.-a) as its primary sources. Bryman (2012) Bryman stated that the government is the largest source of textual data for research discussion, such as Parliamentary Acts and official reports. This research also uses secondary sources, such as data related to cloud computing and cyberspace. Next, the author uses an illustrative method to analyze data introduced by Neuman (2014) based on the concepts of cyber security as non-traditional security (NTS) and criticism of US hegemony in cyberspace.

RESULT AND DISCUSSION

In this section, the author examines how terrorism concerns were strategically employed in shaping the CLOUD Act, utilizing a non-traditional security (NTS) lens that focuses on cyber security. By analyzing the intersection of terrorism and cyber security, the section underscores how these issues contribute to a broader agenda. The author draws upon previous literature on U.S. hegemony in cyberspace to contextualize the act's implications within global power dynamics. This perspective reveals the ways in which U.S. policies around cyber security and anti-terrorism create avenues for exerting influence and establishing control over global digital infrastructures. Ultimately, this approach highlights the CLOUD Act as a mechanism for reinforcing U.S. dominance in the cyber domain.

United States' Exceptional Effort in The CLOUD Act

Many academics have explored the U.S. agenda for combating terrorism from diverse perspectives, providing insights into how it shapes global security policies. Buzan & Hansen (2009), for instance, analyzed the Global War on Terror (GWoT) as a central U.S. response following the 9/11 attacks. They argued that the GWoT catalyzed a new framework for international relations, often described as the dynamic between "the West and the rest." Politically, this agenda not only strengthened alliances among Western nations but also redefined relationships with non-Western countries through security cooperation and ideological influence. As a dominant narrative, the GWoT has frequently been positioned as the successor to the Cold War, framing international security around terrorism and legitimizing U.S. leadership in cyberspace and beyond.

The 9/11 attacks more than twenty years ago in the United States sparked the emergence of issues and efforts to combat terrorism, which are still ongoing today and are the focus of NTS (Hameiri & Jones, 2013). These attacks and efforts to counter terrorism then spread to cyberspace. The Economist's statement in 2010 was one of the drivers of panic regarding the issue of war in cyberspace (Betz, 2012). Even though in May 2013, Obama declared that the war on terror was over, the impact of the war on terror continues until today (Korstanje, 2019). With the character of terrorism, which has a low probability but has a large impact, exceptional political and legal policies emerge, especially in the post-9/11 eradication of terrorism and the war against terror (Broeders et. al., 2021).

Sanders (2012) argues that the US practices exceptionalism, where the US imposes rules on other countries and refuses to apply external rules to the US. Although the US declares its commitment to the supremacy of international law, Sanders stated that US policymakers allow security and intelligence practices that he believes violate legal agreements and commitments, for example, in US actions in efforts to combat terrorism.

In the CLOUD Act as explained in the introduction, the CLOUD Act uses an exceptionalism perspective to achieve its goal of obtaining data from foreign countries (Bilgic, 2018). This was later criticized by the European Data Protection Board (2019) because the CLOUD Act was not in line with privacy protection regulations in several EU countries. In the Frequently Asked Questions regarding the CLOUD Act published by (The

Department of Justice United States, n.d.), it is explained that the objectives of the CLOUD Act are:

> "The United States enacted the CLOUD Act to improve procedures for both foreign and U.S. investigators in obtaining access to electronic information held by service providers. Such information is critical to investigations of serious crime by authorities around the world, ranging from **terrorism** and violent crime to sexual exploitation of children and **cybercrime**."

Bilgic (2018) states that in efforts to prevent terrorism, the US uses excessive surveillance techniques. In this case, the issues of terrorism, violent crime, sexual exploitation and cybercrime are threats that are of particular concern in the CLOUD Act. According to Bilgic (2018), the US government pays special attention to the issue of terrorism and puts aside privacy issues. The US is also starting to rely on data obtained by foreign governments that meets the requirements of the CLOUD Act. Electronic surveillance carried out by the US Government regarding domestic security matters needs to comply with the Fourth Amendment or the Electronic Communications Privacy Act (ECPA). However, other governments working with the US through the CLOUD Act may have more flexible regulations than US standards so that the US can more easily gain access to data within the foreign government's jurisdiction.

Cyber Technology, Cyber Security Concepts, and Cyber Capabilities

According to Hansen & Nissenbaum (2009), the concept of cyber security emerged after the Cold War as a response to changes in technology and geopolitical conditions. Cybersecurity was first presented in the 1990s by computer scientists to emphasize various insecurities in computer networks and threats arising from digital technology that could negatively impact society. Discussions regarding cyber security, which were considered capable of causing problems for the Western world, were conveyed by leading US figures, private companies and the media in the 1990s. Buzan & Hansen (2009) stated that during the Bill Clinton administration, the issue of cyber security became a concern for the US. However, GWOT efforts then made cyber security more complex and taken to a different level.

Hansen & Nissenbaum (2009) stated that the concept of cyber security was initially limited to computer security from a technical point of view, but with securitization, this concept emerged. The concept of computer security is only limited to creating programs that can prevent attacks by exploiting gaps in the system. However, adding the securitization discourse makes this concept a national security interest.

During Obama's leadership, to combat terrorism globally, the US combined the use of cyber technology and kinetic efforts to carry out more effective attacks. The drone war approved by Obama utilizes artificial intelligence (AI) or artificial intelligence to collect intelligence data to carry out targeted killings (McCrisken, 2013; Sanders, 2012). However, Khan et al. (2021) stated that the invasion using kinetic drone tactics, the arrest of civilians and the destruction of infrastructure within the GWoT framework was criticized because it was contrary to social values and general society. Warfare with drones also causes physical separation between drone users and targets (Adamson, 2016; McCrisken, 2013). Through the CLOUD Act, the US can receive intelligence data from foreign governments to launch kinetic efforts in fighting terrorism.

The assertion of global dominance by powerful states through surveillance technology, drone warfare, new military technologies, and intelligence activities occurs alongside the

global activities of non-state actors. The state also does not work alone in demonstrating its dominance in cyberspace. The US, for example, is working with Google Earth on its satellite technology (Adamson, 2016).

An online survey conducted in 2020 among member countries of the International Telecommunication Union (ITU) revealed that the U.S. leads globally in its commitment to cyber security, according to Petrosyan (2021). This commitment is measured by the Global Cybersecurity Index (GCI), which ranks countries based on their effectiveness and dedication to cyber security. The GCI evaluates performance across five key areas: legal frameworks, technical capabilities, organizational measures, capacity building, and international cooperation. Each of these components reflects a country's readiness to combat cyber threats and protect its digital infrastructure. The U.S.'s top ranking indicates its comprehensive and multifaceted approach to cyber security on a global scale, positioning it as a model for other nations in establishing robust cyber defense systems.

Characteristic	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	100	20	20	20	20	20
United Kingdom	99.54	20	19.54	20	20	20
Saudi Arabia	99.54	20	19.54	20	20	20
Estonia	99.48	20	20	20	19.48	20
Korea (Rep. of)	98.52	20	19.54	18.98	20	20
Singapore	98.52	20	19.54	18.98	20	20
Spain	98.52	20	19.54	18.98	20	20
Russian Federation	98.06	20	19.08	18.98	20	20
United Arab Emirates	98.06	20	19.08	18.98	20	20
Malaysia	98.06	20	19.08	18.98	20	20

Picture 2. Ranking of the ITU member countries most committed to cyber security
Source: (Petrosyan, 2021)

In addition to its top ranking in cyber security commitment, the United States is also recognized as the leading nation in both defensive and offensive cyber capabilities, according to the 2023 survey by the Lowy Institute Asia Power Index (2023). This dual strength indicates that the U.S. has developed advanced defenses to safeguard its own digital infrastructure, while also possessing sophisticated tools to conduct cyber operations when required. These offensive capabilities enable the U.S. to disrupt or disable the networks and systems of adversaries, highlighting its global influence as a formidable cyber power. By combining these defensive and offensive assets, the U.S. reinforces its proactive stance in protecting national interests and shaping international cyber norms. This leading position not only fortifies U.S. security but also strengthens its role in establishing standards for global cyber governance.

Picture 3. Country Cyber Capability Rankings 2021-2022
Source: (Lowy Institute Asia Power Index, 2023)

Security Dilemmas Regarding Cyberspace

This evolving cyber security race, marked by states rapidly advancing their digital arsenals, often leaves certain actors—such as activists—without comparable protections or resources. As countries strengthen their cyber capabilities to guard against perceived threats, individuals and groups working across borders become more exposed and vulnerable within this increasingly hostile environment. Consequently, this arms race in cyberspace creates a gap where these under-resourced actors face significant risks, amplifying the challenges they face in advocating for rights and democratic values amidst growing cyber pressures (Brantly, 2014). Furthermore, conflicts in the cyberspace may occur when non-physical information is stored in physical data centers, when intangible data is transformed into commodities within digital capitalism, and when territorial sovereignty is undermined by transnational cloud infrastructures. These conflicts can arise between the processes of commodification and spatialization, among different governance models, and between various stakeholders and interest groups (Tang, 2022).

Liaropoulos (2015) argued when discussing about cyberspace, it is crucial to determine if one perceives it as a worldwide network that encompasses only hardware, software, and information systems, or also includes individuals and the diverse array of social interactions that occur within this network. The issue of cybersecurity not only leads to a cycle of insecurity among nations on a global scale, but it also has adverse consequences within individual governments. The cyber capabilities developed to safeguard and protect a nation's essential national infrastructures are also employed to target its own citizens. Individuals are not the recipients of benefits, but rather the targets of national cybersecurity programs. The consequence of the ongoing competition in developing cyber capabilities is a decrease in the level of freedom on the Internet within individual nations. Filtering technologies that restrict access to specific websites, limitations on encryption usage, the creation of Internet kill switches, and the implementation of surveillance systems to monitor online activity are methods that significantly impact privacy, anonymity, and consequently, security.

Liaropoulos (2015) also stated that Preserving privacy on the Internet is inherently unattainable. Both governments and corporations are extensively gathering private data on a large scale. Search engines and online social networking sites, like Google and Facebook, own comprehensive user profiles, while cell phone firms employ GPS technology to monitor and determine the whereabouts of its customers. Private data is systematically stored, and individuals' online conduct and consumer patterns are linked and transmitted from corporations to governments, often without the users' awareness or agreement.

In the context of cyberspace, human rights pertain to the rights outlined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), as established by the United Nations. These rights encompass freedom of expression, freedom of speech, freedom of opinion, and the right to privacy. In July 2012, the UN Human Rights Council affirmed that the rights individuals possess in the physical world must also be safeguarded in the digital realm (Rossini & Green, 2015).

The effort of US law enforcement in the cyberspace in regards of CLOUD ACT to tackle the issue of terrorism should also be discussed in the perspective of human rights in cyberspace. van Daalen (2023) stated that primary arguments against the Government's attempts to get data through decryption revolve around fundamental human rights, particularly the rights to privacy and freedom of expression. In October 2019, US Human Rights Groups expressed their opposition to the US Government about the CLOUD ACT, which has the potential to facilitate the transfer of personal data to other governments without adhering to conventional legal procedures. A critical human rights protection in the Mutual Legal Assistance Treaty (MLAT) process is a requirement that a U.S. entity, namely the DOJ and a judge, review a foreign request for content to ensure that it does not raise human rights concerns. Such a protection is critical because even generally rights-respecting jurisdictions may have particular laws or practices that raise human rights concerns (Human Rights Watch, 2019).

US Dominance and Hegemony in Cyberspace

U.S. policy on internet governance has often been driven by a strategic aim to promote its political influence globally. Through various initiatives, the internet has been positioned as a tool to disseminate U.S. political ideals and products internationally. This approach aligns with a longstanding national interest of expanding influence abroad to maintain peace and prosperity both domestically and globally. Kiggins (2015) criticizes US policy towards internet multilateralism. Kiggins stated that US policymakers made the internet a platform for expanding US political products and views. These findings align with the "Open Door" approach outlined in US national interests and foreign policy. "Open Door" argues that it is in the US national interest to expand overseas to ensure US peace and prosperity at home and abroad. Regarding multilateralism, policymakers in the US are concerned that multilateralism in global internet governance could hinder the US goal of making the internet a platform for expansion.

In the CLOUD Act, it is stated in “Sec. 105 Executive Agreements on Access to Data by Foreign Governments” that this law is limited only to countries that have domestic laws that comply with US standards regarding the supremacy of law, non-discrimination principles, and respect for human rights (Congress of the United States, 2018). As a relaxation of the MLAT, the CLOUD Act will only be approved by countries trusted by the US (Abraha, 2019).

Rovner and Moore (2017) question the need for a hegemon on the internet. Cybersecurity is a global public good, but cybersecurity cooperation is not easy to form, and other countries do not welcome assistance from the US. Apart from that, there are concerns that state intervention could cause the internet, which was originally an apolitical dimension of space for the exchange of opinions and freedom of thought, to become fragmented when the state uses its interests in cyberspace.

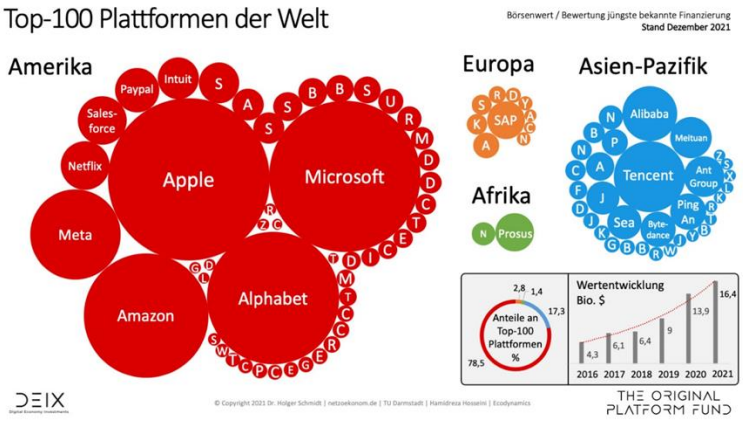
The next argument by Rovner & Moore (2017) is a critique of hegemony in cyberspace. HST is criticized because dominant countries can cause fear in other smaller countries rather than produce peace and prosperity in cyberspace. In addition, Rovner & Moore (2017) explain that to keep global cyber security intact; the US actually needs to eliminate the practices of offensive cyber operations (OCO) and cyber espionage because the global

internet system can become fragile if the dominant country is not sensitive to the impact from the actions of those who prioritize their own interests.

In line with criticism of the hegemon, the formation of the CLOUD Act shows aggressiveness and an effort to establish US dominance in cyberspace. The US effort to be a hegemon can be seen not only in the US's position as the number one country in terms of cyber security commitment and cyber capabilities. The US also dominates online service provider platforms (Andreoni & Roberts, 2020), especially the dominance of the 3 (three) giant cloud computing service providers Amazon, Microsoft, and Google from the US (Vailshery, 2024).

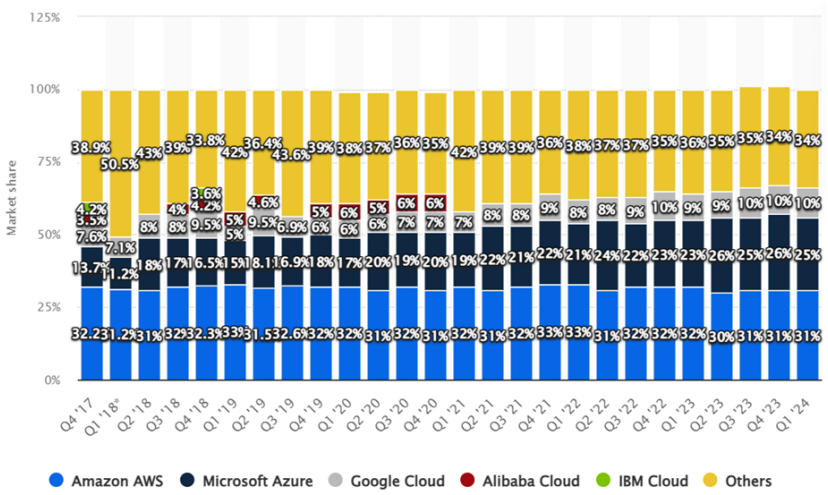
The formation of the CLOUD Act cannot be separated from cloud computing technology, considering that this technology functions as a data centre used to store and manage user data. In the industrial world, the use of artificial intelligence in cloud computing can be used to personalize service offerings to users by analyzing user habits and patterns (Garg, et al. 2023). Therefore, the CLOUD Act is considered a solution for US law enforcement and US-approved foreign countries in obtaining data (Abraha, 2019), but it has been widely criticized for being at odds with digital privacy rights (Cochrane, 2021).

The United States significantly dominates the global digital market, holding a substantial share of the market capitalization of the largest digital platforms. It is home to several key "super platforms," including Microsoft, Apple, Amazon, Google, and Facebook, which collectively account for two-thirds of the total market value. Google alone controls about 90% of the internet search market, while Facebook captures two-thirds of the global social media market. Amazon commands nearly 40% of the world's online retail activity. In the realm of cloud computing, the U.S. leads with over 75% of the public cloud market share alongside China. Additionally, American platform companies represent 40% of global spending on the Internet of Things (IoT) and dominate investments in data centers, which has major implications for data ownership (Andreoni & Roberts, 2020).



Picture 4. Dominant digital platforms and their geographic distribution
Source: Andreoni & Roberts (2020) and Schmidt (2021)

Moreover, according to Vailshery (2024), US plays a pivotal role in shaping the landscape of digital platforms in cyberspace. This dominance is particularly evident in the cloud computing sector, where three major American companies—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud—together controlled over 50% of the global digital cloud computing market from 2017 to 2022. This significant market share illustrates not only the technological prowess of these firms but also highlights how they are integral to the infrastructure of the internet and digital services worldwide.



Picture 5. Cloud computing ranking based on market share from 2017-2024
Source: (Vailshery, 2024)

The implications of this dominance extend beyond mere market share; they also influence legal and regulatory frameworks. For instance, the CLOUD Act allows U.S. authorities to request data from American companies regardless of where that data is stored globally. By framing issues like terrorism as justifications for such exceptional policies, the U.S. government can effectively assert its jurisdiction over data that transcends international boundaries. This strategic move not only bolsters the operational reach of U.S. law enforcement but also reinforces the hegemonic position of U.S. digital platforms in the global cyberspace.

As a result, these policies can further entrench U.S. dominance in digital infrastructure and data governance. By leveraging national security concerns, the U.S. can create a regulatory environment that favors American companies, thereby solidifying their market leadership and extending American influence over global cyberspace. This dynamic ultimately contributes to the broader narrative of U.S. hegemony in the digital age, allowing the country to shape international norms and standards in ways that align with its interests.

CONCLUSION

From the NTS perspective, efforts to establish the CLOUD Act can be seen as a US cyber security effort in preventing things that pose US threats in cyberspace as a new dimension. In establishing the CLOUD Act, the US used the issue of terrorism and cybercrime to obtain data from digital platforms from the US within the jurisdiction of foreign governments. Like other cyber or military operations carried out by the US after 9/11, the issue of terrorism and cybercrime was used as an exceptional measure so that the US could fulfil its national interests by taking shortcuts in executive cooperation. However, the US limits CLOUD Act cooperation to only countries that comply with US standards. The US has been criticized for prioritizing its national interests regarding terrorism and ignoring digital privacy rights. Through establishing the CLOUD Act, US dominance in cyber security efforts and cyber capabilities, as well as the dominance of its digital platforms, especially cloud computing, the US can also be seen as a country that shows its strength and rejects multilateralism that does not meet its standards.

REFERENCES

Abraha, H. H. (2019). How compatible is the US "CLOUD Act" with cloud computing? A brief analysis. *International Data Privacy Law*, *9*(3), 207–215. https://doi.org/10.1093/idpl/ipz009

Adamson, F. B. (2016). Spaces of global security: Beyond methodological nationalism. *Journal of Global Security Studies*, *1*(1), 19–35. https://doi.org/10.1093/jogss/ogv003

Andreoni, A., & Roberts, S. (2020). Governing data and digital platforms in middle income countries: regulations, competition and industrial policies, with sectoral case studies from South Africa Digital Pathways Paper Series. In *Digital Pathways at Oxford Paper Series: Vol. Paper 5* (Issue Paper 5).

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies*, *35*(5), 689–711. https://doi.org/10.1080/01402390.2012.706970

Bilgic, S. (2018). Something Old, Something New, and Something Moot: the Privacy Crisis Under the Cloud Act. *Harvard Journal of Law & Technology*, *32*(1), 321–355.

Brantly, A. F. (2014). The Cyber Losers. *Democracy and Security*, *10*(2), 132–155. https://doi.org/10.1080/17419166.2014.890520

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. *Studies in Conflict and Terrorism*, *0*(0), 1–28. https://doi.org/10.1080/1057610X.2021.1928887

Bryman, A. (2012). *Social Research Methods* (4th Editio). Oxford University Press.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge University Press.

Cochrane, T. (2021). Digital Privacy Rights and CLOUD Act Agreements. *Brooklyn Journal of International Law*, *47*(1). https://brooklynworks.brooklaw.edu/bjil/vol47/iss1/1

Congress of the United States. (2018). *Cloud Act - Clarifying Lawful Overseas Use of Data Act*.

European Data Protection Board. (2019). *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence* (Issue March 2018).

Garg, S., Mahajan, N., & Ghosh, J. (2023). Industry 4.0 and the Digital Transformation of International Business. In G. Singh, R. Goel, & V. Garg (Eds.), *Industry 4.0 and the Digital Transformation of International Business*. Springer Nature Singapore. https://doi.org/10.1007/978-981-19-7880-7

Greiman, V. (2015). Cybersecurity and Global Governance. *Journal of Information Warfare*, *14*(4), 1–14. https://www.jstor.org/stable/26487502

Hameiri, S., & Jones, L. (2013). The politics and governance of non-traditional security. *International Studies Quarterly*, *57*(3), 462–473. https://doi.org/10.1111/isqu.12014

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Human Rights Watch. (2019). *Groups Urge Congress to Oppose US-UK Cloud Act Agreement*. Human Rights Watch.

Khan, S., Sohail, U., & Shah, S. T. (2021). The Violent Toll of Kinetic Counterterrorism: Revitalizing Non-Kinetic Counterterrorism Model. *ISSRA Papers*, *13*, 27–40. https://doi.org/10.54690/issrap.v13ixiii.103

Kiggins, R. D. (2015). Open for expansion: US policy and the purpose for the internet in the post-cold war era. *International Studies Perspectives*, *16*(1), 86–105. https://doi.org/10.1111/insp.12032

Korstanje, M. E. (2019). Terrorism, Technology and Apocalyptic Futures. In *Terrorism, Technology and Apocalyptic Futures*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-13385-6

Liaropoulos, A. (2015). A Human-Centric Approach to Cybersecurity: Securing the Human in

the Era of Cyberphobia. *Journal of Information Warfare*, *14*(4), 15–24. https://www.jstor.org/stable/26487503

Lowy Institute Asia Power Index. (2023). *Cyber capabilities data - Lowy Institute Asia Power Index*. Lowy Institute Asia Power Index.

Lupovici, A. (2023). Ontological security, cyber technology, and states' responses. *European Journal of International Relations*, *29*(1), 153–178. https://doi.org/10.1177/13540661221130958

McCrisken, T. (2013). Obama's Drone war. *Survival*, *55*(2), 97–122. https://doi.org/10.1080/00396338.2013.784469

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches 7th Edition* (7th ed., Issue 1). Pearson Education Limited.

Petrosyan, A. (2021). *Top countries GCI cyber security ranking 2020 | Statista*. Statista.

Poushter, J., & Huang, C. (2019). *Climate Change Still Seen as Top Global Threat, but Cyberattacks Rising Concern | Pew Research Center*. Pew Research Center.

Robinson, W. I. (2020). Global capitalism post-pandemic. *Race and Class*, *62*(2), 3–13. https://doi.org/10.1177/0306396820951999

Rossini, C., & Green, N. (2015). *Cybersecurity and Human Rights*.

Rovner, J., & Moore, T. (2017). Does the Internet Need a Hegemon? *Journal of Global Security Studies*, *2*(3), 184–203. https://doi.org/10.1093/jogss/ogx008

Rutherford, M. (2019). The CLOUD Act: Creating Executive Branch Monopoly Over Cross-Border Data Access. *Berkeley Technology Law Journal*, *34*(4), 1177–1204. https://doi.org/10.2139/ssrn.3508942

Sanders, R. (2012). *Exceptional Security Practices , Human Rights Abuses , and the Politics of Legal Legitimation in the American " Global War on Terror ."* University of Toronto.

Schmidt, H. (2021). *Plattform-Ökonomie*. Netzoekonom.

Schwartz, P. M. (2018). Legal Access to the Global Cloud. *Columbia Law Review*, *118*(6), 1681–1762. https://doi.org/10.2139/ssrn.3008392

Skillicorn, D., Leuprecht, C., & Tait, V. (2016). Computing in Compromised Environments: Beyond the Castle Model of Cyber-Security. In A. Masys (Ed.), *Exploring the security landscape : non-traditional security challenges*. Springer International Publishing Switzerland.

Tang, M. (2022). The challenge of the cloud: between transnational capitalism and data sovereignty. *Information Communication and Society*, *25*(16), 2397–2411. https://doi.org/10.1080/1369118X.2022.2128598

The Department of Justice United States. (n.d.-a). *CLOUD Act Resources*.

The Department of Justice United States. (n.d.-b). *The Purpose and Impact of the CLOUD Act - FAQs*.

Vailshery, L. S. (2024). *Global cloud infrastructure market share 2022 | Statista*. Statista.

van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law and Security Review*, *49*, 105804. https://doi.org/10.1016/j.clsr.2023.105804