Intellectual Discourse

Volume 33 Special Issue 2025

Special Issue on

The Intersection of Theory, Identity, and Security in PCVE (Preventing and Countering Violent Extremism)

International Islamic University Malaysia
https://journals.iium.edu.my/intdiscourse/index.php/id

Intellectual Discourse

Volume 33 Special Issue 2025

Intellectual Discourse is a highly respected, academic refereed journal of the International Islamic University Malaysia (IIUM). It is published twice a year by the IIUM Press, IIUM, and contains reflections, articles, research notes and review articles representing the disciplines, methods and viewpoints of the Muslim world.

Intellectual Discourse is abstracted in SCOPUS, WoS Emerging Sources Citation Index (ESCI), ProQuest, International Political Science Abstracts, Peace Research Abstracts Journal, Muslim World Book Review, Bibliography of Asian Studies, Index Islamicus, Religious and Theological Abstracts, ATLA Religion Database, MyCite, ISC and EBSCO.

ISSN 0128-4878 (Print); ISSN 2289-5639 (Online)

https://journals.iium.edu.my/intdiscourse/index.php/id
Email: intdiscourse@iium.edu.my; intdiscourse@yahoo.com

Published by:
IIUM Press, International Islamic University Malaysia
P.O. Box 10, 50728 Kuala Lumpur, Malaysia
Phone (+603) 6196-5014, Fax: (+603) 6196-6298
Website:http://iiumpress.iium.edu.my/bookshop

Intellectual Discourse
Volume 33, Special Issue on
The Intersection of Theory, Identity, and Security in PCVE (Preventing & Countering Violent Extremism), 2025

Contents

Transliteration Table: Consonants

Arabic	Roman		Arabic	Roman
ب	b		ط	ṭ
ت	t		ظ	ẓ
ث	th		ع	‘
ج	j		غ	gh
ح	ḥ		ف	f
خ	kh		ق	q
د	d		ك	k
ذ	dh		ل	l
ر	r		م	m
ز	z		ن	n
س	s		ه	h
ش	sh		و	w
ص	ṣ		ء	’
ض	ḍ		ي	y

Transliteration Table: Vowels and Diphthongs

Arabic	Roman		Arabic	Roman
◌َ	a		◌ًا، ◌ًى	an
◌ُ	u		◌ٌو	un
◌ِ	i		◌ٍي	in
◌َا، ◌ٰ، ◌َى،	ā		◌َوْ	aw
◌ُو	ū		◌َيْ	ay
◌ِي	ī		◌ُوّ	uww, ū (in final position)
			◌ِيّ	iyy, ī (in final position)

Source: ROTAS Transliteration Kit: http://rotas.iium.edu.my

Intellectual Discourse, special issue 1 (2025) 201–227

ISSN 0128-4878 (Print); ISSN 2289-5639 (Online)

Terrorism Industry: Digital Data Coloniality in Southeast Asia

Mohammed Ilyas*

Abstract: The decolonisation of academia has become a popular topic among scholars, students, and activists in both Western and non-Western contexts. This movement has sparked numerous publications and initiatives advocating for decolonisation, yet the focus has been predominantly on social sciences. In contrast, the phenomenon of digital data colonialism has received comparatively little attention, particularly within non-Western countries. Digital data colonialism merges the extractive practices of historical colonialism with the computational capabilities of modern technologies, allowing for the quantification and commodification of online activities. The main agents perpetuating this form of colonialism are large technology corporations and intelligence agencies from powerful Western nations. These tech companies gather massive amounts of digital data, subsequently selling it to businesses and governmental agencies. The latter utilises the data in the name of national security and the global fight against extremism and terrorism, a practice that impacts both Western and non-Western populations. This paper explores the digital data colonisation of non-Western nations, focusing particularly on Muslim-majority countries in Southeast Asia and the role of Western intelligence agencies and technology companies in this process.

Keywords: Data Colonialism, Coloniality, West, Non-West, securitisation, intelligence gathering.

Abstrak: Dekolonisasi akademia telah menjadi topik popular di kalangan sarjana, pelajar dan aktivis dalam konteks Barat dan bukan Barat. Pergerakan ini telah mencetuskan banyak penerbitan dan inisiatif yang menyokong dekolonisasi, namun tumpuannya telah tertumpu kepada sains sosial.

* Lecturer in Criminology, College of Business, Law and Social Sciences, University of Derby. Email: m.ilyas@derby.ac.uk

Sebaliknya, fenomena kolonialisme data digital telah mendapat perhatian yang agak sedikit, terutamanya dalam negara bukan Barat. Kolonialisme data digital menggabungkan amalan ekstraktif kolonialisme sejarah dengan keupayaan pengiraan teknologi moden, membolehkan pengiraan dan komodifikasi aktiviti dalam talian. Agen utama yang mengekalkan bentuk penjajahan ini ialah syarikat teknologi besar dan agensi perisikan dari negara Barat yang kuat. Syarikat teknologi ini mengumpulkan sejumlah besar data digital, kemudian menjualnya kepada perniagaan dan agensi kerajaan. Agensi perisikan dan sekuriti kerajaan menggunakan data atas nama keselamatan negara dan perjuangan global menentang ekstremisme dan keganasan, satu amalan yang memberi kesan kepada penduduk Barat dan bukan Barat. Kertas kerja ini meneroka penjajahan data digital negara bukan Barat, memfokuskan terutamanya kepada negara majoriti Islam di Asia Tenggara dan peranan agensi perisikan Barat dan syarikat teknologi dalam proses ini.

Kata kunci: Kolonialisme data, Kolonialiti, Barat, Bukan Barat, pensekuritian, pengumpulan risikan.

Introduction

In recent decades, the discourse surrounding colonialism, decolonisation, and coloniality has garnered significant attention among scholars and students in both Western and non-Western contexts (Said, 1979; Connell, 2007; Alatas, 2000; Grosfoguel, 2013; Mignolo, 2011; Mwambari, 2020; Kwet, 2019; Steinmetz, 2017). This growing interest has led to two key outcomes. First, there have been calls to decolonise the social sciences in countries such as South Africa, the United Kingdom, and the United States (Bhambra et al., 2018). Second, scholars like Tuck and Yang (2012) have advocated for radical decolonisation, emphasising the need for "practical decolonisation" and cautioning against what they term "moves to innocence" — superficial gestures that fail to address structural inequalities.

However, discussions concerning digital data colonialism, particularly by Western technology corporations and intelligence agencies in non-Western countries, such as the Muslim-majority nations of Southeast Asia, remain limited. While some scholarship has explored issues related to internet ownership, access, infrastructure, and the exploitation of user data by Western technology giants such as Facebook, Google, Apple, and Amazon (Zuboff, 2019; Mejias and Couldry, 2020,

2024; Jim et al., 2016; Kwet, 2019; Coleman, 2019; Pinto, 2018; Youn, 2019; Monique and Angela, 2019; Notias, 2020), broader critiques of digital data colonialism, especially Artificial Intelligence (AI) as a tool for radicalisation (Nelu, 2024, Burton, 2023) and a form of counter-terrorism and predictive policing have yet to be fully integrated into decolonial frameworks. Although the use of AI has been lauded 'as a magic bullet' to predict extremists, but there are many problems with such technology, ranging from racial bias to misuse by governments (Voronkov and Marie De Meo, (2021). Therefore, interrogation on how AI is/will be used by governments of powerful Global North countries at home and abroad, especially in the Muslim majority contexts, like Southeast Asia Muslim- is imperative to guard against perpetuating the colonialities.

The 2013 Snowden revelations sparked conversations about the extensive data-gathering practices of intelligence agencies from powerful Western nations and their allies, such as the Five Eyes alliance, SIGINT Senior Europe, and SIGINT Senior Pacific. These agencies collect vast amounts of digital data through various means, including internet surveillance, biometric systems, geospatial technologies, and drones. The data gathered enables these Western powers to exert control over global populations, particularly in the realm of securitisation, thus reinforcing their political and economic dominance over rival nations (The Intercept, 2018; Dorling, 2014; UNHCR, 2015; Thoma, 2018; Kaurin, 2019; Jacobson, 2017; Mejias and Couldry, 2020; Babuta et al., 2020). Despite these significant discussions, they have not been framed explicitly through a decolonial lens, leaving a gap in critical engagement with the colonial dimensions of digital data practices in Southeast Asian Muslim-majority countries.

This situation has also contributed to what Byler and Boe (2019) refer to as "terror capitalism," a phenomenon rooted in the global "War on Terror" that raises significant concerns regarding human rights. The war has justified the widespread development and deployment of digital data-gathering and surveillance technologies in counterterrorism initiatives, often at the expense of fundamental human rights. One illustrative example is Faception, an Israeli company that uses machine learning to analyse facial images and purportedly infer individuals' personalities in real time (Faception, 2020). Israel has deployed this type of technology against Palestinians, and in Berlin, the German

government has used similar technology, though it has raised serious ethical and human rights concerns, as documented in reports by Amnesty International (Baz, 2019; Huggler 2017, Amnesty International, 2023).

Another prominent case is the Israeli company NSO Group Technologies, which develops sophisticated spyware that is sold to various governments to surveil individuals deemed to be a "threat" to national security (Marczak et al., 2018). Similarly, Chinese companies like Yitu have collaborated with the Malaysian government to develop artificial intelligence (AI) software, including facial recognition technologies, to assist police forces in identifying criminals (Tao, 2018). The application of these technologies, particularly in the context of digital data surveillance, raises profound ethical issues, including concerns about extrajudicial killings and the deployment of racially biased algorithms. For example, the "Future Dangerousness" program, used in U.S. courts, has been criticised for its reliance on such algorithms (O'Neil, 2016).

Although digital data colonialism grants Western nations significant economic and political advantages, it has also faced considerable critique. Western civil rights organisations have raised serious concerns about data privacy and the ethical consequences associated with these technologies (Mejias and Couldry, 2020). However, these criticisms are predominantly centred on the impact of data practices within Western contexts. In contrast, the broader implications of digital data colonialism in non-Western regions, particularly in Southeast Asian Muslim-majority countries, remain largely neglected. This oversight highlights a significant gap in the academic discourse concerning the global scope and ethical ramifications of digital surveillance technologies, particularly in relation to their uneven and often detrimental impact on non-Western societies.

This paper builds upon and extends the definition of the "terrorism industry" as conceptualised by Herman and O'Sullivan (1989: 55-213). For the purposes of this study, the terrorism industry encompasses a range of actors, including the intelligence agencies of powerful Western countries and their allies, think tanks, lobbying organisations, research centres, security firms, scholars, media corporations, private military companies, technology firms, and non-governmental organisations (NGOs). The most influential entities within this industry are primarily

situated in Western nations or allied states. Emerging as an extension of counterinsurgency studies in the 1970s, the terrorism industry originally developed in response to the perceived threat posed by the Soviet Union to Western powers. However, it was not until the events of September 11, 2001, that the terrorism industry—along with its academic counterpart, terrorism studies—gained significant relevance due to the proliferation of technology and knowledge it generated (Stampnitzky, 2014).

Historically, during the colonial era, counterinsurgency efforts were instrumental in undermining independence movements, such as those in Malaysia (French, 2011; Hack, 1999, 2009). The success of counterinsurgency campaigns has long relied on the effective collection of intelligence regarding movements or groups perceived as threats to national interests (Komer, 1972; Yazid, 2019; Comber, 2008; Karari, 2018; Balce, 2016). In contemporary times, the intelligence-gathering arm of the terrorism industry continues to collect both traditional and digital data on populations, movements, and groups that nations such as the United States and the United Kingdom consider risks to their geopolitical and national interests. This shift to digital surveillance marks an evolution in how intelligence is gathered and utilised in the modern era of counterterrorism.

This paper seeks to initiate a critical examination of the relationship between the terrorism industry and digital data colonialism in Southeast Asian Muslim-majority countries. The scope of this study is intentionally focused, centring on the role of intelligence agencies from powerful Western nations and their allied networks, such as the Five Eyes, SIGINT partners, and SIGINT Pacific. These agencies play a pivotal role in perpetuating colonialities by operating within the broader framework of the terrorism industry. Through the collection and analysis of data, these intelligence agencies produce the knowledge necessary to devise strategies and programs that sustain and reproduce colonial power dynamics in the digital age. This paper has a modest remit and aims to start a discussion on the relationship between the terrorism industry and digital data colonialism and the continuity of colonialities of non-Western countries. The paper focuses on the intelligence agencies of powerful Western countries and their allies (Five Eyes, SIGINT partners and SIGINT Pacific) because they are part of the terrorism industry and play a vital role in coloniality non-Western

countries. The intelligence-gathering agencies provide the data and knowledge to develop strategies and programs that enable non-Western countries to reproduce colonialities.

The paper is organised into three main sections. The first section introduces the decolonial theoretical framework that underpins the analysis. The second section explores the collaboration between intelligence agencies from powerful Western nations and Western technology companies, illustrating how these entities work in concert to perpetuate coloniality. The third section provides an in-depth examination of the digital data colonisation of Southeast Asian Muslim-majority countries by Western powers. In conclusion, the paper calls upon scholars from Southeast Asian Muslim-majority countries to take two critical steps. First, they should adopt a decolonial perspective to analyse how the terrorism industry engages in digital data colonialism, thereby reinforcing coloniality within their national contexts. Second, scholars invested in the decolonisation of Southeast Asian Muslim-majority countries must seek practical methods to implement Tuck and Yang's (2012) recommendations for dismantling coloniality in their respective nations.

Decolonial Concepts

Digital data colonialism, however, is not solely driven by Western technology companies but also by the intelligence agencies of powerful Western nations and their non-Western allies. This form of colonialism leverages advanced surveillance and data extraction technologies for the purpose of digital intelligence gathering. While profit generation can be a byproduct of these activities, the primary motivation for powerful Western states is the acquisition of economic and political advantages over global competitors. This strategy often involves the securitisation of resource-rich non-Western countries deemed as threats to national interests, such as the Muslim-majority countries in Southeast Asia. The revelations from the Snowden NSA leaks exposed the extent of digital data colonialism conducted by intelligence agencies, particularly in the United States and the United Kingdom. These disclosures unveiled the vast scope of surveillance operations targeting billions of social media users and the widespread espionage on both allied and adversarial governments, underscoring the pervasive nature of digital data colonialism undertaken by these nations.

One way to conceptualise the power conferred by digital data colonialism to Western nations and their allies is through the metaphor of a 'God-Eye view,' wherein these actors gain the capacity to see and know everything. Simultaneously, this power entails omnipresence—being everywhere at all times—achieved through the use of advanced surveillance technologies. This 'God-Eye view' represents a continuation of the epistemic dominance that originated with the genocides and epistemicides of the 16th century, which laid the groundwork for Descartes' famous dictum, *Cogito, ergo sum* ("I think, therefore I am") (Grosfoguel, 2013). In this context, the "I" refers exclusively to the white Western male, whose culture and epistemologies were deemed superior, granting him the unique capacity for thought, knowledge production, and agency (Grosfoguel, 2013). In contrast, as Maldonado-Torres (2014) observes, the implicit counterpart to this statement is "I do not think, therefore I am not," which relegates non-Western, non-white individuals and their cultures to an inferior status, devoid of intellectual agency (Quijano, 2007).

In contemporary terms, Descartes' "I" can be interpreted as representing powerful Western countries and their allies. Digital data colonialism grants them unprecedented control over both the present and future. This control enables them to shape, direct, manage, and dominate the futures of non-Western nations, extending their hegemonic influence through the collection, quantification, and commodification of digital data.

The second key concept is coloniality, which Mignolo (2011) refers to as the "dark side" of modernity. For Mignolo, modernity and coloniality are inextricably linked, with colonialities representing the hidden underside of modernity's progress. This interconnected power dynamic has come to shape all aspects of life, including culture, education, politics, and the production of knowledge (Maldonado-Torres, 2007; Grosfoguel, 2006). Coloniality can be understood through three distinct dimensions: the coloniality of power, the coloniality of knowledge, and the coloniality of being. Each of these dimensions explains different facets of the overarching structure of coloniality (Ndlovu-Gatsheni, 2013).

The coloniality of power refers to the persistence of colonial systems of domination, primarily structured around race and racism,

which intersect with other categories of social stratification, such as gender and class. This system forms the organising principle underpinning global capitalism hierarchies, including labour, economic exploitation, and gender inequalities (Grosfoguel, 2011). The coloniality of power is evident at the institutional level, manifesting in the operations of international financial and political organisations such as the International Monetary Fund (IMF), the World Bank, NATO, the European Union (EU), and the United Nations (UN), as well as the intelligence agencies of powerful Western nations (Ndlovu-Gatsheni, 2013; Grosfoguel, 2006).

The coloniality of knowledge pertains to the displacement of local epistemologies and worldviews by Eurocentric forms of knowledge, which claim scientific legitimacy and universality. This epistemic domination results from what scholars like Quijano (2007) have termed the "epistemicide" of non-Western knowledge and belief systems. As a result, intellectual imperialism is perpetuated, creating a situation in which non-Western scholars often seek validation from Western academic frameworks due to the dominance of Western epistemologies, which assert objectivity and universal applicability (Bolivar, 2010; Alatas, 2000; Santander, 2010; Grosfoguel, 2006; Santos, 2014, 2018).

In the context of digital data colonialism, Western technology companies and intelligence agencies maintain the coloniality of knowledge. Through the extraction, quantification, and commodification of digital data, these entities continue to reinforce the coloniality of non-Western nations, such as the Muslim-majority countries of Southeast Asia. Digital data is used to further economic, political, and security policy objectives, thereby perpetuating the structures of domination and control that are characteristic of coloniality.

The third dimension of coloniality is the coloniality of being, which establishes a binary distinction wherein the West is constructed as the "zone of being," while the non-West is relegated to the "zone of non-being." This dichotomy is rooted in Descartes' famous assertion, *cogito ergo sum* ("I think, therefore I am"), implying that only Western, white men possess the capacity for thought and thus the full quality of existence, while the non-Western "Other" is denied this ontological status (Maldonado-Torres, 2007; Grosfoguel, 2016). The coloniality of being is the culmination of the coloniality of power and knowledge,

functioning as a mechanism for the dehumanisation and subjugation of those positioned below the "abyssal line." Decolonial scholars use the concept of the abyssal line to delineate the profound economic, social, cultural, political, and linguistic divisions that exist between the West and the non-West. This divide operates as a tool of oppression and marginalisation, creating hierarchical relations that privilege Western modes of being and knowing. A prominent example of the abyssal line in operation is the "War on Terror and conflicts of self-determination," which has reinforced a new line of demarcation between Muslims and non-Muslims, particularly in Western countries, settler-colonial states, and Muslim-majority nations targeted during the war. In these contexts, Muslims are positioned below the abyssal line, making them subjects of heightened surveillance, data collection on their religious and political affiliations, and state-sanctioned violence in the form of drone strikes, extrajudicial killings, and torture (Raphael et al., 2016; Gordon, 2016; Gallagher, 2015; Fisher, 2013). This violence reflects the broader workings of the coloniality of being, wherein non-Western populations are systematically dehumanised and subjected to colonial forms of control and exploitation.

Intelligence Agencies of Powerful Western countries and Coloniality

As previously noted, the terrorism industry encompasses a diverse array of actors, including Western technology companies and the intelligence agencies of powerful Western nations. This section examines how these intelligence agencies, often in collaboration with Western technology corporations, play a critical role in sustaining the coloniality of non-Western nations through digital data colonialism.Prior to the revelations brought to light by Edward Snowden, little was known about the extent to which intelligence agencies from dominant Western states engaged in digital data colonialism. The Snowden disclosures revealed that agencies such as the United States National Security Agency (NSA) and the United Kingdom's Government Communications Headquarters (GCHQ), with the cooperation of allied nations and Western technology firms, had extensively tapped into global submarine communication cables. Through this method, they effectively colonised internet data from foreign states and their own populations (MacAskill et al., 2013; Davenport, 2015; Ball, 2013).

This clandestine data interception represents a form of digital colonisation, whereby Western powers, through technological dominance, gain disproportionate control over global information flows. By harvesting and surveilling digital data from a wide array of countries, including non-Western nations, these intelligence agencies reinforce existing power asymmetries and perpetuate colonial structures of domination and control.

The Snowden leaks revealed the extent to which the intelligence agencies of powerful Western nations and allied states participate in a long-standing network that engages in digital data colonialism. The most prominent and influential of these networks is the "Five Eyes" alliance, a successor to the Signals Intelligence Cooperation (SIGINT) established during the Second World War by the United States, the United Kingdom, and Australia (O'Neil, 2017). Following the war, the U.S. and U.K. formalised the Five Eyes network by incorporating three additional English-speaking countries—Canada, Australia, and New Zealand—all of which, apart from the U.K., are former British colonies and now settler states. These nations share mutual interests in maintaining the alliance, each contributing unique capabilities, such as technological advancements and strategic geographic positioning.

The Five Eyes alliance has been heavily dependent on technology since its inception. With the advent of satellite technology, the network developed a sophisticated data surveillance program known as Echelon. This program enabled the network to monitor and intercept communications from both private and public sector organisations across the globe (O'Neil, 2017).

> "The United States is responsible for SIGINT in Latin America, most of Asia, Russia, and northern China. At the same time, Australia is responsible for its neighbours (such as Indonesia), China, and Indo-China nations. Britain is responsible for Africa and the former Soviet Union, West of the Urals. Russia's polar regions are Canada's responsibility, and New Zealand's area of responsibility is the Western Pacific." (Richelson, 2012: 349).

Through Echelon and other intelligence programs, the Five Eyes network colonised digital data from numerous countries not only for security and surveillance purposes but also to secure economic and political advantages. This practice underscores the broader framework of digital

data colonialism, wherein the extraction and control of information perpetuate the colonial power structures and global dominance of Western states.

The Five Eyes alliance's mandate is notably broad. Its primary objective appears to be the acquisition of comprehensive intelligence on global events and their underlying causes, spanning areas such as security, political developments, and economic affairs. This vast scope underscores the network's strategic aim of achieving extensive informational dominance to maintain geopolitical leverage.

In 1982, the United States established an additional intelligence network, SIGINT Seniors Europe, which was primarily oriented toward monitoring the Soviet Union during the Cold War. This network's founding and principal members were the same nations involved in the Five Eyes alliance, illustrating the continuity and expansion of Western intelligence cooperation. This period also coincided with a surge in scholarly and policy-oriented discourse produced by the terrorism industry, much of which was focused on framing the Soviet Union as a primary threat (Stampnitzky, 2014). This synchronicity suggests a close relationship between intelligence networks and the production of strategic narratives, as both served to legitimise and reinforce the counterintelligence efforts aimed at containing perceived adversaries during the Cold War era.

The shift in focus for the Five Eyes and SIGINT Seniors Europe towards counterterrorism did not occur until the aftermath of the 9/11 attacks (Solon, 2017; The Intercept, 2018). By 2013, the Five Eyes alliance expanded into the "Fourteen Eyes," incorporating Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, and Sweden (Gallagher, 2018). This expansion reflects the growing transnational collaboration in intelligence gathering. The terms "Fourteen Eyes" and "SIGINT Seniors Europe" are often used interchangeably, despite the conceptual distinction between the networks, leading to some confusion, as both alliances include the same member states (Gallagher, 2018).

In addition to forming the Fourteen Eyes and SIGINT Seniors Europe, the United States established another intelligence division in 2005, SIGINT Seniors Pacific. This Pacific division comprises members of the Five Eyes alliance, alongside South Korea, Singapore, Thailand, France, and India, and is primarily focused on intelligence monitoring

in the Asia-Pacific region, with an emphasis on counterterrorism efforts (Snowden, 2007; Gallagher, 2018). This expansion reflects the increasing geopolitical significance of the Asia-Pacific region and the growing emphasis on intelligence-driven counterterrorism initiatives.

The SIGINT network is an expansive intelligence-gathering framework that involves numerous Western and non-Western nations. Within this network, certain countries, particularly the United States and the United Kingdom, occupy dominant leadership positions, while others function primarily as data providers. The most significant relationship within the SIGINT architecture is the bilateral cooperation between the United States and the "Second Party" members of the Five Eyes alliance, with the United Kingdom serving as a key partner (Greenwald, 2014). In contrast, the relationships between the United States and the "Third Party" countries, which include nations such as Algeria, Singapore, Israel, and the United Arab Emirates, are comparatively less central. Nevertheless, the U.S. maintains bilateral security agreements with several of these Third Party members, enhancing their strategic value.

Despite their secondary status relative to the Second Party members, Third Party nations play a critical role within the SIGINT network by providing intelligence that is essential for the U.S. and other Five Eyes members. This intelligence is instrumental in sustaining the ongoing structures of coloniality that impact non-Western countries. Beyond the Five Eyes alliance, the United States also maintains robust intelligence partnerships with members of SIGINT Seniors Pacific (SSPAC), SIGINT Seniors Europe (SSEUR), NATO, and Israel (Greenwald, 2014; Giosue, 2019). These alliances underscore the transnational and hierarchical nature of the SIGINT network, which perpetuates geopolitical dominance through the extraction and utilisation of global intelligence resources.

Integrating all SIGINT partners into a single, extensive network significantly enhances the intelligence-gathering capabilities of the United States and other Five Eyes members, enabling them to expand their reach in colonising digital data across a broader range of countries. This networked approach increases the efficiency and scope of intelligence operations. For instance, including France allows for more effective data collection from regions such as Africa, South America, and Russia, capitalising on France's strategic presence and capabilities

in these areas (Pfluke, 2019). Similarly, the involvement of nations like South Korea and Germany strengthens the network's ability to closely monitor geopolitical developments in North Korea (Pfluke, 2019). This expanded partnership facilitates the surveillance of a wider range of global regions, further consolidating the geopolitical and economic dominance of the Five Eyes members.

Before the Snowden leaks, there was limited public knowledge regarding the extent to which intelligence agencies from powerful Western nations engaged in digital data colonialism. Key members of intelligence networks, such as the United States and the United Kingdom, exploited submarine communication cables to gain access to vast amounts of internet and telecommunications data. These agencies also deployed advanced surveillance technologies to eavesdrop on global leaders, including leaders from allied countries within their networks, such as former German Chancellor Angela Merkel. The U.S. National Security Agency (NSA) referred to its data surveillance program as PRISM, while the UK's Government Communications Headquarters (GCHQ) named its equivalent program Tempora (MacAskill et al., 2013; Greenwald and MacAskill, 2013). Both programs specifically targeted internet data by tapping into submarine cables, which form the backbone of global internet infrastructure (Digital Methods Initiative, 2020). This allowed intelligence agencies to extract and colonise vast amounts of data from both Western and non-Western internet users, further entrenching the asymmetrical power dynamics inherent in digital data colonialism.

Submarine cables form a critical component of global communication infrastructure, connecting numerous countries through landing stations, each of which may host one or several such stations. Some of these landing stations are strategically utilised as intelligence-gathering hubs, such as those in Oman, which the United Kingdom's intelligence agency uses to collect data from the Middle East and surrounding regions (Wright et al., 2013). Ownership of these cables is often divided among private companies or consortiums, with prominent Western technology corporations, such as Facebook, Google, Microsoft, and Amazon, being key stakeholders. According to media reports, these companies have been implicated in assisting intelligence agencies such as the NSA and GCHQ in tapping into submarine cables (Zimmer, 2018; Gallagher and June, 2018; Greenwald, 2014).

Gallagher and June (2018) note that a significant proportion of global internet traffic passes through the United States, primarily due to two factors: the geographical position of the U.S. between Europe, the Middle East, and Asia, and the dominance of U.S.-based technology companies in the global internet services sector (The Intercept, 2018). This positioning provides the NSA with substantial opportunities to engage in digital data colonialism, as the majority of internet traffic is routed through U.S. infrastructure. Furthermore, this surveillance is facilitated by the Foreign Intelligence Surveillance Act (FISA), which grants U.S. intelligence agencies the legal authority to collect foreign intelligence through electronic surveillance (Congressional Research Service, 2020). This legal framework, coupled with the control over global data flows, underscores the asymmetry of power in digital data colonialism, enabling the U.S. to maintain and extend its geopolitical influence through data extraction.

Intelligence Agencies and Coloniality in Southeast Asian Muslim-majority Countries

Most discussions surrounding digital data colonialism have focused on the activities of the United States and the United Kingdom. However, the Snowden leaks also provided insight into how the Five Eyes and SIGINT Senior Pacific networks operate within the Asia-Pacific region (Snowden, 2007). According to reports from *The Sydney Morning Herald* based on the Snowden disclosures, Singapore, a member of the SIGINT Senior Pacific network, collaborated with the United States and Australia to conduct surveillance on neighbouring countries, including Malaysia and Indonesia (Dorling, 2013, 2014). These revelations not only heightened tensions between Southeast Asian neighbours but also strained relations between Malaysia, Indonesia, and Australia (ABC, 2013). Additionally, the leaks exposed that Indonesia had been a long-term target of Australia's intelligence agency, which used its diplomatic posts across Asia to intercept phone communications and data as part of the broader Five Eyes network's digital data colonialism efforts (MacAskill and Taylor, 2013; Dorling, 2013; Walsh et al., 2015). Australia's intelligence agency reportedly infiltrated Indonesian telecommunications networks, including Indosat and Telkomsel, and monitored Indonesian politicians to assist other Five Eyes members, such as the United States and New Zealand (Dorling, 2014; Beckford, 2015).

These revelations highlight the transnational and expansive scope of digital data colonialism, where intelligence agencies from powerful Western nations, often working in collaboration with regional allies, systematically exploit digital infrastructures to extend their geopolitical influence across both neighbouring and distant countries.

In the case of the United States, Australia's Signals Directorate intercepted communications between Indonesia and the U.S.-based law firm representing Indonesia in trade disputes with the United States (The New York Times, 2014). Similarly, New Zealand's Government Communications Security Bureau (GCSB) leveraged the XKEYSCORE Internet surveillance system, which was accessible due to New Zealand's membership in the Five Eyes alliance, to gather intelligence on the World Trade Organization (WTO) director-general candidates. New Zealand's objective was to support its own candidate, Trade Minister Tim Groser, in his bid for the position. Among those targeted by GCSB was Mari Elka Pangestu, Indonesia's candidate for the WTO director-generalship, as New Zealand sought to prevent her appointment (Gallagher and Hager, 2015).

Beyond Pangestu case, the surveillance extended to other non-Western candidates, including Alan Kyerematen (Ghana), Amina Mohamed (Kenya), Anabel González (Costa Rica), Herminio Blanco (Mexico), Taeho Bark (South Korea), Ahmad Thougan Hindawi (Jordan), and Roberto Carvalho de Azevêdo (Brazil) (Gallagher and Hager, 2015). This pattern of targeting exclusively non-Western candidates underscores the underlying power asymmetries in digital data colonialism, where Western intelligence agencies manipulate global digital infrastructures to preserve their geopolitical and economic dominance. The selective surveillance of these individuals, particularly Mari Elka Pangestu, reflects the broader dynamics of exclusion and control inherent in the practices of digital data colonialism.

Southeast Asian Muslim-majority countries are particularly vulnerable to digital data colonialism due to their reliance on critical communication infrastructures, such as the SEA-ME-WE 3 submarine cable (Dorling, 2013). This cable, which extends from Perth, Australia, and passes through key Southeast Asian nations, including Indonesia, Malaysia, Singapore, and Oman, connects thirty-nine countries, thirty-three of which host landing stations. Spanning four continents, it remains

one of the longest submarine cables in existence (Submarine Networks, 2020). The cable is owned by a consortium of telecommunications corporations, including Singapore's SingTel Optus, British Telecom, and Australia's Telstra, granting these entities access to the data transmitted through the cable (SEA-ME-WE 3, 2020; Dorling, 2013). However, the ability to tap into these cables and extract digital data is not uniformly distributed among all countries. For instance, Pakistan's intelligence agency, ISI, attempted to intercept data at two of the three landing stations near Karachi but lacked the technological capability to do so (Guardian, 2015). In contrast, Singapore, as noted by Dorling (2013), possesses the most advanced signals intelligence capabilities in Southeast Asia and has facilitated Australia's access to data transmitted through the SEA-ME-WE 3 cable.

Tapping into submarine cables allows intelligence agencies from powerful Western countries to capture vast amounts of digital data as it travels between sender and receiver. This interception enables these agencies to utilise the data to further their economic and political agendas, exemplified by the intelligence activities of countries such as the United States, the United Kingdom, Australia, and New Zealand. Through such practices, Western powers continue to assert dominance in the digital domain, reinforcing the asymmetrical power relations that characterise digital data colonialism.

Conclusion

This paper has undertaken the task of examining how the intelligence agencies of powerful Western nations, in collaboration with their allies, engage in digital data colonialism as a means of perpetuating coloniality. Digital data colonialism refers to the exploitation of submarine cables that span the globe, transmitting vast amounts of data from the Internet and other communication channels. Access to this data provides Western nations with the capacity to securitise non-Western countries and assert political and economic dominance over them. This system not only reinforces coloniality but also grants Western powers a form of omnipresence akin to the "God-Eye view," contributing to a potentially dystopian global order.

This scenario raises critical questions for scholars researching the coloniality of non-Western nations and offers pathways for addressing these issues. First, scholars must investigate whether Western technology

companies are sharing the digital data they extract from non-Western countries and with whom this data is being shared. This inquiry leads to two further questions: (1) Are Western tech companies providing this data to powerful Western governments or non-Western regimes? (2) If so, how is this data being utilised by these governments and agencies?

Second, scholars need to explore the motivations behind the digital data colonialism conducted by Western intelligence agencies. Specifically, they should ask: (1) How do these agencies engage in the process of digital data colonialism? (2) Is the primary objective of this data collection to advance the political and economic interests of Western nations in non-Western countries, such as Indonesia? Third, scholars should examine the concept of "terror capitalism" and assess whether the intelligence agencies of powerful Western nations, alongside Western tech companies, are utilising the colonised digital data to create profiles and develop predictive technologies aimed at identifying potential extremists or terrorists. This mirrors the practices of companies like Faception, which claims to offer predictive capabilities based on facial recognition technology. Fourth, scholars must develop tools and strategies to raise awareness among non-Western populations about the practices of digital data colonialism carried out by Western tech companies and intelligence agencies. Fifth, they should advocate for non-Western governments to implement stringent data protection regulations to safeguard against digital data colonialism. Finally, scholars should encourage non-Western governments to be more vigilant in monitoring Western nations' activities, particularly their exploitation of submarine cables and their data interception and hacking practices.

By addressing these key questions, scholars can contribute to a broader understanding of digital data colonialism and its implications for non-Western nations, while also advancing strategies to counter its perpetuation.

REFERENCES

Abadullah, Z,. 2019. Privacy, data security concerns as facial recognition becomes more common. *Channel News Asia*. November, 18. Available from: https://www.channelnewsasia.com/news/singapore/facial-recognition-ai-technology-privacy-data-security-issues-12100592 (accessed 12th December, 2020)

ABC News,. 2013. Malaysia summons Singapore ambassador over spying concerns. *ABC News*, November 27. Available from: https://www.abc.net.au/news/2013-11-27/an-malaysia-summons-singapore-ambassador-over-spying-concerns/5118610 (accessed 12th December, 2020).

Alatas, H,. 2000. Intellectual Imperialism: Definition, Traits, and Problems. *Southeast Journal of Social Science*. (28)1. p23-45.

Amnesty International, 2023. Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT. *Amnesty International*: Available from: file:///Users/elias/Downloads/MDE1567012023ENGLISH.pdf (Accessed on 2 October, 2024)

AR, Z,. 2020. How BN might have won GE14... had Cambridge Analytica stayed alive. *Malay Mail*, January 3. Available from: https://www.malaymail.com/news/malaysia/2020/01/03/how-bn-might-have-won-ge14-had-cambridge-analytica-stayed-alive/1824311 (accessed 15th December, 2020)

Babuta, A. Oswald, M, and Janjeva, A,. 2016. Artificial Intelligence and UK National Security Policy Considerations. *RUSI*, April. Available from: https://rusi.org/publication/occasional-papers/artificial-intelligence-and-uk-national-security-policy-considerations (accessed 15th December, 2020)

Balce, N,. 2016. *Body Parts of Empire Visual Abjection, Filipino Images, and the American Archive*. Michigan: University of Michigan Press.

Ball, J,. 2013. NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*, October 24. Available from: https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls (accessed 12th December, 2020)

Baz, G,. 2019. Artificial or Human: A New Era of Counterterrorism Intelligence? *Studies in Conflict & Terrorism*. (42) 12.

Reuters staff,. 2015. New Zealand spying on Pacific neighbors and Indonesia: Snowden documents. *Reuters*, March 5. Available from: https://www.reuters.com/article/us-newzealand-spying-pacific-idUSKBN0M104R20150305 (accessed 13th December, 2020).

Bhambra, G. Nisancioglu, K. and Cebrial, D,. 2018. *Decolonising the University*. London: Pluto Press.

Biddle, S,. 2018. Face Book uses Artificial Intelligence to predict your future actions for advertisers, says confidential document. *The Intercept*, April 13. Available from: https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/ (accessed 12th December, 2020)

Burton, J,. 2023. Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence. *Technology in Society*. (75) 102262.

Byler, D. and Boe, C,. 2020. Tech-enabled 'terror capitalism' is spreading worldwide. The surveillance regimes must be stopped. *The Guardian*, July 24. Available from: https://www.theguardian.com/world/2020/jul/24/surveillance-tech-facial-recognition-terror-capitalism (accessed 12th December, 2020)

Cadwalladr, C. and Campbell, D,. 2019. Revealed: Facebook's global lobbying against data privacy laws. *The Guardian*, March 2. Available from: https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment (accessed 13th December, 2020)

Cadwalladr, C. and Graham-Harrison, E,. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, March 17. Available from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed 12th December, 2020).

Campbell, D. Write, O. Cusick, J. and Sengupta, K,. 2013. Exclusive: UK's secret Mid-East internet surveillance base is revealed in Edward Snowden leaks. *The Independent*, August 23. Available from: https://www.independent.co.uk/news/uk/politics/exclusive-uk-s-secret-mid-east-internet-surveillance-base-revealed-edward-snowden-leaks-8781082.html (accessed 12th December, 2020)

Coleman, D,. 2018. Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. *Michigan Journal of Race and Law*. (24) 2.

Connell, R,. 2007. *Southern Theory*. London: Polity Press.

Congressional Research Service. 2020. Available from: https://fas.org/sgp/crs/intel/IF11451.pdf (accessed 12th December, 2020)

Comber, L,. 2008. *Malaya's Secret Police 1945–60 The Role of the Special Branch in the Malayan Emergency*. Melbourne: Monash University Press.

Mejias, U. and Couldry, N,. 2024. Data Grab The New Colonialism of Big Tech and How to Fight Back. The University of Chicago Press.

Couldry, N. and Mejias, U,. 2019. *The Costs of Connection: How Data Is Colonising Human Life and Appropriating It for Capitalism (Culture and Economic Life) 1st Edition*. California: Stanford University Press.

Cuthbertson, A,. 2019. China invents super surveillance camera that can spot someone from a crowd of thousands. *The Independent*, October 2. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/china-surveillance-camera-facial-recognition-privacy-a9131871.html (accessed 13th December, 2020)

Davenport, Tara,. 2015. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. *Catholic University Journal of Law and Technology*. (24), 1.

Digital Methods Initiative, 2020. *The Webs*. Available from: https://wiki.digitalmethods.net/Digitalmethods/TheWebs (accessed 12th December, 2020).

Dodd, Vikram,. 2020. Met police to begin using live facial recognition cameras in London. *The Guardian*, January 24. Available from: https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras (accessed 12th December, 2020).

Doffman, Zack,. 2019. Facebook Has Just Been Caught Spying On Users' Private Messages And Data. *Forbes*, January 30. Available from: https://www.forbes.com/sites/zakdoffman/2019/01/30/facebook-has-just-been-caught-spying-on-users-private-messages-and-data-again/#7dfeec6731ce (accessed 14th December, 2020)

Dorling, P,. 2014. Edward Snowden leak: Australia spied on Indonesian phones and data. *The Sydney Morning Herald*, February 17. Available from: https://www.smh.com.au/politics/federal/edward-snowden-leak-australia-spied-on-indonesian-phones-and-data-20140216-32tux.html (accessed 14th December, 2020).

Dorling, P,. 2014. Edward Snowden documents show Malaysia is an Australia, US intelligence target. *The Sydney Morning Herald*, March 30. Available from: https://www.smh.com.au/world/edward-snowden-documents-show-malaysia-is-an-australia-us-intelligence-target-20140330-zqonc.html (accessed 13th December, 2020).

Dorling, P,. 2013. Australian spies in global deal to tap undersea cables. *The Sydney Morning Herald*, August 29.

Available from: https://www.theage.com.au/technology/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html (accessed 13th December, 2020)

Dorling, P,. 2013. Exposed: Australia's Asia spy network. *The Sydney Morning Herald*, October 31. Available from: https://www.smh.com.au/politics/federal/exposed-australias-asia-spy-network-20131030-2whia.html (accessed 13th December, 2020).

Dorling, P,. 2013. Singapore, South Korea revealed as Five Eyes spying partners. *The Sydney Morning Herald*, November 25. Available from: https://www.smh.com.au/technology/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html (accessed 13th December, 2020).

Faception,. 2020. *Faception*. Available from: https://www.faception.com/our-technology (accessed 13th December, 2020).

Fisher, M,. 2013. A staggering map of the 54 countries that reportedly participated in the CIA's rendition program. Washington Post. Available from: https://www.washingtonpost.com/news/worldviews/wp/2013/02/05/a-staggering-map-of-the-54-countries-that-reportedly-participated-in-the-cias-rendition-program/ (accessed on 11 March, 2021)

Gallagher, R,. 2018. The Powerful Global Spy Alliance You Never Knew Existed. *The Intercept*, March 2. Available from: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/ (accessed 13th December, 2020).

Gallagher, R. and Henrik, M,. 2018. The Wire Trap Rooms. *The Intercept*, June 25. Available from: https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/ (accessed 12th December, 2020).

Gallagher, R,. 2015. The Life and Death of Objective Peckham. *The Intercept*. Available from: https://theintercept.com/drone-papers/the-life-and-death-of-objective-peckham/ (accessed on 3 February, 2021)

Gallagher, R. and Hager, N,. 2015. New Zealand Spied on WTO Director Candidates. *The Intercept*, March 23. Available from: https://theintercept.com/2015/03/22/new-zealand-gcsb-spying-wto-director-general/ (accessed 13th December, 2020).

Giosue, L,. 2019. Fourteen Eyes surveillance alliance explained. *Jerusalem Post*, June 3. Available from: https://www.jpost.com/special-content/fourteen-eyes-surveillance-alliance-explained-591436 (accessed 13th December, 2020).

Goel, V. and Masood, S,. 2020. Facebook, Google and Twitter Rebel Against Pakistan's Censorship Rules. *The New York Times*, February 27. Available from: https://www.nytimes.com/2020/02/27/technology/pakistan-internet-censorship.html (accessed 12th December, 2020)

Gordon, R,. 2016. How the US Military Came to Embrace Extrajudicial Killings. *The Nation*, July 18. Available from: https://www.thenation.com/article/archive/how-the-us-military-came-to-embrace-extrajudicial-killings/ (accessed on 3 February, 2021)

Greenwald, G,. 2014. *No Place to Hide, Edward Snowden, The NSA and The Surveillance State*. London: Penguin.

Greenwald, G. and MacAskill, E,. 2013. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, June 6. Available from: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed 13th December, 2020)

Greenwald, G. and MacAskill, E,. 2013. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, June 6. Available from: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed 13th December, 2020).

Grosfoguel. R,. 2016. What is Racism? *The Journal of World Systems Research*. (22), 1. p9-15.

Grosfoguel, R,. 2013. The Structure of Knowledge in Westernised Universities: Epistemic Racism/Sexism and the Four Genocides/Epistemicides of the Long 16th Century. *Human Architecture: Journal of the Sociology of Self-Knowledge*. (11), 8. p9-22.

Grosfoguel, R,. 2013. Decolonising Post-Colonial Studies and Paradigms of Political-Economy: Transmodernity, *Decolonial Thinking, and Global Coloniality. TRANSMODERNITY*. (1), 1.

Grosfoguel. R,. 2006. World-Systems Analysis in the Context of Transmodernity, Border Thinking, and Global Coloniality. *Review (Fernand Braudel Center), From Postcolonial Studies to Decolonial Studies: Decolonising Postcolonial Studies*. (29), 2. p167-187.

Hakim, D,. 2018. Cambridge Analytica's Parent Company Helped Shape Saudi Arabia's Reform Movement. *New York Times*, May 31. Available from: https://www.nytimes.com/2018/05/31/business/cambridge-analytica-scl-group-saudi-arabia.html (accessed 12th December, 2020)

Hack, K,. 2009. 'The Malayan Emergency as Counterinsurgency Paradigm'. *Journal of Strategic Studies*. (32), 3. p383-414.

Hack, K,. 1999. 'British intelligence and counterinsurgency in the era of decolonisation: The example of Malaya'. *Intelligence and National Security*. (14), 2. p124-155.

Hern, A,. 2019. German regulator orders Facebook to restrict data collection. *The Guardian*, February 7. Available from: https://www.theguardian.com/technology/2019/feb/07/german-regulator-orders-facebook-to-restrict-data-collection (accessed 12th December, 2020).

Herman, E. and O' Sullivan, G,. 1989. *The Terrorism Industry: The Experts and Institutions that shape our view of Terror*. New York: Pantheon Books.

Huggler, J,. 2017. Facial recognition software to catch terrorists being tested at Berlin station. *The Telegraph*, August 2. Available from: https://www.telegraph.co.uk/news/2017/08/02/facial-recognition-software-catch-terrorists-tested-berlin-station/ (accessed 14th December, 2020).

Jacobsen, K,. 2017. On Humanitarian Refugee Biometrics and New Forms of Intervention. *Journal of Intervention and State building*. (11), 4. p529-551.

Kachamas, P. Akkaradamrongrat, S. Sinthupinyo, S. and Chandrachai, A,. 2019. Application of artificial intelligent in the prediction of consumer behavior from facebook posts analysis. *International Journal of Machine Learning and Computing*. (9), 1. p91-97.

Karari, P,. 2018. Modus Operandi of Oppressing the "Savages": The Kenyan British Colonial Experience. *Peace and Conflict Studies*. (25), 2.

Kaurin, D,. 2019. Data Protection and Digital Agency for Refugees. *Centre for International Governance Innovation*, May 15. Available from: https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees (accessed 12th December, 2020)

Kwet, M,. 2019. Digital colonialism is threatening the Global South. *Aljazeera*, March 13. Available from: https://www.aljazeera.com/indepth/opinion/digital-colonialism-threatening-global-south-190129140828809.html (accessed 12th December, 2020)

Kwet. M,. 2019. Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*. (60), 4.

Komer, R,. 1972. The Malayan Emergency in Retrospect Organization of a Successful Counterinsurgency Effort. California: Rand.

Lafrance, A,. 2016. Facebook and the New Colonialism. *The Atlantic*, February 11. Available from: https://www.theatlantic.com/technology/archive/2016/02/facebook-and-the-new-colonialism/462393/ (accessed 12th December, 2020)

Lubin, G,. 2016. 'Facial-profiling' could be dangerously inaccurate and biased, experts warn. *Business Insider*, October 13. Available from: https://www.businessinsider.com.au/does-faception-work-2016-10 (accessed 12th December, 2020).

MacAskill, E. Borger, J. Hopkins, N. Davies, N. and Ball, J,. 2013. GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*, June 21. Available from:https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (accessed 12th December, 2020).

MacAskill, E. and Taylor, L,. 2013. NSA: Australia and US used climate change conference to spy on Indonesia. *The Guardian*, November 2. Available from: https://www.theguardian.com/world/2013/nov/02/nsa-australia-bali-conference-spy-indonesia (accessed 12th December, 2020).

McKendrick, K,. 2019. Artificial Intelligence Prediction and Counterterrorism. *Chatham House, The Royal Institute of International Affairs*. Available from: https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf (access 12th December, 2020)

Marczak, B. Scott-Railton, J McKune, S. Abdul Razzak, B. and Deibert, R,. 2018. HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. *Citizen Lab*, September 18. Available from: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ (accessed 12th December, 2020)

Mejias, U. and Couldry, N,. 2020. Resistance to the new data colonialism must start now. *Aljazeera*, April 29. Available from: https://www.aljazeera.com/

indepth/opinion/resistance-data-colonialism-start-200428162353538.html (accessed 12th December, 2020)

Mignolo, W,. 2011. *The Darker Side of Western Modernity: Global Futures, Decolonial Options*. North Carolina: Duke University Press.

Monique, M. and Angela, D,. 2019. (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television & New Media*. (20), 4. p379-395.

Moore, J,. 2018. Cambridge Analytica Had a Role in Kenya Election, Too. *New York Times*, March 20. Available from: https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html (accessed 12th December, 2020)

Mwambari, D,. 2020. The pandemic can be a catalyst for decolonisation in Africa. *Aljazeera*, April 16. Available from: https://www.aljazeera.com/indepth/opinion/pandemic-catalyst-decolonisation-africa-200415150535786.html (accessed 12th December, 2020)

Munck, R. and O' Hearn, D,. 1999. *Critical development theory*. London: Zed Books.

Ndlovu-Gatsheni, S,. 2013. *Coloniality of Power in Postcolonial Africa*. Oxford: African Books Collective.

Maldonado-Torres. N,. 2007. On the Coloniality of Being Contributions to the development of a concept. *Cultural Studies*. (21), 23. p240-270.

Nelu, C,. 2024. Exploitation of Generative AI by Terrorist Groups. 10th June, *International Centre of Counter-terrorism*. Available from: https://icct.nl/publication/exploitation-generative-ai-terrorist-groups (accessed 13th January, 2025)

Nestola, E,. 2019. Why it's too easy to manipulate voters – and steal the EU elections. *The Guardian*. March 6. Available from: https://www.theguardian.com/commentisfree/2019/mar/06/digital-manipulation-eu-elections-personal-information (accessed 12th December, 2020)

Notias, T,. 2020. Access granted: Facebook's free basics in Africa. *Media, Culture & Society*. (42), 3. p329-348.

O'Neil, A,. 2017. Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs*. (71), 5. p529-543.

O'Neil, C,. 2016. *Weapons of Math Destruction*. New York: Crown Publishing Group.

Pfluke, C,. 2019. A history of the Five Eyes Alliance: Possibility for reform and additions. *Comparative Strategy*. (38), 4.

Pinto, R,. 2018. Digital Sovereignty or Digital Colonialism? *Revista International de Direitos Humanos*. (15), 27.

Quijano, A,. 2007. Coloniality and Modernity/Rationality. *Cultural Studies*. (21), 23. p168-178.

Quijano, A,. 2000. Coloniality of Power, Eurocentrism, and Latin America. *Nepantla: Views from South*. (1), 3. p533-538.

Raphael, S; Black, C; Blakeley, R; Kostas, S,. 2016. Tracking rendition aircraft as a way to understand CIA secret detention and torture in Europe. *International Journal of Human Rights*. (20) 1. p78-103.

Richelson, J. 2012. The US Intelligence Community. 6th ed. Boulder. Colorado: *Westview Press*.

Said, E,. 1978. *Orientalism*. New York: Vintage Books Edition.

Santos, B,. 2018. *The end of the Cognitive Empire, the coming of age of epistemologies of the south*. North Corallina: Duke University Press.

Santos, B,. 2014. *Epistemologies of the South Justice against Epistemicide*. London: Routledge.

SeaMeWe-3,. 2020. *Fiber Atlantic*. Available from: http://www.fiberatlantic.com/system/xk14q (accessed 12th December, 2020).

SEA-ME-WE 3,. 2013., *Submarine networks*, August 5. Available from: https://www.submarinenetworks.com/systems/asia-europe-africa/smw3 (accessed 12th December, 2020).

Solon, O,. 2017. It's digital colonialism': how Facebook's free internet service has failed its users. *The Guardian*, July 27. Available from: https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets (accessed 12th December, 2020).

Snowden, E,. 2007. *The Courage Foundation*, March 16. Available from: https://edwardsnowden.com/2018/06/01/sigint-seniors-pacific-successes-highlighted-at-conference/ (accessed 12th December, 2020).

The Intercept, 2018. SIDtoday 2007-01-08: Counterterrorism Analytic Working Group Meets in Madrid. *The Intercept*. Available from: https://theintercept.com/document/2018/03/01/sidtoday-2007-01-08-counterterrorism-analytic-working-group-meets-in-madrid/ (accessed 12th December, 2020).

The Intercept,. 2018. Introduction, U,S. as World's Telecommunications Backbone. *The Intercept*. Available from: https://theintercept.imgix.net/wp-uploads/sites/1/2018/06/direct-path-1529876697.png?auto=compress%2Cformat&q=90 (accessed 12th December, 2020).

The New York Times,. 2014. Document Describes Eavesdropping on American Law Firm. *The New York Times*, February 15. Available from: https://www.nytimes.com/2014/02/16/us/document-describes-eavesdropping-on-american-law-firm.html (accessed 12th December, 2020).

Tao, L,. 2018. Malaysian police wear Chinese startups AI camera to identify suspected criminals. *South China Morning Post*, April 20. Available from: https://www.scmp.com/tech/social-gadgets/article/2142497/malaysian-police-wear-chinese-start-ups-ai-camera-identify (accessed 12th December, 2020)

Thatcher, J. O'Sullivan, D. and Mahmoudi, Dillon,.2016. Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*. (34), 6. p990-1006.

Thomas, E,. 2018. Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database. *Wired*, March 12. Available from: https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh (accessed 12th December, 2020)

Tuck, E. and Yang, K,. 2012. Decolonisation is not a metaphor. *Decolonisation: Indigeneity, Education & Society*. (1), 1.

Santander, P,. 2010. Latin America: Political communication and media discourse in contexts of social and revolutionary transformations. *Journal of Multicultural Discourses*. (5), 3. p227-238.

Stampnitzky, L,. 2014. *Disciplining Terror, How Scholars Invented Terrorism*. Cambridge: Cambridge University Press.

Steinmetz, G,. 2017. Sociology and Colonialism in the British and French Empires, 1945–1965. *The Journal of Modern History*. (89), 3.

Snowden, E,. 2007. *SIGINT Seniors Pacific*. March 16. Available from: https://edwardsnowden.com/wp-content/uploads/2018/06/SIDtoday-2007-03-16-SIGINT-Seniors-Pacific.pdf (accessed 12th December, 2020).

Submarine,. 2020. *Submarine networks*. Available from: https://www.submarinenetworks.com/en/stations (accessed 14th December, 2020).

Submarine cable maps, 2020,. *TeleGeography*. Available from: https://www.submarinecablemap.com (accessed 13th December, 2020).

The Guardian, 2015. Pakistan tried to tap international web traffic via underwater cables, report says. *The Guardian*, July 23. Available from: https://www.theguardian.com/world/2015/jul/23/pakistan-tried-to-tap-international-web-traffic-via-underwater-cables-report-says (accessed 15th December, 2020).

UNHCR, 2015,. Biometric Identity Management System. *UN*. Available from: https://www.unhcr.org/550c304c9.pdf (accessed 12th December, 2020)

Voronkov, V. and Marie De Meo, A,. 2021. Countering Terrorism Online with Artificial Intelligence - An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia. *United Nations Office of Counter-Terrorism.* Available from: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-

terrorism-online-with-ai-uncct-unicri-report-web.pdf (accessed 13th January, 2025)

Walsh, P. and Miller, S,. 2015. Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security*. (31), 3. p345-368.

Yazid, A,. 2019. The Police Special Branch in Countering the Malayan Emergency 1948-1960: An Analysis of Intelligence Tactics and Strategies. *Malaysian Journal of international* Relations. (7), 1.

Young, J,. 2019. The new knowledge politics of digital colonialism. *Economy and Space*. (51), 7. p1424-1441.

Yuniar, R,. 2018. Facebook's Cambridge Analytica scandal puts Indonesia's tech firms on the spot. *South China Morning Post*, April 28. Available from: https://www.scmp.com/week-asia/business/article/2143763/facebooks-cambridge-analytica-scandal-puts-indonesias-tech-firms (accessed 12th December, 2020)

Zimmer, J,. 2018. Google Owns 63,605 Miles and 8.5% of Submarine Cables Worldwide. *BROADBAND NOW*, September 12. Available from: https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/ (accessed 16th December, 2020).

Zuboff, S,. 2019. *Surveillance Capitalism*. New York: Hachette Book Group.

GUIDELINES FOR AUTHORS

Intellectual Discourse is an academic, refereed journal, published twice a year. Four types of contributions are considered for publication in this journal: major articles reporting findings of original research; review articles synthesising important deliberations related to disciplines within the domain of Islamic sciences; short research notes or communications, containing original ideas or discussions on vital issues of contemporary concern, and book reviews; and brief reader comments, or statements of divergent viewpoints.

To submit manuscript, go to http://www.iium.edu.my/intdiscourse

The manuscript submitted to Intellectual Discourse should not have been published elsewhere, and should not be under consideration by other publications. This must be stated in the covering letter.

1. Original research and review articles should be 5,000-8,000 words while research notes 3,000-4,000 words, accompanied by an abstract of 100-150 words. Book review should be 1,000-1,500 words.
2. Manuscripts should be double-spaced with a 1-inch (2.5 cm) margins. Use 12-point Times New Roman font.
3. Manuscripts should adhere to the *American Psychological Association* (APA) style, latest edition.
4. The title should be as concise as possible and should appear on a separate sheet together with name(s) of the author(s), affiliation(s), and the complete postal address of the institute(s).
5. A short running title of not more than 40 characters should also be included.
6. Headings and sub-headings of different sections should be clearly indicated.
7. References should be alphabetically ordered. Some examples are given below:

Book
In-text citations:
Al-Faruqi & al-Faruqi (1986)

Reference:
Al-Faruqi, I. R., & al-Faruqi, L. L. (1986). *The cultural atlas of Islam*. New York: Macmillan Publishing Company.

Chapter in a Book
In-text:
Alias (2009)

Reference:
Alias, A. (2009). Human nature. In N. M. Noor (Ed.), *Human nature from an Islamic perspective: A guide to teaching and learning* (pp.79-117). Kuala Lumpur: IIUM Press.

Journal Article
In-text:
Chapra (2002)

Reference:
Chapra, M. U. (2002). Islam and the international debt problem. *Journal of Islamic Studies, 10*, 214-232.

The Qur'ān
In-text:
(i) direct quotation, write as 30:36
(ii) indirect quotation, write as Qur'ān, 30:36

Reference:
The glorious Qur'ān. Translation and commentary by A. Yusuf Ali (1977). US: American Trust Publications.

Ḥadīth
In-text:
(i) Al-Bukhārī, 88:204 (where 88 is the book number, 204 is the ḥadīth number)
(ii) Ibn Hanbal, vol. 1, p. 1

Reference:
(i) Al-Bukhārī, M. (1981). *Ṣaḥīḥ al-Bukhārī*. Beirut: Dār al-Fikr.
(ii) Ibn Ḥanbal, A. (1982). *Musnad Aḥmad Ibn Ḥanbal*. Istanbul: Cagri Yayinlari.

The Bible
In-text:
Matthew 12:31-32

Reference:
The new Oxford annonated Bible. (2007). Oxford: Oxford University Press.

Transliteration of Arabic words should follow the style indicated in ROTAS Transliteration Kit as detailed on its website (http://rotas.iium.edu.my/?Table_of_Transliteration), which is a slight modification of ALA-LC (Library of Congress and the American Library Association) transliteration scheme. Transliteration of Persian, Urdu, Turkish and other scripts should follow ALA-LC scheme.

IIUM Press (Marketing Unit)
Research Management Centre
International Islamic University Malaysia
P.O. Box 10, 50728 Kuala Lumpur, Malaysia
Phone (+603) 6196-5014, Fax: (+603) 6196-4862
E-mail: intdiscourse@iium.edu.my; intdiscourse@yahoo.com.
Website: http://iiumpress.iium.edu.my/bookshop

In This Issue

ISSN 0128-4878 (Print)

ISSN 2289-5639 (Online)

ISSN 0128-4878

2289 5639