Global Cybersecurity Problematisation

Tracking relations of power within cybersecurity practices

School of Law

Jasper Egbobamwonyi-Bedaux

Thesis submitted for the degree of Doctor of Philosophy

November 2024

Word Count – Chapters and abstract ≈ **71,040**

For my late mother and father, Janet and Patrick. You sowed the seed that made this all possible

Declaration

This thesis has not been submitted in support of an application for another degree at this or any other university. It is the result of my own work and includes nothing that is the outcome of work done in collaboration except where specifically indicated.

……………………………………………………..

Jasper Uyi Egbobamwonyi-Bedaux

Abstract

Focusing on the constitution of cybersecurity as a problem space, this study applies empirical data to test social and political theories against cybersecurity discourses and practices. In particular, those of developed states security apparatuses. It employs data to analyse the relationship between poorer developing states and their wealthier developed counterparts in the context of development (digital divide, capacity building and other efforts designed to respond to such divide), and the challenges of cybersecurity. To do this, the problematisation of cybersecurity is explored through an examination of the role of the United Kingdom (UK) and other Western states and institutions. This role is interrogated within projects delivered through initiatives such as the Commonwealth Cybercrime Initiatives (CCI), and other similar initiatives, delivered by such bodies as the Commonwealth Telecommunication Union (CTU), the International Telecommunication Union (ITU), the UK's Foreign and Commonwealth Office (**FCO**), the European Union Agency for Cybersecurity (ENISA), amongst others. The delivery of such projects in three developing Commonwealth states of Ghana, Botswana and Trinidad and Tobago are case studied. Data is collected and analysed against theoretical concepts of modernisation, dependency and governmentality, to understand the relationship between security, law, language or discourse and development. The aim is to provide new insights into forms of 'governing' that exist through such practices, and their impact on the development of social, political and legal frameworks in such weaker economies. Thus, the study synthesises the question of how these security discourses and practices shape the formation of certain knowledge as "truth", and allow continued dependence of the less resourced developing states on such knowledge. In doing so, it tracks the objectives and effects of power to reveal certain knowledges, techniques or strategies which render cybersecurity intelligible, and normalises its perception as a legitimate problem for global policy and legal concern.

Acknowledgements

I would like to express my sincere gratitude to everyone who have, one way or another been a pilar of some support throughout this entire PhD Journey.

First, I am deeply indebted to my supervisors, Professors Luca Follis and Majid Yar, for their insightful, unwavering and invaluable support. Their interest in the study, meticulous reviews of every draft chapter, the critical and constructive feedback that accompanied such reviews and their words of encouragement at every meeting, have all culminated to shape and refine both this study and my own development. I am truly grateful for their mentorship and dedication throughout.

The journey would never have begun without the support of my family, especially my parents, of blessed memories, who made it possible for me to attain the crucial educational foundation that saw me dreaming of completing a PhD since my secondary school days. While it took several decades to finally make that dream a reality, I remain thankful for their love and care. I am also immensely indebted to my nucleus family; my kids and my partner, for creating a favourable environment which allowed me to pursue this dream alongside other family commitments. Especially my partner who, having been through this process herself, understands what the journey entails. And to my siblings, thank you for all your words of encouragements.

I would also like to thank everyone else I encountered during the different stages of this study, those who agreed to participate in the study and provided answers to some of the questions I had.

Finally, I must also show my gratitude to the Law School here at Lancaster University and the entire FASS team, for providing numerous training and development opportunities throughout, which have proved resourceful and played crucial role in the success of this study.

Contents

List of Figures

List of Abbreviations and Acronyms

ACD	Active Cyber Defence
ACF	Africa Cyber fellowship (programme)
APA	Administrative Procedure Act (USA)
ARPANET	Advanced Research Projects Agency Network
AUC	African Union Commission
BBC	British Broadcasting Corporation
BRICS	Brazil, Russia, India, China and South Africa
BROCA	Botswana Communications Regulatory Authority
CBDR	Common but Differentiated Responsibility
CCDCoE	Cooperative Cyber Defence Centre of Excellence (NATO)
CCI	Commonwealth Cybercrime Initiative
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CJCS	Chairman of the Joint Chiefs of Staff
CMM	Cybersecurity Capacity Maturity Model
COE	Council of Europe
COMNET	COMNET Foundation for ICT Development
COVID	Coronavirus Disease (2019)
CPS	Crown Prosecution Service (UK)
CTO	Commonwealth Telecom Organization
CTU	Commonwealth Telecommunications Union
DARPA	Defence Advanced Research Projects Agency (USA)
DNS	Domain Name Service
DOD	Department of Defence (USA)
DSL	Digital Subscriber Line
ECLA	Economic Community of Latin America
ECOWAS	Economic Community of West African States
EEAS	European External Action Service
EMB	Electoral Management Body
ENISA	European Network and Information Security Agency
EU	European Union
FCDO	Foreign Commonwealth and Development Office (UK)
FCO	Foreign and Commonwealth Office (UK)
GCA	Global Cybersecurity Agenda
GCI	Global Cybersecurity Index
GCSCC	Global Cybersecurity Capacity Centre
GDPR	The European Union's 2016 General Data Protection Regulation
GGE	Group of Government Experts (UN)
GOV	Government
GPT	General Purpose Technologies
GSI	Global Standards Initiative

GVC	Global Value Chain
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean
HIV	Human_Immunodeficiency_Virus
HLEG	High Level Experts Group
HM	Her Majesty
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICDR	International Centre for Dispute Resolution
ICSPA	International Cybersecurity Protection Alliance
ICT	Information and Communication Technology
IDI	ICT Development Index
IMC	Inter-Ministerial Committee (Trinidad)
INE	Instituto Nacional Electoral (Mexico)
IP	Internet Protocol
IRP	Independent Review Process
IT	Information Technology
ITU	International Telecommunications Union
IWF	Internet Watch Foundation
LDC	Less Developed Countries
LIC	lower income countries
LMIC	lower middle-income countries
MDG	UN's Millennium Development Goals
MP	Member of Parliament
MRI	Magnetic Resonance Imaging
NATO	North Atlantic Treaty Organization
NCA	National Crime Agency (UK)
NCRA	National Cyber Risk Assessment
NCS	National Cybersecurity
NCSC	National Cybersecurity Center
NGO	Non-Governmental Organization
NHS	National Health Service (UK)
NORA	National Occupational Research Agenda
NSF	National Science Foundation
NSI	National Security Information
NUPI	Norsk Utenrikspolitisk Institutt (Norwegian: Norwegian Institute of International Affairs)
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development (aka Office of Economic Cooperation and Development)
OEWG	Open-Ended Working Group
ONI	Office of Naval Intelligence
OVP	Online Video Platform
PLA	People's Liberation Army's
QA	Quality Assurance

QC	Queen's Counsel (UK)
REMJA	The Meetings of Ministers of Justices, other Ministers, Prosecutors and Attorney Generals of the Americas
SADC	Southern African Development Community
SOCA	Serious Organised Crime Agency (UK)
SSF	Strategic Support Force
TLAB	Taxation Laws Amendment Bill
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nations Commission On International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization (since 1945; Paris, France)
UNICEF	United Nations International Children's Emergency Fund (now United Nations Children's Fund)
US	United States
USA	United States of America
USCYBERCOM	United States Cyber Command
WCIT	World Congress on Information Technology
WDR	Wide Dynamic Range

List of Appendices

1 Introduction

This study tracks the relations of power within the global cybersecurity discourse and practices. It focuses on the process of constituting cybersecurity as a problem space and actions in response to its challenges. It analyses the relationships created between states as a result, particularly such relationships between the developed states and their developing counterparts. It critically interrogates the role played by developed states within efforts to boost cybersecurity capacity and mitigate the digital divide between them and developing states. Aspects of this relationship are highlighted, and examined through a Foucauldian governmentality lens.[1] Foucault's governmentality can be understood broadly as the art of governing, focusing on how individuals or groups are shaped and influenced.[2][3]

[1] Michel Foucault, *The Foucault Effect: Studies in Governmentality, with Two Lectures by and an Interview with Michel Foucault*, vol 22 (Graham Burchell, Colin Gordon and Peter Miller eds, The University of Chicago Press 1991).
[2] ibid.
[3] ibid.

The study argues therefore, that, while such cybersecurity capacity building efforts may be perceived positively, by all parties as a way to bridge the gap, it nonetheless constitutes underlying power dynamics. By highlighting such underlying aspects of this relationship that are suggestive of "calculative practices" (directly linked to Foucault's governmentality concept),[4] it argues that these practices create an illusionary sense of equal partnership within a certain exercise of power. Thus, the study seeks to demonstrate that cybersecurity actions, such as capacity building programs in developing states, while responding to insecurities in cyberspace, constitute new sites of power and control, like other already well researched sites (e.g., global trade and global politics).

Foucauldian discourse analysis is engaged as a theoretical framework and methodology which critically scrutinizes problematisations. Carrol Bacchi defines problematisations as ways in which certain "problems" are produced and represented in governmental policies and practice. [5] For Foucault, probelmatisation takes on a specific meaning within his broader ideas of power, knowledge and history. In what he termed the 'history of problematics', problems themselves are not natural or objective.[6] Rather, they emerge through historical processes, social practices and political strategies.[7] According to Foucault, what we consider "problems" are actually products of specific historic

[4] Peter Miller and BY Peter Miller, 'Governing by Numbers: Why Calculative Practices Matter' (2001) 68 Social Research 379.

[5] Carol Bacchi, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (2015) 05 Open Journal of Political Science 1.

[6] Michel Foucault, *The Government of Self and Others: Lectures at the College de France, 1982-1983* (Frédéric Gros ed, Palgrave Macmillan 1983).

[7] ibid.

moments.[8] For example, the concept of cybersecurity has a particular history that shapes both our understanding and how we treat it today. Rather than simply trying to provide answers to a problem, Foucault suggests that we analyse problematisations themselves. This means analysing how certain issues have been framed as problems, by whom, and for what purpose.[9] The question therefore is: who benefits from such framing of cybersecurity problems and what impacts do they have? Through analysis of problematisations, their contingency can be revealed. This allows for critique, questioning the assumptions and power dynamics embedded in how problems are defined, presented and represented.

The study seeks to track and reveal these assumptions and power dynamics through engagement with authoritative data. Such data include cybersecurity strategy and policy documents, political speeches and interviews. Contrary to typical policy analysis research which adopts the problem-solving approach, this study utilizes a problem-framing strategy instead, a problem-questioning method suggested by Carrol Bacchi.[10] This provides the analytical structure for the research. In addition to Bacchi's framework, Mitchel Dean's power effects concepts is used to foreground the relations of power within the data and present the findings to reveal how power works and how it is employed.[11]

[8] ibid.

[9] ibid.

[10] Carol Lee Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (Pearson Australia 2009).

[11] Mitchell Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (Tim May ed, McGraw-Hill Education 2007).

The concept of cybersecurity is examined through the evolving representation of insecurity in cyberspace, cybercrime, regulation and policing. It examines political subjects and their place in relation to government actions and practices via the various cybersecurity measures. Thus, the study explores on the one hand, historical and contemporary roles, and perspectives of developed states such as the United Kingdom, in the development of international constitutional models within the trends in laws that are designed to govern cyberspace, cybersecurity strategies, policies and practices. On the other hand, their global cyber dominance ambition is analysed through expressed objectives within their cybersecurity strategy documents, policies, speeches, and rhetoric.

This ambition is explored further through their relations with a group of developing nation-states, both directly and indirectly as part of an international organisation's working group, such as the Commonwealth, NATO, United Nations, and the International Telecommunications Union. Thus, the analysis casts a critical lens on the UK, both on its own cybersecurity practices, and as part of a growing transnational network of economically powerful states, international organisations, multinational corporations, and other non-state actors.

1.1 Rationale and significance

Cybersecurity can be defined as "both about the insecurity created through cyberspace and about technical and non-technical practices of making it (more) secure."[12] While it remains a technical practice at its core, it has become a field of political power struggle in recent years. Particularly as we rely heavily today on internet technologies that form parts of the larger cyber space. This makes security within it rather fluid, complex and one of a global dilemma. This is because it affords both societal benefits, and presents enormous security challenges (ranging from cybercrime to state espionage and terrorism). Its benefits have enabled expansions of ICT in recent decades, bringing about total digitisation of societies, such that the "economy, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it".[13]

Protecting this integrity and ensuring that malicious actors – from the low-level cyber-enabled criminals to terrorist organisations, organised criminal gangs, and military operations from hostile states - are kept at bay, has become a major pre-occupation of governments worldwide. However, developing nations, particularly poorer ones, face the brunt of these challenges due to their limited infrastructural resources, and for reasons often linked to their development status, or the so-called digital divide between themselves and their developed counterparts. This means that, for such countries, apart from having weak infrastructures, they also lack the ability to improve upon their current situation without support from other states and institutions. This lack of capacity renders

[12] Myriam Dunn Cavelty, 'Cyber Security' in Alan Collins (ed), *Contemporary Security Studies* (3rd edn, Oxford University Press 2015).[363]

[13] Government of the United Kingdom, 'National Cyber Security Strategy 2016-2021' (2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>.[13]

these states "weakest links" in the global chain.[14] It therefore creates the basis for arguing that such states need to build their capacity if they are to be part of cyberspace; not only to enable them deal with some of the challenges, but also, so that they present less risk to the entire chain. But what form do these supports take?

One can assume that the supports are intended to assist developing states to achieve some level of capability, and gain the knowledge needed for their development journey, independently. But is that really the case? Is it possible for such states to possess enough capacity and knowledge capabilities to truly wean themselves off their dependence on the richer states? Are there strategies at work to ensure a continued dependence? And if there are, what overall purpose are these strategies designed to fulfil? Which roles do developing states play within this relationship, and how do they perceive their own agency? These are amongst the questions that shape this study, and to which efforts are directed at answering.

To this end, the study seeks to understand and reveal the forms of power that exist within these arrangements which are not readily visible but can be observed using power theories such as those of Foucault. The wider discussions on how power works within and through the current cybersecurity practices is a major focus of this study, particularly how it works through norms development. It also focuses on the relationships created by cybersecurity problems and efforts designed to solve those problems. Specifically, it concerns how these

[14] ibid.

relationships shape the existentialities of weaker nation-states, and impact perspectives as well as the socio-legal-political realities of such states. It examines therefore how power works, consequently, in the representation, production, and reproduction of a 'truth' system within the cybersecurity discourse.

To understand the coherence of this process thus requires unravelling the relationship between security, law, language or discourse and development. And for the purpose of suggesting that this relationship is both a palpable and a necessary object of enquiry, their interrelations are outlined according to a rather broad historical representation. At a hypothetical level, it bears a certain contentious connotation. Historically, conventional legal theory has viewed its objects of study as being the systems or codes that govern, respectively, rhetoric and the application of law as potentialities rather than empirical realities. In both cases, it is often the abstract relevance of a notional system that forms the object of any of such empirical study. Real meaning, actual usage and the historical dimension are commonly overlooked. Even the shallowest of historical examinations, however, will clearly indicate that such accounts of discourse are historically and geographically specific and limited.

However, a suitable theoretical approach for this study is one, not necessarily based on the perception of cybersecurity practices as a continuation of imperial powers over developing states, or one which is essentially designed to seek out the 'subject' elements of such practices or their 'real' meaning or agenda; but rather, one that allows for a deeper explanation of these practices - not only as constitutive discourse which denotes normative roles, rhetoric, knowledge, power, and subjectivity, in such practices, but also one which applies such Foucauldian concept as governmentality, to provide a far-reaching examination. It is therefore argued that the use of language or discourse, as a governmentality tool, necessarily aid law in its role as an instrument of power and control.

A primary goal therefore is to critically assess how contemporary uncertainties or insecurities are governed and subsumed by the security discourses and practices of dominant nations like the UK. The aim is to successfully track and demonstrate the power dynamics created within these discourses and practices and how they shape the so-called Global North and Global South relationship and to demonstrate how this power permeates all aspects of this relationship.

Through this ability to track such power, it is anticipated that one would contribute to, 1) a broader theoretical study of cybersecurity as a social political concept, as opposed to a technical one. And that which needs to understand its problem-solution discourse as such, allowing the not so obvious tactics of power, knowledge claims and other underling controlling effect of power to be revealed in its varied forms. 2) A second relevance is that having gained such insight through theory, it should allow for one to take a stance, aimed at effecting change, or enabling the demand for change, through direct or indirect action – policy, for example as well as practice.

Present cybersecurity trends are analysed, not necessarily by examining the past, to highlight the anomaly of the present, as acknowledge by Foucault, [15] but rather by looking at how specific governmental forms enact and shape the specific legal and socio-political futures of weaker states; as a period, devoid of an era of obsessive readiness, preparedness or not-there-yet discourse. Such discourse, in turn, produces further legitimising discourse or knowledge claims around the 'need' for certain actions, practices, or solutions to be performed. Thus, the study is aimed at understanding what precisely is at stake in governmental cybersecurity practices such as those exercised by dominant actors (state and non-state), and what theoretical and practical implications they present.

Empirical lines of inquiry are directed at interrogating the UK government's global cybersecurity activities through capacity development initiatives such as the Commonwealth Cybercrime Initiative program, as well as other capacity building and capability support for certain developing Commonwealth nations. The objective here remains one which seeks to shift attention away from analysis that emphasises the problem-solution model of cybersecurity for the purpose of providing policy or normative recommendations on what works and what doesn't. Rather, it aims to direct attention towards an analysis, focused on a deeper and more theoretical consideration and understanding of context.[16]

[15] Michel Foucault and Jay Miskowiec, 'Of Other Spaces' (1986) 16 Diacritics 22.
[16] Bacchi, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (n 5).

The ultimate goal is that, through this exercise, contingent processes of rules or social systems and geopolitical tussles will be revealed as they relate to cybersecurity – processes capable of producing discursive knowledge and meaning, and global subjects as a result. It does so with an intention to contribute to the existing body of work on problematisation, politicisation and securitisation of cybersecurity on the one hand; and, and on the other hand, to highlight the exercise of power relations and how such relationships shape the development of laws, legal norms, and shape behaviour or thought, which could in turn serve as tools of social control and domination.

1.2 Background – evolution of cyber insecurity and the need for capacity building

While security threats from the internet was recognised from the early days of the technology, security concerns around cyber in recent years are partly a result of the increased threat levels and reach, and partly due to the increased complexity of the problem which arises as technology advances.[17] Thus, the consensus is that, tackling these cyberspace-related problems requires global, trans-national efforts and commitments to secure, such that the Internet remains a trusted domain for interactions and economic growth. As such, the last couple of decades have witnessed state commitments, asserting their determination to combat these challenges, through tougher and innovative measures. This has led to what is now commonly termed a multi-stakeholder approach, involving multi-

[17] Michael Warner, 'Cybersecurity: A Pre-History' (2012) 27 Intelligence and National Security 781. See also Joseph S Nye, 'Cyber Power' in Joseph S Nye (ed), *The Future of Power in the 21st Century* (Public Affairs Press 2010) <http://belfercenter.org> accessed 27 October 2021.

interest networks of public, private, state and non-state actors and international organisations to address these challenges.

Thus, solutions to cybersecurity problems are advocated by a complex configuration of actors and institutions, with non-state or non-traditional interest groups often positioned at the helm. Understandably so because, historically, the development and growth of cyberspace and related technologies were predominantly fuelled by the private sector's interests, with the state taking a 'back-seat' while enjoying the benefits of the digital revolution.[18] As such, the private sector constituted (and still does) the dominant, and non-traditional actors.[19]However, as cyber insecurity heightens, and as the traditional prominence of the state (as the bearer of the monopoly and legitimacy over state security and defence) appears to wane, recent trends signalled a struggle for control and governance of cyberspace. This prompted state comeback, with the dominant states championing the struggle to regulate, govern and regain their prominence within cybersecurity discourse.

Until recently, the profound international and transnational makeup of actors in the cybersecurity problem-solution discourse dominated scholarly work on the theme. However, this often lacks in theory and methods devised to aid ones' understanding of the complex environment, and the wider implications of the political and legal response to the problems. This study therefore seeks to offer some thoughts for ameliorating this imbalance.

[18] Nye, 'Cyber Power' (n 17).

[19] World Economic Forum, 'The Global Risks Report 2023 (18.ª)' (2023) <https://www.weforum.org/reports/global-risks-report-2023>.

Both the complex landscape of cybersecurity problems, the solutions offered, and the state's renewed focus in recent decades, raises fundamental questions of power and control in international politics. Here, states can no longer take their traditional position as the 'sole security provider' for granted, as their legitimacy, and capabilities are increasingly contested, creating what Kello sees as a 'sovereignty gap';[20] a situation where states are increasingly no longer perceived as the *de-facto* body to rely on when it comes to cybersecurity.[21] However, state response has been vigorous, with securitisation tendencies, presenting a renewed focus on the challenge as one of national security. Thus, risk and threat discourses across all sectors of government, from social, economic, and legal to military defence have become commonplace. [22]

The nature of cybersecurity challenges means, that this focus also extends beyond state borders, resulting in state actors jostling for position, for continued relevance, power, control, and dominance. With cybersecurity taking a securitization turn, the renewed emphasis on risk and similar narratives created the need for action, or 'governing' of conducts in cyber space. [23]

Inherently, the need to control conduct denotes the need for policies, rules, regulations, laws and so on. As legislative duties and powers remain traditionally the exclusive function of the state apparatus (though the involvement/influence of non-state actors on such traditional state functions is

[20] LUCAS KELLO, *The Virtual Weapon and International Order* (Yale University Press 2017). [229]
[21] ibid.
[22] ibid.
[23] Nikolas Rose and Peter Miller, 'Political Power beyond the State: Problematics of Government' (1992) 43 The British Journal of Sociology 173.

prevalent and forms an on-going contestation, particularly in international law), it becomes one area where states are able to exercise their control of the internet space while maintaining some level of power and legitimacy as a result. Hence, the renewed priorities in recent years amongst the 'elite' states, with a focus on ensuring that the space is governed by a rule-based system by which all states ought to abide. This is a re-affirmation of the role of law as a tool for power and control, as it matters who determines the rules. While legislative responsibilities often fall on sovereign states at national levels, it is an open secret that rules set at international level, through treaties for example, are often determined, dictated, or influenced by dominant interests, particularly those of states and non-state interests in the West.

The UK government continues to reaffirm its commitment too, pledging an all-encompassing, robust and resilient national cybersecurity strategy aimed, amongst other objectives, at positioning the UK in a leading role of shaping a global "open, vibrant and stable cyberspace",[24] through development of frameworks and actions to "support international cooperation".[25] Hence, the international focus of the UK's Cybersecurity strategy forms a key focus of this study.

While relationship with institutions such as the UN, NATO, and the ITU are examined in the study, there is a specific focus on the Commonwealth. This specificity is granted as a uniquely placed international organisation whose

[24] Cabinet Office, 'The UK Cyber Security Strategy: Summary of Progress' 1.

[25] Government of the United Kingdom (n 13).[63].

member-states represent more than 30% of the entire world population (many of which form parts of the world's developing and smallest states).[26] It is also an institution with historical British colonial and imperial roots and legacies, and remains a key focus of the UK's foreign policy. Specifically, the works of the Commonwealth Cybercrime Initiative (CCI), along with those of the Commonwealth Telecommunication Union (CTU) and the International Telecommunication Union (ITU), in Ghana, Botswana and Trinidad and Tobago serve as case studies. The CCI was developed in partnership with the COMNET Foundation for ICT Development,[27], the Commonwealth Telecom Organization (CTO), Council of Europe, International Telecommunications Union (ITU) and the UK government. It was tasked with addressing the emerging issues of cybersecurity, cybercrime and provide support for (particularly developing) member states in areas of capacity building. [28]

This study argues that, while the contemporary Commonwealth may seem to have transcended its colonial past, it nonetheless continues to play distinctive roles in global governance, economic, human, legal (rights) and security. It does this through its alliance with the British government, its

[26] thecommonwealth.org, 'About Us | Commonwealth' (*thecommonwealth.org*) <https://thecommonwealth.org/about-us> accessed 21 November 2019.

[27] COMNET is a Malta-based independent Foundation established in the mid-90s, as a joint initiative of the Commonwealth Secretariat and the Government of Malta. The foundation is believed to have a record of work amongst Commonwealth and other developing countries with a mission to help 'realise the transformational potential of ICT for development, amongst such countries'

[28] Commonwealth and Law Ministers and Senior Officials, 'Report of the Commonwealth Working Group of Experts on Cybercrime':, vol 3 (The commonwealth secretariat 2014).

extensive network of other interstates and non-state actors, alongside their basis in, and advocacy of what it regards as the Commonwealth‘s values and norms.[29]

While the influence of the Commonwealth in shaping both the legal and political landscape of member-states may appear insignificant, according to popular debate and literature,[30] the reality appears very different in the least developed and smallest states of the organisation. And within such states, the Commonwealth is often perceived exclusively as an organisation whose primary interests is in the amelioration of standards in poorer developing states. In other words, there is a sense of conviction amongst poorer states within the Commonwealth that they have more to gain from being part of the body. For such states, Commonwealth model laws and guides for good governance, alongside other numerous templates, are often transposed verbatim by local law and policy makers, and are considered parts of such benefits.[31]

On paper, the UK is no longer perceived as the central driving power behind the Commonwealth. Nonetheless, promoting British values and norms globally remains a key focus of its foreign policy agenda and strategies, from trade to education, politics, and security. The Commonwealth is conveniently placed in this regard and seen as a ‘mutual’ and useful ally by the political elites in Whitehall.

[29] Charter of the Commonwealth 2012 (Charter of the Commonwealth).

[30] Stephen Chan, ‘The Commonwealth as an International Organization’ (1989) 78 The Round Table 393 <https://doi.org/10.1080/00358538908453950>.

[31] Zahid Jamil and Council of Europe, ‘Cybercrime Model Laws: Discussion Paper Prepared for the Cybercrime Convention Committee’ (2014) Version 9.

The British monarchy remains the head of the Commonwealth and the UK's influence is prominent in most of the Commonwealth model laws and other documents examined as part of this study. And while such influence may not have been directly orchestrated by the British government, it is however suggestive of underlying power relations that still exist between the UK and the other states through the Commonwealth organisation. This is true for those lesser economies which are often the target recipients of such prescriptive model laws and policies. For such states, their perception of the Commonwealth is one of "a trusted partner, able to link members of the consortium together under a single Commonwealth umbrella".[32] It is therefore unsurprising to note, for example, a British government department role in what is termed "Phase 2" of the CCI's execution program agenda.[33] For such work carried out in Ghana, Botswana and Nigeria for example, the UK National Crime Agency (NCA) was conspicuously the coordinating force behind the project delivery. This included the deployment of criminal justice systems, capacity building, public awareness programs, preparation of ICT infrastructures to support cybercrime investigations, and development of legislative framework needs for the states.[34] The question therefore is, can the role of the UK be simply that of a trusted partner?

[32] The Commonwealth Secretariat (n10)

[33] Commonwealth and Law Ministers and Senior Officials (n 28).

[34] Dave Piscitello and Lara Pace, 'ITAC » The Commonwealth Cybercrime Initiative: A Multi-Stakeholder Approach To Capability Building To Combat Cybercrime' (*Internetac.org*, 2013) <https://www.internetac.org/archives/1787> accessed 19 October 2019.

1.3 Cybersecurity problematisation: an object of study

Indeed, cyber insecurity and the search for solutions to its problem have generated political concerns and discourses, leading to governing techniques designed to legitimise the introduction of new laws, norms and security practices. Such techniques present an exaggerated representation of the threat in what the Copenhagen School refers to as *hyper securitization.*[35] This allows for 'truth' construction of a problem and subsequent normalisation of practices in response to the 'problem'. The responses in turn represent government actions and practices which produce knowledge, generated by the interplay between power relations (which produces or can produce intentions of their own, that are not necessarily shared by any individual or institution).[36]

For Foucault, power manifests in forms of strategies, produced through the concatenation of the power relations that exist throughout society. Such relations materialise wherever there is interaction between entities. They can be about people or states acting on each other. They can also give rise to other perceptions, actions, or relations.[37] Thus, power exists when one party seek to influence the other in ways that may not necessarily follow any form of linear progression, as it can flow in either direction, but often with one emerging as dominant. This relation may not necessarily achieve the impact for which it is

[35] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School' [2009] International Studies Quarterly.
[36] Michael Michel Foucault, *The Archaeology of Knowledge & The Discourse on Language* (Sheridan AM Smith ed, Pantheon Books 1972).
[37] ibid.

intended or may not even have a grand intention.[38] However, the resulting impact, whether intended or otherwise, could go on producing further impacts, which may or may not be apparent to the actors involved.

Thus, the social, economic, legal or political impact of such power relations, between states and its citizens, or between one or more groups of states or between multinational corporations and states, or between two different economic blocs, could progress in a continuum. Yet this may ultimately end up with a life of its own, perpetually reproducing and establishing knowledge and truth, that leads to outcomes that may not have been part of the original plan. This form that power takes also allows it to remain obscured to the ordinary eye.

Therefore, the turn to problematisation in the cybersecurity discourse as an analytical tool allows for a deeper questioning, of the problem itself and of relations emerging from the problematised fields. It allows one to question further, how and why certain behaviours and phenomena become a problem, at a particular point in time?[39] And what 'problems' are the resulting solutions offered and actions truly designed to 'solve'?[40]

For Foucault, the genealogy or historicity of problems entails a bi-directional flow of thought "in which one tries to see how the different solutions to a problem have been constructed; but also, how the solutions result from a

[38] ibid.
[39] M Foucault and S Rabinow, 'Polemics, Politics, and Problemizations: An Interview with Michel Foucault' in Paul Rabinow (ed), *The Foucault Reader* (Pantheon Books 1991).
[40] ibid.

specific form of problematisation."[41] Thus, Foucault describes problematisations as a process by which objects and domains become problems for thought:

> Thought is not what inhabits a certain conduct and gives it its meaning; rather, it is what allows one to step back from this way of acting or reacting, to present it to oneself as an object of thought and to question it as to its meaning, its conditions, and its goals. Thought is freedom in relation to what one does, the motion by which one detaches oneself from it, establishes it as an object, and reflects on it as a problem.[42]

Thus, new problematised fields are produced when existing problematisations appear to have lapsed and do not work for the new situation.[43] Consequently, a new problematisation emerges when new events occur that trigger or "introduce uncertainty, a loss of familiarity." And it is "that loss, that uncertainty“ which comes about as a "result of difficulties in our previous way of understanding, acting, relating" that gives rise to a new problematisations. [44]

> This development of a given into a question, this transformation of a group of obstacles and difficulties into problems to which the diverse solutions will attempt to produce a response, this is what constitutes the point of problematization and the specific work of thought .[45]

Problems and insecurities are contingent thoughts that have emerged throughout time as problematic situations that must be addressed through

[41] Michel Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984*, vol 1 (Paul Rabinow ed, The New Press 1997).[118-119]
[42] ibid.[xxxv]
[43] ibid.
[44] Paul Rabinow, *The Accompaniment: Assembling the Contemporary* (University of Chicago Press 2011). [89]
[45] Michel Foucault, *The Foucault Reader: Michel Foucault 1926-1984* (Paul Rabinow ed, Pantheon Books 1991).[389]

thoughts and actions that are as fresh as the problems. Thus, a problematisation is realised when there is a confluence between the contingent historical phenomenon and the construction of responses to the phenomenon. The problematisation itself regulates how, when and what responses can be given, as responses or actions both sustain and stabilise problematisations. Responses, nonetheless, equally constitute dynamic agents of stabilisation for a problematisation, while establishing a counter movement for its subversion as well.[46]

Thus, analysis based on problematisation of this kind and as employed in this thesis does not seek to make normative judgement between cybersecurity practices, or to determine which one works best, defining them as either good or bad.[47] But rather, the analysis seeks to understand perspectives on cybersecurity problems, such as insecurity and threats, as a decipherable problem space. Most importantly, it seeks to understand the power structure at play in the efforts aimed at providing 'solutions' to the 'problems'. [48]

The purpose of analysing problematisations therefore is to stir up further problematisations, creating new possibilities for thought and action by questioning the established assumptions, as opposed to producing normative answers.[49] This Foucauldian approach can also be understood as a "genealogy of

[46] Rabinow (n 44).

[47] Foucault and Rabinow (n 39).

[48] Michel Foucault, 'Security , Territory , Population. Lectures at the Collège de France' [1977] Differences.

[49] Colin Koopman, *Genealogy as Critique: Foucault and the Problems of Modernity* (Indiana University Press 2013).

problematization"[50] - a form of empirical inquiry whose goal is not to establish prescriptive conclusions, but to focus instead on problematising things even further.

1.4 Research question

In light of the above, a key guiding question of this research is: how are power dynamics manifested within global cybersecurity discourses and practices and how do they shape perspectives around the subject, particularly those of developing states?

1.5 How is the research question answered?

The task therefore is to engage in a typical Foucauldian genealogical manoeuvre to deconstruct the historical fragments of meaning that form the idea of present-day cybersecurity practices. Hence, such cybersecurity practices including initiatives like the CCI and the United Kingdom (UK) Foreign and Commonwealth Office (FCO) Cybersecurity Capacity Building Programme are examined. They are examined through a historical lens to understand how they compare with earlier regimes; how they respond to current phenomenon against other security uncertainties in the past. It does so to show the latter's fundamental discursive structure and to judiciously analyse their limits and potentialities with a focus on power relations.

[50] Collin Koopman and C. Prado, 'Two Uses of Genealogy: Michel Foucault and Bernard Williams', *foucaault's legacy* (Bloomsbury Publishing 2009).[100]

For this purpose, current cybersecurity-related regulations, legal norms, and laws of the case states are conceptualised as unique mechanisms that work towards the creation of subjectivity, both in the national, and international contexts (as apparatus or technology of power*;* that is, any social structure through which we internalise norms and which is designed to arrange and orchestrate one's understanding of oneself as subject within a certain power structure).

It is routinely argued throughout the thesis that the apparatus delineated by law, which establishes legal norms, possesses a 'double-edged sword', crafted for the purpose of forging the harmonising political and social truth of the subject (both individuals and states alike), as to what rights and obligations one ought to seek, as individuals, societies and global citizens, as well as directing such truth in accordance with predetermined legal frameworks. It does so to establish how these rights and obligations may be perceived and performed. Law therefore makes it possible to perceive oneself (both as an individual and as a state) as a legal subject capable of establishing rules and norms of a society, while at the same time being subject of the same rule.

To unearth the functioning of such apparatus, the approach is thus both theoretical and empirical. Theoretically, works in political and social philosophy as well as philosophy of law, are scrutinised to understand how various perspectives determine the shaping of the individual, the state and global society in their expression of truth through legal norms.

Empirically, the study examines the present through a historical lens to provide insight into how different periods in history, such as the imperial and colonial, shape modern post-colonial legal, social, and political perceptions and legacies. How it allows for a continued power relation in practice, enabling enduring systems which establishes constitutional and legal frameworks that are composed and prescribed as a collective legal will, borne out of innumerable conflicting individual truths. Thus, this role is examined through social and security theories, against promoted legal frameworks and rules-based norms such as the one proposed for cybersecurity by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE) report and the Commonwealth model laws for developing countries.

1.6 Thesis Structure

The thesis is arranged over nine chapters. Chapter two deals with how the notion of underdevelopment, which creates the so-called digital divide in the cybersecurity discourse and the social concept of dependency, provide the theoretical background for an analysis of a sociology of law and cybersecurity. Thus, it examines these concepts and discusses theoretical works on development and dependency and considers them against issues raised by such works, and against recent debates on the security-development nexus.

Chapter three introduces the circle of power, through governance and governmentality. It reviews the global South and North relationship further, focusing on the role of actions as governing and governmentality practices in the control of cyberspace, as a new domain of power and political struggle.

governance and governmentality. Drawing upon the works of Foucault, Giorgio Agamben and others,[51] it explores how political strategies promote and seek implementation of a global culture of threat and risk politics. Here the relationship between security and globalization is examined to understand the role of security today as a basic principle of state activity and a vital tool in "political legitimation".[52]

Chapter four discusses the research methodology and demonstrates the method adopted in the interpretation and analysis of the data. It foregrounds Foucault's discourse analysis and problematisation as both research methodology, theoretical and analytical framework used to track the relations of power that is evident through the data. It rationalises enlistment of the Foucault-inspired frameworks of Carol Bacchi and Mitchel Dean in the analysis and presentation of the research findings.

The research question is engaged in chapters five, six and seven, to present an overview of empirical findings. These chapters focus on language, the use of discourse analysis in the reading of empirical data, to reflect both its historical methods and objectives. The results are thematically presented across three chapters to reflect the three elements within Dean's process of codifying power; namely, the truth, norms and power effects.[53] Cybersecurity is firmly embedded into the current international security agenda which has witnessed, to date, adoption of several high-profile declarations of commitment, cooperation

[51] Giorgio Agamben and Carolin Emcke, 'Security and Terror' (2001) 5 Theory & Event 45.
[52] ibid.[24]
[53] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).

and multilateral agreements. Thus, a critical analysis of articulated ideas, policy principles and norms, and model legal frameworks around cybersecurity is undertaken. The focus is to determine the impact of the global securitisation of cybersecurity, on the domestic socio-political and legal structure of the three developing Commonwealth case states.

These are three states at the epicentre of the CCI initiative with different political systems, cultural identities, and social institutions, which are not necessarily reflected in the distinctive ways they are perceived, or by which they themselves perceive the influence of international cybersecurity actors and norms. By exploring the latter's impact in these similar yet diverse settings, the analysis evaluates variations in the impact and perception of law, legal and political norms adaptation across these states.

To this end, chapter five presents a necessary background to the establishment of the Commonwealth Cybercrime Initiative as a multi-stakeholder partnership,[54] created in response to the trending cybersecurity issues.[55] It explores the problem visibility strategy through security narratives and discourses around cyber insecurity evident in strategy and policy documents, reports, and speeches, and examines how such discourse shapes perspectives, which allow for a cybersecurity problem truth to be established.

[54] Commonwealth ICT Ministers, 'Commonwealth Cybergovernance Model' (The commonwealth secretariat 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.> accessed 16 January 2021.

[55] The Commonwealth Telecommunications Organisation, 'COMMONWEALTH APPROACH FOR DEVELOPING NATIONAL CYBERSECURITY STRATEGIES: A Guide to Creating a Cohesive and Inclusive Approach to Delivering a Safe, Secure and Resilient Cyberspace' (2015).)

Chapter six presents the problem diagnosis nature of the collaborative works of the CCI and other similar programmes from all possible perspectives, which codify the norms effect.[56] It present findings to assess the prevalence of a general or common conjecture as to why such a relationship was/is necessary, such that we can support or refute claims often found in global security narratives; of the global nature evident in security problems in general, the interconnectivity of the digital internet space in the case of cybersecurity, which renders it a borderless problem and therefore, requiring, equally, a borderless solution. Thus, the chapter draws attention to the data, to delineate the presence or lack of any critical assessment of such relationship on either side of the partnership, particularly on the part of the receiving states.

Chapter seven discusses perceptions of the case states in relation to state sovereignty and the perceived impact of their collaborations with these initiatives. It explores the power effect element and how this might materialise, in what form and what normative rules emerge, on what discernible principle and how such rules and processes are perceived or adopted.

Chapter eight follows a "loop back to the relations of power",[57] to examine how certain cybersecurity perceptions have been formed across the cases, when they are formed, and for what purpose.

[56] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).
[57] ibid.[77]

Chapter nine summarises the study, highlighting its relevance to the growing literature on cybersecurity and its contributions to the wider discussion that it hopes it has achieved, with suggestions of possible future investigations.

2 Dependency and digital divide: a conceptual lens to understand cybersecurity capacity building practices

2.1 Introduction

This chapter focuses on the relationship between digital divide and dependency. This is intended to examine how it relates to the digital and legal capacity building within cybersecurity initiatives, such as that of the CoE which inspired the CCI. These initiatives are designed to provide development assistance to developing states, both in their implementation of the Budapest Convention and other related standards, including human rights and rule of law principles.[58] The chapter starts by establishing an understanding of the digital

[58] Council of Europe, 'Worldwide Capacity Building - Cybercrime' (*coe.int*) <https://www.coe.int/en/web/cybercrime/capacity-building-programmes> accessed 29 December 2021. See also Council of Europe, 'Cybercrime Programme Office (C-PROC) - Cybercrime' (*coe.int*) <https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-> accessed 29 December 2022.

divide concept and tracks its applicability to digital technology trends across the last few decades. It then discusses key academic reflections on the relationship between digital divide and cyber insecurity which, it is argued, creates a form of dependence on Western security solutions. It does so to ask whether cybersecurity capacity building initiatives could constitute new form of dependency.

Digital divide within this context refers to the development gaps that exist between the economically and digitally advanced parts of the world and the less developed regions. Development gaps are observable across different sectors, whether political, social, economic or judicial. but often interconnect and intersect at the point of economic development. Gaps can also exist between different regions within national borders, with some sections of the same society deemed more disadvantaged than others. This is often a consequence of historical activities in the various regions that come to form a country.[59] However, for the purpose of this review, the focus is on observable development differences that exist between nations at the global level. While inference might be drawn from other kinds of development gaps, the primary focus remains implicitly on the digital technological development gaps between the developed countries in the Global North and the underdeveloped/developing nations of the Global South in relation to cyberspace and its associated issues.

[59] In countries like Brazil for example, the northern and Amazonian parts of the country are generally believed to be more deprived, economically, and otherwise, than the southern parts for reasons that form parts of the country's historical heritage – slavery, colonisation, oppression of the Indigenous people, etc.

2.2 Digital divide, Digitalisation and Cyberspace

Since the Organization for Economic Co-operation and Development (OECD) definition of the term in 2001,[60]digital divide has generated several debates across government and academia. According to the OECD, digital divide represents development gaps that exist between peoples, or:

> households, businesses and geographic areas at different socio-economic levels with regards both to their opportunities to access information and communication technologies (ICTs), and to their use of the Internet for a wide variety of activities.[61]

This definition suggests two possible deficits on the part of such disadvantaged peoples or nations. First, it suggests the lack of access to modern digital technology. Second, it implies the lack of knowledge, education, skills, or the ability to use the technologies to their full developmental advantage. In other words, it suggests both lack in infrastructural development and skill-sets amongst the disadvantaged groups compared to their less disadvantaged counterparts.

For scholars like Ayanso et al., this deficiency exists at global levels, primarily resulting from the poor economic conditions and poorly organised governance in poorer countries.[62] This, they argue, ultimately creates a double-

[60] Organization for Economic Co-operation and Development, 'Understanding the Digital Divide' (2001).

[61] ibid.[5]

[62] Anteneh Ayanso, Danny I Cho and Kaveepan Lertwachara, 'The Digital Divide: Global and Regional ICT Leaders and Followers' (2010) 16 Information Technology for Development 304 <https://www.tandfonline.com/action/journalInformation?journalCode=titd20>.

edged effect on the part of disadvantaged states. [63] That is, not only does it impact developing states' citizens in positions of economic and political disadvantage, but also their overall development. Consequently, developing nations are forced to advance at a much slower pace than their developed counterparts.[64] This gap further widens as technology innovations happen faster, invariably ensuring the economic and political disadvantage and slow development pace of such states, while condemning them to a self-perpetuating cycle of underdevelopment.[65]

Indeed, swift changes that came with the internet in the 1990's captured everyone's attention, particularly that of international institutions along development lines. Understandably so because, the internet was widely touted as the 'game changer' for economic growth and social development. It was changing how we do things with the underlying technology evolving rapidly. adapting to this rate of change posed challenges even for Western nations. For developing nations, the challenges were undoubtably greater. In some cases, it was akin to a situation of 'the train having left the platform', as they were being left behind.[66] Thus, there was an obvious disparity between what is being achieved in the West, in terms of technology, and a near non-existent digitalisation in the world's poorer nations.[67]

[63] ibid.
[64] ibid.
[65] ibid.
[66] ibid.
[67] Mark Warschauer, *Technology and Social Inclusion: Rethinking the Digital Divide* (The MIT Press 2019).

Bridging this gap therefore became a major concern for international institutions like the UN, the World Bank and the International Telecommunication Union and Western states.[68] The recognition by them, along with the desire to help bridge this gap, led to the formation of a range of initiatives and development schemes.[69] Initiatives such as the Information Communication Technology for Development [ICT4D] were hatched, primarily funded through Western state's international development departments and their multinational corporations. [70] According to Guillen and Suárez, the internet's rapid expansion brought into conversation an assortment of interested parties, ranging from state policymakers and defence strategists, to social commentators and academics.[71] For them, some early cyber idealists and optimists from the late 1980s and early 1990s, in their perception of a free and open cyberspace, fantasised about the internet as one way the world could become smaller and more open, with its "decentralising, globalising, harmonizing, and empowering" effects.[72]

Despite this optimism displayed by such earlier perceptions, some academics like Tapscott and Caston, were mindful of the impending inequalities that the internet age could potentially perpetuate.[73] Thus, as early as the mid-late

[68] ibid.

[69] ibid.

[70] Chrisanthi Avgerou, *Information Systems and Global Diversity* (Oxford University Press 2003).

[71] Mauro F Guillén and Sandra L Suárez, 'Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use' (2005) 84 Social Forces 681 <https://academic.oup.com/sf/article/84/2/681/2235280> accessed 9 September 2020.

[72] ibid. Don Tapscott and Art Caston, *Paradigm Shift : The New Promise of Information Technology* (Art Caston ed, McGraw-Hill 1993).[313] Nicholas Negroponte, *Being Digital* (Coronet Books 1996).[229]

[73] Tapscott and Caston (n 72).

1990s, international organizations, governments, think-tanks, and universities warned of a growing digital divide, both within and across countries.[74] Scholars like DiMaggio et al,[75] Norris,[76] Wellman,[77] and Wynn and Katz,[78] argued that despite its revolutionary potentials, the predicted global social, political and economic benefits of the internet are yet to be seen across the board. In theory, according to Guillen and Suárez, a key problem with the optimistic perspective rests on the often too hasty assumptions of modernisation; the assumption that a new technology can serve as a development or civilising enabler for everyone who embraces it.[79] However, the proverbial train may be leaving the station, and far too quickly for such embrace of digital technology to take place on the part of developing countries.

In Guillen and Suarez's view, there is a faction of scholars amongst earlier commentators, who saw a tendency in the rate at which the internet was evolving and warned of the disparity it could create or reinforce between peoples and states.[80] Academics like Mosco, McChesney and Everett[81] for example, claim that, the internet was buttressing existing class divides, and driving further social

[74] Guillén and Suárez (n 71).
[75] Paul Dimaggio and others, 'Social Implications of the Internet', vol 27 (2001) <https://www.jstor.org/stable/2678624> accessed 24 January 2021.
[76] Pippa Norris, *Digital Divide : Civic Engagement, Information Poverty, and the Internet Worldwide* (Cambridge University Press 2001).
[77] Barry Wellman and others, 'Does the Internet Increase, Decrease, or Supplement Social Capital? Social Networks, Participation, and Community Commitment' (2001).
[78] Eleanor Wynn and James E Katz, 'Hyperbole over Cyberspace: Self-Presentation and Social Boundaries in Internet Home Pages and Discourse' (1997) 13 The Information Society.
[79] Guillén and Suárez (n 71).
[80] ibid.
[81] ibid. citing Vincent Mosco, *The Political Economy of Communication : Rethinking and Renewal* (Sage Publications 1996). Robert Waterman McChesney, *Rich Media, Poor Democracy : Communication Politics in Dubious Times* ([New] ed / with a., New Press 2000). Margaret Everett, 'Latin America On-Line: The Internet, Development, and Democratization', vol 57 (1998).

stratifications.[82] In their view, wealthy nations and large multinational corporations, see cybersphere as nothing more than a giant trading platform. They warn of a possible exacerbation of social, economic and political inequalities that the internet will foster, unless cyberspace is seen as a public good to be both enjoyed by and protected for all.[83]

These early analyses of cyberspace seemingly placed the internet in a paradoxical position. On the one hand, it was viewed as an empowering enabler of development. While on the other, it was a runaway train, driving a deepening gulf between the haves and the have-nots.[84] As Castells puts it: "the heralding of the Internet's potential as a means of freedom, productivity, and communication comes hand in hand with the denunciation of the 'digital divide' induced by inequality on the Internet".[85]

In an effort to determine the extent of this divide at the earlier stages, a ITU's 2009 ICT Development Index (IDI) report provided an analysis of the global ICT development based on quantitative data.[86] The report, compared data over a five-year period between 2002 and 2007, and found that the previous decade has no doubt seen "uninterrupted growth in terms of telecommunication and ICT infrastructure development and service uptake".[87] Further, it contends that by 2008, key ICT development milestones would have already been met, with an

[82] Guillén and Suárez (n 71).
[83] ibid.
[84] Manuel Castells, *The Internet Galaxy : Reflections on the Internet, Business, and Society* (Oxford University Press 2001).
[85] ibid.[247]
[86] International Telecommunication Union (ITU), 'Measuring the Information Society The ICT Development Index' (2009).
[87] ibid. [3]

over 4 billion worldwide mobile subscriptions being achieved. This, it reveals, would "translate into a penetration rate of 61 per cent."[88]

With regards to fixed telephone lines, the rate was much lower, at an estimated 1.3 billion, and with a prediction of a quarter of the world's population accessing the internet. According to the report, "despite the high growth rates, record numbers and all-time high penetration rates",[89] there remains a significant divide and substantial differences within regions; with developing and least developed countries having much lower penetration.[90] It cited the US alone, for example, as accounting for over 82% of all "mobile broadband in the Americas", while Japan and the Republic of Korea owned 70% of such connectivity in Asia and Pacific regions.[91] Such was the nature of the disparity. However, it suggests that while there is clear disparity, there is also a growing optimism in the pace of digital penetration within developing countries.[92] This, it claims, is particularly true when compared to other areas of development such as infant mortality, for example.[93] Using Sweden as a benchmark, the report optimistically claims that developing countries were, in 2008, a mere "10 years behind Sweden" in terms of digital development, as opposed to a staggering 72 years deficit when compared to rates of infant mortality.[94] While such optimism may appear reassuring, a 10-year gap between the developed and the

[88] ibid.
[89] ibid.
[90] ibid.
[91] ibid.
[92] ibid.
[93] ibid.
[94] ibid.

underdeveloped nations is indeed significant considering the rate of evolution in digital technology. If we look at current data from 2023, after 15 years, there is evidently steady progress, but the disparity remains significant.[95] While developed countries have achieved a near universal internet access at 95 per cent, "the average for Africa is just 37 per cent of the population".[96]

Indeed, the perceived benefit of digital technology for all in the mid-to-late 1990s ushered in a host of programs designed to assist developing countries in their digitalisation efforts, many of which were carried out under the flagship ICT4D initiative starting from the early 2000s. Promising examples include those geared towards healthcare, financial services, regulatory services, and education. Prominent amongst them were a series of the World Bank's Info-Dev - sponsored programmes such as the Broadband for Africa Backbone, Capacity Building for ICT in Education in Africa - eLearning Africa and the ICT Regulation Toolkit, which was developed under the Global Capacity Building Initiative for Regulators, and in cooperation with the ITU in 2004.

Debates about the digital divide, particularly in earlier literature, focused upon development issues that were both economic and political. However, these earlier works failed to situate discussions around the digital divide within the context of cybersecurity, despite the seemingly obvious correlation between the characteristics of cybersecurity and the potential implied vulnerabilities in a new

[95] ITU, *Measuring Digital Development Facts and Figures 2022* (2022).
[96] ibid.[8]

technology that was still being understood.[97] The link between digital divide and cyber insecurity, particularly as it affects developing countries, only gained traction as serious concerns over digital crime emerged and became widespread from the early 2000s. Analysts, by the turn of that decade, were increasingly aware of the negative impact of the rapid digitisation drive in the developing world; a drive that was being propelled particularly by increasing broadband connectivity in Africa.[98]

According to Kshetri, experts believed that, by 2010, over 80 percent of computer systems on the African continent alone were infested with computer viruses and malwares.[99] This problem is further compounded by the fact that, similarly, over 80 percent of users in Africa, lacked basic knowledge of information technologies required to deal with such problems.[100] For Kshetri, little surprise therefore, why seven of the top ten trojan sources were from Global South countries, based on a 2009 Kaspersky Labs report.[101] To a greater extent, during this period, a number of academic inquiries (albeit not uniform) focused upon cybercrime as an internet age pitfall, and on the vulnerability of poorly equipped information technology infrastructure of developing

[97] Ellada Gamreklidze, 'Cyber Security in Developing Countries, a Digital Divide Issue' (2014) 20 Journal of International Communication 200.
[98] Nir Kshetri, 'Diffusion and Effects of Cyber-Crime in Developing Economies' (2010) 31 Third World Quarterly 1057.
[99] ibid.
[100] ibid.
[101] ibid.

countries.[102] This vulnerability, while not limited to less developed countries in reality, nonetheless presents different kinds of problems for both developed and developing countries.

This claim is supported by Kshetri in their attempt to map the cybercrime footprint across the developing world.[103]They argue that the structural landscape of cybercrime in developing economies was fundamentally different from those of their developed counterparts.[104] For them, the issue of low internet penetration, indicate limited resource allocations to combat crime on the internet. As such, "formal institutions related to such crimes tend to be thin and dysfunctional."[105] Kshetri also presented a socio-economic dimension to the argument. He suggests that cyber criminality is a much more likely prospect in poorer economies because, unemployment conditions are often rife and wages are low. Consequently, people may be left with little or choices to leading cyber-criminal lives.[106]

Cybersecurity is one area where typical digital advancement problems overlap, both in relation to access to technology and knowledge and skills gaps. There are also other aspects to the problem which are not necessarily and sufficiently addressable by concerns relating to access or cyber skills deficiency. (global economic power, defence and legal structure, for example). On the issue

[102]See for example, Niels Nagelhus Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South The Cyber Frontier and Digital Pitfalls in the Global South' (2018) 6597 Third World Quarterly 1 <http://doi.org/10.1080/01436597.2017.1408403>.
[103] Kshetri (n 98).
[104] ibid.
[105] ibid. [1057]
[106] ibid.

of capacity building for the purpose of judicial reforms and establishment of international norms, Zine Homburger attempts to locate the cybersecurity capacity building debate within the context of international norms development.[107] Homburger argues that while it may be necessary for capacity to be improved globally to make adherence to international norms feasible, it also runs the danger of primarily serving the interest of donor states in the case of developing economies.[108]For Homburger, while developing countries appear to have less dependency on the internet due to their low penetration rate, they equally seem to have less desire to take issues of cybersecurity more seriously.[109] Global North actors on the other hand, see the low income nations with their vulnerabilities as weak links in a network that potentially affects everyone.[110] Thus, the need to support such countries moves higher on their political agenda. As such, the problems of poor infrastructures and institutional structures, education and skills , become less of a 'developing country issue', but one that all nations need to be equally concerned about and be willing to address. This appears to have positive twists, as it could be argued that developing countries stand to benefit from such support anyway. But some disagree and see this as undue pressure on developing countries to 'skill-up' and to reform or transform their institutions.[111] The interdependent nature of the internet, they argue,

[107] Zine Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace' (2019) 0826 Global Society 224.
[108] ibid.
[109] ibid.
[110] See Dutch Foreign Minister's Tallinn Manual launch speech for example: Bert Koenders, 'TALLINN MANUAL Launch (2017) The Hague'.
[111] Robert Hunter Wade, 'Bridging the Digital Divide: New Route to Development or New Form of Dependency?' (2002) 8 Global Governance 443.

demands that the developing economies need to be brought along, and up to the standard that has been set by the Global North actors. For them, this need to transform, while it may benefit the developing states, would appear to also serve the interest of the developed countries .[112]

The interest in supporting these states may also depend on the opportunity it affords Western corporations which ultimately benefit from the delivery and implementation of such upskilling or development programs. Therefore, it becomes less of a choice of whether or not to render assistance to the developing states, but rather more of a self-imposed obligation to do so, as part of their external power projection.

For developing states, on the other hand, either in their desire to strive towards some form of development themselves, or because of coercion through the structural global power dynamics (often through trade and investments), are more or less compelled to receive such assistance. The question of whether one has the desire to perform certain actions in order to address one's or the other's needs, demands a brief philosophical explanation below , along with some exploration of concepts of responsibility. This is necessary to introduce the relationship between such actions and dependency. But first, discussions around what constitute digital divide is reviewed along with how its perception and proposed solutions may create an issue of dependency of the South on the North.

[112] ibid.

2.3 Determining the digital divide. What needs are capacity building the answer to?

ICT growth in the last few decades has been impressive, perhaps not to everyone in terms of economic benefit, but in terms of the speed of its spread. On the economics , Carlson's study in 2004 compares the potentials of these new digital technologies to that of the industrial or general-purpose technologies (GPT) of the past, such as the railroads and electricity.[113] In his view ICT appears to be more impactful than these earlier technologies, particularly through its transformation of entire sectors of society, from government, to healthcare, education, finance, amongst others.[114] This transformational ability constitutes ICT as a key economic driver of our time. According to the UN, such role, when properly harnessed, could transform human and social development.[115]

There is an abundance of academic interest to understand digital divide , with many focusing on the divide between nations or within nations, or both. These interests are seemingly in two main camps. One focuses upon measuring and assessing the nature of the divides, the rate at which they are changing. The other on creating understanding of the 'why' of the divide. [116] In other words, what factors determines a digital divide? Data from the latter, for example, as

[113]Bo Carlsson, 'The Digital Economy: What Is New and What Is Not?' (2004) 15 Structural Change and Economic Dynamics 245.
[114] ibid.
[115] Veva Leye, 'UNESCO, ICT Corporations and the Passion of ICT for Development: Modernization Resurrected' (2007) 29 Media, Culture and Society.
[116] Menzie D Chinn and Robert W Fairlie, 'The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration' (2004) document 881.

demonstrated by Chinn & Fairlie,[117] Crenshaw & Robison,[118] and Skaletsky, et al.,[119] amongst others, shows that differences between nations in relation to digitisation, are results of income disparities. According to such data, it accounts for around 20 and 40 percent of the divide in relation to internet and ICT uptake, respectively. [120] To some, the divide could also be accounted for by levels of education or knowledge diffusion, [121] as well as political engagement. [122] Researchers have also attempted quantification of the gaps , while considering their multifaceted nature using predefined indicators such as those of the ITU.[123]

Measuring the divide by focusing on specific digital technologies, such as telecommunications, computers and the internet have also been attempted. In Chinn and Fairlie for example, while looking at comparative data from several countries including Nigeria, Mexico and India, they found evidence which suggests penetration rates as a result of income and human capital disparity, youth dependency ratio, telephone density, legal quality, and banking sector development to be among key determinants of low technology penetration

[117] ibid.

[118] Edward M Crenshaw and Kristopher K Robison, 'Globalization and the Digital Divide: The Roles of Structural Conduciveness and Global Connection in Internet Diffusion', vol 87 (2006).

[119] Maria Skaletsky and others, 'Exploring the Predictors of the International Digital Divide' (2016) 19 Journal of Global Information Technology Management 44 <https://www.tandfonline.com/action/journalInformation?journalCode=ugit20>.

[120] Chinn and Fairlie (n 116).

[121] Boyan Jovanovic and Rafael Rob, 'The Growth and Diffusion of Knowledge' (1989) 56 The Review of Economic Studies, Oxford Journals 569 <https://about.jstor.org/terms> accessed 25 January 2021.

[122] Norris (n 76).

[123] Adnan Al-Mutawkkil, Almas Heshmati and Junseok Hwang, 'Development of Telecommunication and Broadcasting Infrastructure Indices at the Global Level' <www.elsevierbusinessandmanagement.com/locate/telpol> accessed 25 January 2021.

rates.[124] Thus, income poses a key determinant as it impacts almost all other factors.[125]

Therefore, while the need for, and benefit of, digital uptake may be an attractive prospect, low-income countries simply do not have the means to finance it. This invariably means less likelihood of growth in other areas as a result. With the lack of income capacity to finance programs themselves, one could argue that this ultimately translates into, by default, the need to depend on donors, not only to finance the programs, but also be willing to conform to whatever standards and conditions are set by those donors.

What is clear from a review of this literature is that the nature of the digital divide has historically been determined in terms of the available data on internet usage and access to digital devices that enables connectivity. And with the growth in the availability of digital devices (mobile phones in particular) in the last couple of decades, some conclude that the divide appears to have been closing steadily too, through what seem like a wide-spread global telecommunication uptake. A ITU 2014 report for example, suggests that such uptake may have reached a near global saturation at a rate of 6.8 billion subscriptions, out of a possible 7 billion global population.[126]

[124] Chinn and Fairlie (n 116).

[125] ibid.

[126] International Telecommunication Union, 'Measuring the Information Society Report 2014' (2014).

However, measuring the divide in this way is not without flaws.[127] Hilbert argues that, since there appears not to be a finite number as to how many devices one must have, “any analysis that uses the number of subscriptions as a proxy for the digital divide must come to the conclusion that the divide is closing over time”.[128] For Hilbert, such conclusions risks creating the impression of a rapidly closing gap which in turn creates an illusion of the digital divide as a “carrying capacity of internet users”. And “once this carrying capacity is reached, saturation sets in and the divide can only close”.[129] Saturation of device or subscription should not automatically imply a reduction of digital inequality in terms information access, since bandwidth are not globally uniform. Rather, it widens as digital technology advances with the development of innovative systems and heavier demand for bandwidth.[130]

The difference between having access and ‘really’ having access to information is a current reality which may not have been relevant in the past. For example, there was more inequality in the communication capacity in the early to mid-2000s than during the late 1980s when simple analogue phones were in use; simply because, the rapid move to early narrow-band internet and mobile connectivity in the late 1990s and the emergence of DSL and cable broadband

[127] Martin Hilbert, ‘When Is Cheap, Cheap Enough to Bridge the Digital Divide? Modeling Income Related Structural Challenges of Technology Diffusion in Latin America’ (2009) 38 World Development <http://www.elsevier.com/locate/worlddev>. See also Martin Hilbert, ‘The Bad News Is That the Digital Access Divide Is Here to Stay: Domestically Installed Bandwidths among 172 Countries for 1986–2014’ (2016) 40 Telecommunications Policy.

[128] Hilbert, ‘The Bad News Is That the Digital Access Divide Is Here to Stay: Domestically Installed Bandwidths among 172 Countries for 1986–2014’ (n 127).[568]

[129] ibid.

[130] ibid. see also Hilbert, ‘When Is Cheap, Cheap Enough to Bridge the Digital Divide? Modeling Income Related Structural Challenges of Technology Diffusion in Latin America’ (n 127).

internet in the early 2000s, created their own share of inequalities due to the advancements in the technology.

Thus, for Hilbert, while there may be far more people globally today with internet connectivity, there is a sustained and growing digital divide in terms of bandwidth.[131] And as we develop our capacity further, we are faced with more challenges for which the "answer to the connectivity question moves from being a binary black-or-white choice (0–1) to a continuous and incessantly moving grey zone (1– ∞)."[132]

Indeed, this grey zone is increasingly perpetuated with changing complexity of digital innovations. And the concern of a growing divide continues, particularly in relation to security in the last couple of decades. In the recent global Covid 19 pandemic of 2020 for example, fresh concerns emerged on the impact of such divide in relation to access to vaccines and privacy concerns.[133]

2.4 Digital divide and cybersecurity

Most studies on the relationship between the digital divide and cybersecurity revolve around issues of cybercrime, cyber terrorism, and to some extent cyber warfare. Andrea Calderaro and Anthony J. S. Craig,"[134] claims in a

[131] Hilbert, 'The Bad News Is That the Digital Access Divide Is Here to Stay: Domestically Installed Bandwidths among 172 Countries for 1986–2014' (n 127).

[132] ibid. [569]

[133] John Lai and Nicole O Widmar, 'Revisiting the Digital Divide in the COVID-19 Era' (2021) 43 Applied Economic Perspectives and Policy 458 </pmc/articles/PMC7675734/> accessed 15 April 2021. See also Bernardi Pranggono and Abdullahi Arabo, 'COVID -19 Pandemic Cybersecurity Issues' (2021) 4 Internet Technology Letters.

[134] Andrea Calderaro and Anthony JS Craig, 'Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building Transnational Governance of

recent study that, the task of finding a solution to the gap is both critical and pertinent with regards to the "Global South, where internet usage is growing fast, yet the ability to secure the infrastructure is lagging".[135] This fuels cyber insecurity and concerns in relation to cybercrime and cyber terrorism in particular.[136]Strategic partnership with key regional allies is seen as key to ensuring protection of both political and economic interests. However, the challenge of insecurity in cyber space is complex. Distinct levels of digital maturity between countries in the global North and South complicates the task of forming international alliance on cybersecurity issues.[137] It complicates further the issue of knowing who needs help and where, or whose needs ought to be prioritised.[138] Reports such as the ITU's Global Security Index(GSI),[139] and the Oxford University Global Cybersecurity Centre's Cybersecurity Capacity Maturity Model for Nations (CMM),[140] are believed to be key in this regard. [141] They provide useful insights for global policy makers and capacity building practitioners in "gaining a more comprehensive and nuanced understanding of

Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building' (2020) 41 Third World Quarterlyerly 917.

[135] ibid. [917]

[136] Cameron Ortis and Paul Evans, 'The Pacific Review The Internet and Asia-Pacific Security: Old Conflicts and New Behaviour' <https://www.tandfonline.com/action/journalInformation?journalCode=rpre20>. Also see Kshetri (n 98).

[137] Patryk Pawlak, 'Capacity Building in Cyberspace as an Instrument of Foreign Policy' (2016) 7 Global Policy 83.

[138] ibid.

[139] International Telecommunication Union (ITU), 'Global Cybersecurity Index (GCI) 2018' (2019); International Telecommunication Union, *Global Cybersecurity Index (GCI)* (ITU Publications 2020) <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf>.

[140] Global Cyber Security Capacity Centre, 'Cybersecurity Capacity Maturity Model for Nations (CMM)' (2016).

[141] Pawlak (n 137).

the cybersecurity capacity landscape". They do this through their systematic approach to cybersecurity capacity building implementations across the globe.[142]

Both the CMM and GSI uses similar parameters in their identification of capacity deficit, based on five main indicators corresponding to the five pillars of the Global Cybersecurity Agenda (GCA).[143] This includes;

1. Legal Measures – creating effective legal and regulatory frameworks.
2. Technical & Procedural Measures - Controlling risks through standards, organisations, and technologies.
3. Organizational Structures - Devising cybersecurity policy and strategy.
4. Capacity Building - Developing cybersecurity knowledge.
5. International Cooperation - Encouraging responsible cybersecurity culture within society and internationally.

The GSI 2018 report also confirms the correlation between the significant increase in global digitisation and internet uptake, heightened insecurity and the "need for increased cyber protection". [144] Crucially, it warns of a continued disparity:

> visible gap between many countries in terms of knowledge for the implementation of cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), awareness and capacity to spread out the strategies, and capabilities and programmes in the field of cybersecurity. Sustainable

[142] Global Cyber Security Capacity Centre (n 140).[2]
[143] ibid.[2]
[144] International Telecommunication Union (ITU), 'Global Cybersecurity Index (GCI) 2018' (n 139).

> development in this area should ensure the resilient and adequate use of ICTs as well as economic growth.[145]

Insecurity from widespread digitalisation, particularly in relation to states' critical infrastructures such as energy, health, communication, defence, demands that states enhance resilience in the face of an attack. Again, reaching this level of capability remains complicated for developing states, due to the lack of local expertise and limited resources.[146]

2.5 Dependency and digital divide

Wade,[147] Leye[148] and Guillen and Suárez,[149] were amongst the first scholars to forge a link between initiatives aimed at bridging the digital divide and dependency. For them, the pressure on developing countries to adapt, or adopt recommended Western technocratic solutions, amount to their increased dependence on resources that are controlled wholly by developed nations .[150] For Wade in particular, the problem of lack of capacity for developing states, means that they often have little choice but to implement recommended solutions from the West. This include digital infrastructures which rely on rapidly evolving software and hardware systems, which most developing states have neither the capacity or capability to develop or support organically. This,

[145] ibid. [6]

[146] Enrico Calandro and Patryk Pawlak, 'Capacity Building as a Means to Counter Cyber Poverty', *Riding the digital wave: the impact of cyber capacity building on human development* (2014).

[147] Wade (n 111).

[148] Leye (n 115).

[149] Guillén and Suárez (n 71).

[150] See Wade (n 111). Guillén and Suárez (n 71). Leye (n 115).

they argue, leads to a simple case of their increased dependency on Western technology.[151]

Guillen and Suárez however, attempted a succinct theoretical contribution to the study of global digital divides from a cyber or internet diffusion perspectives. Focusing their study on how such divide is impacted by regulatory, political, social, income and cost variables, they conceptualised internet diffusion through the lens of dependency and World System(WS) theories.[152] They argue that analysis using dependency and WS approaches have shown, through theoretical and empirical means that, "developing countries are dependent on the more advanced economies for capital, technology and access to information".[153] Thus, such relationship "perpetuates patterns of inequality at the global level".[154] This suggests that efforts supposedly designed to reduce the gap, not only create a dependency of the weak on the strong, but can also inadvertently (or advertently) help widen the gap they intend to close in the first place.

It is the view of dependency theorists that terms of agreement between developed countries and the less developed economies, usually follow patterns that are typically unfavourable to the latter group, leading to a relative state of impoverishment on their part.[155] This, in their view is akin to argument

[151] Wade (n 111).
[152] Guillén and Suárez (n 71).
[153] ibid. [684]
[154] ibid.
[155] Doug Porter, Deborah Isser and Louis Alexandre Berg, 'The Justice-Security-Development Nexus: Theory and Practice in Fragile and Conflict-Affected States' (2013) 5 Hague Journal on the

propounded by proponents of WS, that the impoverished state of underdeveloped countries, is a result of their 'forced' integration "into the modern "world-system"".[156] A situation which is "created by the capitalist development of Western Europe and its more successful offshoot colonies, e.g. the United States, Canada or Australia", and creates deeper divide between states.[157]

For Guillen and Suarez, what is key in relation to the dependency and WS conceptualisation is that greater economic growth, or social advancement, are not necessarily born out of buying into the Western-styled modernisation. Rather, a rise in internet use is a function of one's status or place in the world system.[158] The logic is that, if the WS status of developed (core), developing (semi-periphery) or underdeveloped (periphery) defines a nation's development opportunities, then technological advancement will predictably continue to increase much more "quickly in countries that enjoy a more favourable position in the international system of states".[159] This means that, the core, at the top, sets the tone and, therefore, will continue to set the tone.[160]

According to Ciborra, existing schemes and implementation of e-governance in developing countries, for example, are often products of European

Rule of Law 310; Lant Pritchett, 'Divergence, Big Time', vol 11 (1997); Lant Pritchett, Michael Woolcock and Matthew Andrews, 'Capability Traps? The Mechanisms of Persistent Implementation Failure' [2012] SSRN Electronic Journal <https://papers.ssrn.com/abstract=1824519> accessed 18 April 2021.

[156] Guillén and Suárez (n 71). [684]

[157] ibid. [684]

[158] ibid.

[159] ibid. [685]

[160] ibid.

or Western-styled model of state e-governance.[161] And like the early modernisation critics, he adds that there is no real evidence to suggest that such adoption of e-governance systems by developing countries could have any real contribution to their absolute development in the first place.[162] Rather, such systems, which are often not appropriate for the developing economies' environment, risk "more cynicism and disillusion, and investments in ICT could turn into some form of growth-reducing rents".[163] For Ciborra, this creates a certain kind of relationship between the weak and the strong that allows the former to be "govern[ed] at a distance (through sophisticated methodologies and technologies)".[164]

One could argue that despite such criticisms or concerns, the fact remains that as the world advances, with developed countries having somewhat peaked in their digital journey, there is a genuine need for developing countries to find ways of tagging along. Or seek ways to embark on their own journey, on their own terms with less competitive pressure. But the criticisms and concerns are not unfounded as evidence exists of past legacies resurfacing in the present, and transcending into the future across the whole development spectrum.[165]

Thus, while acknowledging the potential benefits of digital uptake by developing countries, Wade's concern is directed at the familiar approach of

[161] Claudio Ciborra, 'Interpreting E-Government and Development: Efficiency, Transparency or Governance at a Distance' (2005) 18 Information Technology and People 260.
[162] ibid.
[163] ibid. [270]
[164] ibid. [260]
[165] Wade (n 111).

pushing initiatives under development umbrellas, as the ultimate remedy for underdevelopment that can be "leapfrogged over the more familiar development problems".[166] Such efforts, he claims, often end up "locking developing countries into a new form of dependency on the West".[167] For Wade, international systems and the governing standards are designed and developed by, and for developed countries conditions. Therefore, as developing countries join the global digitalization campaign, adopting these systems and standards either by choice or compulsion,

> they become more vulnerable to the increasing complexity of the hardware and software and to the quasi monopolistic power of providers of key ICT services. Worse, the Western aid industry, by linking aid to good governance and good governance to programs to digitalize the public sector ("e-governance"), may be reinforcing the overall dependency of developing countries.[168]

Therefore,

> Less developed country (LDC) governments should not take the technologies and international regimes as given. They should press for standards and pricing regimes that make it easier for entities in their countries to ac cess the global information economy. They need more representation in the standard-setting bodies and more support in the ICT domain for the principle that 'simple is beautiful'.[169]

The digital divide narrative, according to Wade, is possibly overrated and hardly a divide at all. ICT for development agendas, they argue, assume the presence of a widening digital divide that needs to be closed. However, in relative terms, the West has a higher ICT to population density when compared to

[166] ibid.[443]
[167] ibid. [443]
[168] ibid.[444]
[169] ibid.[444]

developing countries.[170] Citing a World Bank 2001 World Development Indicator report, Wade claims that, less developed countries had, collectively, a larger share of the digital development when compared to their share of global income. [171] In other words, with developing countries accounting for 61 percent of televisions in the world, telecommunication access at 25 percent and internet access at 28 percent, this is more than "their share of (current exchange rate) world income (20 percent)."[172] Thus, when such ratio is understood in relation to "income, the divide hardly exists".[173]

Perhaps, developing countries can push to adopt what works for them and take more charge of their own destiny. But in an interconnected global economic system, this proves a near impossibility. Does this mean that low-income states are perpetually trapped? This may seem the case if one agrees with the argument that, the international institutions and the systems they promote are designed to serve the interests of those who control the institutions. One could argue that developed states also feel a sense of responsibility. This may be either for reasons related to their historical practices, or for reasons of moral or ethical pressures, which are either self-imposed or simply born out of the realisation that a chain is only as strong as its weakest link. To understand the responsibility discourse that is often attached to arguments for solutions to

[170] ibid.
[171] ibid.
[172] ibid.[445]
[173] ibid.[444]

global socio-economic and political issues such as this one, philosophical underpinnings of such discourse at this point will be useful.

2.6 Relations of responsibility in international context

Viewed along the lines of morality and ethics, responsibility can be both attributive and relational.[174] When attributively perceived, responsibility suggests the innate ability of modern humans to feel a sense of accountability for one another. This means that one is intrinsically capable of choosing whether to offer certain responses to the other's needs based on grounds that may be perceived as moral.[175] This action either leads to praise or blame for the performer of such action, depending on the choices made. Thus, attributive responsibility can be seen along consequential lines.[176] However, as a relational notion, responsibility denotes that, in every act, resulting from a feeling of responsibility, there is an identifiable relationship between the performer and the recipient of such performance which triggers the action in the first place.[177] Understanding these characteristics of responsibility helps one identify and reflect on how it is perceived, particularly within the context of geopolitics and international power relations.

The UN's Millennium Development Goals (MDGs) was signed into history, in the 2000s as a key socio-political endeavour to tackle long-standing

[174] Kai Michael Kenkel and Marcelle Trote Martins, 'Emerging Powers and the Notion of International Responsibility: Moral Duty or Shifting Goalpost?' (2016) 10 Brazilian Political Science Review 10 <http://dx.doi.org/10.1590/1981-38212016000100003> accessed 30 December 2020.
[175] ibid.
[176] ibid.
[177] ibid.

global development issues.[178] These include poverty, hunger, and gender inequality, amongst others. While the MDGs present an umbrella agenda for a number of schemes during its first fifteen years, it appears the initiative has to date produced mixed results.[179] While its 2015 report highlights key progress in reducing extreme poverty, increase in children education, decline in HIV infections, amongst others, it equally highlights the relevance of technology in what it calls "sustainable data for sustainable development".[180] The report demonstrates the importance of statistical data gathering, observation and analysis in implementing global development initiatives. Without which, it says, "the poorest people in these countries often remain invisible", and consequently, they remain unrepresented.[181] Crucially, it suggests that not only is the technology gap a handicap for poorer nations, in terms of internet connectivity and digital infrastructure deficiency, but also a drawback in their ability to collect and process data to aid efforts designed to support the closing of such a gap:

> Large data gaps remain in several development areas. Poor data quality, lack of timely data and unavailability of disaggregated data on important dimensions are among the major challenges. As a result, many national and local governments continue to rely on outdated data or data of insufficient quality to make planning and decisions.[182]

[178] Sakiko Fukuda-Parr, Alicia Ely Yamin and Joshua Greenstein, 'Development The Power of Numbers: A Critical Review of Millennium Development Goal Targets for Human Development and Human Rights' (2014) 15 Journal of Human Development and Capabilities 105 <https://www.tandfonline.com/action/journalInformation?journalCode=cjhd20> accessed 24 January 2021.

[179] United Nations, 'The Millennium Development Goals Report' (2015). See also: Yu Sang Chang, Seongmin Jeon and Kudzai Shamba, 'Speed of Catch-up and Digital Divide' (2020) 23 Journal of Global Information Technology Management 217.

[180] United Nations (n 179).[10-13]

[181] ibid. [11]

[182] ibid. [11]

Measuring poverty and hunger however, along with other such development indicators, through data and statistics, relies largely on how such issues are perceived and framed in the first place; whether in terms of the below the dollar-a-day narrative, improvised retroactive determinants or plain reification of the problems.[183] Ultimately, the choice of what is measured and/or treasured rests considerably on those who control the information, knowledge and discourse.[184] As such, the 'controllers' remain in positions of considerable power and privilege, irrespective of whether a data gap exist or not.[185]

Indeed, for Kenkel and Martins, one might argue, as Aristotle once did, that one's responsibility is often understood through one's ability to choose whether to perform an action.[186] The question thus becomes more about what drives that choice. Whose interest determines the choices being made?

The answers to these questions are rarely or never obvious. Perhaps no other philosopher describes the encounter with the 'other' more succinctly, albeit radically, than Levinas. For Levinas, the beginning of our ethical obligations, whether to oneself or to others, can be attributed to the notion of responsibility. And to understand what he terms *the ethics of responsibility,* one must first transcend ontology, as it takes place beyond one's being or self.[187] Levinas argues that ethics resides in the relationship between the self and the other, in a sort of

[183] Rowan Lubbock, 'Development and Imperialism: Rethinking Old Concepts for a New Age' in G Honor Fagan and Ronaldo Munck (ed), *Handbook on Development and Social Change* (2018).
[184] Ashwani Saith, 'From Universal Values to Millennium Development Goals: Lost in Translation' 37 Development and change 1167.
[185] Lubbock (n 183). see also Saith (n 184). Fukuda-Parr, Yamin and Greenstein (n 178).
[186] Kenkel and Martins (n 174).
[187] Emmanuel Lévinas, *Totality and Infinity : An Essay on Exteriority* (M Nijhoff Publishers ; distribution for the US and Canada, Kluwer Boston 1979).

intersubjectivity. And at that point, the primary subject becomes the relationship itself, as the desires of the other is prioritised by the self.[188] Thus, the ability for the self to see and decide whether to attend to the needs of the other is what defines the notion of responsibility within a relation.[189] Viewed along these lines, responsibility ought not to be hinged on selfish interest, but rather on the true desire of the self to acknowledge and respond to the need of the other, as failing this brings about what Levinas sees as a total negation.[190]

Perception of what the needs of the 'other' are, becomes a key preoccupation with one's understanding of what responsibility is. And in Sartre's view, it becomes part of our existence as humans within a global society.[191] Thus, as part of a global citizenry, one ought therefore to feel a sense of responsibility not just to oneself, but also towards others.[192] For Sartre, responsibility at its basic conception is a "consciousness of being the incontestable author of an event or of an object".[193] However, this composition does not necessarily imply accountability. Key to Sartre's claim is that while responsibility does not suggest accountability, it does imply the need for capacity to perform an act that one

[188] ibid. See also Eva Buddeberg, 'Thinking the Other, Thinking Otherwise: Levinas' Conception of Responsibility' (2018) 43 Interdisciplinary Science Reviews 146 <https://www.tandfonline.com/action/journalInformation?journalCode=yisr20>.
[189] Lévinas (n 187).
[190] ibid.
[191] Jean-Paul Paul Sartre, *Being and Nothingness: An Essay in Phenomenological Ontology* (Mary Warnock and Hazel Estella Barnes eds, Methuen 1958).
[192] ibid.
[193] ibid.[553]

supposedly feels responsible for. This capacity therefore translates into power or ability to perform, which could be material, physical or psychological, etc..[194]

The relevance of Sartre's view within this discussion is that, viewed along the context of global relations, responding to the need to tackle a global problem like cybersecurity, suggests an acceptance of responsibility by those with capacity and capability, or power.[195] Thus, in applying Sartre to the issue of bridging the digital divide or cybersecurity capacity building for example, the response of developed states to the needs of developing states, suggests first, an assumption of responsibility. Second, it implies an assumption of responsibility that also presupposes possession of knowledge, capacity and capability (power), that may have been legitimised through historical practices and existing world order to deal with the needs of the under-privileged 'other'.

Therefore, responsibility, in its relational or attributive state, requires some sort of rationalisation or legitimisation in order for it to have relevance.[196] Thus, one could argue that, both acceptance and performance of responsibility to help bridge the digital divide through capacity building initiatives, for example, could suggest an acknowledgement of a position of power conferred on the performer, by both the performer and the recipient of the initiatives, upon whom the action is being performed.

[194] ibid.
[195] ibid.
[196] ibid.

2.6.1 Responsibility as a form of neo-liberal governmentality

What is interesting about capacity building initiatives, such as those on cybersecurity, is the perception of the relationship between Western states and the developing countries. Within this 'partnership', developing states, despite being the 'supported', are supposed to assume (or be given) the responsibility for their own capacity development. This becomes questionable in what looks like a shift of responsibility to parties who lack capacity, since the demand to perform implies a sense of capacity on the part of the performer to enable its capability to perform. In other words, capacity is required for one's ability or power to perform in relation to the needs of oneself or of the other. It also enables the performer to assume a controlling role over what action is perceived to be performed, how such action will be performed and equally, how it ought to be received.

With the wide-spread use of the so-called partnership model in development arrangements (which demands or divert responsibility to receiving states), how is such structure of power understood? In other words, can a developing state, with significant capacity deficiency, genuinely assume a controlling role through capacity development programs, engineered and, in some cases, executed by others? Critics argue that there is more to this relationship than the typical conditions of such arrangements.[197] To some, it

[197] Clive Gabay and Carl Death, 'Building States and Civil Societies in Africa: Liberal Interventions and Global Governmentality' (2012) 6 Journal of Intervention and Statebuilding. Rita Abrahamsen, 'The Power of Partnerships in Global Governance' (2004) 25 Third World Quarterly 1453.

suggests a change in the usual structure in favour of developing countries.[198] Equally, others call for more investigative analysis into such arrangements, to allow for better understanding of the practices and their implications for the centrality of subjectivity in global power relations.[199] For Abrahamsen, while proponents of such multilateral and biliteral arrangements may argue that the richer donor enterprises are “no longer in the business of telling poor countries what to do,” the “extent to which partnerships represent a transformation in North-South relations is both deeply contested and crucially important.”[200]

Understanding what such partnership really means require analysis of power relations that transcend the erstwhile assessments of partnerships along the lines of “power as the capacity of certain actors to control (more or less) directly the actions of others.”[201] In Abrahamsen’s view, such analysis rests on different conceptualisation of power which are centred around the “extent to which power is being transferred from donors to recipients”.[202] This, they argue, is not to suggest that it is entirely irrelevant in such debate on global governance, but that the transfer of power is only one of the ways such transformation happens, and “in which the power of partnerships can operate.”[203] Thus, Abrahamsen contends that:

> too narrow a focus on the transfer of power between partners prevents contemporary analyses from capturing the full significance of

[198] Abrahamsen (n 197). Rita Abrahamsen and Adam Sandor, ‘The Global South and International Security The Global South and International Security’ 1.
[199] Gabay and Death (n 197).
[200] Abrahamsen (n 197). [1454]
[201] ibid.
[202] ibid.
[203] ibid.

> these transformations, as the power of partnerships does not lie primarily in relations of domination, but in techniques of cooperation and inclusion. Analysing these relationships and their role in global governance hence requires a broader conceptualisation that takes account of how strategies of partnership can them- selves act as forms of power through the production of specific forms of legitimate action and agency.[204]

In bringing this philosophical notion of responsibility to bear within the discursive framework of international moral obligations, from responses directed towards global crisis, to those of global governance, it is clear that a sense of responsibility is often felt by actors who assume the position of global leadership. While this position is not fixed, but changes with time (as new global leaders emerge), such actors may perceive the desire to attend to the needs of poorer nations. They may do so as a form of moral duty for which they feel obliged for whatever reason. But such perception or performance also needs a deeper lens to provide insight into connections between power and knowledge that shapes such geopolitical relations.[205]

Academic thoughts along such lines have also attracted focus around the notion of imperialism as a specific material dynamic and organizing principle of global relations.[206] The idea of the core and periphery Cyber-wellness studies carried out by ITU researchers in developing countries,[207] suggests a growing

[204] ibid.

[205] Michael Dillon and Luis Lobo-Guerrero, 'Biopolitics of Security in the 21st Century: An Introduction' (2008) 34 Review of International Studies 265; Michael Dillon, *Biopolitics of Security : A Political Analytic of Finitude* (Routledge 2015).

[206] Lubbock (n 183).

[207] Itu and Abi Research, 'Global Cybersecurity Index and Wellness Profiles' (ITU Publications 2015) <www.itu.int> accessed 18 April 2021.

divide between development objectives, policy intentions of the donor states, and the apparent security vulnerability in developing states.[208]

Such is the perceived reality of the security predicament that appears to be exacerbated as the digital development gap widens. And in Schia's summation, digitalisation for the purpose of development must be concerned with the security reality that comes with it.[209] This demands the need for further development assistance that are specifically focused on security to such countries. Consequentially, like a vicious circle, the wheel of dependence of developing states on solutions to deal with cyber insecurity would appear to spin endlessly.

2.7 Cybersecurity and development

Cybersecurity within the context of this study, is perhaps best understood along the lines of development. That is, as a way individuals, communities and governments are empowered "to achieve their developmental goals by reducing digital security risks stemming from access and use of Information and Communication Technologies".[210] Identifying cybersecurity in this way aids the systematic analysis of capacity building efforts explored in the case study.

The connection between cybersecurity and capacity building as a way of bridging knowledge and capabilities gap, is no doubt developmental and political.

[208] ibid.
[209] Schia (n 102).
[210] Patryk Pawlak, 'Riding the Digital Wave The Impact of Cyber Capacity Building on Human Development', vol 21 (2014). [5]

Evidently, the cyber insecurity situation is complex as no one appears to be spared from its threats. Even for those countries with innovative and robust strategies and capabilities, a catalogue of potential cyber preparedness requirements still exist.[211] These in Pawlak's view, include human resources development, education, raising awareness, improving organisational structures, as well as setting up new institutions and legal frameworks.[212] For developed countries, such systems may already exist that could be readily adapted for new processes and frameworks. However, the situation is more complicated for developing states, and requires ground-up solutions in some cases, with almost all aspects of governmental institutions and civil society requiring external support to facilitate the transformations. [213]

Examples of such support requirements include drafting national cybersecurity strategies, cybercrime legislations and institution building, setting up national cyber coordination centres and building CERTs.[214] For Pawlak, providing support in these areas also presents sensitive "issues of national sovereignty" as it can interfere, or indirectly influence the "functioning of a state and the relationship between governments and their citizens".[215]As such, it creates almost a sort of covert controlling power relation between 'supporting' states and the 'supported' beneficiary states. [216]

[211] ibid.

[212] ibid. See also Pawlak Patryk and others, 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity' (2017) 2 Journal of Cyber Policy 123.

[213] Patryk and others (n 212).

[214] Pawlak (n 137). See also Pawlak (n 210).

[215] Pawlak (n 137). [84]

[216] ibid. [84]

While the transformative idealisation of cybersecurity capacity building may seem plausible to some academics like Schia as a way forward in addressing the needs of insecurity caused by underdevelopment and poor governance, others, have challenged such optimism. For Hameiri,[217] and Kaldor et al., [218] the idea of capacity building could hide underlying interests of certain actors. They argue that there is a danger of preferential social and political arrangement, as Western powers and interests typically dominate such agendas.[219]

For critics of cybersecurity capacity building initiatives, while the motivation for their implementation can be understood along developmental lines, which sees it as a way the 'weaker links' can be strengthened, the overwhelming interest in its rollout remains unconvincing.[220] In their view, there is a growing understanding that such initiatives are designed to achieve other objectives which are far removed from simply development goals.[221]

Capacity building, whether directed at bridging digital divide or strengthening developing states' resilience against cyber threats, or directed in-wards within a country, remains attached to political agendas. It has increasingly shaped debates around internet governance and norms in the last decade.[222] The

[217] Shahar Hameiri, 'Capacity and Its Fallacies: International State Building as State Transformation' (2009) 38 Journal of International Studies 55. See also: Mary Kaldor, Mary Martin and Sabine Selchow, 'Human Security: A New Strategic Narrative for Europe' (2007) 83 International Affairs 273.

[218] Hameiri (n 217). Kaldor, Martin and Selchow (n 217).

[219] Hameiri (n 217); Kaldor, Martin and Selchow (n 217).

[220] See for example: Mark Duffield, *Global Governance and the New Wars: The Merging of Development and Security* (Zed Books 2014).

[221] ibid.

[222] Ronald J Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 Global Governance 339. See also: Homburger (n 107). Also:

Western alliance, have been at the forefront of this debate, despite a growing number of contenders from non-Western nations. Particularly those from the BRICS nations, like India, who are fast becoming technology service providers and key players themselves, while finding their own voice along with China and Russia in the geopolitical debate around cyber space security. It is necessary at this point to introduce debates that have helped shaped perceptions of cybersecurity capacity building from across the global pond in recent years. Specifically, those centred around cybercrime, cyber governance, and global stability in cyber space in relation to norms development, and the role of emerging actors.[223]

Starting with cybercrime, China and Russia, (often with the support of other BRICS nations) have in the past made call for the UN to reopen the conversation on cybercrime with proposals for new treaties and investigative powers to strengthens the UN crime prevention and criminal justice programmes.[224] Such calls usually prove unpopular with Western actors who stand behind the existing Budapest Convention on such issues.[225] A growing section of emerging powers find the conditions of the convention less palatable, and are happy to form new alliances amongst themselves.[226] This suggests the

Robert Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures' (2021) 6 Journal of Cyber Policy.

[223] Pawlak (n 137). Valentin Makarov, Stefan Schandera and Jean-paul Simon, 'The ICT Landscape in BRICS Countries' (2012) 87 Digiworld Economic Journal. See also Ronald J Deibert, 'Circuits of Power: Security in the Internet Environment' in James N Rosenau and J. Singh (eds), *Information Technology and Global Politics* (State University of New York Press 2002).

[224] Makarov, Schandera and Simon (n 223).

[225] Patryk and others (n 212).

[226] Pawlak (n 210). Also: Patryk and others (n 212). See also Pawlak (n 137).

possibility of choice for developing countries, as they may no longer be bound to board the Western-styled 'train'.

Nonetheless, the question of who controls the internet poses conflicting debates between the two main geopolitical factions (the Western alliance and the BRICS nations along with their allies). Both factions hold opposing visions of how matters of internet governance should or ought to be mandated. Questions of which international law should apply and under what circumstances, remain on-going. And according to Pawlak, cybersecurity capacity building initiatives directed towards development, are seen by donor states and organisations as not solely about dealing with technological needs and improving security preparedness of beneficiaries, but rather "as an investment in promotion of their own preferred vision of cyberspace,"[227] similar to how Western-styled cultures were spread to other societies in the past.[228]

Regardless of the donors' vision of cyberspace, it seems that the problematic realities of the true position of developing countries within these arrangements, can only be a priority to donor states, if such realities impact their interest in a less favourable way. Thus, security problems faced by developing nations can really ever be a priority to the donors, if not solving such problems impacts them in some way. In Pawlak's views, cybersecurity capacity building

[227] Pawlak (n 137). [86]

[228] The British Council today, for example, remain focused on this objective of promoting British culture to the rest of the world.

initiatives, for such donor countries, are a strategic tool, deployed in “pursuit of foreign and national security objectives”.[229]

2.8 Conclusion

The purpose of this discussion is two-fold. First, to examine the conceptual framework of cybersecurity capacity building, and second to establish the theoretical background to the question of whether measures designed to bridge development gaps between the digitally advanced states and the less advanced developing nations, in terms cybersecurity capacity, could form a new case of dependency of the weak on the strong. While some literature on the subject are not specific to cybersecurity, they nonetheless provide useful perspectives on the nature of the development inequalities (which allow for certain power structures to form)that exists with regards to new digital technologies. The aim is to provide insight into different perspectives on the relationship between nation states on the opposite sides of the development spectrum, and set the theoretical stage for the analysis. Detailed discussions around the dynamics of this relationship between global cybersecurity, governance and power, will be undertaken next.

[229] Pawlak (n 137). [86]

3 Global cybersecurity and governmentality: Power, security and law

3.1 Introduction

In the last chapter, the link between development, digital divide, and capacity building within the cybersecurity discourse is discussed. The perceived need for cyber capacity building efforts that extend beyond national frameworks is reviewed along its purpose as a response to the growing global insecurity in cyberspace. The understanding that global cybersecurity issues can only be tackled through a concerted effort has equally fuelled growing demands, particularly from First World states, with increasing transnational sense of responsibility, to develop a coherent and coordinated governance approach. Thus, cyber capacity building programmes continue to generate debates within the international context with varying perspectives on assistance from Global North to Global South. Some focus on aiding the development of cybersecurity strategies in technical terms, while others are concerned with policy and regulatory development. This chapter discusses this relationship further, focusing on the role of cybersecurity as a governing and governmentality practice in the control of cyberspace, as a new domain of power and political struggle.

We begin by tracing the changing dynamics of cyberspace control, from the period when the control was widely thought to be somewhat difficult or impossible to place under state regulation, to the growing exercise of authority by various states within the global cybersecurity politics. International power dynamics which allows for such authorities to thrive and grow is discussed. Such dynamics, which form parts of the existing global social order with far reaching implications that are both, constitutive and regulative.

These implications, nonetheless, can be perceived as both positive and negative.[230] For example, the notion that states can borrow ideas, learn, and share best practices from each other, could be considered positive, especially when such exchange happens between states with similar social-political and economic standing. On the other hand, the dynamics can be negative when it creates 'unhealthy' competition between states. A lack of trust of one state's action or intention will sometimes create adversaries and shape their different foreign policies.[231] Again, such negative competition which creates rivalries will often exist between states with similar capacity and capabilities. This is because it reflects struggles for power or resistance to what one may perceive as

[230] Deibert and Crete-Nishihata (n 222).

[231] Ron Deibert, 'Canada and the Challenges of Cyberspace Governance and Security' (2013) 5 The School of Public Policy Publications 1.

dominant behaviour from the other. But how do such dynamics play out between states with dissimilar capacity and capabilities?

One could argue that it is simply not a case of one leading while others follow. Such dynamics when observed, either between stronger versus weaker states, or between states with similar capability, would seem a far more complex relationship, governed by geopolitical power logic.[232] This, according to Herz, creates what he calls a 'security dilemma', which runs through the ages, whereby, the fear of being attacked, subjected, annihilated, dominated or controlled, leads to the constant desire to acquire more power to stave-off the powers of others.[233] The presence of such logic in current cyberspace and security debates therefore forms part of the focus within this chapter.

The spread of norms is also discussed, to understand the role of various actors (particularly state actors) in the proliferation of ideas and practices (around norms and policies) that are geared toward the control of cyberspace. The focus is on the role of such ideas and practices in shaping or constituting domestic government policies, laws, and behaviour within the case states. Therefore, discussions of cybersecurity is engaged as it relates to certain operations of power beyond the conventional understanding of power (as a mode of coercion or as simply a form of geopolitical phenomenon). This is done to review debates on emerging and on-going efforts to regulate cyberspace through cybersecurity strategies and the operations of power within the global

[232] John H Herz, 'Idealist Internationalism and the Security Dilemma' (1950) 2 World Politics 157.
[233] ibid.

information-technological assemblage that shape the development of such strategies.

Thus, the focus of this review is both on the 'government' of cyberspace through cybersecurity practices as well as the diffusion of power among actors. As such, it reflects the relationship between the two concepts of governance and governmentality. Governmentality has been introduced elsewhere in an earlier chapter.[234] However, a brief introduction to the concept of governance and its relationship with governmentality is necessary.

3.2 Governance and Governmentality

Governance and governmentality are two sociological concepts with roots in multidisciplinary and intellectual traditions that intersect around a common thesis – that concerns itself with issues of governing and regulating modern societies, steering, and conducting people, organisations and institutions.[235] In a broad sense, with origins from the social and political sciences, the governance debate focuses on changes that are related to new sets of relations between the state and social matters. Thus, the concept is made popular by its perceived role as a way such changes are analysed, both within the context of the nation-state and in the international.[236]

[234] See Introduction Chapter

[235] Karin Amos, 'Governance and Governmentality: Relation and Relevance of Two Prominent Social Scientific Concepts for Comparative Education' (2010) 12 International Perspective on Education and Society 79.

[236] ibid.

Genealogical accounts of governance as a concept that cuts across disciplines and the changing role of the state in a global setting, have been provided generously by scholars elsewhere.[237] Renate Mayntz for example, provides a concise representation of its historical account in its various embodiments and characteristics, within different academic contexts and meanings.[238] For Mayntz, governance has the capacity to deal with, not just the more specific issues of steering, but can also deal with broader questions of control and regulation.[239] Milton Mueller also provides a descriptive and historical background to internet governance.[240] His work introduces the institutions and debates that have dominated internet governance.[241] In their contribution, Rosenau and Czempiel offers a link between governance at both national and the international, to highlight the morphing dynamics between them, with governance taking a life of its own when applied within the international context.[242]

[237] See: Milton Mueller, Andreas Schmidt and Brenden Kuerbis, 'Internet Security and Networked Governance in International Relations' (2013) 15 International Studies Review 86.; Milton L Mueller, *Networks and States: The Global Politics of Internet Governance*, vol 48 (MIT Press 2010).; Renate Mayntz, 'From Government to Governance: Political Steering in Modern Societies' in Dirk Scheer and Frieder Rubik (eds), *Governance of Integrated Product Policy: In Search of Sustainable Production and Consumption* (1st edn, Routledge 2006); Mark Bevir, RAW Rhodes and Patrick Weller, 'Traditions of Governance: Interpreting the Changing Role of the Public Sector' (2003) 81 Public Administration 1.

[238] Mayntz (n 237).

[239] ibid.

[240] Mueller (n 237).

[241] ibid.

[242] James N Rosenau and Ernst-Otto Czempiel, *Governance without Government: Order and Change in World Politics* (James N Rosenau and Ernst-Otto Czempiel eds, Cambridge University Press 1992) <https://www.cambridge.org/core/terms.https://doi.org/10.1017/CBO9780511521775Downloadedfromhttps://www.cambridge.org/core>.

To most scholars however, governance is generally characterised along two perspectives – the broad and the narrow.[243] In the former, governance denotes an array of mechanisms designed to create order within a population or network of actors, through negotiation, adaptation, compliance, etc.[244] However, in the latter, it signifies various forms of actions, directed towards a collective concern in a network-like structure of systems.[245] In terms of security, this network-like composition of governance, and the changing dynamics of specific constellations of actors within social and security assemblages, find interest amongst commentators, particularly on issues around legitimacy and political authority.[246] In Bevir for example, contemporary interest in governance emerges both within policy development and academic research in response to profound societal changes in their respective areas.[247]

Cybersecurity governance has equally gained both policy and academic interest for reasons related to the profound technological advancements and heightening of the threat politics it attracts. These changes attract similar concerns of providing and organising security services for cyberspace, attracting new actors, and adopting known or new technologies, policies or apparatuses of steering and control. The 'control', however, may not seem that obvious, particularly when viewed as a necessary response to radically changing security

[243] Mayntz (n 237).
[244] ibid.
[245] ibid.
[246] Mueller, Schmidt and Kuerbis (n 237).
[247] Mark Bevir, 'Governance and Governmentality after Neoliberalism' (2011) 39 Policy and politics 457.

dynamics. This is where governmentality comes in, to direct one's attention to that which may not readily appear obvious.

Governmentality as a Foucauldian concept (in a rather different context but similarly situated within multiple disciplines), denotes the general concerns with the issues of governing, ruling, and steering as it applies to modern states. As such, governmentality involves examination of the typical Foucauldian link between power and knowledge. Within the context of security, for example, as propounded by Foucault, it allows for an examination of what, in Larrinaga and Doucet observation, "can be seen as two interrelated dynamics that have marked contemporary global governance: the global governmentalization of security and the securitization of global governance."[248] This affords one a better grasp of "the general economy of power that Foucault saw as generating in the form of rule".[249]

While cyberspace governance deals with the practicalities of ensuring issues of cybersecurity are handled through policies, norms, and the capacity building, etc, governmentality allows for a critical and theoretical orientation towards such issues (and their solutions), focusing on the discourses and what they mean.[250] Thus, governmentality further allows for the use of historical perspectives in its attempt, to analyse and understand such meanings and discourses.[251]

[248] Miguel De Larrinaga and Marc .. Doucet, *Security and Global Governmentality: Globalization, Governance and the State* (Miguel De Larrinaga and Marc .. Doucet eds, 1st edn, Routledge 2010).[2]

[249] ibid.[2]

[250] Bevir (n 247).

[251] ibid.

Arguably, while both concepts exhibit differences, and may have been frequently used separately in literatures, they nonetheless share similar themes. First, both exhibit a preoccupation with the secrecy of the state.[252] According to Bevier, both concepts no longer see the state as a single entity with powers to act independently or otherwise without external influences. Rather, "they disaggregate the state, drawing attention to the diffusion of political power and political action, and exploring the porosity of the border between state and civil society",[253] as well as the private sector.

Thus, for Bevir, literature on governance and governmentality have both shown signs of integration, with governance literature on the one hand, showing interest in beliefs and traditions, with actors ceasing to be perceived as practical and rational seekers of power and as components of the institutional machine. But rather, "interpretive approaches to governance now echo the governmentality literature in recognising that policy actors draw on historically contingent webs of meaning".[254] Governmentality itself on the other hand, "has begun to stray from its roots in the particular theories and concepts of Michel Foucault".[255] This, they claim, is exemplified in the less application of Foucault's genealogy of neoliberalism in such debates. But they are instead often reminiscent of governance literature in their approach, "associating neoliberalism primarily with the marketisation and new styles of public

[252] ibid.[457]
[253] ibid. [457]
[254] ibid.
[255] ibid.

management that accompanied the rise of the New Right in the late 1970s and early 1980s." [256]

The similarities between governance and governmentality, albeit with differences, could inadvertently feed off each other for the benefit of both. Hence, both are integrated in this chapter, to discuss their implications in relation to cybersecurity practices. The focus, therefore, is to exemplify how this manifest within the examination of cyber governance and the perception of state power, dominance and control. It also plays a role in the empirical attempt that this study seeks to employ through the theoretical and analytical brevity afforded by governmentality's interpretative approach to governance.[257]

3.3 State annexation of cyberspace

As defined by the US State Department of Defence Military Dictionary and its Joint Communication System report,[258] cyberspace is a,

> global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[259]

This definition suggests that the notion of cyberspace governance as currently understood by world authorities, extends beyond the internet space. A

[256] ibid.
[257] Bevir, Rhodes and Weller (n 237).
[258] Chairman of the Joint Chiefs of Staff (CJCS), 'Joint Communications System' (2015). Chairman of the Joint Chiefs of Staff (CJCS), 'DOD Dictionary of Military and Associated Terms' (2021) <http://www.jcs.mil/Doctrine/DOD-Terminology/> accessed 7 June 2021.
[259] Chairman of the Joint Chiefs of Staff (CJCS), 'DOD Dictionary of Military and Associated Terms' (n 258).

space within which the internet is part of. It extends, in recent decades, to include other levels of governance, including norms, laws and other levels through which the space is governed.[260] This is contrary to the presumptions of early analysts, who saw the distributed and decentralised architecture as one that would pose a mammoth task to control.[261] While such presumptions was true then, to a large extent (due to the absence of a single global regime for cyberspace governance), it is noteworthy that decisions by states (Mostly US and other Western states), to stay out of the internet governance in the early days, was a conscious one.[262] Considerable insecurity and the need to ensure that the space does not wind up as a lawless 'Wild West' meant that, some control and order had to be brought in.

Safety and security, hypothetically and historically, rest on the state. But in reality, its governance falls under both private and state control. While this is not unique to cyber governance, cyberspace itself is unique in the sense that, it transcends both the physical and virtual realm. On the physical, sovereign state jurisdictional controls and laws may apply. The virtual or information realm on the other hand, is characterised by both economic and political practices that makes state control challenging.[263]

According to Joseph Nye, a lack of cost barrier and ease of access to the new technology makes for easy attacks from the information layer on the

[260] ibid.
[261] Tim Stevens, 'Cyberweapons: Power and the Governance of the Invisible' (2018) 55 International Politics 482.
[262] Deibert, 'Circuits of Power: Security in the Internet Environment' (n 223).
[263] Joseph S Nye, 'The Regime Complex for Managing Global Cyber Activities' (2014) 1.

physical, where resource is scarcer and perhaps a bit more expensive.[264] For Nye, control of the physical realm can have both "territorial and extraterritorial" impact on the informational realm, creating a rather complex governance environment where both private and public actors "cooperate and compete for power".[265] This uniqueness of cyberspace extends to the power which renders it potent in both virtual as well as in other realms outside of cyberspace (as cyberspace challenges are influenced by events or trajectories that are both physical and virtual). For example, security risks or vulnerabilities could come from either or both human errors and hardware weaknesses or software exploits, and so on.[266]

Hence, a multi-layered application which brings together what is often referred to as multi-actors or multi-stakeholders, through a sort of consensus to oversee distinct aspects of cyberspace governance. The World Wide Web Consortium and Internet Engineering Task Force for example, was used to set standards or operational codes, with some commentators contesting the processes and procedures which were deemed shallow and often undemocratic.[267] Seemingly, decisions around what standard applies to what, are often influenced by individual or collective actor's interests. Depending on who or what the actors are, the interest could be either commercial, political or both. And because the integrated internet network and cyberspace are often overseen by private contract, commercial interests invariably play a great part.

[264] ibid.
[265] ibid. [5]
[266] ibid.
[267] ibid.

In the case of such private or non-government bodies', such as the Internet Corporation for Assigned Names and Numbers (ICANN) for example, despite being incorporated as a private entity, albeit a non-profit, its interest nonetheless aroused controversies over the years. Particularly due to the amount of power it wields and its relationship with the US government. Its processes are believed to have morphed since its inception around 2004 to include 'government voices'(that of the US in particular), but without the vote.[268] While ICANN's control may be limited to the virtual realm of assigning top level internet protocol identification codes, otherwise known as 'IP Addresses', and their associated domain names, its governance power has been far reaching.[269] The otherwise indirect influence of the US government in its procedures and practices means that, its legitimacy as an independent body has been contested, with critical scholarship still questioning its neutrality today.[270]

In a recent case before the International Centre for Dispute Resolution (ICDR), for example, the panel deciding in Afilias v ICANN,[271] found that ICANN "violated its commitment to make decisions by applying documented policies objectively and fairly".[272] It also found that it failed in its dealings and communication efforts, "its commitment to operate in an open and transparent manner consistent with procedures to ensure fairness."[273] A brief background of

[268] Jonathan Weinberg, 'ICANN and the Problem of Legitimacy' (2000) 50 Source: Duke Law Journal 187.
[269] ibid.
[270] ibid.
[271] *AFILIAS DOMAINS NO 3 LIMITED v INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS* [2001] ICDR IRP.
[272] ibid. [3]
[273] ibid. [3]

ICANN is necessary at this point to provide context on the debate around its contested neutrality. Particularly as it has had tremendous impact on how the internet governance was shaped over the years, through its exercise of authority which, to some, "looked, walked, and quacked like public regulatory power".[274]To understand the nature of this power being wielded by ICANN, it is important to briefly introduce the concept of the "root" in the internet scheme of things, and government involvement in the control of the internet.

Contrary to what early cyberspace optimists would have us believe, the internet is indeed built around a centralised hierarchical system of domain names (DNS) and its uniquely identifiable numerical addresses.[275] Together, they perform routing function for a vast majority of the internet traffic. At the centre of this system sits the root, a single top-level directory or file. Domain names and IP addresses are by necessity unique to avoid network communication conflicts – the same way no two area post code can be exactly identical. Ensuring this uniqueness means some rules needs to be followed. And to enforce such rules, an authority is needed to allocate, monitor, and prevent that all-important naming or IP conflict. ICANN exists for this purpose. Because the internet is a big part of cyberspace, control of the root grants a singular power in cyberspace to whomever such power or authority is bestowed. Consequently, that body would have the power to create or decide what top level domain names (google.com, for

[274] Weinberg (n 268).[217]
[275] ibid.

example) can be registered, and how these names and their unique routing IP addresses are assigned to the various internet resources.[276]

The ability to decide what and who gets registered also means the ability to decline registration, deregister or terminate a registered name. Crucially, having this power to terminate or otherwise means power to set rules or terms of use, for which the price for violation can lead to termination. This means that registrants are required to agree to certain terms as part of their registration contract, conferring power of control on that authority to enforce different kinds of internet regulations as it deems fit.[277]

The US government controlled the root in the early days, overseeing the administration of the DNS, mainly through its National Science Foundation (NSF), a combination of volunteers as well as recipients of state funds (including civilians and Military bodies).[278] This invariably placed the United States in a sole position of power over the internet core. While this attracted little or no concern while the scope was relatively small, it very quickly became contentious as the internet exploded in its use. The scramble for domain names grew and the economic potentials of the internet soared, particularly around issues of trademark and intellectual property rights.[279] At the same time, the increasing awareness of its potentials along with possible future dependence of global

[276] A Michael Froomkin, 'Wrong Turn in Cyberspace : Using ICANN to Route Araound the APA and the Constitution' (2000) 50 DUKE LAW JOURNAL.

[277] Weinberg (n 268).

[278] ibid. see also Froomkin (n 276). And, John Palfrey, 'The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed' (2004) 17 Harvard Journal of Law & Technology 409 <http://jolt.law.harvard.edu/articles/pdf/v17/17HarvJLTech409.pdf> accessed 1 August 2021.

[279] Weinberg (n 268); Froomkin (n 276); Palfrey (n 278).

communication and society on the internet, ignited concerns from other foreign governmental bodies,(mostly in the EU) of the US' solitary control.[280]

In response, the US government released a white paper, intended to transition the management of the DNS to a private entity. Consequently, ICANN was incorporated as a non-profit private entity with an international group as part of its board.[281] The board focused on undertaking decisions that were set in line with the white paper's agenda. Key amongst these was to open domain name registration functions to more competitors, as opposed to the monopoly previously enjoyed by Network Solutions, Inc. (NSI), as the contracted sole registrant authority up until that point.[282] However, ICANN started enacting and enforcing policies that exhibited arbitration rules in trademark disputes amongst others , demanding agreement to such terms as a prerequisite for the registration of any new domain names.[283] In effect, these set of peculiar rules benefited some actors at the expense of others. It became clear, in spite of continued insistence by both the US government and ICANN, on its role being nothing more than technical management of internet identifiers, that ICANN was engaging in important public decisions.[284] The question therefore became whether a supposedly private entity, wielding such regulatory public power was consistent with one's usual perception of what public authority and policy making was.

[280] Palfrey (n 278).
[281] Weinberg (n 268).
[282] ibid.
[283] ibid. Palfrey (n 278).
[284] Palfrey (n 278); Weinberg (n 268).

Typically, the concept of political philosophy is centred on the difference between public and private actors, with the latter historically often believed to control only such resources which falls within the private realm. Alarm bells would ring therefore, when a private entity seemingly set rules and control public resources with those rules. And according to Weinberg, a private actor exercising that much power as ICANN did, ought to have been "subjected to constitutional restraints designed to ensure that its power is exercised consistently with democratic values."[285] This raised concerns that were both political in terms of public policy and law.[286] The internet may have previously seemed like a small network of known participants, therefore, trust was not an issue. However, that changed rather quickly with its growth, commercial potentials and interests.

While the apparent openness and low barrier to entry had its advantages, it also allowed certain problems, such as crime, cyber-attacks of different forms and magnitude, to thrive, creating heightened feeling of threat of insecurity as a result.[287] Thus, one would imagine that the demand for protection and control of the internet by the state was inevitable. Thus, the response from states created further fragmentation of cyberspace in what some see as a form of

[285] Weinberg (n 268). [217]
[286] ibid.
[287] Laura De Nardis and others, 'Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance'.

balkanisation of the internet, which has allowed for the diffusion of both commercial and public interests.[288]

For scholars like Deibert and Crete-Nishihata, key decisions by countries like the US was made at the beginning, to "separate out institutions of Internet governance from the direct oversight of states",[289] in order to encourage its uninhibited development and growth.[290] However, this created a short-lived perception of the internet as an 'open common', where, according to Mueller, cyberspace was seen as a utopian 'no man's land', deemed free of state control.[291] This decision appears to have worked for whatever intention , albeit short-lived, as it created a framework which brought on-board other governments within the world system.[292] Thus, it encouraged uninhibited participation and innovation from anyone and everyone.[293]

Indeed, security remains a primary responsibility of the state, and with a rising insecurity in cyber space, state involvement was inevitable. Thus, the common-good notion of the internet is soon dispelled, The private sector could

[288] Madeline Carr, 'Power Plays in Global Internet Governance' (2015) 43 Journal of International Studies 640 <http://www.malcolmturnbull.>. see also De Nardis and others (n 287).
[289] Deibert and Crete-Nishihata (n 222). [342]
[290] ibid.
[291] Milton L Mueller, Networks and States: The Global Politics of Internet Governance, vol 48 (2011); Milton Mueller and others, 'Net Neutrality as Global Principle for Internet Governance' (2007) <http://www.fcc.gov/ATT_FINALMergerCommitments12-28.pdf> accessed 25 May 2021; Mueller Milton L., Ruling the Root : Internet Governance and the Taming of Cyberspace. (The MIT Press 2002) <http://search.ebscohost.com.ezproxy.lancs.ac.uk/login.aspx?direct=true&db=nlebk&AN=75989&site=ehost-live&authtype=ip,shib&user=s1523151>. See also: Ronald Deibert and others, 'Access Contested: Toward the Fourth Phase of Cyberspace Controls' in Ronald Deibert and others (eds), Access Contested: Toward the Fourth Phase of Cyberspace Controls (The MIT Press 2011).
[292] Williams J Drake, *The New Information Infrastructure: Strategies for U.S. Policy* (William J Drake ed, English, The Twentieth Century Fund Press 1995).
[293] ibid.

not be left to self-control. Therefore, a number of information controls around the digital space soon to emerged from the state. This brought new forms of governance that were far from the idealistic foundational principles of cyberspace,[294] ushering in a range of "state-based forms of control that are typical of the pre-internet days of territorialized regimes of communications". [295] According to Deibert and Crete-Nishihata, these were actions designed to disrupt the new information highway, allowing the state to "manipulate, and shape information and communications for strategic and political ends". [296] An otherwise perceived cyberspace without borders became a space for state censorship, with restricted access to some information within certain state borders.[297]

While such control at state level may have been basic, it nonetheless kicked off an era of security and privacy concerns, and the debates around internet politics, with justifications for such control thought to be based on both social, political and economic needs. For example, the need to control content that risks sexual exploitation of children, and discouraging the spread of violence or hatred, particularly those of religious nature, the need to protect intellectual properties and safeguard copyrights, and many more. For Nart Villeneuve, [298] this also marked the beginning of censorship for political reasons, as it became possible or necessary for certain governments to prohibit or promote certain

[294] Deibert and Crete-Nishihata (n 222).
[295] ibid.[343]
[296] ibid.[339]
[297] Nart Villeneuve, 'The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace' (2006) 11 First Monday.
[298] ibid.

content to detract from their real political agenda, driving the trajectory of such state involvement into broader areas.[299]

State involvement of this kind became evident from the mid to late2000s, during the civilian protests in Nepal, Burma and China.[300] Similar cases of intentional internet black-outs also occurred in Libya, Egypt and Iran during the so called Arab Spring, in the case of the former two, and the Green Revolution in the case of Iran.[301] However, state interference of this nature was not limited to the so called authoritarian regimes. Otherwise democratic states of the West had their own share of control. An example that springs to mind is the UK government contemplating the need to restrict internet communication in certain areas of the country, to stem the continued violence and disorder during the 2011 riots in London and elsewhere in the country. Consequently, and as described in Casilli and Tubaro's working paper,[302] the interest in greater levels of government control emerged as a range of legal, regulatory instruments that were introduced particularly at national levels.[303] These included laws, policies and access control through service providers.[304]

[299] ibid.

[300] Rebecca Mackinnon, 'Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom', *Liberation Technology in Authoritarian Regimes* (iis-db.stanford.edu 2010). Steohanie Wang, 'Pulling the Plug: A Technical Review of the Internet Shutdown in Burma' <http://www.irrawaddy.org/article.php?art_id=8705.> accessed 7 June 2021.

[301] Human Rights Watch, 'False Freedom Online Censorship in the Middle East and North Africa' (2005).

[302] Antonio A Casilli and Paola Tubaro, 'Why Net Censorship in Times of Political Unrest Results in More Violent Uprisings: A Social Simulation Experiment on the UK Riots' (2011) <http://ssrn.com/abstract=1909467>.

[303] ibid.

[304] ibid.

To advance this discussion through the history of cyberspace, as recorded by the Internet Society, state intervention in the development of cyberspace was never really absent, albeit having a silent hands-off approach at the early stages.[305]Some less conspicuous involvement was always there, from the time of the ARPANET network, which was established by the US Department of Defence's Advanced Research Projects Agency (DARPA), onwards.[306] This sort of control was done either through research funding or direct appointments of key government officials to oversee such projects.[307]

As highlighted by Deibert *et al.*, the visible return of state control was facilitated by the politics of threats and insecurity in cyberspace, although not in the same old Westphalian narrative of state sovereignty.[308] Government interest moved beyond internet censorship of the earlier days which, according to the Open Net Initiative (ONI), were primarily territorial, and focused on controlling the internet within state borders.[309] As the focus shifted beyond territorial control, interest in greater means of control to shape the entirety of cyberspace, saw the emergence of a wider range of interests by the more powerful governments in their outward-looking, sometimes, covert and offensive measures.

[305] Joel Snyder, Konstantinos Komaitis and Andrei Robachevsky, 'The History of IANA: An Extended Timeline with Citations and Commentary' (2017) <internetsociety.org> accessed 7 June 2021.

[306] ibid. see also 'The Internet' (*clintonwhitehouse4.archives.gov*) <https://clintonwhitehouse4.archives.gov/WH/EOP/OVP/24hours/internet.html> accessed 22 August 2022.

[307] Snyder, Komaitis and Robachevsky (n 305). 'The Internet' (n 306).

[308] Ronald Deibert and others, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Ronald Deibert and others eds, The MIT Press 2010).

[309] Helmi Noman and Jillian C York, 'West Censoring East The Use of Western Technologies by Middle East Censors' (2010) <http://opennet.net.>.

A key starting point for such outwards-looking approach emerged towards the later part of the first decade of the 2000s when some of the Western nations began legislating for greater control through the telecommunication and internet service providers in what Ethan Zuckerman describes as, intermediary liability.[310] This meant the devolution of responsibility by the state to the private providers to monitor and police the space. Consequently the private operators assumed certain powers as they were required by the state to archive and share data with intelligence and law enforcement bodies. As such practice grew, so did its abuse by corporations who collected these data. The secret collection of data with regards to people's behaviour in cyberspace became more refined with manipulative capabilities designed for commercial gains.[311] As Deibert and Crete-Nishihata explained, some major operators even resorted to offensive measures in their pursuit, in guise of what is described as Active Cyber Defence (ACD), allowing them to engage in such activities irrespective of territory.[312]

Arguably, internet governance is complex, but also hinges on interests and benefits. According to Nye, the desire for states to protect cyberspace rests on the need to guarantee the protection of those benefits which their societies derive from it, while also defending or protecting their societies against potential threats from the internet.[313] Thus, while some governments may control access through censorship, they nonetheless seek the benefits of connectivity in creating

[310] Ethan Zuckerman, 'Intermediary Censorship' in Ronald Deibert and others (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (The MIT Press 2010) <https://doi.org/10.7551/mitpress/8551.003.0010>.
[311] Deibert, 'Circuits of Power: Security in the Internet Environment' (n 223).
[312] Deibert and Crete-Nishihata (n 222).
[313] Nye, 'The Regime Complex for Managing Global Cyber Activities' (n 263).

an imbalance and complication in reaching a unitary set of norms to govern cybersecurity.

Cybersecurity also means different things to different states due to the fragmentation of norms around it which split states into two broad camps. There is the so-called democratic states camp, which includes Western states and those abiding by similar Western democratic standards. On the other hand, there is the camp of the oft labelled (by those on the former camp) authoritarian states, with Russia and China seemingly leading that camp. For Nye, this sort of fragmentation creates a complication which was visibly animated during the World Conference on International Telecommunications (WCIT), in 2012.[314] While the conference's focus was on reviewing the international telephony regulations, the salient issue was that of internet governance, and the question of who ought to be playing what role, and to what extent. Those regarded as countries with authoritarian regimes, along with a majority of the developing states, supported the idea of a security and development approach which goes in line with the UN, and with whom the ITU is also a key actor.[315] To such states, the ITU is a preferred option as opposed to ICANN, which to them, continues to exist and function primarily at the behest of the United States government.[316]

On the contrary, Western states were alarmed at such prospect. To them, the rigidity of ITU's structure would jeopardise the need for a more fluid and multi-actors' approach, "that stresses the role of the private and non-profit

[314] ibid.
[315] ibid.
[316] ibid.

sectors as well as governments."[317] Crucially, the Western states lost the bid in the final vote which tilted in favour of the other camp by around 39 percent, sparking fears amongst commentators of a looming crisis and fears of a resurgence of a new cold war.[318]

3.4 Forces at work in global cyber control

The issue of state control of the supposedly free and open cyberspace admittedly falls under the rubric of cybersecurity. And as commented by Foucault, a 'culture of danger' is never far away wherever there is liberalism.[319] In Larrinaga and Doucet, security and governance are intertwined, so much so that both terms would appear to mean the same thing.[320] And while this may have always been the case, it has observably developed into a near state of obsession, of one with the other in modern times.[321]

Meanwhile, the threat politics of some security rhetoric in recent decades have left us with a rather sour taste, particularly with such rhetoric around contemporary politics (on terror and terrorism, for example) since the September 11 Twin Tower attack in the United States. As Larrinaga and Doucet wrote: "every seasoned political tactician and marketeer surely knows that nothing in today's world seems to advance the urgency and importance of a claim

[317] ibid. [7]

[318] Mueller (n 237).

[319] Michel Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (Michel Senellart ed, Palgrave Macmllan 2008).

[320] Miguel De Larrinaga and Marc G Doucet, 'Sovereign Power and the Biopolitics of Human Security' (2008) 39 Security Dialogue 517.

[321] ibid. See also: David Grondin and Miguel de Larrinaga, 'Securing Prosperity or Making Securitization Prosper?' (2009) 64 International Journal: Canada's Journal of Global Policy Analysis 667.

more easily than one grafted to security, however tenuous such an operation might appear".[322] And "while there are constant reminders not to take our security lightly, lest we carelessly take our lives and those of others into our own hands, the desired ontological effect of security does not always hold."[323] For them, security:

> certainly, has not met the kind of resistance that other 'modern universal discourses' of European descent have incited from recalcitrant far-off locales as has been the case for instance, with liberalism, human rights, capitalism, or democracy. Its ease of travel may very well make it the quintessential political discourse of modernity.[324]

Indeed, cybersecurity is yet another new addition to the various security concerns plaguing current global society and politics. Thus, as the notion of threats began and continue to emerge, in and from cyberspace, irrespective of its geographical boundaries, there remains the need for states to formulate security strategies that are specific to cyberspace, and place them in positions of influence.

We have learned from globalisation, that states' policies are rarely formulated devoid of their interaction with other states and the wider international system. And as noted by Brian Loader, states in modern societies are integrated into a global order of things, which influences 'who' is 'who', who

[322] De Larrinaga and Doucet (n 248).[2]

[323] ibid.

[324] ibid.

does what, and how things are done.[325] This is due largely to the globalising nature of the cyberspace infrastructure itself, and its developmental origins.[326]

According to Nye,

> Governance of the Internet is not a single-issue area. Its governance encompasses a constellation of administrative and technical coordinating tasks necessary to keep the Internet operational and to enact related public policy. The tasks range from technical standard setting and the administration of domain names and numbers to setting policies related to cyber security and privacy.[327]

While cybersecurity concerns and measures taken by states are motivated by local threats and domestic struggles, of greater importance is their relationship with other states, their perception of the intentions and actions of their adversaries (at all levels), as well as their role in the global institutions such as the UN and NATO. Thus, the issue of cybersecurity and governance, for the sake of ensuring security control, becomes less about security itself, but rather one that is driven by the political value it affords, even at domestic levels. Little wonder, therefore, and in Larrinaga and Doucet's observation, as noted above.[328]

The lack of a common global governance regime when it comes to cybersecurity is amply documented, with many asking why this remains the case. Others theorise on possible future directions that such common global control

[325] Brian Loader, *The Governance of Cyberspace : Politics, Technology and Global Restructuring* (Routledge 1997).
[326] ibid.
[327] De Nardis and others (n 287).
[328] De Larrinaga and Doucet (n 248). [1] See also De Larrinaga and Doucet (n 320).

should take.[329] Such debates, provide a reflection of the social, political, economic and legal environment of the governance of cyberspace, with authors like De Nardis,[330]and Mueller,[331] demonstrating their preference for a form of global governance that is selective, based on what aspect of cyberspace needs governance, and the kind of governance needed, as opposed to that which takes a rather holistic approach.[332] In other words, such governance approach should be one which takes into account the social, political and legal environment into consideration, tailoring governance to suit the needs, rather than a one size fits all approach.[333]

For some however, this approach creates a similarly disjointed array of multiple internet governance regimes and institutions, each targeting different forms of activities taking place, both within and through cyberspace.[334] Examples include various bodies with dedicated roles for specific governance issues, from those designed to deal with norms or standards, technical or administrative, to those focusing on national security, telecommunications, finance, etc.[335]

While some of these regimes may have their origins outside of cyberspace governance, they nonetheless overlap it. And as expressed by

[329] Myriam Dunn Cavelty and Andreas Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science' (2019) 41 Contemporary Security Policy 5.
[330] Laura DeNardis, 'Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance' (2012) 15 Information, Communication & Society.
[331] Mueller (n 237).
[332] DeNardis (n 330); Mueller (n 237).
[333] DeNardis (n 330).
[334] See for example: Mark Raymond, 'Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot' (2016) 10 Strategic Studies Quarterly 123.; See also In Tae Yoo, 'New Wine into Old Wineskins? Regime Diffusion by the Powerful from International Trade into Cyberspace' (2017) 32 Pacific Focus.
[335] Nye, 'The Regime Complex for Managing Global Cyber Activities' (n 263).

Madeline Carr, this multi-dimensional or multi-institutional approach to cyberspace governance has become the *de facto* response to the issue of managing cyberspace governance.[336] Evidently, different aspects of cyberspace governance are overseen by different institutions, whether it is the OECD Tallinn's manual for norms development and governance or NATO or the CCD COE convention for cyberweapons.[337]

While reaching a consensus on who and how cyberspace should be governed remains elusive, individual countries appear set and clear on what/where their strategic goals and focus lie with respect to their interest in securing cyberspace. Thus, their policies express similar strategic goals and focus to that effect. However, the need for an all-encompassing approach to tackling cybersecurity issues appears to be embraced by all. This includes such need to conduct crucial government reforms as well as engaging with public-private partnerships, and cooperating internationally with other states and entities.

A key interest to this study is the question of how these interrelated efforts by the various stakeholders have evolved into what is often referred to as a 'culture of cybersecurity' within the different national strategies. A culture which very much resembles a site of techno-political experiment, where the landscape of the new digital world is carefully conceptualised, framed, negotiated, articulated, and brought to life. The motivation for this experiment calls into question the role of developing states in the construction of this new

[336] Carr (n 288).
[337] Stevens (n 261).

global digital reality, where normative and institutional boundaries are being thought, drawn, and expressed through policies and laws. The focus thus, remains on understanding these regimes and policies beyond their perceived transformations, technical or otherwise, and whether such transformations reflect the interest of everyone or simply those of the designers.

For Stevens, however, the proliferation of these regimes and institutions demonstrates the role of what could be classified as a form of institutional power in the contestation and promotion of "forms of cybersecurity governance", within the international system.[338] According to Stevens, there is a lack of sufficient academic considerations on this form of power, both with regards to cyberspace or the internet itself, and on accounts of its governance.[339] This would seem to support Deibert' s earlier observation that, cyberspace, as an infrastructure (just like any other), is born out of actions that are social in nature, and the result of certain resolves and contentions that shapes social behaviours. As such, it demonstrates "formidable set of real constraints on the realm of the possible", that are built in.[340] Thus, and as might be expected, scholars interested in such topics have developed a focus on "the concerns about the circulation of ideas, the framing role of discourses, and processes of legitimation", as opposed to the "older positivist-materialist notions of state interaction".[341] And as per McCarthy's depiction, cyberspace as a technological institution "prevents or

[338] ibid.

[339] ibid.

[340] Ronald J Deibert, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace' (2003) 32 Journal of International Studies 501.[530]

[341] ibid. [530]

promotes goals in line with the goals of its designers" through its ability to choose which of its practices to include or exclude in its realm of control.[342] This ability, in Steven's claim, represent the sort of institutional power that can be wielded by the most powerful "actors in this technological space",[343] who design and currently control the space.

The US, Stevens argues, as the birth place and original designers of the architecture on which cyberspace rests, along with most of the current rules by which it is functionally maintained, enjoys a certain level of dominance which is supported by this institutional power.[344] This position of power, remains rather unchallenged, as their capability and capacity grant them continued dominance, supported by other powerful Western allies like the UK and the EU, who are allowed to share in the power glory, albeit to lesser degrees. [345] However, China's growing power presents new challenges to that superiority, particularly since the launch of its Strategic Support Force (SSF), to unify the People's Liberation Army's (PLA) cyber, space, and electronic warfare capabilities in 2015. This followed the US's launch of their 2009 Cyber Command (USCYBERCOM).

The current political order, therefore, demands a rethinking of one's conceptualisation of the institutional power of cyberspace, particularly, how it impacts the transfer of knowledge and the provision of support from the

[342] Daniel R Mccarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (Palgrave Macmillan 2015).[67]
[343] Stevens (n 261).[17]
[344] ibid.
[345] See US Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command' (US Cyber Command 2018) <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf> accessed 18 January 2020.

powerful states to the less capable states. Such deliberation allows for better understanding of the role played by those who, by virtue of their capabilities and dominance within the cyberspace architecture, wield power in the space, and in determining how it is governed.

Stevens also explores the analytics of power in the governance of cyberweapons based on Barnett and Duvall's formulations of power, along with three other conceptualisations of power that are manifested in security regimes. Namely, productive, structural, and compulsory power.[346] The reality of the lack of a single governance regime in cyberspace means that there is also no single international consensus on the how and why of cyberspace governance. This inadvertently means that literature on the politics of cybersecurity is often discussed along the lines of global power relations, as well as the national or specific interests of relevant actors. The focus of such debate rarely transcends the great powers of the West, led by the US on the one hand, and the emerging powers of the BRICS states, led by China and Russia. Therefore, there is a need to understand the operations of power in cyberspace beyond such discussions, to explore how power in the cyber-technological assemblage impacts the way power is obtained, sustained, and utilised;[347] Particularly in relation to weaker economies that are not necessarily adversaries of the dominant states, but rather perceived as partners, albeit unequal ones. And as asserted by Bruno Latour in their theorisation of the Actor Network theory for example, an actor's power

[346] Stevens (n 261).
[347] ibid.

becomes evident through the impact its action has on the other.[348] But, this impact can only often become apparent through the display of resistance from the 'other' to those actions.[349] In other words, the presence of power in a given action may be concealed and may not be perceived as such if one fails to recognise it as such, or sees no need to resist. Such power manifests itself through what Latour calls socio-material relations which can, on the one hand be either constitutive or interactive, while on the other hand, it could be expressed directly or indirectly.[350]

To some extent, Latour's conceptualisation mirrors Barnett and Duvall's formulation of power. In the latter's volume on Power in Governance, they attempted a detailed description of these classifications of power-forms more generally within the globalised world.[351] Whereas, Stevens in his analysis, explores the specific manifestations of these powers within the cybersecurity discourse, which offer more relevance to the current study. Nonetheless, both conceptualisation and applications are discussed below for brevity.

3.5 Cyber governance and governmentality

Based on Foucauldian understanding, and as expounded by Barnett and Duvall, power at its productive phase, create social actors through relations that

[348] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press 2005).
[349] ibid. See also: Bruno Latour, 'The Powers of Association' (1984) 32 Sociological Review 264.
[350] Latour (n 349); Latour (n 348).
[351] Michael N. Barnett, *Power in Global Governance* (Michael N Barnett and Raymond Duvall eds, Cambridge University Press 2005).

are epistemic, discursive, pleasurable and constitutive.[352] This resembles the kind of power manifested through law which Zizek, for example, describes as a paradox - whereby it produces freedom on the one hand, and regulates that same freedom and punishes its transgression, on the other.[353] In the case of cybersecurity and governance of cyberspace, the OECD NATO's Tallinn Manual is an example of such power, which is productive in its attempt to legitimise and regulate aspects and practices of, and in cyberspace.[354]

For example, the constitution of the Tallinn Manual process is perceived as a body of knowledge authority, through which cybersecurity ideas, doctrines and policies of its member states are inculcated and promoted to the rest of the world, in a rather hegemonic way.[355] And with regards to the use of cyberweapons as an offensive-defence strategy, the recognition of offensive cybersecurity tools as a form of weapon within the Tallinn Manual, translates, first, into its acceptance or legitimation of its existence. Second, that because it exists, its use will therefore need to be controlled.[356] In other worlds, the development of policies around cybersecurity practices such as the use of cyberweapons, are designed to allow for their use rather than the abolition of

[352] Michael Barnett and others, 'Power in International Politics' (2005) 59 International Organization 39; Barnett (n 351).

[353] Slavoj Zizek, 'Why Does The Law Need An Obscene Supplement' in Peter Goodrich and David Gray Carlson (eds), *Law and the Postmodern Mind: Essays on Psychoanalysis and Jurisprudence* (University of Michigan Press 1998).See, Laurent De Sutter, *Zizek and Law* (1st edn, Routledge 2015). See also Jodi Dean, 'Zizek on Law' (2004) 15 Law and Critique.

[354] Stevens (n 261).

[355] ibid. See also Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 American Journal of International Law 583; Wolff Heintschel von Heinegg, 'The Tallinn Manual and International Cyber Security Law' in Terry D Gill and others (eds), *Yearbook of International Humanitarian Law*, vol 15 (Cambridge University Press 2012).

[356] Stevens (n 261); von Heinegg (n 355); Efrony and Shany (n 355).

such practices. In Barnett and Duvall's terms, a form of productive power is manifested through this central place where rules are set, norms are developed that eventually influences laws that are made, which ultimately determines what will be allowed, for what purpose and by whom.[357]

Understandably, what seems like a disclaimer is expressed by the authors of the Tallinn Manual, discouraging perceptions of the document as "an official document, but rather the product of two separate endeavours undertaken by groups of independent experts acting solely in their personal capacity."[358] Its scope and objective, admittedly, is to provide legal basis for cyber operations or practices by states, in order to facilitate their use while subjecting such actions to regulation within the global cyber landscape.[359] According to Hayden, the Tallinn Manual's endeavour on cyberweapon, for example, the possible transition or translations of its legal principles and *opinio juris* into legal frameworks, policy, of nation states and supranational bodies such as NATO, affords law enforcement and defence departments the legitimation they need to justify their use.[360] Thus, for Stevens, such affirmation supports and allow for the formation of subjectivities, of perceptions amongst the different actors, towards what is

[357] Edward T Barrett, 'Warfare in a New Domain: The Ethics of Military Cyber-Operations' (2013) 12 Journal of Military Ethics 4 <https://www.tandfonline.com/action/journalInformation?journalCode=smil20>.
[358] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N Schmitt ed, Cambridge University Press 2017) <http://ebooks.cambridge.org/ref/id/CBO9781316822524>.[2]
[359] ibid. This is also reflected in the manual's inauguration speech by the then Foreign Affairs Minister Koenders of the Netherlands at the Hague and the Estonian President Toomas Hendrik Ilves, 13 February 2017:
[360] Hayden Michael V., *Playing to the Edge : American Intelligence in the Age of Terror.* (Penguin Books 2016).

accepted as falling under international law.[361] In other words, if certain practices are deemed to be in accordance with the international law of war, for example, they can be deemed legal and permissible.[362] Thus, anyone conducting operations outside these rules, will be transgressing.

While the Tallinn project, may not readily be seen as officially writing the 'rule-book' for cyber governance, it seems to attempt controlling subjectivities through its proposals, which are not particularly welcomed by everyone. Russia's view of the project as a demonstration of Western hegemonic effort, designed to promote US and Western agenda, is one of such disapprovals.[363] Western powers, on the other hand, see such disapproval as a reflection of such states' intention to disregard international law, fuelling further the historic antagonism that exist between both sides, and which continues to be reinforced by issues of cyberspace governance.[364] Thus, cybersecurity practices and operations are produced and legitimised "through these discursive moves and reproduced via further mediations and wider political discourses".[365] And the productive power exhibited through such practices allows for the production of rules or norms around cyberspace governance while reifying power positions in cyberspace.

Authors like Joshua Rovner and Tyler Moore, while examining the relevance of the hegemonic stability theory, contemplates whether the internet

[361] Stevens (n 261).

[362] ibid.

[363] Efrony and Shany (n 355).

[364] ibid.

[365] Stevens (n 261).[10]

or cyberspace need a hegemon in the form of the US.[366] Suffice it to say, that the US is, and has been from the inception of the internet, the unquestionable leader in information and technological development at state participation level. A position that is thus far, almost sustained and secured, given its powerful economic position and strong military stake in cyberspace, also at the level of state participation. Additionally, it has the support of other Western nations, through NATO more broadly , and through its alliance with the Five Eye network (including the UK, Canada, Australia and New Zealand). Thus, structural power is wielded by their collective force to control cyberspace governance.

For Barnett and Duvall, structural power is "the co-constitutive, internal relations of structural positions that define what kinds of social beings' actors are".[367] In other words, "a direct constitutive relation such that the structural position, A, exists only by virtue of its relation to structural position, B."[368] This suggests that the social positions of any given actor in the global power structure impacts their social relational capacities, subjectivities, interests and capabilities, which may result in advantages for some and disadvantages for others.[369]

While the Westphalian structural system, based on the notion of the state as the key authority over population and territory, is relevant for our understanding of global governance more broadly, specific relevance to cyberspace governance and the position of developing states within the global

[366] Joshua Rovner and Tyler Moore, 'Does the Internet Need a Hegemon?' (2017) 2 Journal of Global Security Studies 184.
[367] Barnett and others (n 352). [53]
[368] ibid.[53]
[369] ibid.

power structure, is better understood through the lens of the World System theory, with its notion of the core, periphery and semi-periphery.[370] As with the notion of institutional power described above, structural power is concerned with where power is found rather than what the impacts are. This is because, it "operates as the constitutive relations of a direct and specific, hence, mutually constituting kind."[371]

Distinguishing between the two categories of power may pose a challenge, as the relations between one and the other is evident in both. However, when both forms of power are considered in the case of cybersecurity capacity building programs for developing states, the power exercised by the one providing capacity development assistance, over the one receiving the support, can be said to be structural. This is because, they constitute each other's position directly within a given discursive environment (cyberspace). However, the power can also be institutional, as one (the provider, for example) could constrain, directly or otherwise (e.g., through rules and norms setting for internet connectivity, naming conventions, or norms governing the otherwise complex technology infrastructure and systems) through their position in the World System. And as suggested above, the Western alliance, with the US at the helm, possess structural power as dominant producers and consumers of cyber resources, research, and innovations. Thus, they can control what is allowed and prohibited through their interests and disinterests respectively. This in turn, is

[370] ibid. see also Immanuel Wallerstein, 'The Inter-State Structure of the Modern World-System' in Steve Smith, Ken Booth and Marysia Zalewski (eds), *International theory: Positivism and Beyond* (10th edn, Cambridge University Press 2008).
[371] Barnett and others (n 352).[48]

usually determined by the market, which is also dominated and controlled by the same group of entities.

In the case of compulsory power, a definite control exists, of one over the other.[372] This reflects direct control of A, the wielder of power, over B, the object for whom control is directed.[373] For Barnett and Duvall, this form of power is best observed through the lens of A as opposed to B, and exercised in relations that can be both material, symbolic and normative.[374] A, can be any actor in the relation, whether state or non-state, the giver or the receiver of support, international institutions, and even armed militias.[375] Concurring with Robert Dahl's earlier conceptualisation of this form of power at its purest, Barnett and Duvall wrote, of Dahl:

> For him, power is best understood as the ability of A to get B to do what B otherwise would not do. Dahl's concept has three defining features. One, there is intentionality on the part of Actor A. What counts is that A wants B to alter its actions in a particular direction. If B alters its actions under the mistaken impression that A wants it to, then that would not count as power because it was not A's intent that B do so. Two, there must be a conflict of desires, to the extent that B now feels compelled to alter its behavior. A and B want different outcomes, and B loses. Three, A is successful because it has material and ideational resources at its disposal that lead B to alter its actions. Although theorists have debated whether the relevant resources are an intrinsic property of actors or are better understood as part of a relationship of dependence between two or more actors, the underlying claim is that identifiable resources that are controlled and intentionally deployed by actors are what counts for thinking about power.[376]

[372] ibid.
[373] ibid.
[374] ibid.
[375] ibid.
[376] ibid.[49]

While the relevance of Dahl's formulation is acknowledged, Barnett and Duvall argues that their taxonomy, as expressed above, does not necessarily require intentionality for compulsory power to be present. Rather, "compulsory power, is present whenever A's actions control B's actions or circumstances, even if unintentionally."[377] Thus, power exist even when A is unaware of the unintended consequences produced by their action towards B. Hence, "compulsory power is best understood from the perspective of the recipient, not the deliverer of the direct action",[378] since power produces effects, and such effects will be best represented or observed through B.[379]

A possible drawback in Barnett and Duvall' s argument could be in the compulsive nature of this form of power, which suggests a lack of, or a removal of, any real choice from the object B. The reduction of B to nothing else but that which does what A desires may, at first observation, seem impossible, especially in a global society of independent sovereign states. One expects actors to retain some level of agency, even in circumstances of forceful subjugation such as war. However, in such situations, while the choice to resist or surrender may be the only options available to B, it is equally arguable that B's choice remains ultimately influenced by what A is demanding, whether B's choice complies or in defiance of what A wants. Perhaps further breakdown of the different components of Barnett and Duvall's compulsory power would benefit from more analytical traction further in the thesis when discussed against the cases.

[377] ibid.[50]
[378] ibid.[50]
[379] ibid.

Crucial to this review is the manifestation of compulsory power in actions and intentions of cybersecurity practices of the Western alliance and, perhaps those of China and Russia as well, which prevent or allow the coordination and the formation of a global regulatory or prohibition regime for cyberspace. Noticeably, the issue of state sovereignty is swiftly evoked when considering such discussions. Sovereignty is often perceived as a key attribute, and one of great contestation on issues of global governance generally, particularly on questions of global information and cyberspace governance. This is because, the need for such global coordination stirs up considerations of how much sovereignty a state would be willing to give up, against whatever benefit may lay ahead.[380] Here, we often see contestations of powers playing out, typically between rival superpowers. For example, China and Russia, opposing the European Convention on Cybercrime, over concerns that such transnational coordination to police the internet, would mean a forfeiture of their domestic sovereignty, and jeopardise their own national security in ways they are not prepared to accept.[381]

Indeed, power struggles between rival superpowers usually suggest shifts in power politics. By virtue of their own capacity and capabilities, which grants them new position in the geopolitical relation, emerging superpowers like China and Russia now have increased productive and institutional powers of

[380] Jinghan Zeng, Tim Stevens and Yaru Chen, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"' (2017) 45 Politics and Policy.
[381] 'Cyberpower and National Security' (2013) 35 American Foreign Policy Interests 45.; Joseph Nye, 'How Will New Cybersecurity Norms Develop?' [2018] Project Syndicate.; Mueller (n 237).; Karen Renaud and others, 'Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China' (2020) 80 Public administration review 577.

their own. This in turn, strengthens their compulsory power. Albeit mostly at domestic and regional levels, it also afford them a wider choice at global level. An example that speaks to this situation is their opposition to the Tallinn Process as already discussed. But it does so in a number of other ways.[382]

For Murphy and Kellow, the US and its Western alliance's efforts, through the CCD COE Tallinn process, seek to protect their freedom and access to foreign networks and territories within the international framework, through norms promotion.[383] As such, they are usually unsupportive of any calls for an international treaty, and would rather have the application of existing international law to control cyber operations. China and Russia on the other hand, seek otherwise. Rather, they seek a redrawn treaty that would not violate their sovereignty and also allow them freedom to act domestically, at the least.[384]

3.6 Conclusion

This chapter sets the theoretical, and to some extent, a genealogical background to the research. This is done to allow for a better examination of the research question and provide useful understanding of the analysis that will follow. The role of powerful state actors in global cyber governance through cybersecurity practices, remains a key focus of the study, particularly in relation to less powerful global actors. Thus, the state is central amongst these actors because, as Myriam Dunn Cavelty & Andreas Wenger pointed out, "security

[382] Hannah Murphy and Aynsley Kellow, 'Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Arenas' (2013) 4 Global Policy 139.
[383] ibid.
[384] Zeng, Stevens and Chen (n 380).

politics is inevitably tied to questions of authority and power".[385] While the state is arguably not the only important actor in the space, this focus is nonetheless relevant as "it is at the intersection between state and non-state actors, nationally and internationally, that the specificities of cybersecurity politics emerge."[386]

Cyber technologies, when conceptualised as a form of institutional power, equip those states (with the dominant cyber technologies) with the capability to allow or prevent solutions to the problems of cybersecurity. These are decisions that could be hinged on self-interest or agenda. Such states also, through their existing position in the World System, and the desire to defend that position, will remain keen on developing cybersecurity technologies to project compulsory power, particularly in the form of offensive-defence strategies. Thus, their technological influence, capacity and capabilities in the space afford them structural power.

Expressed willingness by powerful states to unleash offensive strategies in their cybersecurity efforts when necessary, creates contestations and are met with opposition from rival powers, which according to Tim Maurer, makes agreeing to global norms on cyber operations difficult.[387] Hence, we see, for example, the Chinese and Russian opposition to the Tallinn project, based on their perception of its product (The Manual), as an integral part of Western

[385] Dunn Cavelty and Wenger (n 329).[6]
[386] ibid.
[387] Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2019) 12 Hague Journal on the Rule of Law 283; Hannes Ebert and Tim Maurer, 'Contested Cyberspace and Rising Powers' (2013) 34 Third World Quarterly 1054.

productive power. To them, the manual promotes the American-Western dominance in cyberspace.[388]

Crucially, none of these powers are currently concentrated in the hands of a single state. The hegemonic position and ambition of the Western alliance is challenged today by other rising powers who appear to be developing and strengthening their own alliances, creating and promoting their own norms.[389] Thus, they pose a continued threat to the current and future global power structure. As they develop competitive capacity and capability, they will undoubtedly seek to play the power game, and contribute to how governance in cyberspace is shaped.

For the less powerful states with neither capacity or capabilities of their own to compete or reject the power being wielded by the powerful in cyberspace, what does this mean? If capacity and capability translates into power, can the capacity building support by Western states, be genuinely aimed at empowering those recipients? Why might it be in the interest of the great powers, or even the rising powers, to empower them? Would it not seem contradictory to such declaration, to “achieve and Maintain Cyberspace Superiority”, [390]often expressed by the powerful states?

Understandably, the interdependence nature of the internet suggests the need to have less (or zero) weak links, to allow for stronger collaborative efforts

[388] Maurer (n 387).
[389] Zeng, Stevens and Chen (n 380); Maurer (n 387).
[390] See for example, US Cyber Command (n 345). And, Government of the United Kingdom (n 13).

between states in the global cybersecurity campaign. However, if upon being empowered, the weaker states become equally powerful, would they not seek to wield their own power, and offer more resistance to future proposals that they deem unfavourable? These questions will play on one's mind throughout the rest of this study as the research findings are discussed, analysed, and contemplate.

4 Methodology: Design, method and materials

4.1 Introduction

The methodological approach adopted by this study is presented in this chapter. It explains the rationale for the research design and the analytical method adopted. It documents the strategy deployed to track the relations of power within the case data, to provide insight into how power works and is wielded. It outlines the Foucauldian frameworks upon which this strategy is based and how it is deployed to answer the research questions.

The subsequent sections of this chapter are intended to serve the following purpose: 1) to provide details of how Foucault's analytics are used in creating a framework to delineate the object and scope of the empirical analysis. 2) To introduce how the analytical method is developed based on this framework. 3), To explain and highlight the criteria used in the selections of the empirical material, with notes on how primary and secondary sources are engaged in the study.

4.2 Defining the object and scope of study

In satisfying the first objective above, an explanation of how Foucault's notion of problematisation is applied to the data analysis is provided. Problematisation, based on a Foucauldian understanding, sees problems and solutions as both sides of the same argument.[391] Thus, the object of analysis is neither the problem nor the solutions offered to solve the problems. Rather, it is the problematisation logic itself, which allows for a confluence of both the problem and solution that forms the object of analysis. And, alongside this, is the (social economic, and political) conditions that made that relationship possible in the first place. [392]

Similarly, the object of analysis of this study is neither the problems of cybersecurity, nor the practices emerging from actions directed at solving the problems per se. Rather, it is the process of establishing it as a going concern. That is, the process of normalising it as a problem that needs solving. Thus, the study's focus is on the interplay between this problematising process and the social, economic, and political conditions which then results in the production of certain power dynamics. This is not aimed at trivialising the actual difficulties or problems that gave rise to problematisations in the first place. Neither is it suggested that the 'realities' of the situation, (the insecurity of digital technologies and threats) are not entirely pertinent to the analysis. Rather, the focus is on how such situations are represented, presented, and the nature of the

[391] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).
[392] ibid.

responses. Put differently, it is concerned with the question of what mechanisms and techniques are deployed in the problematising process and how they are presented, represented, and made visible, such that a 'problem' case or space can emerge, leading to actions that produces or reproduces certain power relations.[393] Therefore, key to analysing problematisation is that the object of interrogation cannot be situated in the 'problem' itself or in the 'actions' designed to provide solutions or responses to the problem. Rather, the object of analysis resides in the resulting relationship between the problem phenomenon (cybersecurity or insecurity) and the political response (capacity building, training, awareness campaigns, and regulations) to it.[394]

Consequently, the strategy/methodology disposed to analysing cybersecurity problematisation cannot be one that seeks to provide answers to the question of how the problems of cybersecurity are solved, or which approach works best in addressing the issues of insecurity in cyberspace, or how best to regulate the internet. Rather, the strategy positions the notion of cybersecurity at the core of a myriad of conflicting elements to create an understanding of why a cybersecurity problem emerges, why is it problematised in a certain way and at a certain point in time?[395] This sort of interrogation allows a deeper exploration of the notions of cybersecurity beyond what it is represented to be.[396] It allows one to reveal how certain discursive construction of insecurity, threats and risk in

[393] Foucault, 'Security , Territory , Population. Lectures at the Collège de France' (n 48).
[394] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41); Foucault, 'Security , Territory , Population. Lectures at the Collège de France' (n 48).
[395] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).[141]
[396] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).

cyberspace are problematised such that , it enables the production of certain knowledge, political and legal actions and norms, to be constituted and promoted (globally) as 'truth'. One ought to ask therefore: what problems are such actions 'actually' designed to solve? What question, for example, is the global cybersecurity ambitions of the so-called First World states like the UK (through their cybersecurity capacity building efforts in developing countries like Ghana, Botswana and Trinidad and Tobago), designed to answer?

To this end, the research, becomes less about deconstructing what cybersecurity means (in technical, security or legal terms) or what constitutes a robust response to security threats in cyberspace, or how certain states' cybersecurity capabilities are measured, or what the ideal legal framework around it should be. Instead, it becomes more about how the different constitutive elements are engineered in a concerted effort (consciously and/or otherwise) to form the object 'problem'; while simultaneously observing the role these various elements play in the analysed data.

As such, analytical attention is focused not only on how cybersecurity concerns, and actions taken to address those concerns are presented, but also, on the implications of the specific ways these perspectives and actions are organised or orchestrated. For example, how are global subjects or states categorised, grouped, or classified as capable individuals or states or entities that are considered not-there-yet, strong or weak links in the global cybersecurity ratings? Who determines who/what constitutes a hostile state or acceptable behaviour in cyberspace? And what impacts are produced from such classifications and the actionable practices emerging from them?

In analysing such classifications and thoughts, the role of adjudicating between solutions, invariably falls outside the scope of problematisation analytics.[397] Instead, the analysis elucidates the "form of [cybersecurity] problematisation",[398] from whence multiple and sometimes diverging solution-provisions are presented, and how they respond, to further sustain cybersecurity problematisation.[399]

Thus, the object and scope of interrogation of this study can be said to be rooted in "the field of the work of thought",[400] as expressed by Foucault, which means that the object and scope is confined to the analysis of how power works in creating certain perspectives, that enable actions in response to certain problem phenomenon, to create an assemblage of problems and measures to deal with those problems. Consequently, it allows for a continued reproduction of certain power relations and structures.[401] Thus, this research analysis is grounded on the hypothesis that the current trends and practices around cybersecurity or insecurities in cyberspace, signal renewed strategies of how difficult situations are handled in the 'actual' sense. That is, renewed assemblages of heterogenous elements of structures, established throughout history, to produce a modern basis of power.[402] On this basis, the study sets out to

[397] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).[118]

[398] Michel Foucault, *The Essential Foucault* (Paul Rabinow and Nikolas Rose eds, The New Press 2003).; Colin Koopman. Two uses of genealogy: [2009] Michel Foucault and Bernard Williams. In C.G Prado (Ed.). Foucault's legacy.[2009] Bloomsbury Publishing

[399] Ibid

[400] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).

[401] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).

[402] Michel Foucault, *The Birth of Biopolitics: Lectures at the College de France 1978 - 1979* (2008).

understand how this assemblage is manifested within cybersecurity discourses found in governmental thoughts (typically expressed and implied through official documents, speeches, organisational culture, regulations, and laws), and how certain power relations and outcomes are promoted as a result.

What brings this analysis in line with Foucault's genealogy is that it attempts to create an understanding of the present through a loop back to the past,[403] particularly with regards to the historical and traditional role of legal frameworks in shaping desired social fabrics, legal entities, and sovereignties. As with Foucault, this historical reflection is not designed to locate the origin of cybersecurity problems or the origin of geopolitical struggles, whether through legal imperialism or legal transplant from North to South.[404] It is, historical nonetheless to a certain degree. It attempts to track how certain issues of insecurity have always been seen and presented as problems, and how the resulting solutions are produced and made intelligible in accordance with each genealogical moment in time. This sort of historical construction allows one to unlock new possibilities for understanding the present thoughts and actions.[405] Thus, the approach allows one to analyse the present cybersecurity problem as part of an on-going security concern. It further aids the analysis of presented

[403] Rabinow (n 44). [78 and 88]

[404] Michel Foucault and Sylvère Lotringer, 'Foucault Live: Collected Interviews, 1961–1984' [1996] New York: Semiotext (e).[141-142]

[405] Colin Koopman, 'Genealogical Pragmatism: Problematization and Reconstruction' [2011] SSRN Electronic Journal.

solutions to the problem and their constitutive impacts through a sort of a "history of the present".[406.]

4.3 Analysing problematisation

Instrumentalising Foucault's problematisation as object and scope of analysis allows for several options. First there is the approach of analysing the relationship between problems and solutions, which examines types of problem representations that may be at play.[407] Then there is the analytics of power which features such themes or concepts as the juridical model of power, law and sovereignty, biopolitics, bio-power, power and knowledge, and genealogy as a history of the present.[408] Foucault uses these concepts to historically trace the development of new mechanisms or technologies of power; from what he termed the "juridico-discursive" model,[409] which signals the connection to law in his earlier conception of power, as that which is strictly prohibitive and negative,[410] and whose primary goal is to dominate, to the kinds of power which "operate outside the sphere of sovereignty and are 'irreducible to the representation of law'". [411] These are all ways by which empirical investigations and problematisation can be approached through Foucault's work.[412] They are utilised within this study at different points of the discussion and to varying

[406] Rabinow (n 44).[88]
[407] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).
[408] ibid.
[409] Michel Foucault, *The History of Sexuality Volume I, The Will to Knowledge*, vol I (First Amer, Pantheon Books 1978). [82] see also, Hugh Baxter, 'Bringing Foucault into Law and Law into Foucault' (1996) 48 Stanford Law Review 449.
[410] Baxter (n 409).
[411] ibid.[453]
[412] Michel Foucault, 'Discipline & Punish' [1977] Discipline & Punish: The Birth of the Prison; Paul Rabinow, *The Foucault Reader* (1984).

degrees, to support the main governmentality concept. This is similar to how Foucault uses these concepts within his own work.

According to Bacchi, investigating problematisations through empirical data, as with any form of research investigation, suggests a specific focus.[413] This focus is then made possible by a strategic delineation of data sources at the design stage. The criteria for such delineation are driven by how well they can help achieve the research goal. Hence, the study focuses, first, on specific governments and practices. And in this case, the United Kingdom (as a representation of developed states) global cybersecurity ambitions, and actions directed towards developing Commonwealth states (represented by Botswana, Ghana, and Trinidad). Second, it focuses on specific relationships, collaborations, partnerships, and interventions that emerge from such practices to interrogate specific claims to knowledge or truth. In doing so, the goal is to understand varying perspectives (from both sides) to grasp the perpetration of the different claims and their acceptability or contestability as truth. A third criterion rests on the process of governing, and the role law plays through norms development and creation of legal frameworks. Thus, it examines how paradigms of power are arranged, legitimised, and justified through normative claims by the various actors.[414]

[413] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).
[414] M Foucault and S Rabinow, 'Polemics, Politics and Problematizations BT - Essential Works of Foucault', *Essential Works of Foucault* (1997). See also, Nikolas Rose, *Powers of Freedom: Reframing Political Thought* (Cambridge University Press 1999).

With the scope and object of analysis explained, and the main delimitations highlighted, the research strategies are introduced below to explain the method, and how the materials are selected. A non-exhaustive list of materials used is included in the appendix, along with the ethics committee approval for the data collection.

4.4 Employing Carol Bacchi's approach to policy analysis

The choice of Bacchi's approach to policy analysis is justifiable for two main reasons: 1) It is Foucauldian and 2), it is readily adaptable for use within critical socio-legal/socio-political research. This is because Bacchi's approach deconstructs and critiques social 'problems' in context, allowing attention to discourses that frame certain social, legal, or political possibilities at an everyday level. And because it is Foucauldian, it is grounded in poststructuralist theory and discourse analysis, while drawing on the works of other governmentality scholars.

For Bacchi, as with Foucault, problems are not given, but rather are social constructions, challenging claims that presuppose that governmental actions emerge in response to pre-existing problems.[415] Instead, governments are seen as active players in the creation or production of these 'problems'.[416] Seeing governments and their actions in this light, therefore, allows for a shift in

[415] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).
[416] ibid.

focus, away from analysis that is geared towards a problem-solving discourse, to those that focus on problem questioning instead.[417]

Expanding on Foucault's notion of practical or prescriptive texts functioning as a point of departure for identifying problematisations, Bacchi developed her approach to policy analysis against a similar backdrop.[418] For Bacchi, policy texts, for example, provide an ideal source of empirical material because every policy document, report, proposal, and speech, contains its diagnosis of the problem, either explicitly or implicitly.[419] This means that, every such text is potentially prescriptive in nature, because it focuses first, on highlighting the problem, then determines why the problem exists, and finally, lays out solutions. And in doing so, government through such data, suggests a practice that depends on specific problematisations.[420]

Thus, Bacchi recommends 'the task of "identify[ing] deep conceptual premises operating within problem representations" within such textual analysis.[421] This is achieved through first, an identification of the concern (for example, threats of cyber-attack, poor state preparedness, or lack of capability to ward-off attacks). And second, noting what is presented or represented as the 'why' of the problem (such as lack of technical capacity or poor security habits in

[417] ibid.

[418] ibid. see also Bacchi, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (n 5).

[419] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).[1]

[420] ibid.

[421] ibid.[xix]

cyberspace and the role of economic status), which are very often documented in these texts.[422]

With regards to the 'why', analysing what is presupposed means that, such presumptions can often be lifted directly from available official documents. Thus, these documents (policy and strategy documents, and guidelines) often provide a map of what is considered problematic, and usually with prescribed solutions to deal with the problem.[423] However, other data sources are used, complementarily, to grant brevity to both genealogical and spatial context within the data, and to locate the underlying assumptions and knowledge claims that sustain the presumptions about what the problem is represented to be.[424] Hence, materials such as interviews, texts from conference presentations, and speeches are also utilised in this analysis.

On the problem-questioning approach, (of asking, for example, what is the problem represented to be?) Bacchi devised a strategy based on six questions, designed to organise and interrogate a given policy text or data, or any other institutional release, as they often require their audience to apply them based on individual problem representations. This makes the approach rigorous as it demands a level of reflexivity that considers the fact that, "we are immersed in the conceptual logic of our era",[425] and demands that one equally treats one's

[422] ibid.

[423] Carol Bacchi, 'Problematizations in Health Policy: Questioning How "Problems" Are Constituted in Policies' [2016] SAGE Open.[8]

[424] ibid.

[425] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10). [19]

own ideas and assumptions as problem representations whose origin also needs to be reflected upon.[426]

Below are the set of analytical questions recommended by Bacchi which, for simplicity, will be referred to hereinafter as 'question one', 'question two', etc. or 'first question', 'second question', and so on.

1. What is the problem represented to be in a specific policy?
2. What presuppositions or assumptions underlie this representation of the problem?
3. How has this representation of the problem come about?
4. What is left unproblematic in this problem representation? Where are the silences? Can the problem be thought about differently?
5. What effects are produced by this representation of the problem?
6. How/where has this representation of the problem been produced, disseminated, and defended? How could it be questioned, disrupted, and replaced?[427]

This approach provides a useful guide for targeting the problem representation, diagnosis and action within the cybersecurity practices. Thus, it provides structural support for the analysis of the data, organising and concretising the analytical logic while reducing the risk of oversimplification.

[426] ibid.
[427] ibid.[2]

4.5 Interrogating the Operation of Power

To track the relations of power and their impacts, Bacchi's approach is fused with Mitchel Dean's power effect classification.[428] Dean's concept, allows for an understanding of how power works and how it is wielded, particularly in the context of governing, and its effect on individuals, states and institutions, This helps to unravel how political thoughts and perspectives work, and how they operate to create problematised fields.[429] And because this research seek to track relations of power within these problematised fields, Dean's power classification is systematically used to present the findings.

Dean's approach provides a structural way of categorising and tracking power effects using three main elements: First, a truth effect of how a problem is presented and made visible, making the acceptance of what might be otherwise contested appear necessary and vital.[430] Such problems representations are often found, in reports with claims to facts. Statistical data on the daily number of cyber intrusions detected, or data showing widening technology gaps between the developed and developing states is an example of such data. It enables the visibility and legitimisation of the problem as real, creating justifications for government actions, reforms, norms, and rules.[431]

[428] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).
[429] ibid.
[430] ibid. Michel Foucault, 'Omnes et Singulatim: TowardsTowards a Criticism of "political Reason""', *Tanner Lectures on Human Values on Human Values* (The University of Utah 1979).
[431] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).

Second, there is the norm effect.[432] According to Dean, the norm effect follows a sort of urgency once the problem has been established by the truth effect. The function of the norm effect, therefore, is to diagnose the problem and produce blueprints to address it, through specific actions (such as regulations, laws, and capacity development programmes), with the potential to obscure alternative perspectives on the problem.[433] Thus, the norm effect acts as a codifying agent that seals the authoritative assertions of the truth effect, while at the same time concretising such authoritative claims into "normative judgements".[434]

The role that the norm effect plays in the relationship between freedom and dominance causes the third element (power effect) to emerge. This happens when norm is modulated as creating individual freedom. Thus, the power effect serves as a means of execution or solving the problem, [435] enforcing what must be allowed or disallowed, prescribing who or what should be criminalised or made legal - who should adopt certain principles, norms or strategies and for what purpose. As such, the power effect determines whose behaviour ought to be changed or adapted and to what. Which state falls short of the level of preparedness required to meet certain global cybersecurity standards, such that those who are not 'quite there yet' can reach a position of having individual development and freedom.[436]

[432] ibid.
[433] ibid.
[434] ibid. [89]
[435] ibid.
[436] ibid.

The power effect enables the identification of those states that fall within or outside what is considered the norm; who should be allowed into the rule-based global system and who should be sanctioned, when and for what reason. For Dean, through the identification and establishment of the norm and those perceived as outsiders, either by their own shortcomings or sanctions, a "loop back to relations of power" can be followed to ask, in what contexts, when, how, and for whom does the issue of obligation come before freedom?[437]

Dean's process is Foucauldian, based on the idea laid out by Rose and Miller, [438]which suggests that the "problematising activity", [439] of governments, can be found in the specific ways that they operate.[440] Governments, in liberal states, function under this tension that exist between freedom, obligations, coercion, and the ways government within that tension becomes intelligible.[441]Thus, the analysis needs to direct attention to how this tension is designed to work in certain contexts, to fully understand the function of government, and the impacts of their actions.

Dean carried out his analysis of such tension to identify a state of exception applied to behaviours and people that are deemed 'outside' the norm (outside of our moral, social and political existence).[442] A divide emerges in the relationship between what represents the norm and what is the exception to the

[437] ibid. [90]
[438] Rose and Miller (n 23).
[439] ibid. [181]
[440] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11); Rabinow (n 44); Peter Miller and Nikolas Rose, *Governing the Present. Administering Economic, Social and Personal Life* (Nikolas Rose and Peter Miller eds, Polity Press 2008).
[441] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).
[442] ibid.

norm.[443] In other words, who are the 'bad guys' and 'good guys' within the cybersecurity discourse? What or who constitutes a hostile or friendly state? Who decides and sets these labels? For Dean, 'government of problems' is exercised through this relationship which subsequently allows for the visibility of 'the problem' and, ultimately, leads to its diagnosis, and solution recommendations.[444] Thus, the research data is analysed against these effects to reveal the relation and operation of power that exists between states within the cybersecurity discourse.

4.6 Deploying the Genealogy-Inspired Approach to Analysis

Having explained the framework behind the analysis, which has been intentionally detailed, attention is now directed to how the method is directly applied to the research data.

Methodical application of the analytical tools is used in the process of reading, listening, transcribing, thinking and reflecting on the content within the data collected. They are examined with a strategic lens, subjecting the data to a sort of critical or "sceptical reading",[445] as observed by Jerry Gill.[446] That lens is grounded on the assumption that does not see global cybersecurity (within its geopolitical context in particular), as the object of analysis, but rather as an invention of specific perspectives and events, created as an object of political

[443] ibid.
[444] ibid.
[445] Jerry H Gill, *The Tacit Mode: Michael Polanyi's Postmodern Philosophy* (State University of New York Press 2000).
[446] ibid.

control.[447] This means that the resulting problematisation from that process, as opposed to the idea of cybersecurity as a security concern, is what this study sets out to investigate.

Utilizing both Dean and Bacchi's approach, therefore, allows for a demonstration of how a problem phenomenon such as cybersecurity comes to actualise a "visible analytical and permanent reality",[448] while unravelling the technologies of power at play in the framing of discourses around the issue and the legitimacy of the solutions that are ultimately offered. To achieve this, the analysis starts with a logic of codification, like those shared by other practices of critical policy analysis.[449] This involves breaking down large texts into smaller manageable parts. They are subsequently examined and grouped based on the role they perform or their perceived themes within the data. This makes it possible to carry out the analytical process in phases, allowing for the reading and comprehension of the data, as well as enabling the data to be efficiently conceptualised, synthesised and theorised in effective sequences.[450] (See also, Morse.[451])

Before data could be arranged in any structured manner, initial scheming is done and data are grouped into their respective categories based on their perceived role in the overall scheme of things. For example, while the data

[447] Foucault and Rabinow (n 39).

[448] M Foucault, *The History of Sexuality: An Introduction Vol. 1* (1978).[44]

[449] Frank Fischer, Gerald J Miller and Mara S Sidney, 'Handbook of Public Policy Analysis : Theory, Politics, and Methods' [2007] Methods.

[450] Richard H Hycner, 'Some Guidelines for the Phenomenological Analysis of Interview Data' [1985] Human Studies.

[451] JM Morse, 'Emerging from the Data: The Cognitive Processes of Analysis in Qualitative Inquiry'.

collected where classified into top level categories like, developed economies/UK/EU/US and developing Commonwealth States/Ghana/Botswana/Trinidad and Tobago, further subclassification is performed using questions such as; do they provide insight into the visibility of the problem? Is there a problem description or framing evident within the data? How is the problem diagnosed? Is a problem-solving discourse present? What solution to the problem is being offered, recommended, proposed, or instructed? Thus, a list of codes (e.g. problem visibility, threat analysis, problem normalisation and rationalisation, digital divide, security risk) is generated to record data that fit into the various categories and sub-categories.

Separating data in this way works as a form of meta-tagging that can include multiple categories, or position one piece of data within multiple categories, while also serving to provide a picture of various attributes within the data. While some pieces of data may perform more than one role within the overall scheme, each could be separated according to the function that appears to be most dominant.

This approach of breaking down data and categorising them according to their function is borrowed from Dean as opposed to Bacchi, because it became apparent during the process that most of the data followed a pattern which fits well with the format used by Dean.[452] This is because authoritative data in the form of government policies, proposals, strategy documents, and data from structured interviews, often present key points about the facts as a preamble to

[452] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).

what is to come. Bacchi's on the other hand proposes that the analysis starts from a focus on what is proposed as a solution to the problem, such as "identifying how funds are targeted within a proposal", as a way of "identifying dominant problem representation".[453]

These preambles could be in the form of numbers or references to current or past events, claims of impending crisis, backed by proof of investigation, or security interceptions made. Detailed description of the identified situation will usually follow the preamble, to ensure that, proper understanding or severity of the situation is grasped by the reader before any recommendations are introduced. Thus, breaking down a large text into this format proved useful in coding the data based on the truth, norm, or power effects they present.

In dealing with both primary and secondary data from the main case study, sections of the data with descriptive and statistical elements are grouped under the visibility main code (e.g., problem visibility). This is done to highlight the going concern of cybersecurity, or the challenges and perceived reality of the problem are presented or represented. Sub-tagging is then undertaken under the top-level codes, using labels that are reflective of the text: such as perspectives (e.g. the legal, political, or sociological), evidence-based presentation, argumentative description, epistemic claim, statistical claim, and scientific claim. This process is then repeated with the norm and power effects.

[453] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10). [4]

Once the tagging process is complete, they are run against the data to see how their functions within the larger text are made instrumental. To give an example, if the problem or situation is made visible through an evidence-based presentation of the problem (the use of statistical data to highlight the level of internet penetration, data on unprotected computers, frequency of cyber attacks, number of cyber frauds, etc.), what role did such evidence play throughout that data? How are they used? Do they form part of a broad or narrow description of the problem? How are such data linked to solutions proposed?

Thus, descriptive categories appearing to serve the purpose of highlighting the problem (such as the repeat use of threat discourses) within the data, are considered most pertinent in establishing the practices of visibility. In the case of data from the UK and the three Commonwealth states, for example, various forms of perspectives, argumentative descriptions and epistemic claims are identified as the main visibility strategy deployed. Thus, they emerge as the key visibility categories for such data.

A similar strategy of identification and classification based on predefined roles, or meta-function, is applied to all the three functions –(visibility, diagnosis and action or means of acting). Following the example above, each section of text is itemised, summarised, and linked against other parts of the data to compare and confirm their contributory function within the overall data.

Once data is broken down according to their role and their categories established, they are subjected to further reading to break down the text within each meta category. During this process, meta-themes between key rationalities that are used to produce cybersecurity facts and knowledge claims such as interconnectivity, global phenomenon, prevention, and risk became apparent. The capacity of the themes to link across the roles also becomes evident. Thus, a web of relations between categories can be created. For example, a category of evidence-based data may have a direct link to a diagnosis function while adding visibility and action at the same time. As an example, data pointing to facts about cybersecurity, such as information on breaches or attacks that occurred or were blocked, can serve to allow visibility and provide a reality discourse of the threat. Simultaneously, it can aid the problem diagnosis (by providing risk identification discourse) with the aim of providing or recommending possible solutions.

This meta-thematic classification therefore becomes a key analytical instrument for understanding the relations between the categories as it allows for deeper understanding, abstraction and theorisation of the various elements encountered in the data. Thus, as data is broken down and analysed further, meta themes around rationalities, discourses, and techniques emerge. This in turn allowed for deeper classifications along those lines to reveal perspectives, designed to be explored by Bacchi's range of questions. And finally, it provides more distilled research evidence which will be discussed in detail within the sections focused on the research findings.

Because data was sourced across different geographical regions with varied social, economic, cultural, and political structures, some comparative analysis was necessary. This is to determine how the conceptual assumptions around cybersecurity practices and the technologies of power are explored within the sites. As such, the focal categories within the data, along with their identified meta themes, are deployed to explain the commonalities and differences within the relationships between the developed and the less resourced states; Both in relation to the role each play and their individual perception of their own agency (political, social, legal, or otherwise).

Noteworthy here is the usefulness of Bacchi's fifth question ("what effects are produced by this representation of the problem",[454]) in determining the impacts of such subject construction and how this aids the normalisation process within the different perspectives on both sides (North and South). Thus, the analysis contains a necessary comparison, albeit minimal, to avoid subjecting the data to a simple summative process where everything is seen from the standpoint of a single process.

4.7 Empirical materials and data sources

The research data are broadly, primary and secondary. The primary data collection commenced following approval of the survey questions from the Lancaster University Research Ethics Committee in 2019 (see appendix). The data are mainly from interviews carried out with some officials from government agencies in the UK, Ghana, Botswana, and Trinidad and Tobago. It includes an interview with a prominent advisor within the CCI team at the Commonwealth secretariat in London and a telephone interview with the then Director General of Ghana's Cyber Security Authority. Further interviews were obtained from participants who were identified through a snowballing process. This resulted in

[454] ibid. [2]

interviews with state and non-state officials, both from within and outside of the original target countries (such as Canada, Nigeria, and Singapore), to allow for a broader insight into the study.

Participants were also observed, through conversations and interactions at a three-day CyberUK conference, held in Glasgow in 2019.[455] Some snowballing data collection also allowed for interviews with event participants that were deemed useful for the research. Specifically, delegates from the Botswana Ministry of Transport and Communications, and the country's Cybersecurity project team were engaged, and subsequently provided a group response to the interview questions.

The secondary data comes from authoritative government sources as well as from private and non-government sources such as the NCSC, the CCI, the Commonwealth Secretariat, the Commonwealth Telecommunication Organisation, The African Union, the ITU, ENISA, Council of Europe and many more (a non-exhaustive list is provided as an appendix).

The secondary data serves the purpose of conceptualising the primary data as well as aiding the main analysis process. This proved particularly useful as direct collection through interviews was difficult in most of the cases, with many of the intended interviewees either declining the offer of interview or referring an alternative individual with whom interview schedule or response

[455] National Cyber Security Centre, 'CYBERUK 2019 Gallery - NCSC.GOV.UK' (*www.ncsc.gov.uk*, May 2019) <https://www.ncsc.gov.uk/section/cyberuk/2019-gallery> accessed 7 December 2022.

proved unattainable. However, in some of those cases, they provided direction to existing data which provided useful account of government processes, and allowed insight into their perspectives. Thus, the secondary data are pulled from various sources based on the overall role such data performed within the study for the purpose of satisfying both the empirical analysis as well as the genealogical goal of the study.[456]

In summary, the overall data collection has three main sources: 1) primary sources which includes interview data . 2) Conceptualising secondary data from web repositories of government bodies, institutions, private and non-governmental organisation which is used to map and abstract discourses from the various contexts within the primary and secondary sources. 3), additional data for the primary purpose of literature review, but also consisting of data deemed relevant to the "internal analysis" which, by way of the multiple heterogeneous "external relations" of the object of analysis,[457] serves to unravel the harmonising governmental constructs and discourses that renders cybersecurity problematisations intelligible.

4.8 Data Sources selection Criteria

The decision to limit empirical focus to the four case entities is methodological, designed to create a narrow focus for the research, and to effectively and efficiently satisfy the overall study's objective. Selection criteria

[456] Michel Foucault, 'Govemmentality', *The Foucault effect: studies in governmentality* (1991). (1991).
[457]Ibid [77]

for how the data is collected follows the same principle, favouring quality over quantity. Thus, interview candidates were identified and selected based on the perceived higher possibility of obtaining relevant data from them. For example, the senior officer in Ghana not only provided invaluable insight into cybersecurity practices from Ghana's perspective, but also in gaining deeper understanding of the wider role of the CCI and the nature of its projects in developing Commonwealth states.

With regards to the secondary data source, similar focus is directed at those that were deemed relevant to the object of analysis. It was necessary to limit the conceptual secondary data to a period dating back to the early 1990s, to represent the period when cybersecurity began to emerge as an established object of government concern.

The purpose for which the conceptual document was released is also used as a selection criterion. This was useful in selecting data based on their prescriptive nature, for example. Such documents as the Commonwealth Cyber Governance Model,[458] and the World Bank's Combatting Cybercrime Tools and Capacity Building for Emerging Economies,[459]allow the capture of normative claims within the text, along with explicit justifications or recommendations for certain practices, policies, rules, and regulations.[460]

[458] Commonwealth ICT Ministers (n 54).
[459] The World Bank and United Nations, *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies* (Creative C, The World Bank Group 2017).
[460] Foucault, 'Govemmentality' (n 456).

Because this a law school program, the data also needed to include documents with some legal relevance in their context. In doing so, a collection of legal cybersecurity related documents was included to identify those that were relevant (such as the Trinidad and Tobago Cybersecurity Agency Bill,[461] for example).

4.9 Limitations

There are limitations to the methodology employed, particularly regarding the selection of the conceptual secondary data, as they needed to share some similarities contextually, and contain texts that support the same objects (for example, prescriptive and regulatory), with similar policy goals (socio-legal, socio-political, legal, political, or economic). Finally, they needed to contain data that are located within the same knowledge fields (cybersecurity, cybercrime, cyber governance, global politics, and law).

There is also the limitation of the choice of the case states, particularly the choice of the United Kingdom as a representation of a global power, when its global influence may appear to be waning in recent times. Perhaps such a global superpower as the US would have seemed a more suitable choice, especially with its historical role in shaping the internet through bodies such as the ICAAN, and its continued (sometimes covert, but also constitutionally explicit) orchestration

[461] Cyber Security Agency HR Bill 2015 (TT).

of affairs of other states (of weaker economies through the USAID for example, as revealed in the Associated Press (AP) 2014 story).[462]

Indeed, perhaps focusing on the US might have revealed similar dynamics of cybersecurity probelmatisation, or offer more relevant data. However, the choice of the UK and the developing Commonwealth states is one that was motivated by both the stance and focus of the study, both of which are in turn influenced by the interest of the researcher, and the unique relationship between the UK and the Commonwealth.

There is also a possible limitation in the use of Foucault for socio-legal research, which risks pushing the research outside its remit. Despite the ability of Foucauldian concepts, such as governmentality, to uniquely highlight the multi-layered "nature of governmental power",[463] there remains the methodological problem of its application to legal research more broadly (bearing in mind the "contested status of law in Foucault's thought".[464]). But because this is an interdisciplinary study, the concern becomes that of how well suited the chosen conceptual elements are in achieving the desired research goals? How well suited are the materials selected for the conceptual framework, bearing in mind that, even in the field of social sciences and humanities, where Foucault is more directly applicable, there remain challenges regarding the use of Foucauldian

[462] Desmond Butler, Jack Gillum and Alberto Arce, 'US Secretly Built "Cuban Twitter" to Stir Unrest' *AP News* (Washington, 2014) <https://apnews.com/article/technology-cuba-united-states-government-904a9a6a1bcd46cebfc14bea2ee30fdf> accessed 27 December 2019. See also: Bernard Harcourt, *EXPOSED: Desire and Disobedience in the Digital Age* (Harvard University Press 2015).

[463] Darren O Donovan, 'Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls', *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016).[28]

[464] Ibid.

analytics.[465] Colin Koopman and Tomas Matza observed, for example, that one risks:

> on the one hand, warping empirical materials by subjecting them to a framework whose contours were developed elsewhere and, on the other hand, warping concepts by affixing them to new contexts where they do not easily apply, such that we force ourselves to strip empiricities of their historicities.[466]

In dealing with these drawbacks, particularly those that apply to the use of Foucault, it is therefore in one's interest, as well as methodologically imperative, to reflect fully upon the role and appropriateness of each element deployed in the study. It is hoped that this chapter and some sections of the introduction have demonstrated that; either by identifying and explaining the object, field, analytics, concepts, and materials, or/and through the detailed explanations of how everything is put together to deliver the study's analytical strategy.

The use of Foucauldian concepts which has been the object of critique, particularly in response to Agamben's work in *Homo Sacer,* is directed at what Lemke calls a 'statist' orientation of such work, which appears to provide a totalizing assessment of state power, but not necessarily grounded on adequate empirical rigour.[467] Such orientation, for Lemke, fails to provide thorough

[465] Colin Koopman and Tomas Matza, 'Putting Foucault to Work: Analytic and Concept in Foucaultian Inquiry' [2013] Critical Inquiry.

[466] ibid.[819]

[467] Thomas Lemke, *Biopolitics: An Advanced Introduction.* (Monica J Casper and Lisa Jean Moore eds, NYU Press 2011).

understanding of contemporary forms of power.[468] They see a shortcoming in such totalization because of what they see as a “withdrawal of the state”,[469] in the contemporary exercise of power, which is increasingly seeing the transfer of control from the state to science and technology, commercial interests, expert committees, ethics, and civil society.[470]

Agamben, in response, focuses on highlighting his work as belonging to what he sees as philosophical archaeology, as opposed to a historical philosophy.[471] The difference is that a philosophical history cannot be reduced to a documented opinion or perception of philosophers, as it would admittedly never capture the true essence of thought. For philosophical archaeology "the *arche* it seeks can never be identified with a chronological datum”.[472] This is because, for the philosopher, the origin of the philosophical truth does not yet exist at the start of its enquiry. As such, it poses a perceived lack (or indeed, a lack) of an identified and specific object of enquiry. This is because, philosophy, Agamben argues, is built on the failings of the past. Therefore, the beginnings of such a project of enquiry can only act as archetypes that serves only as guidelines for the future – a place that may never be reached.[473]

Conscious of such criticisms, this study nonetheless postulates the argument that while there is the ‘perceived withdrawal’ of the state in

[468] ibid.
[469] ibid. [61]
[470] ibid.
[471] Giorgio Agamben, *The Signature of All Things on Method*, vol 31 (Luca D’Isanto and Kevin Attell eds, Zone Books 2009).
[472] ibid.a [82]
[473] ibid.

contemporary governing technologies, it constitutes all but new ways of understanding the role of the state in current times, and in their control or orchestration of the global socio-political order, while sustaining new forms of liberal governance.[474] Thus, the role of the state (in its many formations) is interrogated in the cases to reveal the configuration of power, albeit discursively diminished in some cases.

This interrogation is done through Foucauldian power concepts nonetheless, allowing the notion of governing to be understood as an analytical domain with a focus on "the practices and discourses that constitute the state in different forms".[475] In other words, the statist concern becomes less relevant because, such analytical configuration allows governing to be understood, not as a domain that has shifted from the grasp of the state, but one whose practices and discourses need to be examined regardless, to understand their different forms of contemporary power. Doing so allows such governing practices to be seen as constitutive elements within a wider field of systems of control, without the need to fall into the statist trap that sees the state as a monolithic element of repressive power.

[474] Kaspar Villadsen and Mitchell Dean, 'State-Phobia, Civil Society, and a Certain Vitalism' (2012) 9 Constellations <https://onlinelibrary.wiley.com/doi/10.1111/cons.12006> accessed 1 December 2022.
[475] ibid.

5 Establishing the truth effect: Global cybersecurity Problem representation within UK, ITU and the Commonwealth data

5.1 Introduction

Within the UK's National cybersecurity strategy, cybersecurity is classified as one of the country's "top priorities alongside international terrorism, international military crises and natural disasters".[476] It also focuses on influencing and shaping the "global evolution of cyberspace in a manner that advances wider economic and security interests".[477] This declaration suggests a cybersecurity problematisation, and the representation of cybersecurity as a

[476]HM Government, '2010 to 2015 Government Policy: Cyber Security' (*gov.uk*, 2015) <https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security> accessed 26 August 2021. See also: Government of the United Kingdom (n 13).

[477] Government of the United Kingdom (n 13).

global issue to be addressed in the interest of the country, much like other global sources of crisis or concern.

The goal of this chapter is to demonstrate "what presumption or assumptions underlie" this sort of "problem representation",[478] and how they are further rationalised to create visibility (truth) of the problem.[479] This is the first step in understanding "the ways in which problems are constructed, practices described and redescribed and invested with purposes, the kinds of solutions offered, and the types of politics they authorize", as the first problematising stage which creates the 'truth effect'.[480]According to Rose and Miller,[481] problem phenomena are sustained through rationalities and technologies of government or governing.[482] They represent the process by which political rationalities are normalized and rendered as objective realities. This process is achieved through strategies and practices that are able to utilise entities perceived as real through such political rationalities. Thus, problem representation aids this process, allowing problematisation to be realised, through perception and practice.[483]

Foucault argued that the various tools of governing (strategic and political policies, discourses and practices) are the binding agent between the

[478] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 49)[5].
[479] Foucault and Rabinow (n 39).
[480] Mitchell Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (Tim May ed, McGraw-Hill Education 2007)[74]; Mitchell Dean, *Governmentality Power and Rule in Modern Society* (2nd ed., Sage 2010).
[481] Rose and Miller (n 23).
[482] ibid.
[483] Peter Miller and Nikolas Rose, 'Governing Economic Life' (1990) 19 Economy and Society 1 <https://doi.org/10.1080/03085149000000001>. [8]

technologies and rationalities of government.[484] This creates the understanding of problematisation as the ’work of thought’ and as a governing practice.[485] Therefore to explore the problematisation of cybersecurity, it is necessary to identify, as a starting point, the connecting elements that make the problem visible, in order to understand how such works of thought function in the creation and deployment of these governing technologies.

5.2 Cybersecurity visibility in the case data

Within the UK and Commonwealth data, there is a clear transposition from the realm of thought to that of practice in relation to the problem of cybersecurity. This is evident in how events are presented to highlight the problem, through certain representations of cybersecurity challenges. Typically, statistical data are deployed but it also involves the constant replay of threat and attack incidences, discourses designed to create increased cybersecurity awareness, and other manifestations of the problem.

As an illustration of such a conceptual and pragmatic function (because it exists both in thought and practice), the launch of the ITU’s Global Cybersecurity Agenda (GCA) in 2007 which was funded by a group of Western states, can be cited.[486] The GCA, for example, marked the launch of coordinated and calculated global cybersecurity monitoring measures, which creates a background to the

[484] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).

[485] ibid. [118]

[486] ITU, Stein Schjølberg and ITU, ‘ITU Global Cybersecurity Agenda: Framework for International Cooperation in Cybersecurity’ (2007).

importance of cybersecurity needs. Its launch reflects the need to make cybersecurity visible. allowing, in turn, for the visibility of the need for a fit, ready and capable global society, as a way of responding to a growing series of cybersecurity challenges.[487] Thus, for a global response to these challenges to be affected, the challenges have to first be seen as pressing and potentially harmful.

> Cybersecurity is one of the most profound challenges of our time. The rapid growth of ICT networks has created new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Governments, firms and individuals are increasingly reliant on the information stored and transmitted over advanced communication networks. The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyberthreats.[488]
>
> When threats to critical infrastructures in the financial, health, energy, transportation, telecommunication, defence and other sectors are taken into account, it is obvious that the situation is likely to get worse.[489]

Global cyberthreats concerns are real, in the sense that true danger exists and economic, social and political damages, are possible. Highlighting the problem is necessary in the traditional sense of any problem-solving strategy. It allows for justification to secure the required support that authorities need to forge their response.

> When several hijacked computers and networks that have been compromised spread over many countries and are used to launch cyberattacks using a decentralized model (based on peer-to-peer

[487] ibid.

[488] Stein Schjølberg, 'ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)' (2008) <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html> accessed 26 October 2021. [2]

[489] ITU, Schjølberg and ITU (n 486). [6]

> arrangements), no national or regional legal framework can adequately deal with such a problem. This challenge can only be addressed globally.[490]

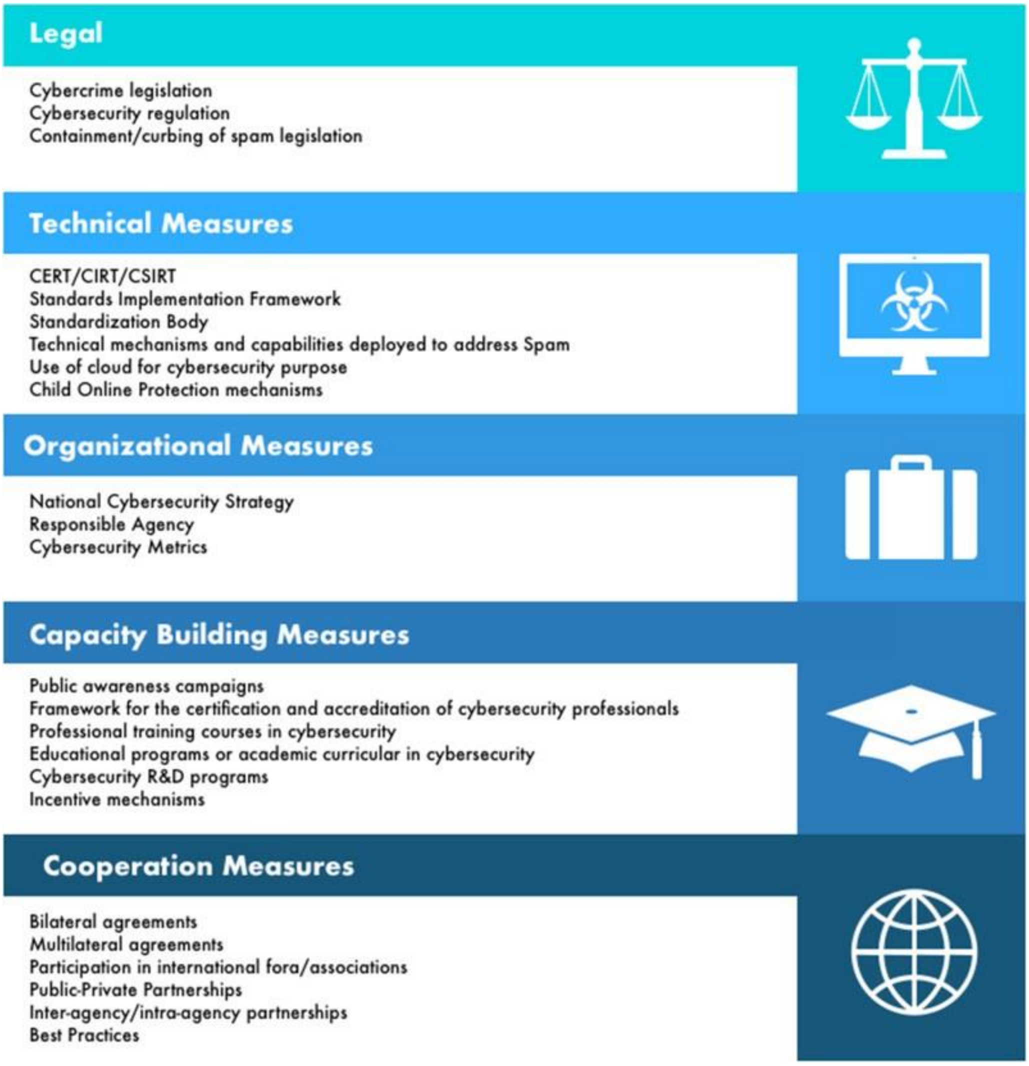
Thus, problem visibility aids the GCA, for example, as it prepares the pathway for acceptance and validation of the problem. This validation in turn allows it to further highlight what the states need, to strengthen efforts in key areas, boost their levels of preparedness, build and strengthen alliances through international cooperation on its key pillars: legal, technical, organisational capacity building and cooperation.[491] Based upon these key pillars, the ITU produces annual global cybersecurity index and wellness profiles.[492] Through conclusions that are drawn from statistics and other data, the index embodies the visibility process in its entirety, by which cybersecurity is taken, from the 'world of thought' to the 'world of being' or practice.[493] And this is made possible through practices of gathering, measuring and calculating data:

[490] ibid. [7]

[491] ibid.

[492] Abi Research and ITU, 'Global Cybersecurity Index' (2014).

[493] Miller and Rose (n 483); Miller and Rose (n 440); Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).



Legal

Cybercrime legislation
Cybersecurity regulation
Containment/curbing of spam legislation

Technical Measures

CERT/CIRT/CSIRT
Standards Implementation Framework
Standardization Body
Technical mechanisms and capabilities deployed to address Spam
Use of cloud for cybersecurity purpose
Child Online Protection mechanisms

Organizational Measures

National Cybersecurity Strategy
Responsible Agency
Cybersecurity Metrics

Capacity Building Measures

Public awareness campaigns
Framework for the certification and accreditation of cybersecurity professionals
Professional training courses in cybersecurity
Educational programs or academic curricular in cybersecurity
Cybersecurity R&D programs
Incentive mechanisms

Cooperation Measures

Bilateral agreements
Multilateral agreements
Participation in international fora/associations
Public-Private Partnerships
Inter-agency/intra-agency partnerships
Best Practices

Figure 1: GCI 2018 indicators per pillar given and its indicators used to measure ITU Member States

Thus, such practice, allows for authoritative claims to be made, by reports of this kind, granting the presentation of its claims as “factual representations of each nation state’s level of cybersecurity development”.[494] The ‘visibility role’ of such report is “to provide a clear perspective on the current

[494] Itu and Abi Research (n 207).[28]

cybersecurity landscape based on the five pillars of the Global Cybersecurity Agenda".[495] And with which, it

> aims at providing the right motivation to countries to intensify their efforts in cybersecurity. The ultimate goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies. [496]

Ensuring that this goal is met, the required level of preparedness must be achieved to ensure that all states are encouraged and supported, to develop their cybersecurity capacity, particularly amongst those for whom the capability to do so themselves is limited or lacking.[497]

> When the Global Cybersecurity Agenda was first launched in 2007, the first iPhone was still a month away from release and Facebook had only been open to users outside universities in the United States for a year. A billion people were online, and there were concerns that the amount of data created, 255 exabytes, would exceed available storage …. . Currently, 3.5 billion people are online and the digital world is estimated to be 44 zettabytes…. In addition, ICT proliferation has affected the broader national ecosystem giving life to new organizational possibilities, such as e-government services, and new economic and productive paradigms such as Industry 4.0 and the broader digital economy. All countries are affected to some extent by the digital divide, and as a key enabler of the economy, society, and government, which rely on digital systems, cybersecurity should be a high priority.[498]

Thus, the question of what the 'problem' of cybersecurity is, can be interpreted in terms of collected data; first about the 'problem', then about the objective figures derived from such data. In other words, and as observed within

[495] ibid.
[496] ibid. [iii]
[497] ITU, Schjølberg and ITU (n 486).
[498] International Telecommunication Union (n 139). [15]

the ITU index data, the issue of whether a problem exist is demystified through data about events that are objectifiable in both numbers and words, with words being used to back up the numerical data and vice-versa.

Thus, data present information that suggests objectivity rather than subjectivity, allowing for the field of visibility to be developed independently of any problematising process.[499] This is so because, the presentation of statistical and other factual information allows for the 'problem' to be seen in isolation, without necessarily making any calculative and analytic techniques behind it obvious. As such the problem is identified and established as pre-dating the problematising actions, that follow, while the effects of this process remain unnoticed:

> 81% of large corporations and 60% of small businesses reported a cyber breach in 2014. With the cost for the worst cyber-security breach estimated between £600,000 to £1.15 million for large businesses and £65,000 to £115,000 for smaller ones, the government must look at new ways to protect businesses and make the UK more resilient to cyber-attacks and crime.[500]
>
> The joint AUC-Symantec report Cyber Crime & Cybersecurity Trends in Africa, published in November 2016, reveals that 24 million malware incidents targeting Africa were observed in 2016.2 A 2017 report from McAfee finds that, in the fourth quarter of 2016 alone, nearly 12% of their African mobile customers reported malware infections.[501]
>
> Vulnerabilities, or exploitable weaknesses, pose a threat to devices, networks, and systems, along with those who rely on them. These

[499] Dean, *Governmentality Power and Rule in Modern Society* (n 480).

[500] HM Government, '2010 to 2015 Government Policy: Cyber Security' (n 476).[4]

[501] Internet Society and African Union, 'Internet Infrastructure Security Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union' <https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/> accessed 12 October 2021. [7]

> vulnerabilities are exploited by attackers to attack an increasingly diverse range of industries, organizations, and targets.[502]

As evident in the quotes above, data is presented such that, the problem of insecurity in cyberspace can be thought, perceived, or seen in the relevant space where the data appears, and in the context they are designed or intended to relate to. Often, the presentation of such statistical data, appears or are presented prior to any textual interpretation or analysis within the text. This approach allows for the passive representation of such data, making the visibility functions and effects of the embedded calculative techniques less obvious, particularly during the subsequent textual interpretation of the problem.

Such approach, however, does not render statistical data passive during the problematising process in its entirety. Rather, and according Bacchi's question number two (see also methodology chapter),[503] such data can be understood as forming an integral part of the conceptual logic behind the visibility and representation of cybersecurity as a problem, as they form the basis for the textual claims. [504]

> [Cybersecurity is a]tier One threat to our national security, alongside international terrorism. The threat to our national security from cyber-attacks is real and growing. Terrorists, hostile states, and cyber criminals are among those targeting computer systems in the UK.[505]
>
> The nature of these threats continues to include activities such as theft (of identity, personal data, and secrets of all kinds), infringement of intellectual property rights, denial of service attacks, defacement, and

[502] ibid.
[503] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).
[504] ibid.
[505] HM Government, '2010 to 2015 Government Policy: Cyber Security' (n 476). [4]

> other sources of disruption. However, large-scale distributed denial of service (DDoS) attacks, misuse or breaches of personal data, and the disruption of critical infrastructure should be of the most concern to Africa[506]

Textual claims, such as above, sets the stage for further actions which feed-off the assumptions created by the successful visibility of the problem. An interesting aspect of subsequent action of claims such as demonstrated in the last of the quotes above, is its prescriptive effect, which directs attention to what 'should be of most concern', while also electing a collective subject called 'Africa'. By doing so, it creates an erroneous unification of the diversity of over 50 different states into a single entity which supposedly has a unified character and common concerns.

Similar means of problem visibility are also used to project the reality of cybersecurity problems into the future. To this end, the funded research report of Symantec and the African Union Commission (AUC) can also be cited.[507] The report provides a glaring statistical account of the current state of global cybercrime and cybersecurity (35 percent increase in ransomware attacks in 2015, for example), and a privileged "peek into the future", into the "risk of things".[508]

[506] Internet Society and African Union (n 501). [7]

[507] Symantec and African Union Commission, 'Cyber Crime and Cyber Security: Trends in Africa' (2016) <https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf> accessed 12 November 2021.

[508]ibid. [9]

In this future, the world is headed for a predicted 20.8 billion internet-connected things. A situation where medical devices, smart televisions, and even cars are at risk of demonstrated proof of concept attacks, click frauds, alongside other vulnerabilities.[509] In addition to its visibility function, this sort of risk projection, or projection of the problem into the future, also serve both the purpose of diagnosing and providing solution to the problem through the sense of urgency it creates.

The legitimising and institutionalising capabilities of statistical data is historically evident, particularly in aggregated population data since the twentieth century, as they are perceived to be more accurate, and provide objective representation of events. With these capabilities, it is easy to see how certain assumptions of the digital divide between states can emerge from the 'truth' representation of the problem, through a practice of lumping together certain groups of countries. The use of expressions, for example, suggesting that cybersecurity threats "should be of the most concern to Africa",[510] is not only indicative of a prescriptive focus of attention towards an entire geographical region that is made up of economically, culturally and politically diverse independent states, but also suggest the presence of discursive assumptions of a common concern between these states, which bear traces of historical power relations.

[509] ibid.

[510] Internet Society and African Union (n 501). [7]

Similarly, as seen within the data sampled across the cases, the demonstration of cybersecurity threats through claims to data, translates into knowledge or possession of knowledge, as the objective means by which 'we know' and therefore, understand the reality of the problem. Thus, it provides the 'knowledgeable' stakeholders with the basis for seeking equally measurable solutions to the problem:

> The government has allocated £860 million until 2016 to establish a National Cybersecurity Programme. The vision of the government is to ensure that a vibrant, strong, and secure cyberspace can enhance the UK's prosperity, national security, and society. [511]
>
> Cybersecurity is paramount for sustaining a technologically sound model. The disruption of electricity or the impairment of financial systems through interference with ICT networks is a reality; these events constitute national security threats….the growing number of connected platforms only serves to offer new attack vectors. There is no going back to simpler times. In embracing technological progress, cybersecurity must form an integral and indivisible part of that process.[512]

Thus, the presence of problem visibility within the data is indicative of the truth effect, as it seeks to establish the reality of the problem and set the stage for formulating solutions at the same time. However, these solutions are embedded within political and government interventions and processes. For target recipients of such solutions (developing states, in particular), their perception of the 'problem' representation is relevant. Thus, one must ask, how

[511] HM Government, '2010 to 2015 Government Policy: Cyber Security' (n 476). [4]
[512] Itu and Abi Research (n 207).[39]

are their perceptions, both of themselves and of the challenges, impacted by these problem representations?[513]

5.3 Cybersecurity rationalisation through calculative practices

Analysing extracts such as the ones provided above, allows one to see how problems are articulated to advance practices of action within the case data. In other words, it creates a link between the 'truth' articulation of the problem to the technology of practice in place, thereby revealing how issues are transformed into programs of thought and work, through what Peter Miller describes as a form of calculated practice.[514]

Calculative practices, in Miller's conceptualisation, allows for certain capacities of agents, organisations, and the connections between them, to be altered. It allows for the reshaping of power relations within these connections which enables new ways of acting upon, and influencing the actions of individual agents and organisations.[515] While calculative practices are active in highlighting the problem, they are nonetheless largely invisible. This is because, they remain intrinsically linked to a certain "strategic or programmatic ambition",[516] "through which programs of government are articulated [made visible] and made operable".[517]

[513] Bacchi, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (n 5); Carol Bacchi, 'Policy as Discourse: What Does It Mean? Where Does It Get Us?' (2000) 21 Discourse 45.
[514] Miller and Miller (n 4).
[515] ibid.
[516] ibid. [394]
[517] ibid. [379] See also Rose and Miller (n 23).

Therefore, examining cybersecurity problematisation allows one to focus on the ways in which calculative strategies can be rendered visible within cybersecurity development practices. As such, it allows for an understanding of how it shapes social, political and economic relations, rather than as a preoccupation with the way in which cybersecurity challenges are shaped by security science or technology. Thus, as a calculative practice, cybersecurity development initiatives represents an important technology of governing by which the security concerns of others are brought to light and subsequently acted upon, such that their conduct can be 'conducted' in specific ways, to satisfy certain objectives.[518]

Viewed along calculative practice's lens, and contrary to its make-belief stance of 'providing assistance to those less capable', global cybersecurity development practices do much more than the advertised purpose of developing or building capacity and aiding preparedness for weaker developing states. Rather, they create specific ways of representing, understanding and acting upon the problem. They do this, as shown in the quotes above, through the highlighting of the problem and emphasising it's cost to society, demonstrating the cost of not acting as well as the benefits of acting upon the problem. Thus, calculative practices create strong basis for identifying and defining rewards and penalties, profits and losses discourses, to which the different actors can respond to.[519]

[518] Miller and Miller (n 4).
[519] ibid.

Hence, there exist a necessary nexus, within the cybersecurity discourse, between the need to establish statistical data, to determine (calculate) and present the problem on the one hand, and the solution offered on the other hand. In other words, creating a strategic connection between the processes of making the problem visible, diagnosing it, and ultimately providing solutions to solve it, with much of the emphasis of such strategy being placed on the benefit of action versus inaction:

> As countries develop, access to digital systems is key.[520]
>
> The internet enables huge opportunities for business and communication, but also some threats and risks. Every country with access to the internet needs to have strong cybersecurity to ensure trust – understanding the risks and being able to respond to them builds confidence within national and international communities, which is especially important for winning foreign investment and trade.[521]
>
> …The [Commonwealth Cyber] Declaration sets the framework for a concerted effort to advance cybersecurity practices to promote a safe and prosperous cyberspace for Commonwealth citizens, businesses and societies. [522]
>
> And the possible beneficial outcome being discursively rationalised as a basis for the need for response:
>
> At the beginning of 2018, 24 of the 40 low-and middle-income countries in the Commonwealth had no to little cybersecurity incident response capability. That is why the UK Foreign and Commonwealth Office (FCO), as part of the UK's commitment to maintaining a free, open inclusive and secure cyber space, partnered with the Singaporean Government and a commercial consortium, consisting of Torchlight Group, Protection Group International and Venues &

[520] Foreign and Commonwealth Office, 'UK Commonwealth Cyber Security Programme: A Selection of Six Case Studies' (2021). [2 – 3]

[521] ibid. [3]

[522] Chatham House, 'Cybersecurity in the Commonwealth: Supporting Economic and Social Development and Rights Online', vol 44 (2018) <https://www.chogm2018.org.uk/sites/default/files/Commonwealth Cyber Declaration pdf.pdf> accessed 25 September 2021. [2]

> Events, to support governments in developing this important capability.[523]
>
> By bringing people together and providing technical advice, the objective is to support public and private sector bodies in the participating Commonwealth countries, to develop and mature their own national cyber incident response capabilities.[524]

Evidently, such claims as above, which suggest the need to support others in their efforts to 'develop and mature', present, by implication, a position of underdevelopment on the part of those recipient states. Therefore, it suggests a re-manifestation of the modernisation agenda whereby, yet again, the 'other' (poorer) states, based on their economic status, inevitably rely on such support. This becomes questionable when considered along the lines of the sort of power relation that may be at play within such arrangements.

Calculative cybersecurity development practices (such as capacity building initiatives in developing states) serve another crucial purpose of linking responsibility and 'calculation', to generate "the responsible and calculating " entity.[525] This allows such practices to be represented, through the recommendations that they provide, as "a body of expertise focused on exacting responsibility from individuals rendered calculable and comparable."[526] For Miller, this is done:

> In its concern with individualising performance, through its attempt to induce individuals to think of themselves as calculative selves, and

[523] Foreign and Commonwealth Office (n 520). [3]
[524] Ibid.
[525] Miller and Miller (n 4). [380]
[526] ibid.

> through its endeavour to enrol individuals in the pursuit of prescribed and often standardised targets.[527]

Thus, as technologies of power, cybersecurity efforts towards developing states, through their manifestations as technologies of government, can emerge as a technology of power. This is achieved through "a mode of action that does not act directly and immediately on others. Rather it acts upon the actions of others and presupposes the freedom to act in one way or another."[528] Hence, while hints of prescriptive calculation are noticeable within capacity building initiatives data, they are not necessarily 'visible' to the targeted 'calculable' states. This is because, they are designed to be less obvious, to avoid their perception as frameworks which are being 'shoved down their throat'. This covertness of such process is made possible through the programmatic process of calculative practices. And the entire process is achieved through efforts designed to make the problem visible, as a starting point.

Indications from the analysed data, suggests the influence of the UK's Foreign and Commonwealth Office on the overall cybersecurity problem visibility across the entire Commonwealth states. But this influence is often strategically deployed. Thus while its focus may sometimes be expressed more broadly in relation to the entire Commonwealth, its capacity development campaigns and fundings are focused on developing Commonwealth states. Its

[527] ibid.

[528] ibid.[381]

Funding of various cybersecurity initiatives, awareness programs, research reports and capacity building campaigns are evidenced, both in its own documents and in the texts of the Commonwealth, ITU, world bank, and many more.[529] These are indicative of the conceptual role played by entities like the UK, in establishing a desired cybersecurity problematisation through various representations of the problem.

Thus, upon the problem being established, diagnosis, naturally follows, with efforts such as those mandated to the ITU and the University of Oxford's GCSCC, amongst others, to carry out reviews of the problem. From whence, justifications for solutions emerge:

> With the World Bank planning to digitally enable every African government, citizen and business by 2030, as part of its Digital Transformation Initiative, ensuring countries have effective cybersecurity capabilities in place is more vital than ever. [530]
>
> To support the Commonwealth's commitment to maintaining a free, open inclusive and secure cyber space, the UK's Foreign and Commonwealth Office funded the World Bank to provide national cybersecurity capacity reviews based on the Cybersecurity Capacity Maturity Model for Nations (CMM) of the Global Cybersecurity Capacity Centre (GCSCC) of the University of Oxford.[531]

Does such involvement and commitment suggest the presence of certain logic of calculative practice, [532]for what cause, and at what cost to whom? Why do they 'really' matter?

[529] See appendix
[530] Foreign and Commonwealth Office (n 520). [13-14]
[531] ibid. [8]
[532] Miller and Miller (n 4).

Practices designed to highlight and deal with the problem of cybersecurity can also be analysed as a calculation of risk. This implies what Dean described as a technology of control,[533] along with what they termed, technology of government.[534] Thus, calculative practices, through the use of reliable and factual data,[535] enables the visibility of the problem which in turn allows for certain ways of "acting upon activities, individuals, and objects in such a way that they may be transformed".[536] Indeed, such use of data to emphasise cyber insecurity, confirms their use in highlighting the visibility of cybersecurity problems. What, therefore, are the problem representations being produced through this visibility? What problem realities are eventually established from within this logic of calculative practices?

5.4 Cybersecurity Problem representations

5.4.1 Cybercrime problem representation

The Commonwealth cyber declaration statement "notes with concern, the challenges faced by Commonwealth developing member countries, particularly less developed countries and small island developing states".[537] Further, it declares its commitment to:

> invest in cybersecurity capacity building, including through the transfer of knowledge and technology, on mutually agreed terms, the

[533] Mitchell Dean, 'Putting the Technological into Government' (1996) 9 History of the Human Sciences 47.

[534] ibid. Miller and Miller (n 4).

[535] Foucault, *The Foucault Reader: Michel Foucault 1926-1984* (n 45).

[536] Miller and Miller (n 4).

[537] The Commonwealth Heads of Government, 'Commonwealth Cyber Declaration' (The commonwealth secretariat 2018). [3]

> development of skills and training, the promotion of education and research, awareness raising, and access to good practice.[538]

However, a key problem representation that is common within the case data is in relation to cybercrime, particularly within the developing Commonwealth states. Consequently, cybercrime appears to form the key focus of data used to establish cybersecurity problem visibility, and of efforts aimed at solving the problem. While cybercrime may be a global concern, there is a peculiar preoccupation in relation to developing states. This is attributed to reasons which, again, relate to development. The rapid uptake in technology, and low levels of security practices in these states, create fertile grounds for cyber criminals to flourish, locally, but with the potential to wreak havoc globally. This borderless nature of cybercrime is acknowledged by all. In its 2014 summary, the Commonwealth Working Group of Experts on Cybercrime noted that,

> [t]here was a sharing of the experiences of many jurisdictions regarding the significant challenges cybercrime presents to national security, to law enforcement, to individuals and to businesses.[539]

And as such, the group of

> ministers resolved to recognise the significant threat cybercrime poses to national security and law enforcement in all countries of the Commonwealth.[540]
>
> It is important that instruments designed to enhance co-operation within a given region should not be so framed as to have the unintended consequence of making co-operation beyond the region more difficult: criminals do not respect boundaries (and indeed exploit any opportunities divergent legislation may present). Subject

[538] ibid.

[539] Commonwealth and Law Ministers and Senior Officials (n 28). [1]

[540] ibid.

> to that, the Group believes that Commonwealth countries should be encouraged to consider becoming Party to any regional and/or international cybercrime conventions and participating in other initiatives to ensure co-ordinated action against cybercrime or, where possible, utilise them as models to guide the development or enhancement of their existing domestic frameworks.[541]

Albeit cybercrime, from non-Western developed states such as China and Russia, is acknowledged, it is however often perceived and represented through the lens of cyber terrorism or state aggression within political discourse. Thus, there is a tendency for cybercrime and cyber terrorism to be used interchangeably in relation to such states, within political speeches, and sometimes in authoritative texts. But this is less the case in relation to most developing states. Indeed, developing states have less cyber capabilities to warrant major terror concerns amongst Western states.

Nonetheless, discursive Western perception of cyber criminals from states like Russia, and their actions as state-funded terrorism, highlights the presence of a visible power struggle between those states, both with regards to the control of cyberspace and justling for global power positions. On the other hand, cybercrime representation in developing states is perceived as a problem which requires certain actions to ensure control of conducts within those states.[542]

[541] ibid.[32]
[542] ibid.[4]

The low capacity and capability of developing states, therefore, offers opportunity for support to be presented through the problematisation of the challenges that they face. Thus, the purpose of cybercrime discourse (albeit cybercrime being a real and growing global menace) in relation to developing states, would appear to be that of covert governing or control. And perhaps to ensure equally, that solutions provided to support such states are designed with such objectives in mind - sufficient to assist them in tackling the 'problem' (to control the problem), but not enough to get them to the point where they become contenders in the power struggle themselves.

To achieve this, a certain level of dependency is maintained and needs to be maintained. This is done through practices that ensure continued economic and political dependency as discussed in earlier chapters,[543] through the position of the West as pace and norm setters and applied through such initiatives as the CCI, providing seemingly comprehensive support programmes, based on predetermined Western-styled frameworks.

While these support programmes may seem purely developmental assistance, their limited capacity makes true competition unlikely. Still, building developing states local defences benefits everyone. It curbs crime for them, and helps developed states manage and control the global problem indirectly. Hence, it reflects a view of problem representation of cybercrime as a technology of control which will be discussed further in chapter six, where the norm effect is explored.

[543] See Part One Chapter Two

5.4.2 Representations based on consensus

Cybersecurity problem claims are not necessarily often based on hard facts, either due to limited research or inherent difficulties in measuring the problem. Instead, consensus of experiences often suffices in creating the necessary dramatic representation of the problem. Words like 'billions of dollars', 'majority of computers in Africa infected with viruses and malwares have no protection' and 'unquantifiable', 'irreversible damage', follows:

> It is not possible to give accurate figures as to the scale and cost of cybercrime, but there is general agreement that it is a fast-growing phenomenon and that, taking indirect as well as direct costs into account, it costs the global economy many billions of US dollars a year.[544]

5.4.3 Result producing problem representation

As observed, problem representations often give rise to other problem visibilities. For example, while cybercrime remains a main preoccupation of cybersecurity, further problems are subsequently identified that may relate to how the problem of cybercrime is addressed, and of how the problem came to exist in the first place. Thus, as part of the practice of establishing visibility of a current challenge, new problems can emerge in the process of diagnosing and finding solutions to the problem:

> The availability of human capacity in managing national cybersecurity responses is a challenge for some Commonwealth member states as the nature of cybercrimes and cyberattacks is constantly evolving. Consequently, two issues come to the fore: the lack of expertise to

[544] Commonwealth and Law Ministers and Senior Officials (n 28). [11]

> tackle cybercrime and cyberattacks in the first place; and keeping this expertise updated to address the evolving threat landscape.[545]

A key problem representation is the lack in both human and technical capacity. Particularly as the emphasis shifts towards designing future cyber resilience strategies .[546] As such, considerable focus is place on building capacity as shown above, to provide human and technical capacity to manage national responses.[547] This is evident across all states, but more pronounced within developing states, where it is seen as a consequence of their underdevelopment, but exacerbated by the rapidly evolving nature of cybercrimes and cyberattacks.[548] This supports the argument, that the faster the pace of technological evolution, the more challenges faced by developing states.[549] And the more challenges they face, the more support they will need, to cope with both the new changes and the challenges that they bring. Hence the suggestion by the quote that, upon dealing with an initial challenge of developing capacity, there is a further challenge of maintaining or updating that capacity on an on-going basis as technology continues to evolve.

The question therefore is, does this translate into a continued production or emergence of a 'revolving door scenario'? Whereby, more support needs

[545] International Security Programme, 'The Commonwealth Cyber Declaration: Achievements and Way Forward', vol 44 (2020) <www.chathamhouse.org> accessed 27 September 2021. [4]
[546] HM Government, 'National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK' (2022); Government of the United Kingdom (n 13).
[547] International Security Programme (n 545).
[548] ibid.
[549] International Telecommunication Union (ITU), *Capacity Building in a Changing ICT Environment* (Suella Hansen ed, 2018th edn, International Telecommunication Union 2018) <https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.01-2018-PDF-E.pdf>.

translate into more dependency of developing states on their wealthier counterparts? Particularly as the concentration of wealth and technological power remains with those states who appear to continue to enjoy such monopoly or hegemony?

5.4.4 Representation based on legislative deficit

Legislative shortcomings also provide further problem representations. This is often tied to the challenges of human and technical capacity shortages. The deficiencies relate to all aspect of cybersecurity concerns, including dealing with issues of threatening behaviour from other states, state aggression and cyberterrorism. The problem visibility created through the expressed need to improve legislative capacity of a state, also perform the role of diagnosing and prescribing solutions to the problem. These roles, nonetheless, are discussed further in subsequent chapters, but worthwhile pointing out how they overlap across the various practices.

Meanwhile, in October 2011, the Commonwealth Heads of Government (CHoG), reiterated their commitment to:

> improve legislation and capacity in tackling cybercrime and other cyber inspired security threats, including through the Commonwealth Cybercrime Initiative (CCI), which had recently been formed to assist developing countries to develop their institutional capacity in fighting cybercrime through the sharing of expertise from existing resources, with particular focus on the Commonwealth Model Law on Computer and Computer-Related Crime2 and also drawing from other treaties,

> conventions (including the Budapest Convention), legal frameworks, toolkits and guidelines.[550]

Here, the Commonwealth, as an institution with Western funders and implementation partners (including the UK, ITU and the Council of Europe), seek to straddle the complex task of digitization in developing commonwealth states, alongside addressing the issue of how cybercrime evolution (which itself is a product of digitization) can be best managed through legislation. This represents yet another case of establishing further visibility through diagnosis and action.[551]

5.4.5 Problem representation through electoral and democratic practices

The concerns over threat of foreign interference in democratic or electoral processes present another area of problem visibility and representation noticeable across the data, particularly in high-income countries like the UK.[552] But for low-income countries, the preoccupations are directed at meeting those basic technological standards required by states, to manage electoral processes more effectively and securely:

> while foreign electoral interventions have not been new, the use of technology to do so has become increasingly prevalent in recent years….To address this, the UK Foreign and Commonwealth Office (FCO), as part of the UK's commitment to maintaining a free, open inclusive and secure cyber space, partnered with the Organization of

[550] Commonwealth and Law Ministers and Senior Officials (n 28). [10]

[551] Dean, *Governmentality Power and Rule in Modern Society* (n 480).

[552] The commonwealth secretariat, 'Cybersecurity for Elections: A Commonwealth Guide on Best Practice' (2020) <https://books.thecommonwealth.org/>.

> American States (OAS) to increase understanding of common cybersecurity challenges in the Americas.[553]

As can be observed in the data, while cybersecurity support initiatives may bear certain traits of what one might call 'governing at-a-distance', they remain seemingly invisible, even to the actors. For example, in an interview conducted with the Ghanan government official, the suggestion that such an initiative could be interpreted as a form of influence and governance itself was swiftly dismissed:

> The relationship with the UK and through CCI project was a bilateral one. Specific initiatives were identified as I've mentioned, in a bilateral collaboration you identify initiatives. So, you want to do legislative review to see any gaps. We are both Common Law countries. So we have common knowledge through the UK with respect to regulation. So that was one of the components. There was probably also the reviewing of the cybersecurity policies to ensure that they are consistent with international best practices around the pillars that were discussed. So eventually, I don't have the specific, but that collaboration, was based on specific initiative that was supposed to be implemented. And there is always positive output from such relationship.[554]

A similar question was posed to a senior member of the Canadian Centre for Cybersecurity (the Canadian equivalent of the UK's NCSC):

> The threat of cyberattacks is real and global, so poses great concerns for all nations and everyone – rich or poor. Democratic or authoritarian, we are all affected. A free, open but secure cyberspace is vital for all country's economy. And because it affects everyone, and

[553] Foreign and Commonwealth Office (n 520). [6 – 7]

[554] The Researcher, 'Interview Conducted on the 22 of May 2019 with Senior Government Official - Ghana'.

> not all states, in fact, no state have the capacity to deal with it alone. We support states with less means to do that, particularly in the Americas. Our support help boost the confidence of such states in their own efforts with cybersecurity going forward.[555]

Such response can be viewed from two possible perspectives. First, it suggests a supposed inability of the agentic self to see beyond what the other desires them to see (in the Ghanian case for example), as a reflection of how such form of power are designed to work. And second, that there remains a conviction beyond doubt in the authenticity of the initiative's intentions (in both cases).

Indeed, it may not be a case of 'either – or'. Both rationalisations point to the same thing. And that is, if one was to view this through Bacchi's fifth question (What 'effects' are produced by this representation of the 'problem'?) and Dean's classification of such effects as a form of power effect, which allows for the deployment of what Foucault referred to as the *dispositifs* or technologies of power, one can begin to see how such practices, not only problematises, but are also designed to operate in certain ways. Such that, what is visible are only those thoughts that are intended as such. Everything else remains obscured to the regular thoughts or the 'naked eye'.[556]

As with the threat representation of cybersecurity risk in other areas, cybersecurity challenges presented within the electoral process have also grown with the increased digitisation of the process. For example, in most developing states, digitisation of the electoral process has been introduced not simply as a

[555] Researcher, 'Interview with SJ - Canadian Centre for Cyber Security CyberUK'.
[556] Dean, *Governmentality Power and Rule in Modern Society* (n 480).

modernisation tool or simply as a way of keeping up with democratic processes in the rest of the developed world. Rather, and perhaps most crucially, as a way by which election fraud could be reduced or eradicated, thereby, allowing for processes by which election results can become more credible:

> As the dependence of all elections on digital technologies grows, so do challenges to the audit process. If IT infrastructure is compromised at any stage of the electoral cycle, then the reliability of the information used to determine the outcome can be questioned. This makes the reliable recording and storage of data critical and emphasises both the usefulness of authoritative paper ballots and forms, and the publication of intermediate and final results.[557]

The notion of digitisation itself, however, sets up the stage for the problem visibility through its truth effect. It determines what ought to be considered credible as a result. Thus, it establishes the need for digitisation in the first place, as a necessity for the modern and progressive society, thereby rendering its push to different aspects of society governance (including electoral processes) uncontested. And as will be demonstrated in chapter six, upon setting up the visibility, acceptance and acknowledgement of the problems, the norm effect, through problem diagnosis sets in. This then allows the final rules of the game to be set or legalised, as will be discussed in chapter seven, where the notions of 'credible' and 'fraudulent' emerge, which, in effect, determine or control how things ought to be done.

[557] The commonwealth secretariat (n 552). [86]

Therefore, parts of this mechanism of power working together, place certain actors in control, determining what electoral or democratic practices are considered fraudulent or otherwise. As such, it sets the standard for what is, and who is considered to be on the right side of the norm. What constitute the correct ways of conducting democratic elections. What election practices are considered right or wrong, free, fair or fraudulent – essentially, how electoral outcomes are to be determined. What sort of digital solutions should be employed to guarantee these electoral standards, prevent deviation from the norm or allow its enforcement, and ultimately, produce the desired outcomes.

Clearly, there are several examples of this dichotomous nature of digitisation across all states. Digital technology's security concerns present challenges for all. In the case of the developed states, such security concerns are dealt with through self-funded research development and innovative solutions. On the contrary, developing states are often dependent on the benefits of such innovation being offered to them from the outside.

In the Commonwealth Cybersecurity for Elections Best Practice Guide, 2020, for example, it notes an over 70 percent use of manual processes in the entire electoral exercise for small island developing states like Trinidad and Tobago.[558] The remaining process, it claims, is carried out with some electronic support in the vote tallying exercise.[559] This is a near direct contrast with the data provided for the electoral and voting method in high-income

[558] ibid.[56]
[559] ibid.

Commonwealth states like the UK, where a little over 30 percent represents manual processes and almost 70 percent is manual, supported by electronic tally.[560] However, the situation is slightly different in other low-and-middle-income states like Ghana and Botswana. The largest difference found here is in the use of electronic voting machines and e-voting pilot for non-resident citizens (around 35 and 11 percent respectively) - a practice which is not found in the election processes in either the high-income commonwealth states or the small island developing states.[561]

Clearly, this seemingly increased digital uptake in the developing countries suggest the need for such nations to employ digital means to curb the presupposed fraud-ridden electoral processes of those states. Thus, a dilemma is felt more, within such states who are encouraged and, or chooses to adopt digital improvement to reduce their endemic election malpractice and corruption. But at the same time, they are faced with the security challenges that such digital improvement presents. Again, because they are yet to acquire the necessary skills or capacity to effectively deal with the challenges, they can only resolve to the support of high-income member states.

It seems therefore, that in all these problem representations, the emergence of the field of visibility is observed through the feeling of responsibility that is assumed by the support funders. Recipient state governments also assume such responsibility (or are 'encouraged' to do so, once

[560] ibid.

[561] ibid.

visibility and acceptance of the problem is established), to provide preventative measures to the problem. It does so by creating a connection between cybersecurity threats and risk to the wider issues of political or governmental responsibilities, while playing to the narrative of a global common interest.

> Countries should review best practices to synergize cybersecurity strategy across the Commonwealth. There is currently a lack of coherent strategy of addressing cyber incidents within the West African Commonwealth community for example. While each country is responsible for its own national strategy, it is important to recognize the transboundary nature of cyberthreats. This means not only having a multi-stakeholder approach but also having coordinated strategies that facilitate regional and community resilience.[562]
>
> We are in an era of changing economic circumstances creating both opportunity and uncertainty, giving rise to new trade and economic patterns together with unforeseen threats to peace and security, and a surge in popular demands for democracy, human rights and for broadened social and economic opportunities […] Cyberspace provides this [previously unimagined] access [to information and communication between individuals across our planet], helping us to bridge the digital divide while influencing every aspect of our economic and social activities. Cyberspace is becoming our global central nervous system.[563]
>
> Enjoyment of [its] benefits relies upon its safety, security and resilience[..] Governments, industry, civil society and users have a shared responsibility to tackle those threats to society.[564]

But how much of this is really about the collective community, or the whole ‘we’ or ‘us’ discourse? Indeed, it is arguable as to whom this discursive ‘us’, ‘we’ or ‘our’ refers. Without doubt, both cybersecurity challenges and their impact affects everyone. But who gains more or loses more from its problems?

[562] International Security Programme (n 545).
[563] Commonwealth ICT Ministers (n 54). [1]
[564] ibid.

According to statistics from various sources, most cyberattacks (of financial crime nature) on Western states, originates from predominantly Global South states such as Brazil, Iran and Nigeria.[565] But while such states are also higher targets themselves, Western states, albeit having much more robust defence or measures in place, appear to be more at risk of losing more in the event of an attack, particularly those targeting the banking sector or other critical state infrastructures. A case in time is a recent ransomware attack on the NHS here in the UK, even as this chapter is being written in August 2022, which targeted a critical digital service for the emergency 111 service.[566]

As hinted earlier, presentations of statistical data or references to such data, create a link between what the problem is represented to be and the actions or attention that it demands thereof in response. However, in analysing texts such as the extracts above, it would appear that, the confirmation and validation of a problem, and its visibility, are not necessarily defined simply by statistical figures, or accounts of facts based on available data. Instead, it is the way in which cybersecurity political or governmental responsibility are represented within the discursive framework of political will. This is done in addition to the actions, which are ultimately legitimised and sustained by calculative practices through data. Hence, statement like this for example:

> In light of the threat to socio-economic development posed by attacks on Internet infrastructure, it is the responsibility of all stakeholders,

[565] International Telecommunication Union (n 139).

[566] https://www.bbc.com, 'NHS 111 Software Outage Confirmed as Cyber-Attack - BBC News' (*https://www.bbc.com/*, 6 August 2022) <https://www.bbc.com/news/uk-wales-62442127> accessed 26 August 2022.

> including governments and Internet service providers, to agree upon solutions to ensure the Internet in every country remains safe, secure and resilient.[567]

5.5 Cybersecurity risk representation

The connection between rationalisation of cybersecurity problem through calculative practices, and the historical cybersecurity problematisation discourse can be reviewed using Bacchi's questions two and three: "what presuppositions or presumptions underpin this representation of the problem?" and "how has this representation of the problem come about?"[568] Calculative practice, creates a "condition of government",[569] and allows for the intelligible problem representation of cybersecurity within political discourse. At the point in which the problem is rendered intelligible, further calculative practices are incorporated to form risk 'mentalities'.[570] This process is present particularly when risk-producing situations are induced through calculative practices that in turn create further fields of visibility of the problem.[571]

> The malicious use of Information and Communication Technology (ICT) by state and non-state actors creates risks for all states, and the misuse of ICTs may harm international peace and security…. malicious activity committed by non-state actors for criminal purposes puts populations, livelihoods and economies at risk.[572]

[567] Internet Society and African Union (n 501). [7]

[568] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10). [xii]

[569] ibid.

[570] Michel Foucault, *Security, Territory, Population Lectures at the College de France, 1977-78* (Michel Senellart and others eds, Pbk ed, Palgrave Macmillan 2009).

[571] Robert Castel, 'From Dangerousness to Risk' in Graham Burchell and others (eds), *The Foucault effect: studies in governmentality.* (The University of Chicago Press 1991).

[572] Chatham House's International Security Department, 'Cybersecurity in the Commonwealth: Towards Stability and Responsible State Behaviour in Cyberspace', vol 44 (2019) <https://chathamhouse.soutron.net/Portal/Default/en-> accessed 25 September 2021. [5]

Thus, once visibility is established, assertions can then be made that professes normative or authoritative knowledge of the situation, as it affects certain groups, states, or societies.[573] In other words, the establishment of problem representations through the risk logic, allows for certain assumptions or presumptions to emerge, which in turn produces practices that constitute a technology of government.

Thus, the built-in assessment contained within the working processes of the various cybersecurity development initiatives, for example, serves this purpose (along with other functions) of identifying and highlighting issues or situations that can be defined as threatening, or posing security risk. And as a result, they establish further visibility of the problem, which further allows for the intelligibility of the problem and the production of normative understanding of the problem, leading to even more assumption of actions to solve the problem.

> Classification of cybercrime and related activities as a security matter often reflects a combination of an assessment of the risk or probability that an attack will occur, and the magnitude of the potential harm were an attack to succeed. Offences against state interests, such as espionage or terrorism offences, will always be regarded as cybersecurity matters, but economic forms of cybercrime will only be included if they either are linked to such offences (e.g., frauds that finance terrorist activities), or are of sufficient magnitude to damage the state's overall economic stability. There may be special concern if a 'cyber-attack' is thought to be launched from another state or if the motivation of the attackers is to gain policy influence or extort policy changes through the commission of crime or the threat of crime. When

[573] Foucault, *The Foucault Effect: Studies in Governmentality, with Two Lectures by and an Interview with Michel Foucault* (n 1).

> these interests are engaged, 'cybercrime' begins to overlap significantly with concerns about 'cybersecurity'.[574]

And when it comes to solving the problem, for developing countries, the support of the West is never far behind:

> Botswana partnered with the United Kingdom's Home Office to host the inaugural UK-Commonwealth African countries National Cyber Risk Assessment (NCRA). The Botswana team liaised with their UK counterparts and aided on the project.[575]

Indeed, risk assessment and representation within these projects are designed to aid a form of preparedness for what might, or could happen as opposed to stopping or eradicating the threats altogether.[576] This means that the relevance of such risk management efforts allow for perpetual need for continuous assessment, and monitoring regimes. Thus, risk rationalities classify what it sees as threat to security, highlighting the imminent danger it poses, creating further justification for a continued rehashing of the problem. As such, it creates a situation of constant expansion of policy scope, inaugurating new programs and practices, and perhaps, further dependency on those best poised to deal with the problem (typically Western states), by those less capable of doing so themselves.

Furthermore, risk strategies or risk calculations may demand even more data to support its claims. Therefore, demand for more data will almost

[574] Commonwealth and Law Ministers and Senior Officials (n 28). [26

[575] Foreign Commonwealth and Development Office and The Commonwealth, 'African Cyber Experts Fellowship : Lessons Learnt Report' (Protection Group International 2020). [9]

[576] ibid.

inevitably create further requirement for recurring research or review of existing security situation. Such reviews may also be used to create further problem visibility – in a continuous cycle of 'knowing the problem' and 'acting on the problem that we know exist'.

Hence, these practices suggest such actions that not only create a field of cybersecurity problem visibility at levels of global and national institutions, but also, activate cybersecurity risk assessments and prevention measures as 'fit for purpose', thereby creating on-going and "active, technical process" of cybersecurity control or governing as a result.[577] Consequently, key players in this orchestration of cybersecurity visibility field, (the UK, ITU and the Commonwealth), end up acquiring certain risk technologies and practices through this process of creating visibility,[578] with which they maintain their relevance in the global political economy.[579]

5.6 Conclusion

This chapter focuses on discussing the role of problem visibility in the problematisation of cybersecurity and its effects in relation to some of the case data. What is suggested through the data is the possibility of a mechanism of governing that is integral to the security apparatus, which allow for certain problem representations of cybersecurity challenges; A mechanism, by which the ends and the means of governing resides at the location of population – regional,

[577] Miller and Rose (n 440).[65]

[578] Majia Holmer Nadesan, *Governmentality, Biopower, and Everyday Life* (Routledge 2008); Dean, *Governmentality Power and Rule in Modern Society* (n 480).

[579] Miller and Rose (n 483).

national or global.[580] Phrased differently, it suggests a calculative deployment of certain assumptions and risk discourse in problem representations of cybersecurity challenges, preventative and protective tactics, as ways by which the problem can be seen, and acted upon. This bears a likely consequence of establishing a biopolitical problem-field that brings together multiple elements, which produces coherent and legitimate discursive problem fields. Consequently, it allows for certain practices to be justified and made intelligible.[581] How the manifestations of this practice of problem validation (truth effect) are progressed through to the diagnosis and normalisation function will form the focus of the data to be discussed in the subsequent chapters.

[580] Foucault, *Security, Territory, Population Lectures at the College de France, 1977-78* (n 570).
[581] Dillon (n 205).

6 Establishing the norms effect: Cybersecurity capacity building in developing Commonwealth states – why does it matter?

6.1 Introduction

Fields of visibility were identified within the data in the previous chapter to highlight how the truth effect is realised through representations of cybersecurity problems.[582] It provides a basis to understand the conceptual logic that underpins global cybersecurity practices. Through the data, it is shown how calculative practices are deployed to incorporate techniques of threat analysis, based on events that can be represented through verifiable information.[583] This technique is supported by the process of monitoring data, through what Miller

[582] Dean, *Governmentality Power and Rule in Modern Society* (n 480); Dean, 'Putting the Technological into Government' (n 533).

[583] Peter Miller, 'Governing by Numbers: Why Calculative Practices Matter' (2001) 68 Social Research 379.

calls, surveillance through statistical data.[584] We demonstrated how this data is utilised through presentation, and as emblematic means of rationalising global cybersecurity threats and risk. A key function of the problem visibility is to establish the problem as truth. It allows for its acceptance , and the acknowledgement of the need for solutions. This is followed by a process of understanding the problem, to determine the appropriate 'fix'. The focus of this chapter, therefore, is on such processes that are undertaken to understand the problem further ("Construction of the norm" effect through diagnosis of the problem).[585]

Using Bacchi's third question: "how has this representation of the 'problem' come about?",[586] relevant texts are examined, to discuss the question of how historic relations of power are built-upon, through knowledge claims that paves the way within the problematisation of cybersecurity. In doing so, cybersecurity efforts that are designed to further one's understanding of the problem, while suggesting solutions to fix the problem at the same time, are analysed. Thus, it includes examination of how cybersecurity issues are transformed into a factual problem-reality that requires specific knowledge to provide possible solution.[587]

According to Bacchi, before solutions are offered, the cause of the problem are both identified and understood. Thus, one ought to ask: why is

[584] ibid.
[585] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).[122]
[586] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10). [3]
[587] Dean, *Governmentality Power and Rule in Modern Society* (n 480).

cybersecurity a problem?[588] Identification of the 'why' is crucial to understanding the problematising tactic, because it allows for certain entities, conditions, etc., to be acknowledged and set as being contributing or responsible factors for the problem. In the case of developing Commonwealth states for example, part of this 'why' element includes the identification of the digital capacity divide between poorer states and their wealthier counterparts, which render such states more vulnerable. This also implies a development divide across multiple areas along the development spectrum – social, political, judicial, and so on. And in turn, it impacts certain relations of power, particularly in relation to the positioning of subjects vis-à-vis other subjects and, or things.[589]

Highlighting the capacity deficits which present major challenges for developing countries, not only allow for further problem visibility, but also serve as a way by which the problem is diagnosed . Thus, states' development status act as a key catalyst for the discourse around risk of cyber threats, cyberattacks cybercrime, etc. In the ITU's 2020 Global cybersecurity index for example, the link between the development status of a state, and their susceptibility to cyber threat is acknowledged and established when it states:

> The Global Cybersecurity Index reveals that cybersecurity is truly a developmental issue, and that there is an urgent need to address the

[588] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10); Bacchi, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (n 5).
[589] Dean, *Governmentality Power and Rule in Modern Society* (n 480); Nikolas Rose, 'The Politics of Life Itself': (2016) 18 http://dx.doi.org.ezproxy.lancs.ac.uk/10.1177/02632760122052020 1 <https://journals-sagepub-com.ezproxy.lancs.ac.uk/doi/abs/10.1177/02632760122052020> accessed 18 August 2022; Michel Foucault and James D faubion, 'Truth and Power', *Power: Essential Works of Foucault 1954 - 1984* (Penguin Books 2010).

> growing cyber capacity gap between developed and developing countries by fostering knowledge, upskilling, and building competencies. We need to close this gap by going to the roots and building capacity in terms of digital infrastructure, digital skills, and resources in the developing world. Thus, the challenges faced by both the states themselves and the wider regional or international bodies becomes that of identifying the causes of such vulnerability.[590]

Statements like this could be seen as one, designed to frame our understanding of cybersecurity challenges in a certain way, to allow for their normalisation and legitimisation of subsequent practices.

6.2 Diagnosing the problem - thought structures.

6.2.1 What is to blame for cybersecurity challenges?

As expressed by the quote above, the increasing vulnerability of developing states is linked to the digital gap. Therefore, as a way demonstrating the norm effect function of diagnosing the problem,[591] it is necessary to interrogate the construction of the notions of capacity gap and the discourse on 'why' close the gap. According to the ITU index, capacity gaps are based on indicators, like weak digital infrastructure, limited digital literacy and skills shortages. The ideas then follow certain knowledge claims, the perceived attitude of developing state governments towards cybersecurity, as well as analysis of behaviours of such states, alongside their population.

[590] International Telecommunication Union (n 139). [iv]

[591] See Methodology Chapter

While such reports often present or acknowledge the complexity of cybersecurity challenges faced by all, they nonetheless provide risk diagnosis of the problem based on individualised outcomes of such analysis. Thus, they frame individual-level state attitudes, behaviours, etc., to explain risk at a global level. This is a consequence of the perception of the cyber domain itself as a 'global common',[592] which makes it possible for reflections on individual responsibility towards a common "clarion call" amongst actors.[593] Hence, such expressions as 'there can be no weak links' within security discourse. For Miller, this coalescing of "individual responsibility and calculation: to create the responsible and calculating individual" (state or population), is key to our understanding of risk calculation practices as technologies of government.[594]

However, the process of individualising risk is not realised within the risk rationalities itself. The genealogical discourse around the capacity deficit of developing states, appears to provide continuous and further reaffirmation of the following: First, it affirms the problematisation of the phenomenon and the specific impacts it has on such states. And second, it sustains the need for their more developed counterparts to support them in the process of dealing with the problems identified.[595]

[592] Severine M Rugumamu, 'Capacity Development in Fragile Environments: Insights from Parliaments in Africa' (2011) 7 World Journal of Entrepreneurship, Management and Sustainable Development 113.
[593] ibid.[129]
[594] Miller (n 583). [380]
[595] ibid.

Between the affirmation of cybersecurity problems, and the need to address the challenges, lies the process of establishing the 'why such impact' discourse. This then attempts to paint the 'how we got here' picture of the problem, identifying its root causes, and so on. This stage, as evident in the data, provides accounts of poorer developing states as a collective, marred by common developmental problems, often exemplified by their choice of political orientation (dictatorships, authoritarian governments that lacks democratic principles, for example), poor leadership in government, crippling corruption, etc.[596] In other words, it allows for the emergence of a shift from the discourse of technical and instrumental deficit (infrastructures and skills) to moral failings (corruption, insufficient democracy, transparency, honesty). As such, the Western states are not only presented as more technologically advanced, but also morally advanced, as they implicitly represent the ideals of good practice, democracy, transparency, rule of law, etc.

In some cases, social and cultural attributes are used, as they appear to serve the purpose of establishing the role of such social-cultural, and even environmental factors, in determining what the assumed typical risk of cybersecurity problems are amongst such states. Thus, an array of problematised fields starts to emerge and become entangled in the risk representations, narratives or analysis of the social-economic and political ills of such states –

[596] Rugumamu (n 592).

hence such narratives as those which highlight poor digital infrastructure, for example, the lack of skilled human capacity, and so on.[597]

The rapid up-take of digital technology in poorer developing states (growth of internet and mobile phones penetration for example), is also not spared in the discourse. The increased pace can imply a problem, when rate of access to such new technology is not matched by rate of development in other capacities. Particularly in relation to capacities that are needed to prepare for the associated security risk, as can be seen here in the Commonwealth and Chatham House's report on cyber governance:

> Another challenge identified was the pace at which digital uptake has occurred in Commonwealth countries. On the one hand this has created many opportunities, however, the quick uptake has meant that some basic challenges, such as affordable access and skills have not been dealt with properly. In many instances, the conversation has jumped, perhaps prematurely, to more sophisticated areas, such as the potential impacts of AI, without resolving the basic issues first.[598]

From the above, it is clear that there is an implicit developmentalism at work, whereby it implies, that societies must or should go through stages of maturation, and therefore, ought not to 'get ahead of themselves' in seeking to become like the 'advanced' nations, without passing through the required stages of development.[599] The notion of developmentalism, according to Arturo Escobar, suggests a state of being, alongside discursive practices, actions and the

[597] ibid.

[598] Chatham House's International Security Department (n 572). [4]

[599] Arturo Escobar, *Encountering Development : The Making and Unmaking of the Third World* (Princeton University Press 2011).

establishment of institutions that establishes development as a project (technical, political, intellectual, ethical, etc).[600] This sort of developmentalism further impacts the formulation of subjectivities, creating what Cruikshank described as, "conscience, identity and self-knowledge".[601] And as such, it dictates not only the form assumed by agency, but also establishes new forms of subjection, while at the same time, introducing, legitimising or normalising, and institutionalising certain discourses that shape how the self is imagined and related to.[602]

Thus, the problem representation of cybersecurity is invariably linked to multiple factors in the efforts to account for difficulties faced by developing states as they consider their 'mandatory' digital transition, and transformation in the modern global society.[603] Amongst such factors, as implied by such statement above, is the way in which rights (development right of the individual) are deployed within certain development context, to establish and "put into motion new ways of being and relating to the self".[604]

While cybersecurity challenges is serious, the risk construction of states' insecurity in the digital space remains that which is based on individual choice.[605] This therefore denotes an individualised narrative of risk – that is, a risk assumed by the individual state, determined by the choices they have made in the past, or current decisions in relation to the problem (including also, the impact of the

[600] ibid.
[601] Barbara Cruikshank, *The Will to Empower : Democratic Citizens and Other Subjects* (Cornell University Press 1999).[21]
[602] ibid.
[603] ibid.
[604] Sumi Madhok, *Rethinking Agency : Developmentalism, Gender and Rights* (Routledge 2013). [2]
[605] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).

choices they must now make concerning the future, going forward). For developing states, this can mean significant pressure from the 'knowledge' nations and institutions, which leads to the ready acknowledgment and acceptance of whatever recommendations for action that is being proposed for them. Particularly when damning reports such as below are made regarding the digital development status of such states:

> Most of these countries were at the initial stage of developing services exports and the same issues came up in almost all of them, the only difference being the intensity. [606]
>
> Furthermore, there is no authority (ministry) responsible for services development as it is only recently that politicians and policy makers have been waking up to the potential of the sector. But while there is a need to change the mindset of such public officials, the weakness of institutional support is not solely the responsibility of the public sector. The private sector often lacks knowledge of the international markets for services and the means to penetrate these.[607]

Thus, despite the 'global common' discourse, and given its identification as a problem with interconnected global impacts, one might be tempted to question the individualisation of its risk in some of the political discourses.

> There is no straightforward answer to the challenges the world is currently facing across all political systems and spectrum. There is no rulebook or step-by-step guide to combating the distribution of malicious or malign targeted information campaigns. Instead, we need to focus our attention on longer-term solutions and begin to sow the seeds to empower our nations to make adequately informed decisions when participating in democratic processes. It is the responsibility of each administration, in collaboration with big data companies or information holders, to ensure and foster reliable information and

[606] The Commonwealth, *Promoting IT Enabled Services*, vol 3 (Nikhil Treebhoohun ed, Commonwealth Secretariat 2011). [28]
[607] ibid. [15]

> critical thinking by the public in order to maintain healthy democracies.[608]

An attempt to rationalise this individualised position, as observed, may suggest the role of real or presumed state sovereignty granted to all states;[609] However, this may not always be the case in real terms for some. More so, when such states remain in a form of economic, and sometimes political dependency. While the notion of state sovereignty not only entails "rights but also obligations that seek to safeguard other states and human beings",[610] it is conceptualised and defined by international law as means of achieving the wellbeing of a state, which is "manifested through the full enjoyment of human rights internally and the peaceful coexistence of nations externally".[611]

Thus, while the problem of cybersecurity present a global challenge, individual and independent states remain sovereign, regardless, under international law. Therefore, states must be seen (at least discursively) as such, to start with. Consequently, cybersecurity risk narratives are mainly viewed from this perspective, albeit with the possibility of it being otherwise in practice. In other words, the acknowledgement and respect for the rights of individual state sovereignty must be perceived as such, in order to guarantee the acceptance of what is diagnosed, before the proposed subsequent 'fix'. This is a tactic that is

[608] Cybersecurity Program of the Inter-American Committee against Terrorism, 'Cybersecurity Considerations for the Democratic Process for Latin America and the Caribbean' (Organization of American States 2019). [19]
[609] Talita Dias and Antonio Coco, 'Cyber Due Diligence in International Law' (2021).
[610] ibid. [103]
[611] ibid.

very well understood by the 'knowledge' actors. Hence, a seemingly show of respect for individual state sovereignty is often observed as a precursor to actions that are subsequently proposed. As such, it becomes a prerequisite that must be satisfied before any form of implementation of the proposed action is carried out.[612] Hence, there is a common trend, within authoritative texts, that are built around capacity building programs, with references to the capacity needs of states being assessed on case-by-case, region-by-region basis, and so on. And with the ultimate decisions on how to proceed with such recommendations, when to proceed and what to proceed with, supposedly resting on the individual host country.[613]

For example, and according to the Commonwealth working group of experts on cybercrime:

> The Group recommends the creation of special co-operative relationships among the smaller developing countries as well as between developed and developing countries to build law enforcement and preventive capacity and to maintain it on an on-going basis, for example including the development of regionally-based investigative or emergency response resources, and the sharing or provision of investigators, forensic facilities and similar resources on a case by case basis as needed, and to explore the practical, legal and sovereignty aspects of such arrangements.[614]

Indeed, when this is analysed further through Bacchi's fourth question, an understanding of individualised risk in the face of a global problem becomes

[612] Chatham House (n 522); International Security Programme (n 545).
[613] De Nardis and others (n 287).
[614] Commonwealth and Law Ministers and Senior Officials (n 28). [7]

clearer.[615] Thus, one can see how risk individualisation suggests the presence and use of the contributing factors described above.[616] It suggests their use within a narrow framework that appears to focus primarily on the rationalisation of the notion of individual choice, through the examination of the economic, technological, political and social factors. And that individual state choice, in relation to how cybersecurity concerns are dealt with, is presented as an essentialist view of the agentic self.[617] However, this is assumed equally for every state, but with varying degrees of responsibility. Thus, the construction of the agentic self, further allows for the problem visibility, presented through the conceptual logic of risk rationalities that allows for new thoughts or practices by which the desired reality is understood, diagnosed and normalised. But most crucially, this is done without a necessary acknowledgement of the discursive historical formulations of their economic (dependent) status in which they are so often trapped.

As a result, when considered along the lines of Bacchi's second question, the emergence of a pattern becomes apparent in relation to the problematisation of cybersecurity challenges.[618] It becomes possible to see how such problematisation is presented as objective and novel to some degree. And despite the purported need for individualised assessment, which ought to result in applicable or appropriate solution recommendations, such problem diagnosis would seem to remain built on certain assumptions and presumptions of cyber

[615] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).
[616] Madhok (n 604).
[617] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).
[618] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10).

risk and threats, which produces recommendations that are rarely challenged or never challenged.

> The Group recommends that Commonwealth countries develop effective prevention strategies in co-operation with the private sector and civil society, having regard to the need for preventive measures to be co-ordinated internationally. Specific elements should include the development and maintenance of appropriate technical security measures, training directed at specific situational threats or risks, and educational and awareness raising programmes directed at general populations.[619]

In this regard, the narrative on the need for states to build cybersecurity capabilities and create public cyber awareness, is emphatic and loaded with empowering discourses. This seemingly situates individual state needs, based on its unique status and problems, at the centre of key decisions made with regards to the type of solutions offered:

> Knowledge sharing and dissemination can take place through both training workshops and through formal and informal networking among participants at the national and regional levels. Regardless of the approach, it is important to promote beneficiary involvement to ensure sustainability and ownership, and to tailor the training session depending on the needs of the various stakeholders.[620]

Therefore, emphasising individual risk through the acknowledgement of state's ownership of the problem and choice, allows individual responsibility to

[619] Commonwealth and Law Ministers and Senior Officials (n 28). [8]
[620] The World Bank and United Nations (n 459). [235]

emerge.[621] Thus, the emphasis becomes less about such factors as poor digital infrastructure and the lack of human capacity, albeit forming part of the key focus, which directs attention to the social-economic divide and structural institutional weaknesses of the individual states. Rather, the conduct of states and their choices remain central to the attention given to the solutions offered.[622] These choices also enable their classification, into those that are conforming, and those that are not. Here, the former is perceived as progressive and liberal and thus, on the side of the 'good', while the latter is tagged authoritarian, oppressive, and treading evil lines.

> You've got authoritarian regimes including North Korea, Iran, Russia and China using digital tech to sabotage and steal, or to control and censor. And perhaps we saw that most ruthlessly recently when the military junta shut down the internet in Myanmar.[623]
>
> So our challenge is to clarify how those rules apply, how they are enforced, and guard against authoritarian regimes bending the principles to meet their own malicious ends.[624]

Arguably, cybersecurity challenges in developing states are continually positioned as a matter of developmental choices that individual states make. The general acceptance of discourses around the democratic processes, for example, the endemic corruption within the governments and their lack of focus on

[621] Pat O'Malley, 'Risk and Responsibility' in Andrew Barry, Thomas Osborne and Nikolas Rose (eds), *Foucault and Political Reason, Liberalism, Neoliberalism and Rationalities of Governmentality* (The University of Chicago Press 1996).

[622] ibid.

[623] Dominic Raab, 'CYBERUK Conference 2021 : Foreign Secretary ' s Speech', *How the UK will lead internationally in protecting the most vulnerable countries* (National Cyber Security Centre 2021). [6]

[624] ibid. [12]

creating sustainable and lasting economic and political systems that could aid better security preparedness.

Thus, certain demands are made, often from those in the knowledge (power) position, that calculatedly emphasise choice rather than mandate. However, the reverse would seem the case in reality. The Budapest convention on Cybercrime for example, recommends that all states ratify and sign, to become party to the convention. A demand that requires states' consideration for the purpose of what it represents, as opposed to mandating them to do so:

> The United Nations General Assembly recommended that UN member states use existing frameworks, including the Budapest Convention to "ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime".[625]
>
> With the Budapest Convention on Cybercrime an instrument providing guidance is already available and widely used by countries of all regions of the world as a benchmark, as recommended by the UN General Assembly (Resolution A/RES/64/211).[626]

But, once such a convention or treaty is held as the *de facto* authority, along with the associated discourse (or reality, to put it more objectively) of cybersecurity issues, very few countries, if any, will consider it otherwise, or have any real choice to do so. Particularly once such treaty is held and recommended as the *de facto* norm by the elite states. This happens first, through the

[625] Council of Europe and Data Protection and Cybercrime Division of the Council of Europe, 'Global Project on Cybercrime - The Cybercrime Legislation of Commonwealth States : Use of the Budapest Convention and Commonwealth Model Law' (2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb rev_final_CoE.pdf> accessed 6 September 2022. [16]

[626] ibid.

normalised reality of the problem – in other words, the reminder or embedment of the threat discourse. And second, through the established status of the elite states and promotion of their own agenda via various funded initiatives. Third, the autonomy of weaker states is eroded by the digital reality they face, and the economic structures that underpins it. And as officially expressed by the Attorney General of Australia during a 2011 Council of Europe convention on cybercrime, Australia's interest in being party to the Budapest convention is encouraged "simply because the modern ever-changing world demands it".[627] And there is simply no running away from that, else, one risk being included in the 'other' classification.

Therefore, the power of choice is really in the hands of those who can affect, or determine such classification. Practical and efficient co-operation does appear central to the drafting of such conventions, as well as other proposals for solutions to cybersecurity problems and capacity building initiatives. This also suggests a sort of 'in-it-together', or 'collective responsibility' discourse ('collective', only of those who comply or are willing to comply). An example can be cited in the convention's Articles 24 and 35, where it stresses the need for a global central co-ordination point, through which, members to the convention are required to provide support and assistance to one another on a real time, and round-the-clock basis.[628] Suffice it to say, that the cybersecurity discourses are prominent with this sustained narrative of the necessity for such collective spirit. The recent ITU's 2020 index also draws reference from the challenges of the

[627] ibid.
[628] Convention on Cybercrime 2001 (European Treaty Series - No 185) 6.

current global health pandemic in its reassertion of the importance of such need for cooperation:

> One of the lessons from COVID-19 is that collective action problems like health or cybersecurity, need to be tackled with an interdisciplinary and holistic approach. Tackling all pillars of the GCI – legal, technical, organizational, capacity development and cooperative measures – will require connecting people to each other and building trust. Beyond working together within countries, countries may need to support other states less able to address cybersecurity challenges, such as least developed countries, small island developing states, and landlocked developing countries. [629]

Thus, there remains an inherent or implied notion of both individual and collective responsibility that is unavoidable in these suggestions, recommendations or claims to uphold an individual country's sovereignty. After all, it is the responsibility of a sovereign state to secure and protect its 'territorial infrastructure' and population against attacks of any sort, cyber or otherwise. But at the same time, acknowledging the cross-jurisdictional nature of this problem makes the case for the collective responsibility an equally viable one.

The issue of the cross-territorial nature of cybersecurity problems which creates the need for states cooperation will be discussed in more details in the next chapter, where the power effect (solving the problem) function will be looked at. However, it is deemed worthy of a brief mention here in this chapter as it plays a part in the diagnosis stage through its ability to help justify recommendations and offer solutions.

[629] International Telecommunication Union (n 139). [24]

6.3 Normalisation of cybersecurity challenges and assessing needs

Normalisation ('legalisation') of cybersecurity threats and challenges is a process that is intrinsically linked to the notion of apportioning responsibility to the risk presented.[630] Again, the focus of this exercise is less about determining the positives and negatives of cybersecurity issues, or adjudicating between the various methods by which the issues are resolved. Neither is it about providing graded classification between how thoughts around such issues are framed. Rather, the goal remains that of examining how such framings are made possible and for what purpose. As such, the discussion within this chapter remains less about assessing the various cybersecurity capacity building initiatives in terms of how well they work, or whether or not they are fit for purpose. Rather it concerns itself with how they are made possible while at the same time, attempting to unravel the ends that they are designed to justify.

One way cybersecurity capacity building practices discourses are made possible is through rationalisation of the problem which leads to the normalisation of cybersecurity challenges to start with. Normalisation itself is necessary to allow for the acceptance of the problem which subsequently sets up the problem for a 'fix'. Antonio Reyes lays out a few strategies by which political and social practices are normalised or legalised (using both words interchangeably), and how this process is achieved through discursive

[630] Antonio Reyes, 'Strategies of Legitimization in Political Discourse: From Words to Actions Introduction: Legitimization in Discourse' (2011) 22 Discourse & Society.

construction and framing of the issues and solutions.[631] One of such strategies involves the deployment of emotions, or "the appeal to emotions",[632] as they put it. This allow perceptions of an issue to be skewed or orchestrated towards a particular outcome.[633] It involves, for example, how actors are represented and the attachment of different qualities to them based on who they are and the actions they perform in the problematised field:

> Several Commonwealth countries, such as the UK, Singapore and Canada are leading examples Index of 2018 (The Economic Times 2018), and some other Commonwealth countries (such as Kenya, Rwanda and South Africa) have shown significant strides in digital transformation. However, 31 out of 53 Commonwealth countries are classified as 'small states' and continue to face considerable challenges in terms of internet adoption, e-governance, the high cost of technology, lack of digital infrastructure, limited human capital and a weak private sector. According to the latest United Nations E-Government Survey (United Nations 2012), more than half of the Commonwealth's small member countries (17 out of 31 states) are ranked in the bottom half of the rankings in terms of their online government services. ICT penetration in these economies is affected by their unique geographic, demographic, social and economic challenges, and is marked by small populations spread over large geographical areas, low levels of skills, high vulnerability to natural disasters and climate change. [634]

As a result, a 'them' and (or versus) 'us' narrative (of a more cynical and even sinister nature) also starts to emerge. The use of the 'them' and 'us' discourse, as briefly hinted above, is evident and often presented in numerous authoritative texts that centres around cybersecurity issues, such as strategy

[631] ibid.
[632] ibid. [788]
[633] ibid.
[634] The Commonwealth, 'The State of the Digital Economy in the Commonwealth' (The commonwealth secretariat 2020). [24]

documents, policy guidelines, reports and speeches. The presence of such proclamations seldom reflect anything else other than that which are aimed naturally to portray both negative and positive qualities of actors, depending on which side of the 'them' and 'us' group they belong. For example, cyber criminals and all other such actors, including 'rogue' states, both in cyber space and the physical world (rogue by virtue of being subjectively portrayed as such), falls under the negative connotation of the 'them'. The rest, those seemingly trying to do something about the problem, are framed positively as the 'us'.

In reality, this sort of discourse, as observed within the data, is played out in most speeches, reports and policy documents sampled. The UK Foreign Secretary's speech at the 2021 CyberUK conference, for an example, demonstrates this succinctly.[635] While seemingly proud of the UK's technological prowess as a global "massive force for good",[636] they painted a picture of polarising identities of global actors in cyber space, with the 'other' or 'them' group representing a darker 'evil' force:

> The Integrated Review highlighted the increasingly competitive world we live in, and the clash of values that is playing out today between the countries that want to protect and preserve a system based on open and outward looking societies, and those on the other hand who are promoting an authoritarian international system.
>
> We can see this clash between authoritarian and democratic states playing out very directly, right now, in cyberspace.

[635] Dominic Raab, Foreign Commonwealth and Development and National Cyber Security Centre, 'CYBERUK Conference 2021: Foreign Secretary's Speech - GOV.UK' (*gove.uk*, 12 May 2021) <https://www.gov.uk/government/speeches/cyberuk-conference-2021-foreign-secretarys-speech> accessed 4 September 2022.

[636] ibid.

> You've got authoritarian regimes including North Korea, Iran, Russia and China using digital tech to sabotage and steal, or to control and censor. And perhaps we saw that most ruthlessly recently when the military junta shut down the internet in Myanmar.[637]
>
> These hostile state actors and criminal gangs want to undermine the very foundations of our democracy.[638]
>
> And let's be clear, when states like Russia have criminals or gangs operating from their territory, they cannot hold up their hands and say [its] not them but they have a responsibility to prosecute them, not shelter them.
>
> These cyber-attacks pose a real risk on a daily basis, because what they really want is to undermine our confidence in doing simple things, like checking our bank balance or paying for a food order online. So, we've to adapt to that threat, not just to defence to defend our way of life.[639]

Conjuring up this negative 'them' or 'other', and the positive 'us or 'self' through specific discourse or practice, not only allow for further visibility of the problem, but also suggest a perceived knowledge of the problem. This helps bring the problem to its normalised life, facilitating the acceptance of proposed solutions to the problem. For example, the Foreign Secretary provided accounts through statistical data to allow for the problem to be seen, while employing statements such as the one above to ensure that a certain line of thought about the problem is sustained, through strategies that identifies the 'whys' of the problems, serving as a precursor for the actions to follow:

> Against that backdrop, let me set out three practical concrete ways in which we are upping our game … first, we are building our domestic defences … We're not just going to guard against attacks, we are going

[637] Raab (n 623). [8]
[638] ibid.
[639] ibid.

> to target and impose costs on those who are taking aim at us. …. ultimately, the difference between us and our adversaries isn't just about our capabilities. It's about how we choose to use them…. We demonstrate respect for international law. And we use our capabilities to defend our citizens, to safeguard international collaboration as a force for good in the world. Whereas our adversaries use their cyber power to steal, to sabotage and to ransack the international system. And that brings me to my third point which is how we are working with like-minded partners, to make sure that the international order that governs cyber is fit for purpose.[640]

Here, we see that actions that would otherwise be considered negative and evil or aggressive when pursued by a 'them' group, is normalised through such expressions as: 'ultimately, the difference between 'us' and our adversaries isn't just about our capabilities. It's about how we choose to use them. We demonstrate respect for international law'. Thereby, suggesting the use of selective moral judgements which assert that, as long as such aggression is coming from 'us' (respecters of the law), such actions are deemed positive and normal because 'we', as the civilised West, the global gatekeepers, use such offensives to defend the international order or alliance of the 'us'.

A second normalisation strategy according to Reyes, is executed through the creation of a hypothetical future.[641] In the case of cybersecurity, this demonstration of a hypothetical future can be seen through the positioning of a threat-based future, where the likely negative or tragic future consequences of cybersecurity problems are drummed-up to emphasise the urgency for action.

[640] ibid.
[641] Reyes (n 630).

> An important aspect in the developmental process of a national cybersecurity strategy is having a clear set of objectives on the protection of critical infrastructure. Ensuring continuity of operations at the national level is an ongoing challenge for countries. Critical infrastructure, such as electrical grids, water purification plants, and transportation systems, continue to face cybersecurity risks. The potential consequences of an incident impacting critical infrastructure are high, and the strategy should result in greater attention to risk management efforts intended to reduce the likelihood and escalation of a high-consequence event..[642]

We can observe thus far, the equating of the need for action to the need to build capacity to deal with the problems of cybersecurity. Problem normalisation discourses like these establish risk and threats as solvable problems, but only if states rise to the challenge and grow their cyber defence (and offense) capacity and capabilities.[643] Otherwise, states risk creating a future haven for cyber criminals, or risk being grouped amongst the 'them', or considered sympathisers of such group. Hence, the need for certain states to be perceived as aligning with the 'us', through willingness to develop their capabilities, adopting the required legislative instruments in the process and building their law enforcement capacity at the same time, and so on.

Historical precedents play a part in this sort of discourse that is aimed at a hypothetical future. For example, the use of calculative references to past attacks and their consequences and hence, the possible future disruptions as

[642] International Telecommunication Union (n 139). [9]

[643] Nir Kshetri, 'Cybercrime and Cybersecurity in Africa' (2019) 22 Journal of Global Information Technology Management 77 <https://www.tandfonline.com/action/journalInformation?journalCode=ugit20>.

attackers grow in strength and improve their attacking prowess. Again, an example of this can be seen in the same speech by the UK Foreign Secretary:

> As you'll remember on this day, 4 years ago, computers across the NHS suddenly flashed up a red screen. With an image of a padlock and the words: "oops, your files have been encrypted." There was a demand for a bitcoin payment, and 2 countdown clocks. One for when the ransom demand would be doubled, and another for when the files would be permanently destroyed. Staff were locked out of the computers they use to access records and book appointments. They couldn't operate MRI scanners, blood-storage fridges, and even operating theatre equipment were knocked out. This was the so-called WannaCry attack.[644]

It is important to note that, rationalisation also represent another form of normalisation strategy, and often operate alongside this conjecture of a hypothetical future. Its purpose, in this regard, is to seek justification through reason, to rally support for its agenda,[645] as demonstrated within this quote :

> If these people had actually turned up and mounted a physical attack like this in the real world, there would have been outrage with camera crews and public debate …. But think about it for a moment. In an age when there are three and half billion people on smartphones around the world. When we go online to shop, bank and stay in touch with our friends and family. When MRIs and other hospital equipment is computerised. When your fridge can tell Asda that you're low on milk. And when almost everything has a digital dimension. At what point do we wake up and realise that online is a major part of the real world that we live in. And that's why it's so vital that we adapt.[646]

Normalisation through rationalisation is typically evident in a seemingly transparent demonstration of specific processes and procedures that are used to arrive at whatever decision or recommendations that is being proposed. Its goal

[644] Raab (n 623).[1-2]
[645] Reyes (n 630).
[646] Raab (n 623). [2]

is to suggest or appeal to the reasoning of recipients, of the ‘thoughtful and evaluated’ steps taken to produce the presented outcome. Along these lines, in the case of cybersecurity capacity building efforts, and as expressed by Reyes, rationalisation ought to be seen as a form of “*modus operandi* defined and shaped by and from a specific society”.[647]

Take an example of the specific case of capacity building programmes to support developing countries in their fight against cyber insecurity. While their blueprints, are shaped around the defined and expected capacity levels of Western states, discourses around their recommendation for use by less developed countries are often constructed around the need to make them relevant to the target society. In other words, clear narratives are often expressed through such recommendations, which suggest the need for adaptations based on the society in which they will be used or applied. This is a form of rationalisation which seek to appeal to the reason of the general audience, but more specifically to the targeted audience.

Thus, it allows statements like the need to ’consult and work with the local governing authority' to be perceived as rational. Because it suggests that careful considerations are taken to ensure the needs are specific to the target region, before deciding on the final flavour of support to provide. But crucially, it is also designed to create the perception that the target remains the most

[647] Reyes (n 630). [786]

important consideration in the plan, and that all efforts are focused on guaranteeing the benefits to the target state.

Examples of this are observed in the various support initiatives. In its own release, the Commonwealth describes the CCI as one which "seeks to leverage the strengths of its individual partners to address Cybercrime needs of individual countries in a cohesive manner".[648] And as part of its approach, the initiative is expected to:

> (i)Conduct independent, holistic needs assessments for developing Commonwealth states in terms of their capacity to address the threat from cybercrime (covering all components from national strategy and legal framework to CIRT and public awareness); (ii) further a needs assessment, and where the necessary level of state commitment is identified, to co-ordinate comprehensive, long-term programmes of assistance, harnessing the motivations of governments, international organisations and the private sector;[649]

The CCI's overall methodology, which lays emphasis on assistance, based on the needs of the individual developing Commonwealth state, is perhaps best demonstrated in the quote below from an Octopus conference presentation on the initiative's first project in Ghana:

> In January 2012 the Ghana Ministry of Communications requested CCI's assistance in developing a cybersecurity strategy and the establishment of a national CIRT. In the following month the CCI sent out a team from SOCA, ITU and ICSPA to conduct a Needs Assessment. In April 2012, the CCI submitted a Needs Assessment Report to the Minister and in August 2012 the Minister submitted a further and more developed request for assistance in line with the Report's recommendations. This was shared with the partners with the result that offers of assistance and/or funding were identified against all elements of the request. In January 2013 the CCI sent the proposal to

[648] Commonwealth ICT Ministers (n 54).

[649] Commonwealth and Law Ministers and Senior Officials (n 28). [34]

> the Minister and in April 2013 a meeting took place in which the proposals were discussed and agreed. These included a University Partnership to promote joint research and training programmes; assistance in establishing a CIRT with ITU; assistance from SOCA and the CPS in conducting a resource and training needs analysis for the criminal justice system; and a scheme in which the IWF will provide a reporting line for child abuse images.[650]

Similar needs assessment in other developing Commonwealth states, including Trinidad and Tobago and Botswana, were conducted, expressing the desire to tailor support to individual states, based on their needs rather than that of the funders:

> More recently Needs Assessment teams have been established to examine requests from Kenya, Trinidad and Tobago, The Gambia and Uganda. [651]
>
> Training is an essential element in the building of capacity against cybercrime, but it is important to bear in mind that there are no 'one size fits all' solutions. What is appropriate depends on a number of considerations.[652]

Despite the importance of this strategy of appealing to reason employed in this way, the display of expertise and understanding of the problem also allows for a generalised normalisation and acceptance of the problem regardless. This then grants certain authority to some actors, thereby strengthening their position of power in the process. [653] This may be the case, irrespective of whether

[650] ibid.Colin Nicholls, 'Coopration Against Cybercrime', *OCTOPUS CONFERENCE 2013 - Workshop 1 : Policies , activities and initiatives on cybercrime of international organisations* (The commonwealth secretariat 2013). [5]
[651] Nicholls (n 650). [4]
[652] Commonwealth and Law Ministers and Senior Officials (n 28).[39]
[653] Raab (n 623).

or not the products of such knowledge are individualised or presented in the same likeness as desired by the one who created it, or the one offering the recommendation. Thus, it becomes more about the authority that such knowledge produces or reproduce through its deployment in the first place; something that may not necessarily be obvious.

Evidently, in the case of cybersecurity, this authority comes from historical positions of expertise, occupied by certain states and institutional actors, who have long established themselves as innovative and authoritative sources of cyber intelligence and power, guaranteed by their economic and political strength in global affairs. Again, this is exemplified in the UK's Foreign Minister's self-exhortation or magniloquence on Britain's cyber power ambition:

> So, we're good at this and it's not just a one off.... When it comes to business growth, the UK has the most tech unicorns in Europe.... So, the point I am making is innovation is in our DNA. And that's why the Integrated Review of foreign policy identified science and technology as one of our great strengths, which we must nurture and reinforce in the years ahead.... But don't forget that Belfast is a world-leading cybersecurity hub, and a top international investment location for cybersecurity firms.... The tech sector is thriving across the whole of the United Kingdom. So, it's not just at home but in 2019 we exported cyber products and services worth £4 billion.... So, UK tech creates jobs and protects our security. But it is also helping us to be an even stronger force for good in the world.[654]

Thus, it seems that, such claim to expertise and knowledge in turn, grants actors like the UK free reign on presenting information in a formal context, producing official and institutional discourses, and so on.[655] According to Reyes,

[654] ibid. [4]

[655] Reyes (n 630).

wielding such "authority constitutes a strategy to legitimise action,"[656] irrespective of how such authority was created, achieved or obtained.[657] Actors with authority as such, will therefore naturally remain more convincing with regards to their perceptions, thoughts and actions around global issues. Consequently, their influence on how global issues like cybersecurity are resolved, their recommendations for solutions, etc., will always be more valued and readily heeded by the less powerful states.[658]

In the preceding chapter, we see how the use of calculative practices, derived from statistical data, allow for additional validation of this authority, particularly as such actors are able to display some levels of "precision and exactness" through numbers.[659] Thus, the display of such knowledge reinforces their ability to identify and highlight the problem, normalise the challenges it creates, provide 'trusted' diagnosis of the problem and finally, allow for the design of solutions to the problem that are ultimately uncontested and willingly accepted, whether or not such solutions are indeed appropriate for the target.

Such is the sentiment that was clearly observed by consultants at the Council of Europe, who carried out a review of the use of existing cybercrime model laws at the time, in "the context of the only existing and effective global

[656] ibid. [786]
[657] ibid.
[658] Susan U Philips, 'Language and Social Inequality' in Alessandro Duranti (ed), *A Companion to Linguistic Anthropology* (John Wiley and Sons Inc 2007).[475]
[659] Teun Adrianus van Dijk, *News as Discourse* (L Erlbaum Associates 1988).[84]

treaty on cybercrime, the Budapest Convention".[660] They observed that there were:

> States, in particular those that possibly lack the necessary skills to draft cybercrime and electronic evidence laws, which rely upon such divergent or poorly drafted models laws are likely to incorporate these into their legislation. They may do so under the mistaken belief that since these models appear to be supported by international organizations, they represent a certain level of quality and international best practice. Having gone through the arduous process of drafting and passing legislation they may come to realize, possibly when they seek to cooperate across borders with law enforcement or seek their cooperation that they face challenges due to their having followed such poor and divergent model laws.[661]

Indeed, the display of all the above strategies in the normalisation of cybersecurity problems, can also be conveyed altruistically.[662] In other words, there is almost always a conscious effort to ensure that, neither the analysis of the problem, its diagnosis, nor the proposed recommendations, are conveyed in such ways as to suggest that they are, indeed, driven by individual state or institution's interest.[663] Rather, they are often framed as serving the interest of the 'other' (receiving party), the region or the entire global community.[664]

According to Rojo and Dijk, such actors' call-for-action, the design of policies, guidelines, the setting up of new frameworks, and the need for any other form of actions of governments and international institutions, are usually framed such that, it portrays the benefit of doing so, to the targeted state, the entire

[660] Jamil and Council of Europe (n 31).
[661] ibid. [3]
[662] Reyes (n 630).
[663] ibid.
[664] ibid.

group, population, or global society.[665] As such, they may be directed towards certain communities within a state, or external communities elsewhere, where the notion of a moral responsibility to support those less fortunate societies or communities form part of the general overarching discourse. The discursive expression to be a 'stronger force for good', the differences that such efforts make in transforming lives of people in poorer nations, and so on.[666] Hence, the normalisation of cyberspace as a public and common domain and therefore, the perception of its problems and proposed solution as an equally shared responsibility and an act, directed towards a common good respectively.[667]

Thus, one finds in the case data, the identification and diagnosis of cybersecurity risk or vulnerabilities in developing states infrastructures that are strategically presented in such ways as to appeal to both reason and responsibility. Below, for example, instances of attacks are cited to generate this risk awareness:

> Mexico's Instituto Nacional Electoral (INE) filed criminal charges after an unprotected database of 90 million voter registration records was found hosted on Amazon Web Services. The institute suspected the data had been leaked by one of the political parties, which are given copies… An investigation showed the database had been accessed 2,400 times from 14 internet protocol (IP) addresses.[668]

[665] Luisa Martín Rojo and Teun A Van Dijk, '"There Was a Problem, and It Was Solved!": Legitimating the Expulsion of "illegal" Migrants in Spanish Parliamentary Discourse' (1997) 8 Discourse & society 523.[528]
[666]Raab (n 623). Rojo and Van Dijk (n 665).
[667] Raab (n 623); securityweek.com, 'UK Foreign Secretary Calls for Cooperation on Cybersecurity | SecurityWeek.Com' <https://www.securityweek.com/uk-foreign-secretary-calls-cooperation-cybersecurity>.
[668] The commonwealth secretariat (n 552). [38-39]

The ensuing diagnosis facilitates and encourages the need for states to plan, and be prepared for future eventualities. As such, security vulnerabilities or insecurity becomes embedded in the normative understanding of what security practice or behaviour is, and what it means to be exposed to these security risks. In other words, security vulnerabilities become equated to economic status which results in unprotected or poor security behaviour or practice, in such a way that it suggests that certain state behaviours, their attitude towards cyber risk and poor security practices, form part of a challenging 'global one society' ideology amongst actors.

> priority for governments of some developing countries with limited budgets. Some Caribbean countries, for example, need to prioritize investment in housing, protection from natural disasters, or improving the physical security of critical infrastructure, before they can invest in cybersecurity. Therefore, the provision of international support to Caribbean cybersecurity capacity-building is essential.[669]

As such, there is a normalisation of not only the problems and proposed solutions, but also the normalisation of what constitute responsible choices in relation to security practices. This is done by demonstrating the irrationality or consequence of lax security or allowing oneself to remain vulnerable.

> Cybersecurity capacity-building requires investment and momentum. Therefore, the political leadership of a country must be convinced of the importance of cybersecurity and of the risks of not prioritizing it. Political support for prioritizing cybersecurity must be maintained throughout political change.[670]

[669] Chatham House's International Security Department, 'Cybersecurity in the Commonwealth: Building the Foundations of Effective National Responses in the Caribbean', vol 44 (2019) <https://www.lacnic.net/1030/2/lacnic/initiatives> accessed 25 September 2021. [3]

[670] ibid.

Undeniably, this is augmented further through demonstrable claims to knowledge about the problem, and knowing how best to tackle it, how to put in place security best practices, what capacity shortcomings need to be addressed, and so on. Because the poorer states are not in positions that enable them to contest such claims to knowledge, proposals for solution are also easily acknowledged and accepted:

> Renewed engagement with the government of Ghana has brought about presidential endorsement of the CCI programme in the country. A comprehensive resource and training needs analysis for the criminal justice system is being conducted in collaboration with the United Kingdom Crown Prosecution Service, and university collaborations have been set up between the countries to develop technical skills. The CCI is [also] working closely with the International Telecommunications Union in Ghana. An official launch for the programme bringing together all stakeholders is scheduled for March 2014.[671]

The normalisation of certain practices as rational, on the basis of being perceived, or proven positive ability to improve or build capacity, creates a further representation of the problem that queries and determines what falls within or outside of the acceptable norm of security practices. It produces a continued binary conceptualisation of the 'them' and 'us'. A conceptualisation that runs through all the various strategies of normalisation described above, determining the constant production of two sides and/or groups or perspectives that enables the 'otherness' to be reproduced on an ongoing basis. Such conceptualisation allows for the observation of the Foucauldian concept of

[671] Commonwealth and Law Ministers and Senior Officials (n 28). [3]

rejection and division within such construction.[672] And as observed by Rojo, within this Foucauldian concept, while division enables the internalised ‘us’ and the exclusive external ‘them’, rejection on the other hand, encapsulate the ideological state of the ‘other’ as irrational, immoral, evil, that ought to be kept at arm’s length.[673]

As exemplified by the Foreign Secretary’s speech cited earlier, there is a sense of attribution of value or performance by the opposing groups. Actors diagnosing the problem and/or recommending actions or laying claims to knowledge of the problem, and therefore offering solutions to the problem, clearly see themselves as belonging to the ‘us’ group: the group with the disposition to “performing rational, moral, correct and respectful behaviour, and fights for the right cause (democracy, freedom, the innocent, defenceless and suffering people, etc.)”.[674]

Thus, the separation and rejection of the ‘them’ from the ‘us’, by the ‘us’ group, is constructed through what the other (‘them’ - hackers, hostile states, cyberterrorist, cybercriminals, authoritarian state, etc.) represents in the mentality of the ‘us’ or ‘self’ group. As such, the discourses are validated through their powerful influences within the global institutional authorities, their league of nations or alliances such as the Five Eyes, the Commonwealth of Nations, the European Union, NATO etc. This power and influence, allows them to be

[672] Foucault, *The Archaeology of Knowledge & The Discourse on Language* (n 36). See also Luisa Martín Rojo, ‘Division and Rejection: From the Personification of the Gulf Conflict to the Demonization of Saddam Hussein’ (1995) 6 Discourse & Society 49.
[673]Rojo (n 672).[50]
[674] Reyes (n 630). [788]

represented ultimately as truth, creating a dramatized reality of the problem and provoking fears and worries as a result.[675]

Therefore, the question of why cybersecurity capacity building matters, and who or what security practices fall within or outside the norm, becomes one that establishes individual or collectively-based construction of morality that sees prudent actors' behaviour as the norm, or see their perceived prudent practices as acceptable, while anything else is rejected.[676]

Ultimately, the relevance of such perceived notion of prudence-based practice is that it creates a link between the 'positive' practice of the 'us' group, and the feeling of responsibility that goes with it, both individual and collective. Thus, and to summarise this based on O'Malley's conceptualisation, the governing rule of prudent and responsible practice, therefore, serves mainly to situate the problem of cybersecurity within developing states, through its power of knowledge claim.[677] That is, its ability to determine what needs to be diagnosed, what sort of capacity deficit exists, and what needs to be prioritised, etc.[678]

[675] Renaud and others (n 381).
[676] O'Malley (n 621).
[677] ibid.
[678] ibid. see also Renaud and others (n 381).

6.4 Conclusion

As a technology of government, the diagnosis phase of the problem of cybersecurity, which has been exemplified in this chapter through the process of determining the capacity needs of certain countries, implies the normalisation of cybersecurity capacity building practices as a matter of rational decision or thought, rather than a perception of it being a discursive practice that is entirely rooted in relations of power. The appeal of these practices seem based on reason, established to provide certain levels of robustness or preparedness for states, in order to assist them with the challenges they face, and to mitigate against future risk.[679] This observation, when viewed objectively, suggests nothing other than that, which is visible or obvious. Nonetheless, it also suggests the need for further questioning when examined through philosophical lens as has been attempted here, through conceptualisations that implies the presence of an underlying rationality underpinning such practices.

Thus, associating cyber capacity building with the notion of rationality and responsibility is underpinned by the assumption that if poorer developing countries are given access to adequate knowledge about how to deal with the problems of cybersecurity, then certain rational order of things may logically follow. This is somewhat like the saying that, if you teach the hungry to fish, you would have fed them forever. What rationalisation does here in this regard is that it allows for a certain connection to be made such that, when that, which is

[679] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10). See in particular, Q3 and Q4

informed by the knowledge impacted, and that which is considered the norm or best practice is implemented, underlying behaviours, practices and actions, irrespective of what they imply, becomes invisible.

Consequently, certain historical, economic, social and political privileges, advantages, exclusivities, enjoyed by certain groups, which continue to sustain what is considered best practices or acceptable cybersecurity choices, are also concealed and overlooked. Thus, the process of normalisation regulates or controls how the differences are determined – what is best practice and what is not. And it does so through the narratives of individualised risk and the responsibility, which occupy our thoughts and render the idea (whatever idea is been pushed) justifiable.[680] The relevance of this framework of thought, and/or the control of it, evident in the implementation of actions designed to solve the problem, will therefore form the focus of the next chapter.

[680] ibid; Bacchi, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (n 5).

7 The power effect: Cybersecurity and the politics of international cooperation – political and legal perceptions vis-à-vis agency

7.1 Introduction

The focus of the discussion thus far, centres around cybersecurity problematisation as a phenomenon that is made visible; that is, as a phenomenon that is measurable, monitored, calculated, represented and presented as an ongoing concern. The representation of a cybersecurity problem as a diagnosable phenomenon has been discussed as a rationalised concept that is tied to normative constructions of security or insecurity. Thus, the last two chapters sought to unravel both the visualisation and rationalisation of the problem as necessitating certain forms of action to resolve. This examination of the problem visualisation and rationalisation is relevant as it allows for the analysis of cybersecurity representation and enables our understanding of the conceptualisation of the problem within government and institutional texts.

Particularly important is the understanding of such texts as that of 'knowing', or their interpretation of situations that have evolved into something that is problematic or perceived as such.[681]

Knowing or acknowledging that a problem exists, therefore, represents the first step towards efforts to try and diagnose or understand the problem, before attempting a solution. Hence, and in line with Dean's framework, the focus of the preceding two chapters centres on discourses and practices designed to create, first the truth effect, through the desired visibility of the problem, followed by those geared towards building certain rationalities around the problem to establish the norms effect. This paves the way for the examination and further analysis of discourses and practices around solutions, both proposed and implemented, as 'actions' to deal with the problem of cybersecurity and their construction of the power effect.

In line with the focus of the study, the discussion is not aimed at establishing the quality of these solutions, or the value that they present in terms of how effective they are at dealing with the problem (such as their success in developing highly skilled technical capabilities or creating a robust legal framework to deter and deal with cybercrime, for example). Instead, the interest of the discussion, in line with Foucauldian problematisations, is to examine such solutions as forms of 'governing', carried out through thoughts and actions.[682]

[681] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).
[682] ibid.

In doing so, a return to Bacchi's initial question is necessary: that which establishes the problem and queries the data on what solutions are being proposed to solve the 'problem', and how (and perhaps why) the solutions emerge in the first place.[683] As argued by Bacchi, since one's perception of the problem determines what is ultimately proposed as a solution, it is equally true to say that analysing what is 'a solution', "will reveal how the issue is being thought about".[684] In other words, how do solutions to the problem materialise and evolve during the course of 'dealing' with the 'problem'?

In interrogating the data, and examining proposed solutions to the problem of cybersecurity, particularly as it relates to poorer developing states, one must note that such solutions, in terms of actions and how they are constituted, form parts of the discursive field or context, created by those with knowledge, that are ultimately established as truth.

Multiple solutions to the problems of cybersecurity are often proposed and/or implemented by various actors, and may appear individualised at times. This is based on the understanding that every individual state is unique (to a degree) and, thus, they present differing knowledge, capabilities and problems. Nonetheless, it is also agreed that they remain connected to the same discursive *milieu*, where the problem has been identified and made visible, and therefore become 'known', established as 'truth' or 'reality.' As such, it becomes clearer to see how actionable recommendations constitute prescriptive proposals, as they

[683] Bacchi, 'Problematizations in Health Policy: Questioning How "Problems" Are Constituted in Policies' (n 423).
[684] Bacchi, *Analysing Policy : What's the Problem Represented to Be?* (n 10). [3]

are designed to remedy the situation, and appear to come from a position of knowledge and authority (power).[685] In other words, they constitute further knowledge-producing proposals and actions that expand and extend the discourse even further. At the same time, they expand the fields of practices, from among the various knowledge actors (leading to the need for further data collection, continuous capacity assessments, further recommendations, proposals and actions):

> The GGE and OEWG present opportunities to gather more evidence on the harm that attacks cause and bolster this knowledge base. This is particularly the case since threats in cyberspace have various impacts on different states. For example, while one country may consider an attack against its critical national infrastructure as the biggest threat from cyberspace, another country, with a lower level of digitization, may view the impact of disinformation and fake news on its democracy as a greater threat.[686]

Since this creates a continuous expansion of fields of action, the claim to knowledge or truth is also allowed to establish itself further within the discursive space. The question, therefore, remains: what further impacts are produced as a result? In trying to provide answers to such question, first, certain actions or claims to knowledge that are evident within the research data will be discussed. Notably, those which suggest techniques of government that rely on such claims to advance the power dynamics. Second, the notion of freedom is examined against given data, in relation to the purported freedom of states to make their own choices. This is done in order to understand how 'freedom' may represent a

[685] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).

[686] Chatham House's International Security Department (n 572). [6]

kind of tactics of 'government'. Finally, contrasted against the notion of freedom, that is in turn guided by an obligated responsibility to act, the promotion of international collaboration or cooperation as a key action in response to cybersecurity challenges is queried, to reveal its role within the 'governing' process.

7.2 Establishing technologies of 'government' – knowledge and power

With various solutions targeting developing states' cybersecurity problems, an increase in new forms of data monitoring and calculative practices can be observed with varying forms of expert opinions being presented. This creates further expansion of the discursive space, as well as the 'governable' spaces in relation to cybersecurity. It establishes a sort of knowledge-action nexus that enables further knowledge control relation between actors. However, actions proposed as solutions may not necessarily present limitless power for those actors within the knowledge group. Neither does it explicitly suggest the presence of such a knowledge-control relation. Rather, knowledge control is often implied, through its focus on establishing a certain discourse that suggests for example; knowledge sharing, knowledge transfer, 'shaping' or establishing the necessary frameworks (and behaviours) through education and collaboration – direct training through workshops, providing guidelines and materials for developing national frameworks, including templates and model policy documents and model laws.[687] In other words, sharing a particular knowledge, or attempting to shape one in the image of another, suggests representation and acceptance of the shared knowledge as truth, thereby according it a certain level of *de facto* status:

> International cooperation, particularly through knowledge sharing and capacity-building efforts was again raised as an essential requirement for overcoming the identified challenges to cyber governance.[688]
>
> Sharing experience on e-governance and smart cities: Commonwealth initiatives by small states, coupled with knowledge sharing on both a north-south and south-south basis, by leading digital Commonwealth states, can help foster development. The sharing of lessons and best practices in e-governance can further help the process.[689]

The sharing and acceptance of knowledge as the-go-to solution is not, by itself, a terrible thing. To suggest otherwise would mean failing to recognise the benefits of such endeavours. Knowledge sharing has its place, and its benefits cannot be overstated. However, while recognising this fact, there remains a need to understand how such endeavours might shape relationships emerging from such activities. In other words, how the positions occupied by the different actors within this relationship, may impact or dictate the global or default order of things. The Commonwealth cyber governance model, for example, which was drafted following the Abuja convention in 2013, spells out principles, designed to guide Commonwealth states in their planning and implementation of “practical actions in policy development, regulation and legislation, cross-border

[687] Foucault, *The Archaeology of Knowledge & The Discourse on Language* (n 36).
[688] Chatham House’s International Security Department (n 572). [5]
[689] The Commonwealth (n 634). [20]

collaboration, capacity building, technical measures and other operational activities."[690] Within these guidelines, education, and cooperation form key parts of what is advocated as critical to solving the global cybersecurity challenges.

Observing this critically, the need to educate the recipient group, assumed by the donor group, already suggests a knowledge gap that could be filled through learning from, and collaborating with, those who already know. In the case of some developing Commonwealth states, the level of this knowledge gap may be as wide as can be, from total beginner to advanced, since many such countries had near to zero existing capacities. This therefore creates an imbalance in the knowledge sharing or knowledge transfer relationship, leading to actions based on almost one directional flow (from North to South, but never the other way round).

This form of action, for Foucault, can also be understood in terms of how the deployment of power is rationalised.[691] Put differently, it demonstrates how knowledge is used to deploy a certain power that allows those in possession of such knowledge to wield particular forms of power to achieve or promote desired objectives.[692] The existence of a knowledge divide, in relation to technology more generally, means that the fields of action, and, most importantly, the control of such action, is somewhat restricted to those with expert knowledge and proprietary ownership. Therefore, access to such knowledge is equally

[690] Commonwealth ICT Ministers (n 54). [1]

[691] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41).

[692] ibid.

controlled by those with the associated power, and by whatever *modus operandi* is set by them.[693] This in turn, leads to what Rabinow and Nicolas describes as "strategies for intervention upon collective existence in the name of life," applicable to security, health, and so on (often by those who trade the 'concerned' versus the 'vulnerable' card). [694]

For Rabinow and Nicolas, these sort of strategies, at the very onset, are directed towards global populations that "may or may not be territorialised" based on any given nation state or society, region or any specific community.[695] However, the attention of such strategies is soon specified and directed along the lines of what they call "biosocial communities", categorised by geography, race, religion, gender, ethnicity, and economic and political development status.[696] Thus, the process of rationalisation which is subsequently embedded in the risk discourse associated with such concern, allows for the transfer of responsibility. In other words, it allows for the mode of subjectification to emerge, by

> which individuals [within these collectivises] are brought to work on themselves, under certain forms of authority, in relation [to] truth discourses, by means of practices of the self, in the name of their own life, or health, that of their family or some other collectivist, or indeed in the name of the life, or health of the population as a whole. [697]

[693] Paul Rabinow and Nikolas Rose, 'Biopower Today' (2006) 1 BioSocieties 195.
[694] ibid. [195]
[695] ibid. [197]
[696] ibid. [207 and 211]
[697] ibid. [197]

As described by Rabinow and Nicholas, this process engages the discourse in two dimensions: 1) a causal one, which attributes the cause of the problem or risk, albeit sometimes subtly, to certain individual actions or omissions. 2) a moral dimension demanding an equally moral obligation to act, not only for the sake of the individual, but for the collective good of all.[698] The second dimension therefore, triggers action or a 'call to action' from amongst all, to all actors. Indeed, this appeals to everyone, stressing the need to act, not just individually, but collectively and in unity for strength; emphasising the need to form partnerships, build alliances and collaborate in implementing these actions.

What this mode of subjectification does, therefore, is that it creates an illusion of a common response to a common risk, threat or problem, regardless of who possesses the knowledge to respond. Hence the usual emphasis on inter-agency and inter-state cooperation, and the need to support those lacking, through various initiatives:

> Failure to actively collaborate and share information might leave the country isolated and vulnerable to threats. There is strength in knowledge sharing and adopting non-binding norms that promote cooperation among the cybersecurity nations. [699]
>
> Enhanced knowledge might be accomplished through the networking of judges and prosecutors, and regularly making caselaw and other resources available… All states and institutions face difficulties in curating and disseminating knowledge. While creating special cyber units and cooperation mechanisms is important, standardized training, on-the-job training and ad hoc courses or informational bulletins for authorities at all levels can all be used to facilitate and

[698] ibid.

[699] Foreign Commonwealth and Development Office and The Commonwealth (n 575). [16]

> further the process. It is important that knowledge be shared as broadly and as routinely as possible.[700]
>
> The collaborative security approach to Internet security recognizes that people are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for its prosperity and potential. The approach emphasizes five principles: preserving opportunities and building confidence; collective responsibility; security solutions fully integrated with rights and the open Internet; security solutions grounded in experience, developed by consensus and evolutionary in outlook; and targeting the point of maximum impact – think globally, act locally.[701]

This mode justification renders the discourse in a sort of perception-shaping dimension, as it allows for a form of "genetic" global citizenship to emerge in individual thoughts, even from those at the lower end of the knowledge-power spectrum. Hence, we see examples of actions or responses emerging from such dimension commonly expressed in political speeches and texts. This is echoed, for example, in the speech by Ghana's Communications Minister at the 2019 Council of Europe's 21st plenary of the Cybercrime Convention Committee:

> We intend to continue to ensure we collectively secure our digital economy, as a chain is as strong as its weakest link. We need Nigeria, Niger, Kenya, Uganda and all other countries in the region on board to build a strong cyber secure ecosystem for the digital revolution in Africa to succeed. The African Continental Free Trade Area, which has come into force, and which will be headquartered in Ghana, will be largely driven by technology. It is crucial to ensure that our collective efforts to criminalize illegal and criminal cyber activity are also

[700] The World Bank and United Nations (n 459). [243]
[701] Internet Society and African Union (n 501). [27]

> continent-wide and indeed global, as we build resilient systems. We must stand together to win the fight against cybercrime![702]

Indeed, similar thoughts are also echoed by those states and institutions of 'knowledge', to support weaker countries in those efforts described by the Ghanian Minister, to 'win the fight', 'solve the problem', and so on.[703]

Along with other states and regional bodies of those on both ends of the knowledge spectrum, we see demonstrations of this thought in their cybersecurity strategy documents, including the cyber declarations of regional bodies, such as the African Union and the Association of Caribbean States, for example.[704] However, the imperative to act, particularly on the part of the knowledge entities, as expressed through these thoughts, does not suggest control of the process of action, or control of the problem itself through direct actions alone (such as regulation and creating norm-based frameworks). Rather, other less direct means of control are implied. These include education, motivation through incentivising and the propagating of certain discourses (such as the 'them and us' discourse), which highlight and encourage the individual state's responsibility as it applies to behaviours, relations and choices in cyberspace.

[702] Ursula Owusu-ekuful, 'Ghana Will Get African Countries to Accede to Budapest Convention' (2019).

[703] Government of the United Kingdom (n 13). See also Cabinet Office, 'National Cyber Security Strategy 2016-2021 - Progress Report' <http://www.nationalarchives.gov.uk/doc/open-> accessed 5 August 2021.

[704] African Union Convention on cyber security and personal data protection in Africa 2014 (African Union Convention) 0. See also Declaration on the Commonwealth Connectivity Agenda for Trade and Investment. And Cybersecurity Program of the Inter-American Committee against Terrorism (n 608).

> Government incentives for cybersecurity development lags behind. Fostering cybersecurity at a national level needs to be accompanied by the promotion of a cybersecurity culture, encouraging an attitude shift among business leaders, away from cybersecurity as an information technology-related problem, to a more holistic outlook that values the role of cybersecurity in improving overall business efficiency and performance. Cybersecurity precedence among organizations is a process that requires the availability of infrastructure and mechanisms to encourage cybersecurity adoption. Countries fostering cybersecurity development in the private sector and encouraging development of cybersecurity-related companies is reflected in the integration of incentives within their cybersecurity framework.[705]

Thus, in terms of solutions to cybersecurity problems and how such solution recommendations are propagated, through the discourse of knowledge transfer or knowledge sharing, there is a sustained thought of a global responsibility to provide those less capable with assistance, and enable them to exercise their own responsibility over their own choices. As such, the process creates the notion of self-improvement of the individual onto itself.[706] This exemplifies actions of governing, which influences 'biopolitical conduct of conducts', without inordinately making such interference obvious.[707]

But how can one better understand the biopolitical implications of these actions and the presumed individual freedom, choices and responsibilities beyond that which is actually expressed?

[705] International Telecommunication Union (n 139). [18]

[706] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319). See also Michel Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (Michel Senellart and others eds, Pbk ed, Palgrave Macmillan 2007).

[707] Miller and Rose (n 440).

7.3 Actions of 'government' and individual choice and/or freedom

Following Foucault's conceptualisation of government as that which designates how conduct is undertaken, the discursive logic of individual freedom or choice, in the face of actions designed to solve the problem, can be explained as the void or distance that emerges from a growing expertise of the problem-producing conditions, alongside the conduct of individual entities that allows for a less optimal reality to be created.[708] In other words, there exist a tension between the need to govern and the notion of individual freedom. And if explained along the lines of cybersecurity problems, the presence of this void (distance, gap in digital capacity between actors), and when matched against the notion of state sovereignty or individual freedom, implies a seemingly inherent imbalance and biopolitical dilemma of the distance or gap. Thus, the coalescing of both the distance and the impeding limitation to close the distance, imposed by the discursive logic of freedom, would seem to allow for a continued presence of distance. As a consequence, it creates a continuous state of opportunities for certain bodies, donor-states, and institutions (those with perpetual answers to the problem) to respond and provide those individual states on the far end of the distance, with a viable route to the desired actions or solutions. Thus, it allows for the alignment of both the interest and desires of the state-in-need to the biopolitical and economic desires and interest of the donor group. In other words, there is a need for the notion of collective responsibility to be projected in

[708] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).

the proposed actions or solutions, which presupposes its task as, on the one hand, that of aligning the desires and interest of those affected by the limitations or gaps, to the biopolitical and economic desire and interest of the collective, on the other hand.

Consequently, a buy-in by the individual state is made possible, thereby producing individual perspectives (on all sides) that see and acknowledge the supposed benefits of the optimised process of action, or solution to the problem (such as the possibilities of cyber risk prevention, through cyber awareness campaigns, training, and investing in the necessary digital infrastructure). And crucially, it creates perspectives that see or rationalise such actions as processes located or deployed onto the self, for the benefit of the self, without paying much attention to who else might also be benefiting, and in what ways.[709]

> Over sixty countries have been engaged with UNCTAD thanks to the financial support of Finland and Spain. Capacity-building activities have strengthened the knowledge of policy and lawmakers with regards to the legal issues surrounding e-commerce and international best practices, allowing them to formulate laws that correlate with their regional frameworks.[710]
>
> The two vital components of improving cybersecurity capacity and creating a strategy are public awareness and political buy-in. Political buy-in can be gained by prioritizing cybersecurity over politics by, for example, conducting regular threat assessments… There are unique challenges facing Caribbean (and other Commonwealth) countries and they should therefore be treated on an individual basis. It is up to the individual countries to take the advice of regional and international organizations, to make it their own and to create national schemes that improve the country's overall cyber safety framework…

[709] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319). Also see Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).

[710] The World Bank and United Nations (n 459). [235]

> Countries should be willing to take small steps to develop their cyber safety frameworks….[711]

Indeed, one can allude to the idea that these are all suggestive of 'governmental' actions, designed to mould perspectives, allowing for a perceived freedom of choice as well as the acceptance of responsibility of the individual in its self-government, without excessive interference (both political and public) from the outside.[712] And as contextualised by Foucault, an observation of how biopower is formed is realised through this sort of mechanism.[713] A mechanism which, on the one hand creates a tension between the seemingly infinite power of biopolitical control or order, and on the other hand, employs the allures of the self-autonomy-touting liberal political discourse or rationalities.[714]

Thus, a technique of governing observed within texts such as quoted above, can further be understood along the lines of what Foucault explains as, the response to the tension that can be observed in neoliberal governmental tactics; techniques of government that exist between a mandate (either given or obtained) to govern, rule or perform action, and the need or freedom of the individual to choose.[715] In other words, 'the solution' to 'the problem', while it may perform governing actions, it is expected to do so by ways of encouraging or projecting individual freedom, rather than a forced or coercive recommendation of action (when comments like: 'It is up to the individual countries to take the

[711] Chatham House's International Security Department (n 669).

[712] (Miller and Rose 2008). [4]

[713] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).

[714] ibid.

[715] ibid.

advice of regional and international organizations' are made, for example). This is done to allow for a managed 'conduct of conduct' from within, albeit directed from the outside. That is, a form of self-regulating governing technique, but at the same time, allowing for a type of governing at a distance.[716]

Thus, the objective of such action becomes that of promotion, campaign of a perceived self-governance framework or self-help guides, through visible discursive encouragements for self-responsibility, freedom to choose, and to some degree, freedom of conduct. But in the end, its impact is such that, it ultimately allows for the desired political, economic and even social objectives of certain actors to be achieved, whatever they might be. But crucially, this is achieved not by coercion, or any form of 'hard sell', resulting from resistance, but rather through this strategy with its prudential undertone. As such, rather than having such effect that may be resisted, it instead allows for the development of perceptions of gratitude and feeling of indebtedness on the part of the receiving entities:

> As a developing country, Botswana has seen an influx of ICT devices some of which are substandard and may be harmful to consumers, a challenge that we are addressing. We continue to benefit from ITU Recommendations and Studies to make our ICT environment a more conducive one. The increase in the use of ICT has not spared Botswana in the challenges of Cybersecurity. Through the assistance of ITU's IMPACT partnership we have been able to set up structures to address this challenge. Further, we recently undertook a capacity building programme on Cybersecurity and Assessment for our stakeholders.

[716] Nikolas S Rose, *Governing the Soul : The Shaping of the Private Self.* (2nd ed., Free Association Books 1999). See also Rose, *Powers of Freedom: Reframing Political Thought* (n 414). And Rose and Miller (n 23).

> Going forward, Botswana continues to count on the ITU for the continued growth of its ICT sector.[717]

According to Miller and Rose, encouragement and promotion of subjectivity through this notion of individual independence, renders the perspectives, desires, and conducts of the subjects as objects of certain political actions.[718] While this may suggest a sort of indirect or covert discipline, it however appears far removed from the central focus of such governmental tactics, at least when such expressions are observed 'as-is' within the text.[719] For Foucault, discipline is a form of power that seek to shape individuals into a desired outcome, but in a rather subtle way. This is achieved through training, measuring, normalising judgements and continuous reinforcement of the norm via certain institutions.[720]

Thus, on a closer observation, techniques of government that seek to align subjects of certain practices to desired governmental objectives, become noticeable. Not necessarily through visible disciplinary tactics that seek overtly to make the subject 'docile', but rather, through its encouraged participation, and inculcating the idea of independent sovereignty and freedom. This is affected through face-value rhetoric that is designed to create the perception or illusion of respect for individual strengths and weaknesses, acknowledgment of

[717] Thari G Pheko, 'Speech by the Chief Executive Botswana Communications Regulatory Authority'.[2]

[718] Miller and Rose (n 440).

[719] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan ed, Second Vin, Vintage Books 1991).

[720] ibid.

geographical or territorial boundaries, and of cultural and political dynamics, in the solution offering. Therefore, when certain cybersecurity capacity development programs are promoted and recommended for developing states, a sense of self-ownership of such programs is projected towards, and felt by the targeted states, which obscures any covert objectives that might lie beneath.

> As a country, we are grateful to have found partnership in the Council of Europe and other partners such as the World Bank, UNICEF, United States Government, Africa Union and our domestic supporter – the National Communications Authority (NCA) in our efforts to address cybercrimes. We are grateful to the Council of Europe for their strong commitment to Ghana especially in the area of capacity building.[721]

Hence, the goal of these projects (whether legal or technical capacity building), becomes more about matching the goals and interests, first, of those providing the support, and second, to the needs and desires (already created through problem visibility and diagnoses) of the individual state, while focusing on the compatibility of the solutions to their individual values at the same time. In other words, the actions become less about identifying and fixing the problem. Rather, it becomes more about aligning the solution to certain objectives, often economic objectives of those proposing the action.

> The Government's first and overriding priority is to protect and promote the interests of the British people through our actions at home and overseas… Our foreign policy rests on strong domestic foundations, in particular our security, resilience and the strength of our economy…the international order is only as robust, resilient and legitimate as the states that comprise it…. this means tackling the

[721] Cybersecurity.gov.gh, 'Legislation on Cybersecurity Will Address Weaknesses in Our Cybercrime Laws' (*cybersecurity.gov.gh*).

> priority issues – health, security, economic well-being and the environment – that matter most to our citizens in their everyday lives. In the years ahead, our national security and international policy must do a better job of putting the interests and values of the British people at the heart of everything we do.[722]

While this governing technique may not directly employ a disciplinary approach as described by Foucault, it is not completely absent, despite the notion of individual state freedom or sovereignty presupposing otherwise. One could argue that, directing the implementation of a cybersecurity solution (spearheading capacity building programs in developing states), or seeking to ensure that certain actions are carried out by some states (such as the ratification of the Budapest convention for example), constitute the regulation or control (albeit indirectly) of individual state freedom. Particularly when they are 'bound' by those choices due to the existing development gaps. While regulation of individual freedom in this way may also appear unforced, it is important to note, that technologies of government and the rationalities employed, are not necessarily made up of single homogenous problem-fields. But rather, a culmination of numerous and complex heterogenous elements that are continuously being aligned, adjusted and adapted to satisfy current, on-going or emergent discourses.[723]

In the example of the Budapest convention, whereas states are not necessarily bound to its membership, or forced to adopt any other non-binding

[722] HM Government, 'Global Britain in a Competitive Age' (2021) <www.gov.uk/official-documents> accessed 10 September 2022. [12-13]

[723] William Walters, *Governmentality : Critical Encounters* (Routledge 2012). See also Foucault and Rabinow (n 39).

norms, the promotion of such norms or rules by the elite states and institutions, from whom their own source of capacity development is hinged, renders the notion of freedom of choice meaningless in this regard. Therefore, while key disciplinary elements might not be so obvious within the tactics deployed, they are visible, albeit hidden within the generalising logic of a global regulatory solution to the problem. Thus, it is at the point of identifying those developing states that may be at risk or vulnerable, and at the point when their individual needs are classified and assessed against the 'standard', lies the beginning of the site of disciplinary tactics – setting standards and benchmarks for what constitute cybersecurity best practices, and so on. While it may not be explicitly declared, the discourse and rationalisation that creates the 'them' and 'us', sets such standards as the *de facto* standard or norm, by which those on the 'us' side ought to, or are expected to achieve or, at the very least, strive to achieve or abide by.

Despite the individualisation of the risk, and the way the problem is diagnosed and solved (which may suggest freedom of choice), there is a subtle level of compulsion, which is admitted by actors on all sides. For example, when expressions like, 'stakeholder collaboration is a must', 'states must do this or that' to ensure the best approach is deployed in building a secure cyber space. However, this compulsion can be seen (and is perhaps intended to be seen) simply as part of the tactics of government that is built around security, and whose interest is nothing but the safeguarding and promotion of certain standards, norms or values, as opposed to that of discipline. And in Foucault's understanding, while such technique is indeed distinguishable from disciplinary tactics, both tactics remain, nonetheless, as something designed to exercise control.[724] In other words, while one appears to represent a technology of government that is concerned with the individual self, the other reflects a technology that allows the individual to be replaced by processes of generalisation or collective.[725] Consequently, a perception is produced which appears to deflect focus from the notion of the individual state, and towards the larger notion of a collective global society.

Consequently, a pattern appears within the data, that suggest a technology of government which feeds-off the knowledge it has, both of its own position or power in the world order, and of the developmental characteristics of developing states and their vulnerabilities. As such, we find suggestions of these tactics that reflect symptoms of techniques of government, that capitalises on this notion of the collective vulnerability, which requires, equally, a collective effort to control. At the same time, it emphasises the notion of cooperation, through support and partnership, as necessary key lines of action:

> Moreover, the small populations and isolated locations of some Commonwealth countries do not make them any less vulnerable to cybercrime. Indeed, in some respects they may well be more vulnerable to the commission of cybercrime and to its adverse … If small developing countries are not supported in developing and maintaining security and other capacities at levels consistent with other countries, they risk becoming attractive to offenders as a safe haven from which other locations can be attacked, and this provides

[724] Foucault, *Discipline and Punish: The Birth of the Prison* (n 719). See also disciplinary power, normalisation and statist in: Michel Foucault, *Society Must Be Defended: Lectures at the Collège de France 1975 - 1976* (Mauro Bertani and others eds, 1st edn, Picador 2003).

[725] Foucault, *Society Must Be Defended: Lectures at the Collège de France 1975 - 1976* (n 724).

> an incentive for developed countries to provide such assistance and for developing ones to accept it.[726]
>
> The collaborative security approach to Internet security recognizes that people are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for its prosperity and potential. [727]

Through problem identification and diagnosis, a technique of government that feeds on these vulnerabilities is able to emerge as a form of response or proposed action. As such it governs, rules and controls through this logic of pre-empting, identifying and rationalising the problem, which allows it to regulate uncertain or risky phenomenon such as cybersecurity; such that the individual within this common collective might be protected, and allowed to operate within a framework that has, as its priority, the wellbeing of everyone within it, and the desire to ultimately protect everyone as a result.

Foucault describes this as a "mechanism of security", whose purpose is to evaluate and predict future dangers (such as cyberattacks and cybercrime) and the likelihood of them occurring.[728] This is done, not necessarily to prevent those threats from occurring (since their realities are equally established as inevitable or unavoidable within the discourse), but rather for the purpose of achieving sufficient levels of preparedness, to mitigate the risk of them happening (either defensively by deflecting or catching and stopping it in its

[726] Commonwealth and Law Ministers and Senior Officials (n 28). [22-23]
[727] Internet Society and African Union (n 501). [27]
[728] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706). [22]

track, or offensively by demonstrating strength which can also act as a form of defence or deterrence). Thus, as part of this process, several strategies are deployed, but with a common objective of keeping the problem under control. And in the process of achieving this objective, there is also the continuous need to 'conduct' certain actions, primarily by creating norm-based environments for all to live by, and ensuring that all bodies are held on tighter leashes. Again, while not necessarily coercive, it is nevertheless disciplinary in character.[729]

Hence, various methods are devised, often around the notion of partnership, following the rationalisation of the problem and justification for the collective necessity to protect the common space. The idea of partnership, collaboration and cooperation is therefore pushed and encouraged, as a necessary solution whereby everyone, particularly the vulnerable, wins. And as described in a recent UK FCDO guidance document, in relation to its lessons learnt report on the African Cyber Expert Fellowship program, with reference to the participation of Botswana:

> during the Africa Cyber fellowship programmes, international collaboration was promoted and enhanced. Over this period, Botswana learnt and adjusted her cooperation and collaboration efforts. Botswana has used the Africa Cyber Fellowship to promote cooperation with her international partners. The Fellowship is an ideal environment through which Botswana could reach out, since she is introduced to many potential partners in one place.[730]

[729] Foucault, *Discipline and Punish: The Birth of the Prison* (n 719).

[730] Foreign Commonwealth and Development Office and The Commonwealth (n 575). [13]

Arguably, developing countries may benefit from these supports and partnerships, but what are the trade-offs?

7.4 The 'government' of international cooperation in cybersecurity actions

Indeed, the nature of cybersecurity demands a certain level of collaboration between multiple actors and across multiple geographical boundaries. This is necessary to allow for effective actions, to tackle the challenges. As with other security challenges, there is also discursive need for a neoliberal notion of global cooperation between actors in responding to these challenges; such that, there appears to be an equally neoliberal demand for global peace, law, and order. In other words, demands for the promotion of the idea of a global common structured along a standard framework or template, designed by a select few powerful states and considered as development panaceas to be prescribed to everyone else.

In satisfying these demands, there is a further requirement which Suvi Alt describes as, "wholesale reshaping of human subjectivities",[731] in the global society, particularly in places believed to be at risk and vulnerable (due to the usual suspects – economic status, development status).[732] Consequently, certain attributes or qualities are also demanded, particularly those Alt refers to as,

[731] Suvi Alt, 'Beyond Bricks and Mortar: Peace-Building in a Permanent State of Adaptation BT -' in Sandro Mezzadra, Julian Reid and Ranabir Samaddar (eds), *The Biopolitics of Development: Reading Michel Foucault in the Postcolonial Present* (Springer India 2013) <https://doi.org/10.1007/978-81-322-1596-7_6>. [4] see also Tina (A C) Besley, 'Governmentality of Youth: Managing Risky Subjects' (2010) 8 Policy Futures in Education.

[732] See topics on the visibility of the problem in previous chapters

"*homo economicus",*[733] which for them, are often played out in the demand placed on global entities (particularly those deemed 'not there yet'), to become more adaptable or more conforming.[734] Being adaptable, thus implies investing in the 'self' (either through self-efforts, own initiatives, own finance, or owning up to one's self-responsibility to perform certain actions, whether one has the capacity to do so, or not). And perhaps, by agreeing to be funded and supported by others, to reach a certain point of self-development (by accepting this responsibility and taking part in the prescribed capacity building programs and following certain guidelines, for example) and self-governance.

This global push for adaptability through self-development, is a continuous process which seeks to maximise, improve or build capacity in response to challenges that appears to be equally continuous and endless. However, what is revealed is that the development of the self is not necessarily self-originating or self-initiating, and by no means self-supporting development. Because of the wholesale need to adapt, those with better capacity and knowledge are aptly positioned to contribute to the common knowledge needed to be self-supporting. Consequently, they are also better equipped to support others, forming partnerships that are not only intended for the individual partners, but, presumably, intended for the collective global good.

> Several agencies are assisting developing countries within their mandates, and inter-agency collaboration is growing. An example is the jointly organized briefing of Commonwealth parliamentarians by UNCTAD, the CTO and the Commonwealth Parliamentary Association

[733] Alt (n 731). [88]
[734] ibid.

> during the Commonwealth Cybersecurity Forum in 2013. Another example is the joint workshop on the harmonization of cyber legislation in ECOWAS that took place in Ghana in March 2014. The event was organized by UNCTAD, UNCITRAL, the African Centre for Cyberlaw and Cybercrime Prevention, CoE, and CCI...UNCTAD has built a network of institutions with which it regularly partners with on different projects and activities. Many of them contributed to the development of the Cyberlaw Tracker database, which maps laws in the areas of e-transactions, data protection, cybercrime and the protection of consumers online.[735]

Despite the focus on human development or security by the archetypes promoted by the various institutions and development agencies, "the subjectivity they are aimed at developing is one that is stripped of any capacity to conceive an ability to achieve security".[736] At the same time, objection to such promoted ideals is 'forbidden', unless such opposing voices are prepared to be in the 'other' camp.

One could argue therefore, that being adaptable is akin, almost, to being coerced through the discursive process of urging action, or the feeling of being required to be doing something about a globally accepted problem that affects everyone; particularly when there appears to be no alternative. Put differently, being adaptable within the context of reshaping of the individual subjectivities, through training and capacity building, for example, demands some form of surrender. This can be achieved through acknowledgement and acceptance of the problem and renouncement of the individual will to resist whatever change is

[735] The World Bank and United Nations (n 459). [235]

[736] Sandro Mezzadra, Julian Reid and Ranabir Samaddar, *The Biopolitics of Development: Reading Michel Foucault in the Postcolonial Present* (2014). [4]

being proposed. This is particularly so when one's ability to resist is hampered by the development gap or incapacity. This, in effect, reduces the so-called freedom to act or choose, when such situations of the individual depend on external resources. Hence and as postulated by Mezzadra, et al:

> The correlation of development with security at work here functions to feed and support the political imaginary of neoliberalism predicated as it is upon the belief that a global order of self-securing subjects is the first foundation of a more secure form of world order. But in essence what we are seeing imagined here is a world depopulated of human subjects amid the reduction of human life to the properties and capacities that define non-human living species: adaptation. Worse, subjects that, in their humanity, do not or cannot adapt are constructed as threats to peace, order and 'good governance'.[737]

It would seem therefore, that the wholesale global cybersecurity effort discourse does not, indeed, translate into individual freedom, particularly for the weaker and less independent states. The reality remains such that, those states simply cannot afford to reform or adapt on their own strengths alone. Neither can they simply afford to refuse the quest for reform and adapt to the changing landscape altogether.

Within the case data , similar neoliberal strategy is observed, which exemplify how such strategies are employed by cybersecurity practices, through the various initiatives, driven by the need to develop a rule-based system, to reshape the political, economic and social arrangement within cyberspace. Because such drive, which re-tasks the role of the collective and the individual responsibility, allows for the neoliberal extension of free markets into all aspects

[737] ibid. [5]

of the cybersecurity discourse and practices (through the acknowledgement of the notion of multi-stakeholder approach for instance, involving private and public alliance, etc).

The discourse on the need for capacity building to develop cyber resilience is one that suggests, or pre-empt the calamitousness of the problem, and one which, at the same time, interpellates the subject, who is endlessly required to see, acknowledge, and act on the problem. Thus, for such subjects, success in the global society is predicated on their willingness to adapt or engage with the proposed solutions to the problem. As such, one finds expressions of affirmation by such subjects in their 'visionary' declarations, as a manifestation of their preparedness to adapt, and formulate their desired cyber future.[738]

In a Trinidad and Tobago's Working Group on Cyber-crime meeting for example, the state's vision in relation to cybercrime is expressed as one that is focused on:

> a secure and resilient cyber environment, based on collaboration among all key stakeholders, which allows for the exploitation of ICT for the benefit and prosperity of all.[739]

In Ghana, Botswana, and elsewhere, the lyrics are the same, either when sang by themselves or voiced on their behalf, by those who take it upon

[738] Ministry of National Security, 'Eighth Meeting of the REMJA Working Group on Cyber-Crime (Washington D.C. - Feb 27 & 28, 2014)'. [4] See also on Botswana: lessons learned, Foreign Commonwealth and Development Office and The Commonwealth (n 575). [9]

[739] Ministry of National Security (n 738). [4]

themselves to provide the desperately needed support that such states need. As exemplified, again by the UK FCDO report:

> One of Botswana's National Cybersecurity Strategic Objectives is on stakeholder collaboration and cooperation. The country believes that the best approach in building a secure cyber space is to work with others. Therefore, during the Africa Cyber fellowship programmes, international collaboration was promoted and enhanced.... European Union Cyber Resilience for Development (Cyber4Dev) a flagship EU cyber cooperation and collaboration project, partnering with developing countries. Botswana was introduced to the programmes and potential of being a member, through one of the ACF Donor presentations.... Botswana partnered with the United Kingdom's Home Office to host the inaugural UK and Commonwealth African countries National Cyber Risk Assessment (NCRA). The Botswana team liaised with their UK counterparts and aided on the project. This was possible through contacts established at ACF meeting.... She [the UK] was able to also guide Botswana on other initiatives which the country was unaware.[740]

The resilient 'subject' must therefore continuously strive to adapt to the changing world, not necessarily as a key player in the game-changing solutions proposed, but, as a player regardless, a stakeholder. In other words, a subject, that acknowledges and identify with the perceived threats as a reality of modern global society. As such, it also accepts the responsibility to play its part in the world order, no matter how minuscule. This perception, for example, is observed in the following extract from the Commonwealth Cyber Declaration. A declaration that embodies the entire Commonwealth, notwithstanding the fact that a very high proportion of states within the Commonwealth are developing and small/small island states:

[740] Foreign Commonwealth and Development Office and The Commonwealth (n 575). [9]

> We, as Commonwealth Heads of Government, commit to…
>
> Promote stability in cyberspace through international cooperation. Recognising the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace, we: 1. Commit to the establishment of effective and proportionate domestic cybercrime and cybersecurity frameworks that take into account principles in existing international instruments, acknowledging the evolving tactics of cybercriminals and the transnational nature of cybercrime. Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime.[741]

Part of such responsibility and commitment to adapt, lies in its willingness and acceptance of the necessary solutions, rules, injunctions or proscriptions, that are established to aid its preparedness, in relation to the endemic threats and dangers associated with the challenges faced. Therefore, as a governmental tactics, developing resilient subjects entails the calculated erosion of certain existing habits – social, political and economic habits and inclinations - and installing new adaptive ones in their place.[742] According to Ried, for such subjects, becoming resilient means willingness on their part, to accept the "imperative not to resist or secure themselves from the difficulties they are faced with but instead adapt to their enabling conditions via the embrace of neoliberalism".[743] And the acceptance of such imperative and embrace of the global order, constitute a form of discipline that is reflected in

[741] The Commonwealth Heads of Government (n 537).

[742] Julian Reid, 'Interrogating the Neoliberal Biopolitics of the Sustainable Development-Resilience Nexus' in Sandro Mezzadra, Julian Reid and Ranabir Samaddar (eds), *The Biopolitics of Development: Reading Michel Foucault in the Postcolonial Present* (Springer 2013).

[743] ibid. [13]

proclamations, expressed by stakeholders within the cybersecurity discourse from across all cases observed.

7.5 Conclusion

The issue of cybersecurity is overseen by the development of cybersecurity strategies. This is the case for every entity, whether state or non-state. Cybersecurity strategies articulate plans for how cybersecurity concerns are addressed. For certain developing states, generating these strategies is a challenge. Implementing programs and processes outlined in the strategy poses even greater challenges. As such, they are often quick to welcome any offer of support from countries like the UK, not only to create these strategies, but also, and often, to support execution and on-going implementation of the programs. States like the UK and international bodies like the Council of Europe, on the other hand, appear willing to render this form of support, which is enthusiastically welcomed by the recipient developing states, often unconditionally, and without many concerns. In fact, calls for assistance are often initiated by the developing states themselves. But at what cost, if any, to the developing countries are these 'supporter-supported' relationships?

Security strategies of any state, whether cyber or conventional , are underpinned by state interests. First, it is in a state's interest to ensure that its security apparatus is robust and resilient. Second, that its robustness enables it to defend itself and withstand threats from both internal and external adversaries. And third, its security preparedness should allow for offensive capabilities when necessary.

Indeed, state security is sensitive and a show of weakness is not one any well-meaning sovereign state would want to bask in. Therefore, there ought to be concerns when a state or a political union like the EU, seek to finance and orchestrate the development of another state's national security strategy, while overseeing its implementation and workings.[744] And as expressed in the 2015 ITU index report, cybersecurity is "a sensitive issue, whether from a government or private sector perspective".[745] However, what is most revealing in the data is that such concerns does not appear to register prominently. Neither do they seem to be readily grasped within the political discourse amongst the recipient developing states.[746] Indeed, when government officials of Ghana and Botswana were asked questions to that effect, their responses mirrored the usual discourse of:

> International cooperation is important and a key focus here. Cybersecurity is a global concern and Cybercrime is a borderless issue. So, you can't do it alone. It doesn't matter how well you are able to deal with domestic issues. You certainly need collaboration with external international parties.[747]

Some expressions of concern are, nonetheless, observed within the data. Perhaps, only observed in relation to cybersecurity for elections, where concerns for interference from the outside, over the electoral and democratic process, is cautioned against:

[744] Rose and Miller (n 23). (Rose 1990, 1996; Rose and Miller 1992)

[745] Itu and Abi Research (n 207). [29]

[746] The Researcher (n 554).

[747] ibid.

> Co-ordination and co-operation must, however, be done with care, to avoid public concerns around foreign interference in elections, and to maintain as full visibility and governance of the supply chain as necessary to ensure security.[748]

Overall, perceptual concerns with regards to the relationship between developing states and their developed counterparts, in terms of cybersecurity practices, remain scant. Instead, what is deduced and expressed is a conviction on the one hand, by developed states and institutions like the Commonwealth, of what their role is within the relationship:

> we protect the vulnerable in society in their use of Cyberspace; we, individually and collectively, understand the consequences of our actions and our responsibility to cooperate to make the shared environment safe; our obligation is in direct proportion to culpability and capability.[749]

For the developing states, on the other hand, the focus appears centred around growth and development. Justifiably so because, the problem of cybersecurity is convincingly depicted and accepted as a fundamentally developmental problem:

> Many least developed countries consider cybersecurity primarily as a means to extend the benefits of ICTs through the delivery of secure and high-trust services in sectors such as health, commerce, public administration and finance. Their needs, priorities and strategies in cybersecurity are not necessarily the same as those of the most developed countries.[750]

[748] The commonwealth secretariat (n 552). [115]

[749] Commonwealth ICT Ministers (n 54). [4]

[750] ITU, Schjølberg and ITU (n 486). [10]

Thus, it is this disparity in both the needs and priorities of states that makes it difficult to see how such relationships might be based on equal footing, despite their claims to commonality and collectivist paradigms. And if the relationships are not equal, does the inequality necessarily suggest any form of unfair disadvantages or advantages on either side?

The focus has been on understanding, based on data, certain conditions that may shed light on possible answers to such question. What has been demonstrated is how cybersecurity concerns are presented, represented and problematised in (political) discourses, through techniques that are internal to the security apparatus. That is to say, by way of its preoccupation with certain events, where the global society is represented as both the end and instrument of government.[751] In other words, there is a tactical use of cyber (in)security as a means of bringing about the visibility, diagnosis and remedying of what is considered a problem that has emerged from our 'new' interactions with cyberspace.

The result of such tactical deployment is the birthing of cybersecurity as an emerging biopolitical problem sphere, which allows multiple elements to be brought together, to create a discursive space that is coherently rationalised and legitimised by all parties involved (with the Western states, and the global institutions under their control, at the forefront of that coherent campaign, articulated in such ways that, the least developed countries of the South are

[751] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).(Foucault 2007: 105)

seemingly left hypnotised by the charms of such eloquence, and the benefits it promises).[752] And in the end, it allows also for certain actions and practices to obtain similar status, obscuring even more any chance of a clear-cut answers being afforded to the question.[753] Nonetheless, a final opportunity will be seized upon in the following chapter to draw on the discussions so far, with the aim of providing further answers, and offer a deeper reflection on what might be taking place.

[752] In Foucault, biopolitics and governmentality are intertwined and work together. Biopolitics is a specific form of governmentality that focuses on the subject and allows governments to shape and manage them in ways that would not be possible through traditional means alone. Governmentality, therefore, provides the framework and tools for realising biopolitical strategies.

[753] Dillon (n 205). see also Stephen J Ball, 'Subjectivity as a Site of Struggle: Refusing Neoliberalism?' (2016) 37 British Journal of Sociology of Education 1129 <https://www.tandfonline.com/action/journalInformation?journalCode=cbse20> accessed 11 September 2022.

8 Cybersecurity problematisation and impacts – tying it all together

8.1 Introduction

In chapters 5, 6 and 7, cybersecurity problematisation was discussed, broadly in relation to the data from across multiple sources, using the three elements within Dean's power concept (truth, norms and power effects, respectively).[754] In this chapter, a reflection of the constitutive impacts of these elements across the three developing commonwealth states (Ghana, Botswana and Trinidad and Tobago) is examined further. The analysis is done against the interactions of these states with Western-styled cybersecurity initiatives (such as the CCI), to examine their impacts on norms and idea formation, for example, within these states.

Thus far, the aim has been to unravel techniques of government that are evident across a range of data from multiple sources, including those from

[754] Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11).

outside the case states. For example, in Chapter Five, the emergence of calculative practices and the use of data monitoring or surveillance was reviewed as a key tactic which allows for the visibility of the problem of cybersecurity, as a key strategy in ensuring its presentation as an ongoing concern.[755] The deployment of normalisation techniques, evident across the data, is then revealed in Chapter Six, as a fundamental process by which such problems are understood and further diagnosed. And finally in Chapter Seven, similar governmental tactics are discussed through examination of evident efforts, or actions designed to solve the problem of cybersecurity. The focus of this chapter is to tie together the various themes expounded thus far, to unravel impacts and perspectives across the specific case states. For structural flow, the discussion will seek to address three main areas.

First, the constitution of cybersecurity problem as a governable problem-field is examined, looking at the commonalities or similarities of such themes across the states. In addition, the operation of power is examined, in its biopolitical forms (disciplinary, sovereignty and security), and the tactics they employ (through law, discipline, and control). This allows further examination of the different possible forms of power and how they emerge in the data related to the individual states.

The second observes the way such operation of power varies between the states and their impact within the respective developing countries. These

[755] See for example, Abi Research and ITU (n 492). And International Telecommunication Union (n 139).

states are further assessed in the chapter to provide deeper insight into the assemblages of power and their specific contextualisation within the texts. It does so by focusing on how subjects and processes of normalisation are represented and presented within the data across the states. [756]

The final task of the chapter concludes the discussion and presents a final summary of the analysis. It draws on themes discussed throughout the thesis, but more specifically within the later chapters, to provide a summary of the work carried out during this exercise, and a final reflection on the problematisation of cybersecurity and the impact of Western-engineered practices on the construction of normality across the case states and the world.

8.2 Reviewing cybersecurity problematisation across case texts

8.2.1 Common themes

Governing through freedom

As discussed in Chapter Seven, a projection of freedom in the cybersecurity discourse allows for the intelligible perception of the problem of cybersecurity risk, threats, etc., as truth. This creates a need for solutions, designed to deal with the problem, through the articulation of freedom as a form of governing without coercion.[757] According Bröckling, et al, "freedom is an

[756] Kaspar Villadsen and Ayo Wahlberg, 'The Government of Life: Managing Populations, Health and Scarcity' (2015) 44 Economy and Society 1 <https://www.tandfonline.com/action/journalInformation?journalCode=reso20> accessed 23 November 2021.

[757] Ulrich Bröckling, Susanne Krasmann and Thomas Lemke, *Governmentality: Current Issues and Future Challenges*, vol 71 (Routledge 2011).

indispensable instrument of the liberal art of government", consisting of "a more or less systematized and calculated form of exercising power, not directly affecting individual and collective agents and their options for action, but rather intervening indirectly in order to structure fields of possibility".[758] Hence the question of how the problems of cybersecurity can be resolved becomes high on everyone's agenda (including both the governing bodies and those that are being governed). At the same time, it allows certain governing objectives of specific actors to be achieved. Hence, and as a preamble to their offer of solution, sentiments like the below extract are resounded to create further justification for the visibility of the 'needs' of a particular group and the presumed benefits of recommended on-going actions:

> Governments in Africa today have moved ICT discussion form infrastructure to cyber security. A decade ago, infrastructure was a major challenge to many African countries... Many countries have invested in massive in-country infrastructure and the access challenge is waning. The networked computer infrastructure coming up in many African countries has open up cyber space to many more citizens and accompanying this, the risk of using the Internet. A few countries like Tunisia, South Africa and Kenya already have a CERT in place. Many countries are also in the process of developing cybersecurity policy and strategy (including formation of CERTs).[759]

In Lemke's argument, governmentality works through this notion of freedom which allows for certain objectives to be realised through neoliberal

[758] ibid. [5]
[759] Republic of Ghana Ministry ofCommunications, 'National Cyber Security Policy & Strategy'. [12]

representations.[760] These representations, evident across the cybersecurity discourses, presupposes an understanding of the problem or the need to understand the problem, to allow for one's focus, on the outcome-orientated nature of individual or collective actions, designed to ameliorate the problem. Hence, the discursive need for a state to develop its cybersecurity capacity, the pride in feeling a sense of empowerment, or relishing the need to be motivated to do so, as evident by the languages of government representatives.

Such sentiments, when expressed by developing state leaders, often cite existing Western states or bodies as a reference point, or benchmark. An example can be found in the speech by a Trinidad and Tobago Minister of National Security in his proposed Bill for the country's need to create a dedicated Cybersecurity Agency:

> After the expiration of the IMC, Mr Speaker, such cohesion within the Government is lacking and is specifically needed to treat with the ever changing nature of ICT and cybersecurity threats. It is therefore intended that the Cybersecurity Agency, as a national agency, will bring together key stakeholders, both governmental and private sector, in addressing cybersecurity issues. Such an agency is not uncommon as the European Union has the European Union Agency for Network and Information Security (ENISA). ENISA is the European Union's response to the cybersecurity issues of the European Union. It is the 'pace-setter' for Information Security in Europe, and a centre of expertise.[761]

[760] Thomas Lemke, 'Foucault, Governmentality, and Critique' (2002) 14 Rethinking Marxism 49 <https://www.tandfonline.com/action/journalInformation?journalCode=rrmx20>.

[761] Gary Griffith, 'Minister Griffith Speaks on Cyber Security Agency Bill 2014 | Trinidad and Tobago Government' (*gov.tt*) <http://www.news.gov.tt/content/minister-griffith-speaks-cyber-security-agency-bill-2014> accessed 14 September 2021.

According to Foucault, by giving off this sense of freedom, or feeling of empowerment, particularly through support and encouragement directed towards the subject, forms of power are exerted on such subjects that can be conceived as techniques of government through freedom.[762]

Strategy of prevention

Evidence of prevention strategies, both in the broad cybersecurity discourse and across texts within the states, reveals, to a degree, functions of power similar to that of freedom in its manifestations. This is demonstrated, for example, through the promotion of education and training, which represent forms of empowerment and support. Thus, such tactics, through their focus on empowering poorer developing states by way of training, educating and sharing knowledge, seek to influence, change or achieve desired objectives through a perception of motivation, collaboration and partnership, thereby obscuring its prescriptive nature in the process.

While such efforts may appear prescriptive, even to the 'ordinary eye', the intended perception is that of freedom, granted to make decisions on such concerns, not for the benefit of the proposing state, but for the benefit of the individual recipient state. This, as we have seen, is made possible through the equally individualised risk discourse; the notion that, while there is a collective risk in relation to cybersecurity, the risk to the individual state is real, nonetheless. Hence the conviction, amongst recipient states, of their own

[762] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).

responsibility and their own need to take control of the situation, as demonstrated in this strategy declaration, for example:

> The strategy will help initiate a systematic national programme to defend cyberspace from threats irrespective of their origin. Critically, the strategy prioritises cyber threats and risks as well as allocation of responsibilities, to ensure that all relevant stakeholders accept responsibility for and take appropriate steps to enhance cybersecurity. As a result, the strategy aims to improve security by creating stakeholders awareness on relevant risks, preventive measures and effective responses.[763]

Individualisation of risk and responsibility

As exemplified in the previous chapter, the individualisation of risk faced by developing states and the discursive responsibility allocated to them through the notion of freedom, result in the tactics of risk problem visibility that can be seen across all case data. How the resulting individual responsibility is perceived, alters not only their sense of ownership of the situation regarding their individual states, but to the entire global society. In other words, it produces both a sense and pride of belonging to the 'right side'. This is relevant because, risk representation, as a technique of government, creates a responsibility rationality whereby, the risk responsibility resides not only within the individual, but contains an element of fluidity, or is allowed to move from the individual to the collective, and vice versa.[764] Thus, both the problem as well as actions needed, become collective and global. Or perceived as such, with the responsibility to

[763] Botswana Ministry of Information Communications and Technology, 'National Cybersecurity Strategy'.[12]

[764] O'Malley (n 621). See also Nikolas Rose, Pat O'malley and Mariana Valverde, 'Governmentality' (2006) 2 Annual Review of Law and Social Science 83 <www.annualreviews.org>.

manage risk being charged, not only to the individual state, but equally offered to everyone through the discourse of support and collaboration:

> Collaboration and cooperation will be established with all relevant multi-stakeholders including nationally and internationally institutions to share information and experiences in addressing Cyber Security challenges.[765]

This creates a complex web of illusionary perceptions about its actions and intentions. Thus, the individual (state) is discursively charged with the responsibility to manage this risk through its own freedom and ability to make the right choices: to take up offers for capacity building programmes, for example, choosing to work with international (Western developed states) collaborative partners, to participate in (suggested and recommended) training programmes and workshops (often delivered by Western partners and based on curriculum adapted from their best practices) to facilitate knowledge transfer, and so on.

Discourse on the economics, the rationality and efficacies of cybersecurity programmes

Another commonly themed observation across all data is that of rationality based on the economics of cybersecurity risk. Here, rules or standards of economic reasoning and the global preoccupation with efficiency, economic growth and development, sets the tone for such rationalisation discourse. Again, this is made apparent through a demonstration of expertise by the developed

[765] Botswana Ministry of Information Communications and Technology (n 763). [16]

actors, in their professed understanding of the problem. Such demonstration, as illustrated in the last three chapters, is used to impact the different stages of the governing process – from visibility, through diagnosis, to solving the problem through actions.

Through demonstration of expertise and exercise of knowledge power, some groups (in our case the United Kingdom in particular, along with other alliances of equal status), through their initiatives, allow for the creation of economic norms across multiple global spheres, both within and beyond that of the traditional market. Thus, we see such transcendence of norms of economic governance within healthcare, education, security, and the creation of preventative strategies, which not only focuses on the economics, but also, on the moral.[766] And the moral, in turn, legitimises the need for certain actions that are subsequently rationalised against these economic standards.

Notably, the presence of this governing tactics is observable within the case data, as will be demonstrated below, not necessarily in its true expressive form, but rather, in its biopolitical form. The biopolitical form it takes is reflected in its obsession-absorption with new forms of collaborations, partnerships, the need to build capacity across states, creating a multi-stakeholder alliance involving private-public partnerships, building solution consensuses or commissions, etc. And as expressed below by the Trinidadian Minister:

> Mr. Speaker, Trinidad and Tobago's position on the importance of cooperation with respect to the detection, investigation and

[766] Besley (n 731).

> prosecution of cybercrime is in keeping with the views of the international community as evidenced at the Commonwealth ICT Ministers Forum held in London in March 2014 … which approved the principles of the Commonwealth Cyber-governance Model and Trinidad and Tobago adheres to that model. Primary among which is the reinforcement of the principle that nations must act individually and collectively to tackle cybercrime. Through the development of relevant and proportionate laws and the elaboration of international recognition standards and good practices to deliver security and establish effective government structures and the mechanisms that support collaboration and cooperation among governments and, of course, relevant international organizations, the private sector and other stakeholders, to prevent and respond to incidents of cybercrime.[767]

As has been questioned throughout, the direction of flow of knowledge required to establish such international collaboration, determines both the source of the knowledge, and as such, the source of the associated power. If that is the case, one could deduce that, while it may be entirely incorrect to assume that developed states have very little or no dependencies on the knowledge coming from the developing states in relation to the subject under analysis, the direction of flow of the knowledge transfer discourse is clear. Within these arrangements, developing states are more likely to depend on knowledge (technological, legal,) flowing from their developed counterparts, as opposed to it being the other way round. Thus, initiatives designed to build capacity and aid knowledge transfer or knowledge sharing between North and South, suggests who the actual importers and exporters of such knowledge are.

While it may be argued that states like the UK engage in their own internal cybersecurity capacity programs, this is done mainly in-house (for

[767] Ministry of National Security (n 738). [12]

example, programmes developed and executed through its own institutions and governmental bodies, such as the University of Oxford Centre for Capacity Building). Thus, while the UK may or may not have engaged or commissioned external resources (through funding, knowledge, etc.) from other states or bodies, there seems to be no citing, within available data, of suggestions that indicate or propound the idea of an actual importation of cyber capacity knowledge from developing or least developed states by the UK or any other developed state in their own capacity building efforts. And as expressed in the Commonwealth's State of Digital Economy report in 2020, "just six Commonwealth countries make up 98.8 per cent of the Commonwealth's total high-tech exports as of 2017".[768] This reflects the stark reality of the "disparity in ICT trade participation",[769] development, income, power and control between states that are supposedly part of a single entity known as 'the Commonwealth'.

Therefore, capacity development efforts in developing Commonwealth states are products, thoughts and practices emerging from developed states, not only in the problem-solution discourse and practice, but also, as demonstrated, through problem identification, visibility and diagnosis. Thus, one could argue that, this suggests a developed states' exportation of biopolitical models of governing, through the discursively rationalised processes of cybersecurity risk representation, risk management, validation of standards, norms or best practices, that are based on its own systems (that are both market and politically-

[768] The Commonwealth (n 634). [15]
[769] ibid.

inspired).[770] In other words, biopolitical because, through the practices of risk governing, such export seeks to ensure, sustain and improve entities to allow for their regulation or control.[771] Further, these practices are hidden behind the notion of partnership, collaborations, support etc. And above all, often with a rationalisation based on the economic advantages of doing so:

> Unsurprisingly, the digital divide translates onto advanced digital infrastructure: 20 out of 31 Commonwealth countries fell below the world average score on UNCTAD's Business-to-Consumer E-Commerce Index in 2016 (UNCTAD 2018). Of these 20 Commonwealth countries, 15 are in Africa and 15 are categorised as LICs or lower middle-income countries (LMICs).[772]

Therefore, digital capacity building provide means of bridging this gap to allow for states to achieve the economic benefit, to open up:

> new pathways for development, offering Commonwealth countries new and diverse opportunities to: increase productivity, output, growth and employment; connect economically with large and dynamic diasporas; access global trade and financial markets; increase participation in global trade by taking advantage of the unbundling of production processes within larger GVCs; and drive down the costs of trade.[773]

And be open to cooperation and support in the effort to allow for such benefit to be achieved:

[770] O'Malley (n 621).

[771] ibid; Rose, O'malley and Valverde (n 764); Rabinow and Rose (n 693).

[772] The Commonwealth (n 634). [17]

[773] ibid. [20]

> The long-standing spirit of co-operation in the Commonwealth can play a major role in supporting our member countries to harness the benefits.[774]

Strategy of identity construction

Another observable common theme across the case data relates to the construction of identity. Such construction indicates the perception or reflection of each state on itself and its role in relation to its place within the global cybersecurity landscape. Thus, discourses that are focused on one's perception of oneself (the state as an individual or self) and on creating a positive representation, are formulated as part of the governmental tactics or strategy.

> In light of the threat to socio-economic development posed by attacks on Internet infrastructure, it is the responsibility of all stakeholders, including governments and Internet service providers, to agree upon solutions to ensure the Internet in every country remains safe, secure and resilient.[775]

As such, efforts designed to govern both the self and the entire global population are hinged on the successful deployment of this strategy. While the strategy of identity construction is common across the case data, there are differences in their formulations from state to state. However, these differences are even more pronounced when compared along the line of the developed and developing states divide. In other words, while there are differences between states more generally, there are similarities amongst states of equal economic and political status. As will be demonstrated below, the formulation of identity

[774] ibid. [5]

[775] Internet Society and African Union (n 501). [7]

construction within texts from Botswana, Trinidad and Tobago and Ghana, for example, employs this strategy explicitly for the purpose of self-challenge, a positive means of challenging one's self-identity, to encourage improvement or change within oneself, while recognising the need for support from others:

> Our mission is to determine, analyse and address the immediate cybersecurity threats posed on identified critical national information infrastructure by providing adequately, protection for the critical national information infrastructure and over time become a self-sufficient country attending to its cybersecurity needs.[776]
>
> The cybersecurity policy will address major cyber risks facing Ghana from attacks on the national information infrastructure. The policy seeks to address the lack of awareness of risks users and businesses face doing business in cyber space. The problem of "Sakawa" which has tarnished Ghana's cyber credentials as a haven of cyber fraudster will be addressed by the policy. The policy also addresses the need to develop technology framework for combating cyber-attacks and capacity building for cybersecurity expects to make Ghana self–sufficient in the fight against cybercrime and in the near future create a culture of cybersecurity in Ghana.[777]

Albeit, recognising also that such self-belief and confidence and the means of achieving such self-sufficiency, is made possible, in part through support from the most knowledgeable states:

> The nature of cyber space is borderless and complex; this implies that managing risk is a shared responsibility beyond Government alone… International collaboration is therefore key in ensuring presence of capacity and mechanisms to handle cyber threats from a foreign adversary as well as provide assistance to international allies when required.[778]

[776] Republic of Ghana Ministry ofCommunications (n 759). [20]
[777] ibid. [21]
[778] Botswana Ministry of Information Communications and Technology (n 763). [29]

Conversely, similar strategy formulation within the developed states data, serves or suggest a different purpose. Whereby in the case of the developing states, the focus is directed in-wards (while looking outward for support), its use within the developed states' data is designed to establish the self, albeit as a gatekeeper of the entire global population.

> Cyber space is not – and must never be – a lawless world. It is the UK's view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain. The UK has always been clear that we consider cyber space to be an integral part of the rules based international order that we are proud to promote. The question is not whether or not international law applies, but rather how it applies and whether our current understanding is sufficient.[779]

Thus, while such strategy might engage identity construction, its formulations are rarely explicit. Rather, it engages in the description of such formulation through extensive narratives around its intentions for cyber power and the needs of the entire global population, to help 'lift up' the less capable states, their expectations of them, beliefs and values and how the entire global population ought to be construed. And above all, its willingness to promote a specific 'this way of doing things' that is based on its own construction of 'how-to', to the rest of the global society, particularly those in the Global South:

> We want to see international law respected in cyberspace, just as we would anywhere else. And we need to show how the rules apply to these changes in technology… So, our challenge is to clarify how those

[779] Jeremy Wright, 'Cyber and International Law in the 21st Century' (2018) 2018 Chatham House Speech 19 <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>. [5]

> rules apply, how they are enforced, and guard against authoritarian regimes bending the principles to meet their own malicious ends. [780]

Indeed, this strategy, while it is implied through expressions as above, and despites the many forms through which subjectivities are constructed, the role of the strategy is undoubtably visible. Particularly in the discursive nexus that exist between, on the one hand, its desire to shape the narratives of cybersecurity challenges, the risk realities of cyber-attacks, threats, and the identities of 'dependent' developing states, on the other hand, who rely on their support to deal with those realities. In this discourse, and as an occasioned prerequisite for such support been granted, these 'needy' societies must adapt to the 'new' ways of thinking and of doing things. Thus, they are required to adjust their laws, acquire new technical abilities and capacities to do so. They must learn new skills to allow them to deal with the issues of cybersecurity and to be afforded the possibility to progress through modernisation, and be counted amongst those subjects in the 'us' group, even if it is on its fringes.

Thus, the process of adaptation, transformation and transition, from a position of no capacity to that of having capacity, lends itself, first, as an opportunity (for the knowledge exporters) to advocate for the desired state of play, and promote the desired identities that are mirrored in their own image. Second, for the importers of the knowledge or those with the knowledge gaps, it presents itself as freedom and opportunity, to experience and emulate the

[780] Raab, Foreign Commonwealth and Development and National Cyber Security Centre (n 635); Raab (n 623). [12]

coveted identities of the expert exporters, but with their own feeling of responsibility, a shared responsibility for that matter, to enact those rules that are suggestive of a self-governing sovereign state.

What is observed here, is the notion of 'truth' as it relates to these 'rules of play' and what it means. The argument is that what is being passed as truth is not necessarily true in the context of how things 'really' are. Thus, the representation of truth, albeit not necessarily true, impacts the relations of power as well as the perception of the 'self'.[781] In other words, when observed through Foucauldian lens, the impact of this 'truth effect' suggests a nexus that allows for the normalising objectives of authoritative narratives, that are tied to one's self-aspirations and expectations.[782] This is the case because, one's construction of one's own identity is influenced by, and dependent on, certain practices or experiences that are in turn based around relations, and experiences derived from certain specific contexts and discourse.

Consequently, while the deployment of power, observable within the case data from the developing Commonwealth states, may take, or appear to take different forms, the discourse on their cybersecurity needs or the potential benefits of digital transformation for economic growth and prosperity, may represent pervasive strategies and techniques, designed by the promoters of the elite 'us' group, towards the global population. But more specifically, towards the

[781] Eva Sørensen and Peter Triantafillou, *The Politics of Self-Governance* (Eva Sørensen and Peter Triantafillou eds, 1st edn, Routledge 2009).)
[782] Besley (n 731)..

developing states, upon whom this discourse of transformation and transition is often and continually directed and deployed:

> In this context, the 2030 Agenda for Sustainable Development and the EU Consensus on Development focuses on People and Peace. The new EU focus on Digital4Development also highlights how cybersecurity can be an enabler for development whilst also noting the risks posed by cyber "insecurity".[783]
>
> The development of a comprehensive legal and regulatory framework on data can in fact be the key to unlocking digital trust for e-commerce in many developing Commonwealth countries.[784]Contrary to many developed countries in both the earlier and current phases of digitalisation, most developing countries lack policies governing the collection and use of data (as discussed in Section 5.1), increasing the risk of their data being controlled by whoever gathers, stores and has exclusive rights on the data.[785]

Ironically, the last sentence of the quote above, appears to warn against a form of dependence that could occur, should such opportunities not be sought. But in reality, such dependence is unavoidable for developing states, particularly those with smaller economies.

8.3 Discussing the common biopolitical techniques

Common observable problem-fields emerge across the data, both in the form of problematised phenomenon (such as cybersecurity), and in the form of problematised groups or states. That is, in the same way that the issue of cybersecurity is problematised, some states, are also represented as problem-spaces by virtue of their genealogical and biological classification, as well as their

[783] Jan Sadek, 'EU Cyber Resilience for Development Project Launch Address by Ambassador Jan Sadek'. [3]

[784] The Commonwealth (n 634). [112]

[785] ibid. [121]

contemporary ‘sub-standard’ developmental status. This is evident, for example, in the classification of some as ‘weak links’ in the global cybersecurity effort,[786] which rationalises calls for collaborative efforts to assist their transformation, because what impacts ‘us’ by ignoring ‘them’, is far greater. Hence the argument that such an approach to the problem of cybersecurity, suggests the constitution of the problem as a biopolitical problematisation of how the problem can be governed, regulated or managed or controlled.[787] This is not dissimilar to what Foucault conceptualised as a biopolitical problematisation of the regulation of life or man.[788] A form of biopower, that is, a “biopolitics of the population” which according to Foucault, is “not applied to man as a body, but to the living being; ultimately, to man as species.”[789] In other words, what is observed in this problematised field, which appears to focus on the global population (the need to build a strong global cybersecurity through support or ‘giving life’ to the weaker members of the group), is akin to the discourse of the human species emerging as objects of global strategy of power or biopower.[790]

Thus, this global strategy of power is activated through the desire of the powerful states, in their quest for global authority, and through their efforts to secure and promote every ‘life’ as it relates to cyber space.[791] ‘Life’ here,

[786] Koenders (n 110).See also reference to Ghana Minister speech

[787] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319); Rose, ‘The Politics of Life Itself’: (n 589).

[788] Nikolas Rose, *The Politics of Life Itself* (Princeton University Press 2007). See also Dillon and Lobo-Guerrero (n 205).

[789] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706). [490]

[790] ibid.

[791] Foucault, *Society Must Be Defended: Lectures at the Collège de France 1975 - 1976* (n 724).Foucault 2003

therefore, is guaranteed or secured when it is visible and controlled through regulations or norms, designed by the same higher authorities. And as such, the objective or function of governmentality here, is the activation of cyber space as free and open space that everyone should enjoy, and hence, the promotion of practices designed to sustain 'life' within it, and indeed, all 'lives' for that matter.

For Foucault, biopolitics suggest the realignment of current and historic elements that are both discursive and material. This can be conceptualised to function as governmental techniques and discursive articulations that ultimately render certain groups (disadvantaged developing states, for example), as targets of global politics.[792] Thus, the presence of such groups, or the visibility of their cybersecurity problems, becomes the governmental focus in providing answers to the question of; what must the global society and its gatekeepers concern themselves with? What must the rich and powerful West do to support the poor and weaker nations of the South?[793]

In this case, and in the words of such gate keepers, securing cyber space and ensuring a rules-based system, deployed to govern activities and behaviours in cyber space, becomes their duty-bound call.[794] As such, this preoccupation with the problem emerges as a governmental tactic, established through actions that can be conceptualised as arts of governing in relation to Foucault's *dispositif*

[792] ibid. See also Polly Sylvia, 'The Performance of Security as a Site of Biopolitical Struggle' (2014) 14 Cultural Studies ↔ Critical MethodologiesCritical Methodologies 451.
[793] (Foucault 2007: 350)
[794] Raab, Foreign Commonwealth and Development and National Cyber Security Centre (n 635).

or apparatus of security, as forming parts of the biopolitical mechanisms.[795] The *dispositif*, according to Foucault, represent a form "composed of heterogeneous elements that have been stabilized and set to work in multiple domains",[796] operating as a result, through the "said and unsaid" medium across different contexts or domains.[797]

One might ask at this stage, how is this all playing out within the context of cybersecurity and across our case spheres? What is revealed within the case analysis that might suggest new rationalities of the 'ideal' within this context and their associated fields of actions? As part of this relatively comparative (although not readily conceived as such) discussion, possible answers to these questions is, first, explored, before examining areas where individually diverse features are observed within the case data.

Evidently, common problematisation of cybersecurity is arguably present across the case data. This is demonstrated in their shared pre-occupation, which allows for a global perception of the problem as both the end and governmental instrument. [798] In other words, a common strategic deployment of rationalities and technologies of security exists within the data that attempt a rather productive 'governmentalisation'[799] of the problem-field in

[795] Foucault, *The Essential Foucault* (n 398).
[796] Michel Foucault, *The Essential Foucault Selections from Essential Works of Foucault, 1954-1984* (Paul Rabinow and Nikolas Rose eds, The New Press 2003). [55]
[797] Foucault, *The Essential Foucault* (n 398).
[798] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).
[799] Peter Triantafillou, *New Forms of Governing* (Palgrave Macmillan 2012).

similar ways.[800] This suggests that, by looking at the similarities, connections can be drawn between similar observations in governmentality literature, with examples that present or imply neoliberal governmentalities in the form of governmentalized or controlled problem-fields.[801] In other words, the notion of the presence of such governmentalized fields, which allow for the identification or labelling of certain actions, practices, solution to problems and policy reforms, as neoliberal. This is so because, such problem-fields imply a form of constituted structure or practice that describes them in that way, particularly through the emergence of economic rationality that seeks a securitised life mode.[802] An identification which is further made possible by implying that those practices and solutions, are deemed the *de facto* organising schemes, norms or standard value systems, frameworks or anything else defined as such.[803]

One must also ask whether these common features form sufficient justification to characterise them as suggestive of how the problem-space is controlled or governed. If the answer is in the affirmative, what then is the relevance of the data used in this analysis, or how appropriate are they as empirical texts in an enquiry focusing on, what might be seen as, a neoliberal problematisation of cybersecurity? To help understand this question, further insight is provided on the use of governmentality as an analytical category.

[800] Dillon (n 205).
[801] Triantafillou (n 799).(Triantafillou 2012; Sorenson and Triantafillou 2009; Ball and Junemann 2012).
[802] Nicholas J Kiersey, 'Scale, Security, and Political Economy: Debating the Biopolitics of the Global War on Terror' (2009) 31 New Political Science 27.
[803] Stephen J Collier, *Post-Soviet Social Neoliberalism, Social Modernity, Biopolitics* (Course Boo, Princeton University Press 2011). See also Rose, O'malley and Valverde (n 764).

8.4 Deployment of governmentality as a meta-analytical category

While the use of governmentality or the exploration of government ‘actions’ beyond what is outwardly expressed may appear complicating, the prospect of examining neoliberal affinities across authoritative texts from multiple sites, is reassuring. This is because, its potentials are underpinned by the fact that it challenges the typical narrative of development, independence, progress and modernisation.[804] It does so by attempting to unravel the processes of ‘government’ and identifying elements of such actions as biopolitical forms of security, as opposed to its perception as simply activities designed to provide solutions to a known problem or phenomenon . Thus, identifying similarities, as has been attempted thus far, in the use of certain tactics that suggests the presence of governmentality functions, helps highlight the common denominators within the mechanisms of power - which, according to Foucault, “are an intrinsic part of all [...] relations and, in a circular way, are both their effect and cause“.[805] However, to explore and explain the deeper “operational logics, forces and dynamics at play in a specific configuration of power relations”,[806] there is also a need to identify and analyse the different elements of power configurations across the cases.

Providing answers to such question of how governmental subjects are framed in the pursuit of a governable global society, within a specific biopolitical

[804] Walters (n 723).
[805] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706). [2]
[806] ibid.

sphere, presents us with an example. As an object upon which power can be exerted, the global society is at the centre of the fields of thoughts. In other words, it does not determine the heterogenous processes of subject formation deployed by those who govern it. As such, it functions or operates within the framework of the political fields (thought and action). However, one must also accept that, while the construction of the global population, as object, allows for the visibility of certain similarities, behavioural characteristics and co-relations in practices or actions, to be revealed, it does not provide sufficient account of power as it applies in specific context. The reason is that such power is shaped by complex networks or relations, events and things.[807] Therefore, one's observation can never really be conclusive, but one should seek to understand them, nonetheless.

For Foucault, what is central to all of this is the understanding that, the various rationalities, discourses, tactics or techniques of the different power apparatuses, are not formed in isolation.

> At a given moment, in a given society, in a given country—a technology of security, for example, will be set up taking up again and sometimes even multiplying juridical and disciplinary elements and redeploying them within its specific tactic.[808]

Rather, there are new forms of biopolitical assemblages (cybersecurity, in our case), that are contingent and exist with, and present multiple *dispositif* elements (which may be legal or disciplinary in nature). However, and according

[807] Dillon and Lobo-Guerrero (n 205). See also, Villadsen and Wahlberg (n 756).

[808] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706). [23]

to Rabinow, these elements, while connected to the assemblages, they remain different.[809] As opposed to the *dispositif* of government, assemblages of power are "comparatively effervescent, disappearing in years or decades rather than centuries".[810] The *dispositif* on the other hand, allow for the obtrusion of certain elements or structural framework of things, which in turn hegemonize the assemblage of power.[811] Thus, the presence of techniques, and discourses (such as *dispositif* elements) within an assemblage of power (such as cybersecurity), becomes part of, and absorbed into the main apparatus. For Koopman, the result of the boundless potentials of rehashing and merging diverse elements that constitute our 'reality', leads to this outcome.[812] As a consequence, the success of this process lies in the coherent organization of these elements, considering the specific context and purpose they are directed toward or applied in/to.[813]

8.5 Demonstrating variations between the case data – contexts and assemblages of power

In directing attention to observable variations between the cases, the goal is to pinpoint specific themes within the different referent data in relation to how the common biopolitical problematisation themes, shared by all the cases, are defined further into other distinct assemblages of power. Thus, the analytical focus here is on how the issue and practice of normalisation is used and to what

[809] Foucault, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984* (n 41); Rabinow (n 44).
[810] Foucault, *The Essential Foucault Selections from Essential Works of Foucault, 1954-1984* (n 796).[56].
[811]Villadsen and Wahlberg (n 756).
[812] Koopman and Matza (n 465).
[813] Villadsen and Wahlberg (n 756). See also, Koopman and Matza (n 465).

effect. Because normalisation plays a key role in the construction of power relations, the aim is to demonstrate further how such power works within the case-contexts.

8.5.1 Strategy of Security – rights as a constitution of the political subject

In The Will to Knowledge, Foucault describes biopower as a form of "power that exerts a positive influence on life, that endeavours to administer, optimize, and multiply it, subjecting it to precise controls and comprehensive regulations".[814] For Foucault, it is necessary for the mechanisms of power to find new and creative ways of constituting the subject. Here, for example, he identified law and governmental practices as key players in the process.

With regards to law, its fundamental problem,

> will no longer be the foundation of sovereignty, the conditions of the sovereign's legitimacy, or the conditions under which the sovereign's rights can be exercised legitimately, as it was in the seventeenth and eighteenth centuries.[815]

Rather, it becomes more of a problem of "how juridical limits to the exercise of power by a public authority" can be set.[816] This, Foucault believes, was resolved in the nineteenth century through the "juridico-deductive" approach, which operates from law in its classical form, to "define the natural or original rights that belong to every individual. And then, to define under what

[814] Foucault, *The History of Sexuality Volume I, The Will to Knowledge* (n 409). [137]
[815] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).[39]
[816] ibid. [39]

conditions, for what reason, and according to what ideal or historical procedures, a limitation or exchange of rights was accepted”. [817] In other words, an approach which builds on the notion of “the rights of man in order to arrive at the limitation of governmentality” through the idea or “constitution of the sovereign”.[818]

Across data from the developing Commonwealth states, a similar approach is observed. Here, the notion of state sovereignty is presented such that the developing states, as subjects, appear as incumbents of rights at its natural and original form, at least according to the customary international law.[819] This demonstrates a deliberate constitution of such sovereign states as subjects of rights - a common feature within the cybersecurity capacity building discourse, where efforts are made to ensure that supported states are intentionally regarded as sovereign states, and therefore, should not be made to perceive any recommendation for action as prescriptive, or suggestive of a diminished sovereignty. And as expounded by Bröckling et al.,:

> Governmental practices rarely operate by direct command and control. Both the principle of obedience and—even more so—the exercise of constraint are very costly and tied to great risk. It seems more effective to guide individuals and collectives “through their freedom,” in other words to prompt them to govern themselves, to give them positive incentives to act in a certain way and understand themselves as free subjects.[820]

[817] ibid. [39]

[818] ibid. [39]

[819] Till Müller, ‘Customary Transnational Law: Attacking the Last Resort of State Sovereignty’ (2008) 15 Indiana Journal of Global Legal Studies 19.

[820] Bröckling, Krasmann and Lemke (n 757). [13]

Similarly, the Commonwealth Cybersecurity for Elections Best Practice guide cautions against this tactic:

> Cybersecurity co-operation does, however, remain challenging for some EMBs, who must avoid the perception of international regulatory capture, particularly where electorates commonly express distrust about electoral governance or where international tensions exist. Co-operation should be carried out openly and clearly, with clear tasks and reasons for such co-operation, to ensure that public trust is not endangered.[821]

Indeed, this given freedom or supposed rights is also expressed in national cybersecurity strategies, allowing the "juridico-deductive" approach to reach a near perfect alignment between the subject and the object of power.[822] And in the case of cybersecurity, this is done through the positioning of the problem (in poorer case states) under the legitimacy (albeit illusionary, created through discourses) of the sovereign authority, the seeming respect for the right of a sovereign authority to make its own decision, to defend itself, etc. But at the same time such states are expected to respect rules of the game, as expressed by the UK Attorney General, Jeremy Wright QC MP, in a Chatham House speech in 2017:

> Online as well as everywhere else, the principle of sovereignty should not be used by states to undermine fundamental rights and freedoms and the right balance must be struck between national security and the protection of privacy and human rights.[823]
>
> I have talked about the behaviour to be expected of states in cyberspace and their entitlement to defend themselves but having a

[821] The commonwealth secretariat (n 552). [102]
[822] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).
[823] Wright (n 779). [11]

> legal framework within which to act is not the same as having the practical capacity to act, and the UK needs that too. [824]

Consequently, the creation of specific laws, targeting the various problem areas, are used to create normative and security order through legal rationalities or techniques, orchestrated to ensure the desired behaviour permissible in cyber space. Thus, new and existing rules are promoted at global levels, with the construction of equivalent models encouraged at local levels. Therefore, it becomes more of the case of how such legal rationalities are perceived within the biopolitical/geopolitical governance context.

Looking at the Commonwealth cybercrime model laws, for example, one could argue, that the legal rules are not necessarily designed to confer rights on the sovereign state. Rather, such model laws function as a global governmental practice to ensure obedience or enlist a followership of the collective sovereignty conferred on the entire global society. The collective sovereignty here being, that which is predetermined by the elite states. Thus, various tactics are employed other than law, ensuring the desired objectives through heterogenous means necessary.[825] An identifiable objective here being the alignment or government of non-docile subjects, which are rights-aware and freedom-aware, and are confident in efforts that professes such assumptions.

[824] ibid. [12]

[825] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).[99]

The juridico-deductive approach, therefore, allows law and sovereignty to be aligned, along with other elements, which in turn allow the discursive subjects of rights and freedom to emerge, while other objectives remain hidden.[826] Evidently, the biopolitical ambitions within the cybersecurity practices, allow these subjects of rights to be formed through these heterogenous arrays of techniques (through the presentation of equality, freedom, global justice, etc. against the background of the cybersecurity threat politics).

Another observed variation within the case data is that the construction of the subject of rights are context specific. For example, within data from the UK and other Western states and non-government institutions, attention is not drawn predominantly towards the liberal dispensation of the subjects as rights-bearing individuals (when the subjects are developing states). Rather, the focus is on the notion of commonality of the problem. In other words, the need to fix cyber space for the common interest of the global community, based around the need for a common political will for openness, equality, democracy, solidarity, is stressed, as opposed to directing focus onto themselves. Thus, the use of subjects of right as a biopolitical mechanism in this context, and in relation to the developed states and their activities in the developing states, necessitates an assemblage of such subject through politicised narratives of the global collective.

In other words, the problematisation of cybersecurity challenges through practices such as capacity building, development of model laws, etc. is

[826] Ben Golder, *Foucault and the Politics of Rights* (Stanford University Press 2015) <http://ebookcentral.proquest.com/lib/lancaster/detail.action?docID=3568975>.

focused, not only on those subjectivities whose values mirror those of the West, or those that are more likely to be subversive, rebellious or defiant of Western values and agendas (like China, Russia, Iran, etc.). Rather, the focus is typically on such subjects which, despite their claim to cultural or political sovereignty, are more susceptible and agreeable to Western approaches. Subjects like the developing Commonwealth states, who relish the idea of the collective, or whose perception of the idea of cooperation rests mainly on the understanding of the cybersecurity problem 'truth', as defined by the dominant states. And above all, those who primarily recognise the perceived benefits of solutions emerging from digitally advanced sources, as opportunities to mitigate the risks of insecurities and improve their own economic advancement.

Hence, the perception of such states is what that sort of biopolitical mechanism seek to mould, as reflected in one of the interviews, which suggests a 'we need them more than they need us' mentality. For example, the senior officer in Ghana, when asked about the focus of the country's cybersecurity framework, and the role played by its collaboration with other developed states and international institutions in shaping this focus, parts of the response went as follows:

> You certainly need collaboration with external international parties.We have bilateral collaborations. We have voluntary collaboration or cooperation and we have other later cooperative arrangements, all of which have helped us, more than anything else in developing our own systems….
>
> I think in 2014, 2015 thereabout, I personally coordinated projects between the commonwealth cyber crime initiative with the government of Ghana and that led to signing of an MoU (mommerandum of Understanding) But I must say that relationship didn't go far in terms of implementing the various initiatives that were supposed to be implemented.

> … but you know, cybersecurity is a broader area with different players. So the UK Government is one of the players indeed. We have learned from their practices and I have visited the UK National Cybersecurity Center and so we have exchanges with them.
>
> They have supported our work currently in terms of building the structure. But they are one out of several players we have.
>
> World Bank is one of our partners. The Council of Europe is our partner. ECOWAS West African Union is another. Then the US government, through their strategic governance Partnership initiative, UNICEF is also one of the party that support us for Child Online Protection issues.[827]

8.6 Understanding normalising power and its effects across case context

According to Bröckling et al., rationalisation and practices of government produce subjects by "invoking and legitimizing certain images of the self while excluding others." This suggests that such entities are to a greater extent, self-aware, as opposed to being misled, or misguided, and therefore, understand their rights. They also identify with their place in the world order, alongside everyone else, sharing similar concerns about the future of the global society. This is evident when governments, irrespective of their economic status, make pronunciations like, 'our responsibility as global citizens, to do X or Y' or 'fight against Y and Z,' and so on.

Central to Foucault's ideas on power is the notion that, power is manifested through the apparatuses of security, sovereignty and discipline.[828]

[827] The Researcher (n 554).

[828] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).

This is done in ways that allow them to occupy the governable spaces in their distinct ways.[829] For example, whereas "sovereignty capitalizes a territory, raising the major problem of the seat of government",[830] discipline on the other hand, "structures a space and addresses the essential problem of a hierarchical and functional distribution of elements".[831] Security, however, will seek to organise the "*milieu* in terms of events or series of events or possible elements, of series that will have to be regulated within a multivalent and transformable framework."[832] Thus, the three different apparatuses are able to function, albeit differently, in the same normalising *milieu*, almost in collaboration, buttressing and augmenting one another.

Thus, normalising power is produced through these three elements. Sovereignty, however, is played out through law, because law and discipline are advanced on the difference between what is allowed, and what is outlawed. In other words, law can only exist where there is an understanding of what is permissible (normalised) and what can be transgressed (not normal or outside the norm). Here the function of the law becomes that of maintaining a certain *status quo*, of the allowed or permissible, while banning the 'other' or anything else that is contrary to the norm. And it does so, not through its focus on the positive, but rather, through its fixation on the negative (the problem), through problematising tactics (curating the visibility of the problem and orchestrating

[829] ibid. See also, Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).
[830] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706). [35[
[831] ibid.
[832] ibid.

its diagnosis).[833] Its ultimate goal becomes that of reinstating the desired *status quo* or normalised version of event, the so called ‘order’. Order, therefore, according to law, becomes that which is achievable through control or regulation, the elimination, alienation and prevention of that which is forbidden, or that which becomes considered as the problem.

Discipline on the other hand focuses on the positive, or the permissible. Thus, discipline’s focus is on prescribing that which ought to be or, in most cases, must be done to be on the right side of the allowed. In other words, it recommends sovereignty, or the norm (law), thereby expressing more interest in the subject, as opposed to the law itself, whose real interest in the subject emerges post or from transgression, hence an object of control, employing discipline only in its actions.[834]

Security seek neither to forbid nor to prescribe. Its focus, on the other hand, is reactive to events, phenomenon or perceived reality (albeit negative which in some sense, a perception it also helps to create) with a responsibility of ensuring that the necessary checks, regulations, etc., are in place in order to correct or control this negative reality.[835] Thus, normalising power through sovereignty (by way of law) and discipline, work together by creating or seeking to create a desired reality, such that, it proposes (prescribes, in some cases) norms that meet or fit the desired reality.

[833] Dean, ‘Putting the Technological into Government’ (n 533).

[834] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).

[835] ibid. [47]

In effect, normalising power works to create two groups of subjects: first, those that it considers complaint, accepting of its proposed (prescribed) norms and frameworks, abiding by those norms, and thus, on the side of the normal. Second, those who reject the notion of the 'established' norm , or its transgressors and, therefore, fall outside the norm. The objective of biopolitical normalisation, therefore, becomes that of creating various forms of norms as applicable to the created reality or phenomenon, establishing rules and monitoring behaviours with the goal of ensuring that subjects are kept within the acceptable parameters of what is considered normal, thereby facilitating its control.[836]

Normalisation tactics, as already discussed, relates to how cybersecurity challenges are presented, represented and diagnosed.[837] The interest here, however, relates to its deployment in relation to law or the legal system, designed to codify the system of norms around cybersecurity practices. The questions attempted remain focused on; how are such techniques represented within the case data? What role do states like the UK play in shaping this system of norms and for what purpose? To examine these questions further, we examine the processes of normalisation based on what is revealed in the case data, and provide better insight into the role of such mechanism of power.

[836] ibid. [63]

[837] See chapters five and six

8.6.1 Processes of normalisation and its impact

Techniques of normalisation take multiple forms and draw strength from equally heterogenous discursive functions which work through networks of power. These functions may intersect or overlap each other sometimes, while, at other times, they could stand in opposition. As processes of normalisation, they may be at work together at any one time, as observed within the case data. The argument is that these processes are deployed through forms of biopolitical logic, articulated for the purpose of garnering alliances amongst the developing Commonwealth states and the global population, to attract the right sentiments and voices towards its orchestrated 'reality'.

As observed within the UK government policy paper: *Global Britain in a Competitive Age*,[838] the primary focus of the state is aimed at attaining "responsible and democratic cyber power."[839] An ambition which it seeks , amongst other things, through its influence, within global politics, economic status, technological prowess, a whole-of-nation cyber ecosystem, offensive cyber capabilities, and diplomacy. Through this new ambition, it recognises the need to maintain power through its defence of the *status quo,* to protect its interest in the world, alongside the need to employ measures, designed to sway or "shape the international order of the future" in its own interest.[840] Thus, its role as a key player in the normative control of cyberspace can only be achieved

[838] HM Government, 'Global Britain in a Competitive Age' (n 722).
[839] ibid. [35]
[840] ibid. [12]

through its promotion of a perceived "free, open, peaceful and secure cyberspace".[841]

Perhaps, the problem of cybersecurity is no more glamorised than the opportunity of acquiring power that comes with solving its 'problems'. This is embodied in efforts that are overtly expressed, as seen above and demonstrated further below, as it becomes very less about solving a problem, but seizing the opportunities that such a problem creates.[842] Crucially, this appears to be done as a way of regaining or developing new political power. Particularly through development of legal frameworks, setting the parameters for what is acceptable and what is not and prescribing such frameworks to the rest of the world:

> Cyberspace is getting larger, not smaller. Its influence on international relations is growing not shrinking. So, it is ever more important, and part of the UK's role in global leadership, to do what we can to ensure the law applies in cyberspace too.[843]
>
> To build international consensus on the role of international law in this area, the UK, together with other states, has engaged in negotiations under a mandate from the UN Secretary General to progress multilateral agreement on the parameters of responsible state behaviour in cyberspace.[844]

This expressed desire to dominate and control, is also suggestive of a biopolitical normalisation whereby, the challenges of cybersecurity are rehashed, not necessarily in light of its negative and malicious forms, but whose positive function - that of opportunity rather than threat, is harnessed, albeit biopolitical.

[841] ibid. [41]
[842] ibid. see also Britain in the World Project at Policy Exchange, 'Making Global Britain Work' <www.policyexchange.org.uk>.
[843] Wright (n 779). [16]
[844] ibid. [6]

This is reminiscent of a new era of colonising ambitions, paving the way for a new age of global supremacy through cyber strength, power and dominance, while at the same time, employing biopolitical means of normalisation in its efforts.

> Keeping the UK's place at the leading edge of science and technology will be essential to our prosperity and competitiveness in the digital age. Our aim is to have secured our status as a Science and Tech Superpower by 2030, by redoubling our commitment to research and development, bolstering our global network of innovation partnerships, and improving our national skills – including by attracting the world's best and brightest to the UK through our new Global Talent Visa. We will lay the foundations for long-term prosperity, establishing the UK as a global service, digital and data hub by drawing on our nation's great strengths in digital technologies, and attracting inward investment.[845]
>
> Shaping the open international order of the future: we will use our convening power and work with partners to reinvigorate the international system. In doing so, we will ensure that it is one in which open societies and open economies can flourish as we move further into the digital age – creating a world that is more favourable to democracies and the defence of universal values. We will seek to reinforce and renew existing pillars of the international order – such as the UN and the global trading system – and to establish norms in the future frontiers of cyberspace, emerging technology, data and space. [846]

Joseph Nye identified three possible aspects of power. One is about "getting others to do what they would not otherwise do".[847] A second focuses on constructions that frame issues in one's interest. And a third shapes the desires, interests and preferences of others, exerting "power by determining others'

[845] HM Government, 'Global Britain in a Competitive Age' (n 722). [6]
[846] ibid. [20]
[847] Nye, 'Cyber Power' (n 17). [2]

wants."[848] For Nye, while power or ambitions of power within information technology is not necessarily novel, cyber power on the other hand is. Thus, the ability of powerful states to adapt and frame the assemblage of cyber power in ways that serves their interests, allowing them to control and influence norms within the space, is central to their ambition; From a simple notion of developing capability to a guaranteed "cyber superpower" as expressed within the UK policy statement.[849]

Therefore, this discussion is motivated by the biopolitical turn that such ambitions take. And as observed within the quotes above, such strategies which abandon coercion and calculatedly desist from the need to be overtly prescriptive, in order to disguise its real objectives, are indicative of biopolitical mechanisms working together.

8.7 Techniques of normalisation in developing states

Indeed, multiple normalisation practices are noticeable at any one time. This is sufficiently exemplified within the data whereby certain cybersecurity risk-averse practices are romanticised. For example, the discourse on the economic benefit of the internet and the need to create a culture of cybersecurity awareness, to ensure that countries are reaping the benefits.[850]

The presence of a perceived constant threat is another. Focusing on the 'pleasures' of cyberspace in this way, enables the challenges to be seen, not

[848] ibid.
[849] Government of the United Kingdom (n 13).
[850] This is a common thread that run across all cyber security strategy, plan or policy

simply as a problem, but as an opportunity to control the entire cyberspace. Again, tactics, that employ governmentality to encourage buy-ins from everyone, to gain their support, fight off resistance, and 'empower' everyone to take ownership of the problem, and speak the same cybersecurity language as the rest of the civilised international community:

> The need to create a culture of security which is absent today due to lack of awareness of the enormous threats that users of Internet are exposed must be addressed by a national cybersecurity policy. Awareness creation of the risks Internet users and other stakeholders are exposed to can drastically mitigate the risks of cyber attacks and consequential loss of revenue. This will create a very conducive environment in the information economy where Ghanaians can create worth in peace without fear of harassment by cyber-criminal and fraudsters.[851]

Thus, the effect of recasting rationalising discourse as serving biopolitical interests (such as the buy-ins from developing states), suggests a normalisation that is thus biopolitical. As such, a problem reality is created which then creates the need for a global army of cyber experts and professionals, to meet the demand for action. The entire society therefore needs to be cyber aware. Training needs for the entire public and for the trainers becomes hot topic, even in developing states. At the same time, cybersecurity experts and cyber education professionals are fed into the scheme, instructed on the operations of the normalising processes, through special government training programs, regular educational curriculum, etc. All to further feed multifarious interests that may be economic, geopolitical and more.

[851] Republic of Ghana Ministry ofCommunications (n 759). [15]

> Cyber threats by their nature do not discriminate between big and small institutions…
>
> There are many examples of cyber incidents against multi-national corporations and individuals. Cyber threats can be complex. Therefore, ordinary individuals with less sophistication and means may require to be continuously assisted and educated, to keep up with evolving threats. These threats and risks are ever presents. Therefore, it is very important that Government and other key stakeholders, play an active role in addressing the National Cybersecurity Strategy.[852]

As well as discourses that are fed through a paradigm of 'innovate or die' as a condition of a modern prosperous society:

> Botswana is experiencing a growing dependence on Cyberspace for the delivery of services essential to people's daily lives, commerce, National security, innovation and the general free flow of information. The increasing dependency on ICTs by both public and private sectors, makes protection and sharing of information more critical in order to protect the economic interests and security of Botswana and her citizens.[853]
>
> iv) Training, specifically in the area of cybersecurity needs to be improved; all stakeholders such as regulators, Law Enforcement Agencies, Judiciary, Prosecutors, Service providers, Financial Institutions, service providers need to have adequate capacity and capability to handle matters related to cyber security.[854]

Noteworthy to this discussion is the goal of the developed states and other global institutions (who not only make these training recommendations, but are also actively engaged in their delivery) which seek to avoid making such recommendations appear prescriptive, such that one remains conscious of existing norms that separate what's normal from that which is to be avoided.

[852] Botswana Ministry of Information Communications and Technology (n 763). [5-6]
[853] ibid. [11-12]
[854] ibid. [9]

Romanticising security problems thus, is a calculative effort to highlight practices (cyber fraud, *Asaki*, malicious state behaviour, etc.) that are considered counterintuitive to the security narratives and, therefore, enemies of the developmental and economic benefits. Asserting these negative practices, therefore, allows them to become naturally visible parts of the problem.

Herein lies the operations of normalisation that is intramural to security; allowing the norms to be formed through knowledge rather than an overt separation of the normal from the abnormal. In other words, setting the stage for the norm to be formed through observation and identification of bodies and their desires, allows us to understand how certain cybersecurity practices can be normalised and render developing states agreeable followers and willing adopters of model laws and training programs developed elsewhere in the North, as demonstrated here:

> we recommend that Botswana should domesticate the SADC Model Law on Data Protection as such model, in our opinion is fully compliant with best practice.[855]
>
> Finally, fostering Networks of Cyber Expertise and Cooperation. Here we seek to support and promote regional and international cooperation on cybersecurity issues. Through increased awareness of cybersecurity best practices and the sharing of information and experience, Botswana will have the opportunity to further enhance its/her capabilities to deliver cyber resilience.[856]
>
> Under the auspices of the HIPCAR Project, and my colleague explained what that is, but basically, that is to say that the project to enhance the competitiveness of the Caribbean through the harmonization of ICT policies. So, Mr. Speaker, legislation and regulatory procedures through which Trinidad and Tobago was able to benefit from model legislation texts which were developed in accordance with the international and regional best practices using technology, neutral

[855] BOCRA, 'Development of a National Broadband Strategy' 9. [7]
[856] Sadek (n 783). [5-6]

> language which is also very critical and significant, which further underscores the importance of cooperation and collaboration with regional and international neighbours.[857]

Romanticising cybersecurity best practices, as cited in the Botswana government text, performs well as a strategy of security, cementing a notion of collectiveness once again, as opposed to the promotion of individual efforts amongst such states. This is because, the effect of the normalisation strategy allows for a perception of such monolithic tendency as one which is not representative of statistical normality, particularly if we consider the interconnectedness of the problem. Thus, the understanding (at least for the poorer nations) is the acceptance of the power of knowledge through which the richer states can govern. The perspective effect of seeing it as one which seizes the natural processes and desires and shortcomings of the outside, peripheral societies, used calculatedly to minimise or obscure the biopolitical realities of its intentions in the actions towards the problem.

Thus, security normalisation identifies the desire for the benefits of modern technology amongst poorer states, their pursuit of economic growth, digital transformation and technological advancement. It sees their desire to reach new heights as internal to the process of constructing the global society. And from this recognition, it creates an opportunity for intervention. And doing so in such fashion serves to limit or minimise any sense of coercion.

[857] Ministry of National Security (n 738). [10]

Therefore, the desire of poorer economies to pursue their own cyber ambitions and bring improvements to their societies, serves as a biopolitical resource for the wealthier states. This is because, for developing states, their focus would appear to be on attaining such improvement with less concern about falling for the same 'old trick'. Such that even the Commonwealth report on digital connectivity, [858] and on Cyber-governance (cited below), warns against such circumstances or possibilities, when the so-called collaborations risk creating such position for the developing states.

> At the same time, while it was acknowledged that cooperation is essential to promote a secure cyberspace, cooperation between countries needs to be made on a clear basis as there is a risk if cooperation extends to the extent that it becomes a dependency, particularly in the critical national infrastructure sectors. [859]

Nonetheless, while these techniques of government may not always be hidden, they remain effective regardless. This is because, those targeted may have fewer alternatives, to subvert such situation, as they are seemingly trapped in this circle of dependency, which form parts of the objective of such mechanisms.

Normalisation, therefore, must be seen as any practice that cuts across normalising processes derived from realities (statistical, political, social economic, etc), to the romanticised model of best practice, or *status quo,* that correlates with the mechanisms of discipline and, therefore, serve as a way of

[858] The Commonwealth (n 634).[24-25]
[859] Chatham House's International Security Department (n 572). [5]

measuring relations and situations.[860] The data exhibits suggestions of various forms of this normalisation, spanning across the different groups. And as can be seen from the quotes, suggestive elements of the security apparatuses are visibly at play.

There are also similar prescriptive tactics of normalisation with perceived disciplinary norm effect. An example of such effect can be observed through Foucault's notion of "dividing practices,"[861] which is discernible when one examines the question of whose cybersecurity is being problematised, and whose is not. Particularly in terms of how the subject is formed in the first place. This is demonstrated, first, in the identification, presentation or representation of the subject as a somewhat weaker link in the chain, followed by the subsequent normalisation of the challenges of cyber insecurity it faces. This allows for further normalisation of the subject's need for empowerment, such that, they can lay claim to their right to cyber ambitions and achieve their full potential. And in the process, they are equipped with the means to understand the difference between what's normal and what is not. In other words, they are disciplined through law and norms to create a demarcation between good and evil. Consequently, they become convinced of their future ability to participate in the protection of the space, as part of the 'common forces for good', both in the interest of themselves and the global community.

[860] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706).
[861] Michel Foucault, 'The Subject and Power' (1982) 8 Critical Inquiry 777.1982 [777]

Thus, the campaign for cyber armies is promoted, which must be trained to respond to threats and become forebearers and protectors of rights, enabling states to uphold sovereignty or enforce the law. Therefore, the circumscription of rights and obligation follows, through a discursive succession of common interest, values, ideas or common good. Hence, the separation of those whose subjectivities places them outside the compliant group, suggests the activation of the disciplinary norms as a way to respond to the "other", while maintaining a group of those with common interest. Most importantly, that group of common interest, such as the Commonwealth, is not all equal in status. Rather they are structured and governed by hierarchical systems, with the powerful naturally positioned at the top. And in most cases (as with the Commonwealth), elite sub-groups are created which together, must 'conduct the conducts' of the entire group through mechanism discussed so far.

Consequently, the *status quo* must be defined, and norms must be orchestrated to sustain this system. One remains or is allowed to remain within this structure for as long as one plays by the rules of the *status quo.* Thus, their efforts remain focused on maintaining the hierarchical *status quo* through the norms or standards that they set as best practice.

Perhaps, it is the interest in creating a global society of states with common interest and values, through a notion of a discursive egalitarian society, that allows the problematisation of cybersecurity to emerge, as with most other phenomenon before it. This is because, the geopolitical threat appears to pose the real concern for states in reality (particularly wealthier states for whom the *status quo* has been a product of their own formulation) as opposed to the threat of cyber insecurity. More so, as the question of who controls the internet or cyberspace increasingly becomes the main preoccupation of these powerful nations.

As Dominic Raab bragged in a 2021 speech: "Now according to Harvard's Belfer Centre, the UK is already a top-3 global cyber power, alongside the US and China".[862] Hence the need for that "dividing practices" which allow for the separation of those willing to sign-up to the rules-based order from those that think otherwise.

> So as well as all the opportunities for economic growth and the wider emancipation if you like, of the citizen we see online, I want to talk to you today about how we will continue growing our capabilities to defend the UK's interests online, and, at the same time, how we will deliver our vision of being a leading responsible cyber power, working with our partners to shape cyberspace according to our values.[863]

Therefore, the globalised cybersecurity 'subject of rights' translates into cooperation or participation of those signing up to a global community of discursive common interest and values, which normalises certain practices and rules, with a dividing or otherwise disciplinary and security grasp (for those who chose to be on the outside), thereby creating a further dichotomous 'them and us'. This dichotomy, as observed within the data, is realised and rationalised in several ways too. One of which, as discussed in Chapter Five, is made possible through the visibility of the problem, aided by statistical data, to create a picture of the problem, and the role played by different actors, both in relation and comparison to the desires of the global population.

[862] Raab, Foreign Commonwealth and Development and National Cyber Security Centre (n 635). [3]

[863] ibid.

Another observation is the cybersecurity problematisation of certain states in relation to their security stances, values, cultures, and even identities (with regards to what the dominant group considers distinctly civilised and democratic). As postulated in Foucault's notion of 'state racism', the dominant economies of the Global North appear to define this normality.[864]Thus, the problematisation of cybersecurity challenges in poorer Global South regions and the seemingly racialisation of cybersecurity criminality or malicious behaviour of certain Global South states, allow for a concomitant construction of a normalised Global North ideology, values and practice, that is deemed refined and considered best practice. Noteworthy is the way this dichotomy normalises what it considers good security subjectivity (in other words, those subscribing to its rights-base values, democratic principles, etc.), as Western subjectivity, while those who dare think differently, form the opposites of such framings.[865]

Indeed, those perceived on the opposite ('oppressive regimes and flaunters of human rights', for example) can only ever be subjectivities emerging from outside of the Global North. In fact, 'oppressive', as a term, is never used when describing any Global North developed state practice, even when it may appear so. Rather, oppressive practices are regarded as 'foreign' and as such, only expressed when referencing non-Western practices of those who fall into the group of the 'them'.[866]

[864] Foucault, *The History of Sexuality Volume I, The Will to Knowledge* (n 409).

[865] Raab, Foreign Commonwealth and Development and National Cyber Security Centre (n 635). See also Keon speech, Koenders (n 110).

[866] Koenders (n 110); Raab, Foreign Commonwealth and Development and National Cyber Security Centre (n 635).

On the contrary, one could describe certain practices performed by Western powers as oppressive. As an example, when suspected criminals or terrorists are locked up indefinitely without trial, or when journalists and activists like Wikileaks' Julian Assange and whistle-blower Edward Snowden are persecuted for revealing secret oppressive practices of Western states. Rather, this is often framed (when discussed at all) in terms of complex social and security processes, requiring complex rationalisation of actions that are professed to be at best, interpreted as social, security, political or geopolitical struggles. But, without the need to associate them with any recognisable Western values or culture.

Such 'out of character' security behaviour, when engaged by Western states, are seen as important and consequential problems that must be examined through legal, democratic, social and, above all, security perspectives (again, as seen in the justification of why such 'violators' like Assange must face the full wrath of the law). In other words, if a Western state such as the US, must behave in a way resembling those of the so-called authoritarian and oppressive states, their actions must have a juridical, social, security and political, rationality to it.

A continuous dichotomy remains as a result, with an equally continuous representation of practices that rests on whose side of the geopolitical line one stands. This is mostly obvious in the assumption, that non-Western states practices are 'foreign' to Western values, which could be a result of the multiplicity of culture, religion, race, etc. And the economic status from whence those worrisome practices emerge, typically represents the sources of some of the cybersecurity challenges faced by those states, which ultimately spill over to the rest of the global society.[867] For example, international cybercrime from internet fraud is adequately attributed to poor economic conditions in the communities where it is most rampant. The West, however, is assumed to be immune from this sense of multiplicity or duality because, they share common values, religion, culture, etc. As such, their challenges in terms of cybersecurity, are seemingly less problematised (or not in the same sense as elsewhere). Thus, norms are promoted to whip the rest into shape, based on the acceptable Western values, which the non-Westerners are framed to emulate.

Viewed along these lines, normalising power would appear as oppressively disciplinary in the sense that, it focuses on the norm, from whence it seeks some sort of compliance, or resistance, with resistance simply giving rise to new and further justifications for the norm's adoption or the creation of more norms. This allows it to maintain the division between what is normal and what is not. And as expressed by Foucault, "it is not the normal and the abnormal that is fundamental and primary in disciplinary normalization, it is the norm" itself,[868] in order to accommodate for its controlling tendencies.

Therefore, the resulting effect is that, the division allows for a perception of the Western values as synonymous with best practice, even amongst those to whom the biopolitical mechanism are targeted.[869] This is possible because the norm effect offers those who do not oppose its subjugation, a rather 'positive' or

[867] Nye, 'The Regime Complex for Managing Global Cyber Activities' (n 263).

[868] Foucault, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (n 706). [85]

[869] Ministry of National Security (n 738). See also, Sadek (n 783).

'privileged' position, whereby its security subjectivity, albeit problematised at the point of seeking its effect, can eventually become of lesser concern, as it plays along with the demands of the governing states. Thus, the norm effect in the end, maintains a level of duality in that, it concerns both security and state differences, dealing with the problems while drawing and controlling the lines of normality, not only in terms of technological, legal, but also along the lines of values, culture and religion. And in doing so, it reveals both security and disciplinary forms of power.[870]

Therefore, the norm effect, within the cases, appear, on the one hand, to focus on supporting the cybersecurity environment in the global society, through efforts aimed at minimizing the risk of cybersecurity ills, thereby bringing about what it considers a 'normal' environment. On the flip side, it seeks to identify and transform causes of the risk within the individual states. Hence, we see a convolution of both the truth, power and norm effects within these constructions, as they work together, to strengthen relations of power that is focused on establishing the boundaries of social acceptability and privilege.[871] The result, of course, is that it creates a further nexus between the different mechanisms, to assert what security in the cyber age ought to look like, within a discussion of the global identity and social reconstruction.

[870] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319); Dillon and Lobo-Guerrero (n 205).

[871] Patricia Hill Collins, *Black Feminist Thought : Knowledge, Consciousness, and the Politics of Empowerment*, vol Rev. 10th (Routledge 2000) <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=70795&site=ehost-live&authtype=ip,shib&user=s1523151>.

8.8 Conclusion

Cybersecurity probelmatisation has been examined in this chapter through a review of its common and varied aspects within the data . The common threads, running across the data are identified in relation to how cybersecurity is rendered problematic through similar mechanisms and rationalities. The discussion reveals similar problematisations that appear biopolitical in use and thought, evident in their employment of certain governing techniques and rationalities to create visibility, intelligibility and governance of the problem.

We observe how problematisations come into being through assemblages and their resulting impacts. The truth effect that they produce, for example, manifest itself in its assertions of the subject in specific ways as it relates to the different or specific subject of risk and rights. As such the manifestation of power and its effects appear different, but are indeed the same across the data.

For example, whereby in the case of developed states and global institutions, the production of an identity formation field is observed through the notion of ‘oneness’, ‘common good’ or the idea that the problem affects all of us, therefore, ‘we are all in it together’. Such discourse of togetherness or equality implies a truth effect, such that when latched on by developing states, it create a sense of belonging to a specific group (of the ‘good guys’), which then allows them to differentiate themselves from others, and be proud followers of what they consider best practices. This oneness discourse is the marker of ‘Westerness’, which itself is a product of identity that has been curated over the centuries, and informed by the notions of racial and cultural superiority, and the relentless discourse of the West as a progressive and pioneering bunch.

Therefore, subjects are empowered through this identity construction as bearers of rights, permissible only for as long as they remain on the right side of the rules of engagement. And as rights bearers, they are granted access to a seemingly unequivocal notion of equality which then allows for certain hierarchical order of things to be formed: The construction of the 'us' versus 'them', where the performative perceptions of the 'Westerness' and the 'non-Westernhood' are re-enacted in the form of exclusion and inclusion.

On the subject of risk however, fields of uncertainty are created. Here, uncertainty as a real problem of cybersecurity also implies a truth effect, but of risk.[872] And risk, as a truth effect, allows for a form of strategy that is used to manage that risk, but in a not so political way. In other words, because of the truth effect, managing that risk is seen as a collective effort (lest one may risk being ostracised). And for developing state actors, this becomes a never ending state of vulnerability and risk. Thus, they are addressed as subjects of risk, but also, free entities with choice and responsibility of what they do with that risk and vulnerability.

Finally, the normalisation of cybersecurity problems also creates truth effects. It does so through its constitution of new entities or identities as well. Here, risk discourse appears both as a calculative practice and as a connection

[872] O'Malley (n 621).

between challenges and opportunities. Thus, and as this risk is seen and accepted as such , the risk entity or subject, constructed by disciplinary power through the norm effect, is transmuted into adaptable subjects of security.

9 Conclusion and closing remarks

9.1 Introduction

This chapter concludes the thesis and serve the purpose of highlighting the connection between the research findings, the research questions and goals. It reflects on the theoretical and practical implications of the study and engages the discussion in three main parts. The first provides a summary of the research questions, the analysis process deployed and how answers to the questions are approached. A second part reflects on some of the positives and shortcomings of the process and what could have been done differently or could be done differently in future research projects. Finally, the theoretical and practical implications are discussed. The focus, with regards to the theoretical implication, rests on the use of Foucauldian concepts, their relevance, and prospects in relation to cybersecurity problematisation and practices. The practical implication on the other hand, highlights the social and political relevance of the study and how aspects of the study might translate into action.

9.2 Answering the research questions

A key goal of the study was to track forms of power activated through relationships between developed and developing states, with regards to the global cybersecurity problem. The thesis examines the question of how certain operations of power are manifested within this relationship through discourses and practices, and how they shape perspectives around the subject. Thus, the core argument is that the problematisation of global cybersecurity establishes it as a governable problem-space which enables certain governing techniques to emerge.

To support that argument, problem representations of cybersecurity are demonstrated through data, as constitutive biopolitical products. It is shown that, such representation constitutes legitimising mechanisms which enable the covert control of subjects, but through non-coercive techniques of governing. Using Foucauldian concepts, the data is interrogated based on Dean and Bacchi's frameworks, with which it demonstrates how the challenges of cybersecurity are made visible, reflected upon, and ultimately managed through actions; Albeit, with underlying governmentality that is embedded within these techniques or technologies of action.

Hence, the research followed an initial hypothesis and objective, to explore cybersecurity as a problematised field, not only to identify the notion of the subject as an object, impacted by power, but also to examine the connection between the subject, political and governing effects of the ontological domain of the authority that exudes such power.[873] For Butler,

> To be critical of an authority that poses as absolute is not just to take a point of view but to elaborate a position for oneself outside the ontological jurisdiction of that authority and so to elaborate a certain possibility of the subject.[874]

Therefore, "one has to be able to think beyond the domain of the thinkable that is established by that authority and on which that authority relies".[875]

Taking a leaf from such suggestion, problematisation is deployed as a means of conceptualising cybersecurity practices as discourse. Doing so allows one to capture ways such practices "shape the world through the framing of social 'problems' and governmental 'solutions' and the construction of concepts, categories, distinctions and subject positions".[876]

The choice of global cybersecurity as a governmental practice , is motivated in part by its topical nature at the time, which renders it a contested area of global regulatory and policy concern. And by its inherent nature of jurisdictional complexity, cybersecurity has also exposed underlying complex connection between epistemological enquiry and governing power. As a result, it creates a fertile ground upon which the contingent nature of its challenges or

[873] Judith Butler, 'Critique, Dissent, Disciplinarity' (2009) 35 Critical Inquiry 773.
[874] ibid. [790]
[875] ibid. [790]
[876] Susan Goodwin, 'Analysing Policy as Discourse: Methodological Advances in Policy Analysis' in Lina Markauskaite, Peter Freebody and Jude Irwin (eds), *Methodological Choice and Design* (Springer 2011).

notion of insecurity has in turn, become products of power mechanism in its interactions between states.

9.2.1 The Analysis

The data analysis was aided by Bacchi's line of questioning policy text particularly at the stage of reading and codification. This granted in-depth insight into the data and allowed for a systematic presentation of the discussion using Dean's power concept. Hence, the research outcomes are thematically discussed in chapters five, six and seven to reflect the truth, norms and power elements contained within Dean's framework. These elements are brought together in chapter eight to reflect on their effects and add a comparative element to the analysis.

The approach followed a process of examination of data that are used to 'paint a picture' of the problem. This involves analysing the use of various discursive techniques that are sometimes backed by statistical or monitoring data, to represent the state of cyber insecurity, risks and threats that states and individuals face on an on-going basis. It reveals how the use of such statistics, along with other rationalising discourses, allows the representation of cybersecurity threat and risk, to be established as truth.

Next, it explores the possibility of calculative discourse to establish how they are used, to justify solutions based on coherently crafted knowledge claims.

Finally, it examines specific resolves, which, having been established as necessary, through practices observed in the first two phases, are observed as representing rationalised tactics of political intervention.

Consequently, problematising processes are observed, and their tactics are revealed as strategic governmentalisation of cybersecurity problems, within a biopolitical construct of the problem as one that is, and should be governable. That is to say, that these processes create certain realities which allow truth claims to emerge. As such, cybersecurity practices becomes ways through which, both the nature of the problem and the mode by which the problem is managed, are determined by dominant authorities, who assert knowledge claims, establish boundaries, proclaim political legitimacy, and consequently control.

Therefore, justification or rationalisation of certain cybersecurity actions are observed as informed by truth claims and executed through 'persuasive' means (freedom and responsibility), which allows certain actors to exercise global governance of cybersecurity dominance.

While acknowledging the need for preventative security strategies, the research main preoccupation is on how they are deployed to govern. For example, emphasising freedom to choose and individual responsibility to oneself and to self-regulate, particularly within the context of a global phenomenon, represents new ways by which social, economic, and political life can be regulated, at a distance, and in a non-coercive or unsuspecting way.[877]

Identifying such trends within the cybersecurity data, allows the data to be understood beyond what they are intended for. Therefore, their effect,

[877] O'Malley (n 621). See also, Andrew Barry, Thomas Osborne and Nikolas Rose, *Foucault and Political Reason, Liberalism, Neoliberalism and Rationalities of Governmentality* (Andrew Barry, Thomas Osborne and Nikolas Rose eds, The University of Chicago Press 1996).

whether intended or otherwise, furnishes one with better understanding of contemporary dynamics of 'government mentality' and how we are governed. Thus, ontological presence of this governmentalized ways of governing is observed which allow for the illustration of what Rose describes as, the "new formula of government - one inclusive and solidaristic, one individualizing and responsibilizing."[878] All at the same time and one, where the connection "between government, expertise and subjectivity would take place".[879]

This is a Foucauldian approach which scholars over the years, have found relevant in their own studies. Scholars like Rose and Miller and Dean, for example, explore this extensively in their governmentality literature. So has Triantafillou, who provides accounts of their own analysis of these governing processes that are present within political public discourse.[880]

For Triantafillou in particular, the Foucauldian line of enquiry is specifically useful when directed at examining the commonalities that exist between research cases, as opposed to one that focuses on their differences. Focusing on the differences between cases detracts attention from the underlying power effects that may be prevalent. Whereas, identifying the common themes that run through cases, allow such practices to be understood as belonging to problematising traits, which they termed "hegemonic ".[881] In other words, while the cases may or may not share similar political identities, cultural

[878] Barry, Osborne and Rose (n 877). [48]
[879] ibid. [52]
[880] Triantafillou (n 799).
[881] ibid.

or historical contexts, they are nonetheless influenced by similar ideologies and problematisations.

Thus, the visibility created by dominant discourses on cybersecurity risk and threats which are reinforced through statistics and knowledge claims for example, enable socially and politically significant meanings to be extracted and examined within the efforts designed to solve the problem. As such, it frames seemingly harmless strategies, but are indeed, far from being harmless. Rather, they form parts of the engine that seek to make the system run in a desired way (how states should be organised, how the market should operate, what rules should govern this or that, etc). Therefore, this desire to correct or fix a problem-field, justifies and fuel the desire for reform that is purported to guarantee efficient, secure, and fairer societies amongst other benefits.

We also demonstrated how they sustain biopolitical control of subjects in the process. Through its establishment of truth (calculative practices, measurement, performance indicators, etc), certain connection between knowledge and politics is allowed to emerge. This is done in such ways that they are not necessarily determined by the desires of, or the impacts it may have on the individual state. But rather, they are focused more specifically on knowledge and power formation - exploiting the power of that knowledge in determining how things are to be done, who determines what constitute transgression or otherwise, what capacity gap exist, what solutions works best, etc.[882].

[882] Miller and Rose (n 440).

Examining cybersecurity problematisation through the common themes across the data is not without its own problems, and may perhaps suggest a less rigorous academic effort on one's side. It may also allow the study to be deemed as a conceptual over-simplification of the notion of a dominant neoliberal ideology that is supposedly spread across all aspects of 'life'. This, of course, is not the intended assumption of this study. To do so will be tantamount to the reduction of cybersecurity practices, in its entirety, to a single underlying purpose of producing, reproducing, and enabling subjectivities that can be controlled in this neoliberal frame of things.

To avoid such conclusion, distinguishing elements within the data were engaged in chapter eight. While the governing techniques described are not always overtly reflected in the data, they are 'present' within it regardless, in the form of orchestrated interplay between neoliberal suggestions and the divergent framings, rhetorical practices and structures. Therefore, it was necessary to observe and reflect on the differentiating themes to tease-out the rather covert tendencies within.

Doing this meant a deeper re-interrogation of the data to gain further insights into the representation of cybersecurity problems and the rationalisation of its solutions. This meant understanding how rationalisation is deployed and used within an array of context-specific tactics to create an assemblage of security governance, through notions of freedom and responsibility.[883] Consequently, the different presentations of normalisation, which facilitates cybersecurity problematisation that produces equally different subject situations are revealed, as ways of responding to specific regional situations, based on economic status, geography and race.

Indeed, the data from both developed and developing countries reflect common problematisation of technical knowledge gaps and the general state of cybersecurity capacity in poorer states, stressing the effects of such condition on their overall preparedness, their risk exposure as well as the choices they can make in response. Analysing how such problematisation is constructed across both sides, enabled the demonstration of the different contextual representation of the cybersecurity problem.

For example, within the texts from both divides, the construction of a successful cybersecurity agenda is framed within the social, political, and economic growth discourse (directed towards developing states and projected onto the self when such discourse is repeated within data from developing state itself). Data from developed states however, when directed onto itself, project discourses of global power ambitions. This is done through own knowledge claims and the interlocutions that centres on the nature of cybersecurity and its challenges, emphasising cooperation needs of states towards a common interest.

Such position allows for the observation of what emerged, in the study, as a form of binary constructions of subjects, along the lines of 'them' versus 'us',

[883] Stephen J Collier, Andrew Lakoff and Paul Rabinow, 'Biosecurity: Towards an Anthropology of the Contemporary' (2004) 20 3.

and the ‘in’ or ‘out’ classification of entities. Through such classification, disciplinary mechanisms of governing or regulation are deployed, based on whatever rules or norms have been set, imagined and projected, on grounds of political and economic status, historical circumstances, race, etc.

These grounds, afford different parties different prospects and loci within the power dynamics and for determining, negotiating, and shaping such relations. Thus, both similar and distinct trends are observed across these texts, seemingly working together, to suggest the presence of complex power formations that also appear to have unidirectional flow attributes. Therefore, whereas discourses from developed state would amount to projections of power through knowledge assertions and capacity, those from the developing states reflect at best, projections of the self in desired images of the wealthier states, through actions recommended by them and a reamplification of their (Western) rhetoric.

9.2.2 The problematisation framework

As acknowledged above, to simply situate neoliberal tendencies as political ideologies, rationalities, or dominant problematising fields, would amount to simple reduction of complex situations. Doing so, according to Collier, *et al.*, may not afford one the possibility of formulating theoretical challenges to the governing process.[884] Conversely, simply directing analytical focus on specific

[884] ibid.

actions or practices to determine their effectiveness or discursive role, would also not provide one with enough analytical breadth and depth, if one fails to identify the power connections that are embedded in such practices. Therefore, it becomes a question of how these power formations and their effects can be best understood while recognising possible contradictions and discernible variations in the contingent assemblage of problem fields across political settings, global and local institutions, etc.

This is the task that analysing problematisation, according to Foucault, sets out to achieve; to enable the identification of that which is accepted as an absolute truth without recourse to questioning and genealogically rooting its problematisation, locating the problem or perceptions which informs the present.[885]

Thus, the use of Foucault's problematisation in this analysis proved useful in examining the similarities and differences in the deployment of the mechanisms of power from across different local empirical settings. For example, in the previous chapter, we explored the link between the operations of power, their similarities across the different states contexts, and the different impacts, particularly in the context of the developed versus the developing states. Here, brevity is accorded to the analysis in the sense that it serves as a link between the common abstraction, legitimisation, rationalisation, across the data, of cybersecurity issues as a problem of government (requiring control), to the formation of subjects that are both specific but covert, as well as the construction

[885] Foucault, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (n 319).

of norms and relations. And in doing so, the biopolitical role that the various practices, norms or discourse play is revealed.

9.2.3 Analytical limitations

Two possible limitations were anticipated: The first relates to the predominant use of authoritative texts (such as policy and strategy documents) as empirical data, and second, how the use of such text fits in with the discourse analysis and Foucauldian theoretical framework used to ground the analysis.

With regards to the extensive use of policy and strategy data, while the argument for its use in the methodology chapter holds true (because they sufficiently represent both thoughts and actions of government), further analytical nuances could have been achievable through interviews. This was intended for the study and attempts were made to secure more interviews with suitable officials which would have guaranteed such relevance. However, this proved difficult during the data collection stage for several reasons; from lack of interest or lack of response from most of the officials that were identified and contacted. Some responded but were unable or less willing to grant interviews. Others provided references and direction to online repositories and other available resources as suitable sources for information.

Therefore, while interviews with a handful of key personnels were secured and used in the analysis, extensive conversations with more of those internal to workings of the data, would have proved invaluable and allowed for further insight into the workings of such data, and as means by which the empirical materials could have been further corroborated.

In terms of the use of Foucault, attempts is made throughout to link the data with the specific Foucauldian concepts deployed, with efforts directed at avoiding conceptual generalisation.[886] As such, the concepts satisfies the objective of grounding the analytical focus of the study, because it provided rigor, making the comparative analysis less easy in terms of analysing the different ways that the concepts manifested themselves across the different case data.

Perhaps a limitation for using Foucault remains in its uncritical application. This might suggest a level of bias emerging from certain centrism to Foucault's theoretical, social, and political stance. Admittedly, this is intentional, as to do otherwise would detract from the choice of Foucault in the first place. However, whatever limitation might exist in its use, what is relevant is whether its application has been effective within the chosen context. The focus throughout has been on ensuring that the concepts were, and it is hoped that they have indeed been effective. Indeed, theory, will not and does not have to appear in the same light in every discipline or study after all. And as expressed by Spivak, "one carves out a provisional field and a provisional traffic of essence" in one's own work.[887]

9.3 Implications

The implications of this study are both theoretical and practical. On the theoretical, the use of Foucault concepts like biopolitics has been given greater

[886] Foucault, *The Foucault Effect: Studies in Governmentality, with Two Lectures by and an Interview with Michel Foucault* (n 1).

[887] Sara Danius, Stefan Jonsson and Gayatri Chakravorty Spivak, 'An Interview with Gayatri Chakravorty Spivak' (1993) 20 boundary 2 24. [36]

attention in analysing public policy and security discourse, especially through studies in governmentality.[888] Utilizing these concepts in this study provide theoretical contribution to the study of cybersecurity problematisation, particularly with regards to how relations of power are impacted by neoliberal considerations and thoughts as discussed in chapters six and seven.[889] In other words, the analytical interaction with biopolitics allows one to define the point of departure from where governmental power and neoliberal thought is observable or produced, devoid of a general subsumption of the empirical data in a reductionist oversimplification of the claim being suggested through the data.

A particular relevance of this is that, while phenomenological or psychoanalytical considerations may allow for such observation of power mechanisms through other concepts, such as discipline, security and sovereignty, there is a risk of some manifestations of power to go unnoticed. Biopolitics, however, has a far-reaching quality that allows one to reveal cross-contextual effects of power that may not readily appear as systemic, but also contingent. This, makes it possible to see how, within the empirical materials, cybersecurity practices (such as capacity building programmes, establishing rule-based system through the Budapest Convention), emerge not simply as a growing manifestation of power relations, but also as part of an ongoing problematisation

[888] Miguel De Larrinaga and Marc .. Doucet, *Security and Global Governmentality: Globalization, Governance and the State* (Miguel De Larrinaga and Marc .. Doucet eds, 1st edn, Routledge 2010); see also Miguel De Larrinaga and Marc G Doucet, 'Sovereign Power and the Biopolitics of Human Security' (2008) 39 Security Dialogue 517. See also Dillon and Lobo-Guerrero (n 205).

[889] See chapters six and seven

of how to sustain certain *status quo*, to guarantee a successive global control (or government) of entities (or 'life', according to Foucault.)[890]

Thus, the overriding theoretical implication of the use of these Foucauldian concepts allow for the contingent historical, and ongoing elements that may vary empirically, from place to place, to be sufficiently addressed and viewed from across different discourses that are produced (such as those around risk, responsibilities and threats).

At the same time, it allows the possibility of accentuating the role of these discourses on a global scale, but with local impacts through its growing globalised and market-based objectives of (political, economic, juridical) domination and power. As argued throughout, such objectives are consequences of the continuous production of heterogenous representations of what constitute modernity or progressiveness, by the self-acclaimed superior groups, projected onto others, through the mechanisms discussed (economic rationalities of cybersecurity risk, the need for rule-based orders, etc.), designed to reconstruct perpetual power.[891]

The practical implications emerges from gaining such insight through theory. It allows one to take a stand (social, political and legal stance), which can be derived from one's understanding of how power, knowledge and actions work within the global cybersecurity geopolitical landscape. To reflect on such

[890] Foucault, *Society Must Be Defended: Lectures at the Collège de France 1975 - 1976* (n 724).
[891] Collier (n 803). See also Dean, *Governing Societies : Political Perspectives on Domestic and International Rule* (n 11). Dillon and Lobo-Guerrero (n 205). And also Rabinow and Rose (n 693).

practical implications, we can summarise how the analysis relates to an array of issues within the cybersecurity politics more generally, and to the power dynamics, more specifically, between powerful Western states and their developing states counterparts on grounds of social, political, and legal justice or development.

A recent speech from the European Commission by the EU's High Representative for Foreign Affairs, Josep Borrell, in October 2022 can be cited.[892] Borrell, in this speech, epitomises the ongoing reproduction of the 'us' and 'them' discourse. While addressing the new crop of future European diplomats (as ambassadors and agents charged with the responsibility of projecting European power to the rest of the world), he emphasises the need for the perpetuation and continued domination of the Western superior ideal, which must be safeguarded through a continuous calculative practice (of 'engagement', partnership, knowledge) when he stated:

> Yes, Europe is a garden. We have built a garden. Everything works. It is the best combination of political freedom, economic prosperity and social cohesion that the humankind has been able to build - the three things together … The rest of the world… is not exactly a garden. Most of the rest of the world is a jungle, and the jungle could invade the garden. The gardeners should take care of it, but they will not protect the garden by building walls. A nice small garden surrounded by high walls in order to prevent the jungle from coming in is not going to be a solution. Because the jungle has a strong growth capacity, and the wall will never be high enough in order to protect the garden. The gardeners have to go to the jungle. Europeans have to be much more

[892] EEAS Press Team, 'European Diplomatic Academy: Opening Remarks by High Representative Josep Borrell at the Inauguration of the Pilot Programme | EEAS Website' (*European Diplomatic Academy*, 13 October 2022) <https://www.eeas.europa.eu/eeas/european-diplomatic-academy-opening-remarks-high-representative-josep-borrell-inauguration_en> accessed 20 October 2022.

> engaged with the rest of the world. Otherwise, the rest of the world will invade us.[893]

As observed by past scholars with similar practical research implication stance, social, political and juridical effects could be achieved through such approaches to knowledge which seek to scrutinise the taken for granted in every day discourse as has been demonstrated within this thesis.[894] Mol for example, suggests the need to reflect on one's research method as serving the purpose of creating what they termed "interferences" (disruptions) to our view of the world, as opposed to means by which we 'see' the world, or how the world is designed to appear to us.[895] Such interferences ought not be, or expected to be fundamentally different from the researcher's own stance. Thus, if one agrees with such position, then the question becomes that of how one's research analysis has paid homage to this claim?

Concepts such as biopolitics and governmentality, afford one this possibility. They allow those 'hidden' problematising mechanisms within the cybersecurity practices and discourses to be brought afront, to reveal their role and impacts within the case data. Thus, in doing so, the research provides one with competing views and therefore, allows for meta-narratives to such truth

[893] ibid.
[894] Chela Sandoval, *Methodology of the Oppressed* (University of Minnesota Press 2000). See also Boaventura de Sousa Santos, *Another Knowledge Is Possible: Beyond Northern Epistemologies*, vol 32 (Boaventura de Sousa Santos ed, Verso 2007). See also, Annemarie Mol, 'Ontological Politics. A Word and Some Questions' in John Law and John Hassard (eds), *Actor Network Theory and After*, vol 47 (1st edn, Blackwell Publishers 1999). And Gayatri Chakravorty Spivak, *The Post-Colonial Critic : Interviews, Strategies, Dialogues* (Sarah Harasym ed, Routledge 1990).
[895] Mol (n 894). [74]

claims to the formed that are capable of reshaping political actions and policies that are capable of deconstructing or decolonising problematising practices that form parts of governing actions.

What is certain from this study is that, through the case data, the biopolitical or governmentality objectives and dispositions of certain cybersecurity actors are real. They remain active and continue to reproduce forms of problematising discourses of security, knowledge, risk, responsibility, capacity building, partnership and collaboration. And as technology advances and takes new dimensions (through Artificial Intelligence or Machine Learning and Automation), its nexus with security will continue to shape new discourses, knowledge, truth claims and other practices, that will require theoretical attention to be drawn to them in the future, to achieve practical objectives.

Furthermore, the digital, economic, legal and other developmental, gaps will almost certainly never be closed, and will remain for some time to come. And as expressed by Borrell, the "gardeners" of the West understands their current position of power within the global world order. What more will be of most priority to them other than to ensure that their "garden" continues to flourish, albeit surrounded by the "jungle".

Thus, the cravings of the West for continued power and to remain as leaders of knowledge and the rule-based world order, can only suggest that it is not in their best interest for the "jungle" to become an equally beautiful "garden".

And indeed, to keep the “jungle” away from challenging the garden, the jungle needs to be “engaged.” In other words, suppressed, controlled, and managed. [896]

9.4 Closing remarks

This study is a theoretical experiment executed through thought, analysis, and critique. It is hoped that its objectives, which can be described as emerging from one’s desires or interests, have been achieved to some degree, through interpretations accorded to the cybersecurity practices and discourses reviewed. It is also hoped that these interpretations have created a two-way nexus between the developed and the developing states angles of the investigation. This is important because, as is evident from the study, the problematisation of cybersecurity issues flow both ways. In other words, there is the problematisation by others and of oneself (although sometimes through covert influence by others), which takes the form of self-actualisation of one’s own position (that can be tilted by the position of power through biopolitical mechanisms). Thus, and on a final note, this two-way connection, if indeed has been successfully identified and established, is expected to allow a form of self-realisation, on either side, while also understanding how one’s position is impacted from the outside.

[896] EEAS Press Team (n 892).

10 Bibliography

Abi Research and ITU, 'Global Cybersecurity Index' (2014)

Abrahamsen R, 'The Power of Partnerships in Global Governance' (2004) 25 Third World Quarterly 1453

Abrahamsen R and Sandor A, 'The Global South and International Security The Global South and International Security' 1

Agamben G, *The Signature of All Things on Method*, vol 31 (Luca D'Isanto and Kevin Attell eds, Zone Books 2009)

Agamben G and Emcke C, 'Security and Terror' (2001) 5 Theory & Event 45

Al-Mutawkkil A, Heshmati A and Hwang J, 'Development of Telecommunication and Broadcasting Infrastructure Indices at the Global Level' <www.elsevierbusinessandmanagement.com/locate/telpol> accessed 25 January 2021

Alt S, 'Beyond Bricks and Mortar: Peace-Building in a Permanent State of Adaptation BT -' in Sandro Mezzadra, Julian Reid and Ranabir Samaddar (eds), *The Biopolitics of Development: Reading Michel Foucault in the Postcolonial Present* (Springer India 2013) <https://doi.org/10.1007/978-81-322-1596-7_6>

Amos K, 'Governance and Governmentality: Relation and Relevance of Two Prominent Social Scientific Concepts for Comparative Education' (2010) 12 International Perspective on Education and Society 79

Avgerou C, *Information Systems and Global Diversity* (Oxford University Press 2003)

Ayanso A, Cho DI and Lertwachara K, 'The Digital Divide: Global and Regional ICT Leaders and Followers' (2010) 16 Information Technology for

Development 304 <https://www.tandfonline.com/action/journalInformation?journalCode=titd20>

Bacchi C, 'Policy as Discourse: What Does It Mean? Where Does It Get Us?' (2000) 21 Discourse 45

——, 'The Turn to Problematization: Political Implications of Contrasting Interpretive and Poststructural Adaptations' (2015) 05 Open Journal of Political Science 1

——, 'Problematizations in Health Policy: Questioning How "Problems" Are Constituted in Policies' [2016] SAGE Open

Bacchi CL, *Analysing Policy : What's the Problem Represented to Be?* (Pearson Australia 2009)

Ball SJ, 'Subjectivity as a Site of Struggle: Refusing Neoliberalism?' (2016) 37 British Journal of Sociology of Education 1129 <https://www.tandfonline.com/action/journalInformation?journalCode=cbse20 > accessed 11 September 2022

Barnett M and others, 'Power in International Politics' (2005) 59 International Organization 39

Barnett MN., *Power in Global Governance* (Michael N Barnett and Raymond Duvall eds, Cambridge University Press 2005)

Barrett ET, 'Warfare in a New Domain: The Ethics of Military Cyber-Operations' (2013) 12 Journal of Military Ethics 4 <https://www.tandfonline.com/action/journalInformation?journalCode=smil20 >

Barry A, Osborne T and Rose N, *Foucault and Political Reason, Liberalism, Neoliberalism and Rationalities of Governmentality* (Andrew Barry, Thomas Osborne and Nikolas Rose eds, The University of Chicago Press 1996)

Baxter H, 'Bringing Foucault into Law and Law into Foucault' (1996) 48 Stanford Law Review 449

Besley T (A C), 'Governmentality of Youth: Managing Risky Subjects' (2010) 8 Policy Futures in Education

Bevir M, 'Governance and Governmentality after Neoliberalism' (2011) 39 Policy and politics 457

Bevir M, Rhodes RAW and Weller P, 'Traditions of Governance: Interpreting the Changing Role of the Public Sector' (2003) 81 Public Administration 1

BOCRA, 'Development of a National Broadband Strategy' 9

Botswana Ministry of Information Communications and Technology, 'National Cybersecurity Strategy'

Britain in the World Project at Policy Exchange, 'Making Global Britain Work' <www.policyexchange.org.uk>

Bröckling U, Krasmann S and Lemke T, *Governmentality: Current Issues and Future Challenges*, vol 71 (Routledge 2011)

Buddeberg E, 'Thinking the Other, Thinking Otherwise: Levinas' Conception of Responsibility' (2018) 43 Interdisciplinary Science Reviews 146 <https://www.tandfonline.com/action/journalInformation?journalCode=yisr20 >

Butler D, Gillum J and Arce A, 'US Secretly Built "Cuban Twitter" to Stir Unrest' *AP News* (Washington, 2014) <https://apnews.com/article/technology-cuba-united-states-government-904a9a6a1bcd46cebfc14bea2ee30fdf> accessed 27 December 2019

Butler J, 'Critique, Dissent, Disciplinarity' (2009) 35 Critical Inquiry 773

Cabinet Office, 'The UK Cyber Security Strategy: Summary of Progress' 1

Calandro E and Pawlak P, 'Capacity Building as a Means to Counter Cyber Poverty', *Riding the digital wave: the impact of cyber capacity building on human development* (2014)

Calderaro A and Craig AJS, 'Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building' (2020) 41 Third World Quarterlyerly 917

Carlsson B, 'The Digital Economy: What Is New and What Is Not?' (2004) 15 Structural Change and Economic Dynamics 245

Carr M, 'Power Plays in Global Internet Governance' (2015) 43 Journal of International Studies 640 <http://www.malcolmturnbull.>

Casilli AA and Tubaro P, 'Why Net Censorship in Times of Political Unrest Results in More Violent Uprisings: A Social Simulation Experiment on the UK Riots' (2011) <http://ssrn.com/abstract=1909467>

Castel R, 'From Dangerousness to Risk' in Graham Burchell and others (eds), *The Foucault effect: studies in governmentality.* (The University of Chicago Press 1991)

Castells M, *The Internet Galaxy : Reflections on the Internet, Business, and Society* (Oxford University Press 2001)

Chairman of the Joint Chiefs of Staff (CJCS), 'Joint Communications System' (2015)

——, 'DOD Dictionary of Military and Associated Terms' (2021) <http://www.jcs.mil/Doctrine/DOD-Terminology/> accessed 7 June 2021

Chan S, 'The Commonwealth as an International Organization' (1989) 78 The Round Table 393 <https://doi.org/10.1080/00358538908453950>

Chang YS, Jeon S and Shamba K, 'Speed of Catch-up and Digital Divide' (2020) 23 Journal of Global Information Technology Management 217

Chatham House's International Security Department, 'Cybersecurity in the Commonwealth: Building the Foundations of Effective National Responses in the Caribbean', vol 44 (2019) <https://www.lacnic.net/1030/2/lacnic/initiatives> accessed 25 September 2021

——, 'Cybersecurity in the Commonwealth: Towards Stability and Responsible State Behaviour in Cyberspace', vol 44 (2019) <https://chathamhouse.soutron.net/Portal/Default/en-> accessed 25 September 2021

Chatham House, 'Cybersecurity in the Commonwealth: Supporting Economic and Social Development and Rights Online', vol 44 (2018) <https://www.chogm2018.org.uk/sites/default/files/Commonwealth Cyber Declaration pdf.pdf> accessed 25 September 2021

Chinn MD and Fairlie RW, 'The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration' (2004) document 881

Ciborra C, 'Interpreting E-Government and Development: Efficiency, Transparency or Governance at a Distance' (2005) 18 Information Technology and People 260

Collett R, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures' (2021) 6 Journal of Cyber Policy

Collier SJ, *Post-Soviet Social Neoliberalism, Social Modernity, Biopolitics* (Course Boo, Princeton University Press 2011)

Collier SJ, Lakoff A and Rabinow P, 'Biosecurity: Towards an Anthropology of the Contemporary' (2004) 20 3

Collins PH, *Black Feminist Thought : Knowledge, Consciousness, and the Politics of Empowerment*, vol Rev. 10th (Routledge 2000) <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=70795&site=ehost-live&authtype=ip,shib&user=s1523151>

Commonwealth and Law Ministers and Senior Officials, 'Report of the Commonwealth Working Group of Experts on Cybercrime':, vol 3 (The commonwealth secretariat 2014)

Commonwealth ICT Ministers, 'Commonwealth Cybergovernance Model' (The commonwealth secretariat 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.> accessed 16 January 2021

Council of Europe, 'Cybercrime Programme Office (C-PROC) - Cybercrime' (*coe.int*) <https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-> accessed 29 December 2022

——, 'Worldwide Capacity Building - Cybercrime' (*coe.int*) <https://www.coe.int/en/web/cybercrime/capacity-building-programmes> accessed 29 December 2021

Council of Europe and Data Protection and Cybercrime Division of the Council of Europe, 'Global Project on Cybercrime - The Cybercrime Legislation of Commonwealth States : Use of the Budapest Convention and Commonwealth Model Law' (2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb rev_final_CoE.pdf> accessed 6 September 2022

Crenshaw EM and Robison KK, 'Globalization and the Digital Divide: The Roles of Structural Conduciveness and Global Connection in Internet Diffusion', vol 87 (2006)

Cruikshank B, *The Will to Empower : Democratic Citizens and Other Subjects* (Cornell University Press 1999)

'Cyberpower and National Security' (2013) 35 American Foreign Policy Interests 45

Cybersecurity.gov.gh, 'Legislation on Cybersecurity Will Address Weaknesses in Our Cybercrime Laws' (*cybersecurity.gov.gh*)

Cybersecurity Program of the Inter-American Committee against Terrorism, 'Cybersecurity Considerations for the Democratic Process for Latin America and the Caribbean' (Organization of American States 2019)

Danius S, Jonsson S and Spivak GC, 'An Interview with Gayatri Chakravorty Spivak' (1993) 20 boundary 2 24

De Larrinaga M and Doucet M. ., *Security and Global Governmentality: Globalization, Governance and the State* (Miguel De Larrinaga and Marc .. Doucet eds, 1st edn, Routledge 2010)

De Larrinaga M and Doucet MG, 'Sovereign Power and the Biopolitics of Human Security' (2008) 39 Security Dialogue 517

De Nardis L and others, 'Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance' de Sousa Santos B, *Another Knowledge Is Possible: Beyond Northern Epistemologies*, vol 32 (Boaventura de Sousa Santos ed, Verso 2007)

De Sutter L, *Zizek and Law* (1st edn, Routledge 2015)

Dean J, 'Zizek on Law' (2004) 15 Law and Critique

Dean M, 'Putting the Technological into Government' (1996) 9 History of the Human Sciences 47

——, *Governing Societies : Political Perspectives on Domestic and International Rule* (Tim May ed, McGraw-Hill Education 2007)

——, *Governmentality Power and Rule in Modern Society* (2nd ed., Sage 2010)

Deibert R, 'Canada and the Challenges of Cyberspace Governance and Security' (2013) 5 The School of Public Policy Publications 1

Deibert R and others, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Ronald Deibert and others eds, The MIT Press 2010)

——, 'Access Contested: Toward the Fourth Phase of Cyberspace Controls' in Ronald Deibert and others (eds), *Access Contested: Toward the Fourth Phase of Cyberspace Controls* (The MIT Press 2011)

Deibert RJ, 'Circuits of Power: Security in the Internet Environment' in James N Rosenau and J. Singh (eds), *Information Technology and Global Politics* (State University of New York Press 2002)

——, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace' (2003) 32 Journal of International Studies 501

Deibert RJ and Crete-Nishihata M, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 Global Governance 339

DeNardis L, 'Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance' (2012) 15 Information, Communication & Society

Dias T and Coco A, 'Cyber Due Diligence in International Law' (2021)

Dijk TA van, *News as Discourse* (L Erlbaum Associates 1988)

Dillon M, *Biopolitics of Security : A Political Analytic of Finitude* (Routledge 2015)

Dillon M and Lobo-Guerrero L, 'Biopolitics of Security in the 21st Century: An Introduction' (2008) 34 Review of International Studies 265

Dimaggio P and others, 'Social Implications of the Internet', vol 27 (2001) <https://www.jstor.org/stable/2678624> accessed 24 January 2021

Drake WJ, *The New Information Infrastructure: Strategies for U.S. Policy* (William J Drake ed, English, The Twentieth Century Fund Press 1995)

Duffield M, *Global Governance and the New Wars: The Merging of Development and Security* (Zed Books 2014)

Dunn Cavelty M, 'Cyber Security' in Alan Collins (ed), *Contemporary Security Studies* (3rd edn, Oxford University Press 2015)

Dunn Cavelty M and Wenger A, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science' (2019) 41 Contemporary Security Policy 5

Ebert H and Maurer T, 'Contested Cyberspace and Rising Powers' (2013) 34 Third World Quarterly 1054

EEAS Press Team, 'European Diplomatic Academy: Opening Remarks by High Representative Josep Borrell at the Inauguration of the Pilot Programme | EEAS Website' (*European Diplomatic Academy*, 13 October 2022) <https://www.eeas.europa.eu/eeas/european-diplomatic-academy-opening-remarks-high-representative-josep-borrell-inauguration_en> accessed 20 October 2022

Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 American Journal of International Law 583

Escobar A, *Encountering Development : The Making and Unmaking of the Third World* (Princeton University Press 2011)

Everett M, 'Latin America On-Line: The Internet, Development, and Democratization', vol 57 (1998)

Fischer F, Miller GJ and Sidney MS, 'Handbook of Public Policy Analysis : Theory, Politics, and Methods' [2007] Methods

Foreign and Commonwealth Office, 'UK Commonwealth Cyber Security Programme: A Selection of Six Case Studies' (2021)

Foreign Commonwealth and Development Office and The Commonwealth, 'African Cyber Experts Fellowship : Lessons Learnt Report' (Protection Group International 2020)

Foucault M, 'Discipline & Punish' [1977] Discipline & Punish: The Birth of the Prison

——, 'Security , Territory , Population. Lectures at the Collège de France' [1977] Differences

Foucault M, *The History of Sexuality: An Introduction Vol. 1* (1978)

Foucault M, *The History of Sexuality Volume I, The Will to Knowledge*, vol I (First Amer, Pantheon Books 1978)

——, 'Omnes et Singulatim: TowardsTowards a Criticism of "political Reason""', *Tanner Lectures on Human Values on Human Values* (The University of Utah 1979)

——, 'The Subject and Power' (1982) 8 Critical Inquiry 777

——, *The Government of Self and Others: Lectures at the College de France, 1982-1983* (Frédéric Gros ed, Palgrave Macmillan 1983)

——, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan ed, Second Vin, Vintage Books 1991)

——, 'Govemmentality', *The Foucault effect: studies in governmentality* (1991)

——, *The Foucault Effect: Studies in Governmentality, with Two Lectures by and an Interview with Michel Foucault*, vol 22 (Graham Burchell, Colin Gordon and Peter Miller eds, The University of Chicago Press 1991)

——, *The Foucault Reader: Michel Foucault 1926-1984* (Paul Rabinow ed, Pantheon Books 1991)

——, *Ethics: Subjectivity and Truth: The Essential Works of Michel Foucault, 1954-1984*, vol 1 (Paul Rabinow ed, The New Press 1997)

——, *Society Must Be Defended: Lectures at the Collège de France 1975 - 1976* (Mauro Bertani and others eds, 1st edn, Picador 2003)

——, *The Essential Foucault* (Paul Rabinow and Nikolas Rose eds, The New Press 2003)

——, *The Essential Foucault Selections from Essential Works of Foucault, 1954-1984* (Paul Rabinow and Nikolas Rose eds, The New Press 2003)

——, *Security , Territory , Population: LECTURES AT THE COLLÈGE DE FRANCE, 1977-78* (Michel Senellart and others eds, Pbk ed, Palgrave Macmillan 2007)

——, *The Birth of Biopolitics : Lectures at the College de France, 1978-79* (Michel Senellart ed, Palgrave Macmllan 2008)

——, *The Birth of Biopolitics: Lectures at the College de France 1978 - 1979* (2008)

——, *Security, Territory, Population Lectures at the College de France, 1977-78* (Michel Senellart and others eds, Pbk ed, Palgrave Macmillan 2009)

Foucault M and James D faubion, 'Truth and Power', *Power: Essential*

Works of Foucault 1954 - 1984 (Penguin Books 2010)

Foucault M and Lotringer S, 'Foucault Live: Collected Interviews, 1961–1984' [1996] New York: Semiotext (e)

Foucault M and Miskowiec J, 'Of Other Spaces' (1986) 16 Diacritics 22

Foucault M and Rabinow S, 'Polemics, Politics, and Problemizations: An Interview with Michel Foucault' in Paul Rabinow (ed), *The Foucault Reader* (Pantheon Books 1991)

Foucault MM, *The Archaeology of Knowledge & The Discourse on Language* (Sheridan AM Smith ed, Pantheon Books 1972)

Froomkin AM, 'Wrong Turn in Cyberspace : Using ICANN to Route Araound the APA and the Constitution' (2000) 50 DUKE LAW JOURNAL

Fukuda-Parr S, Yamin AE and Greenstein J, 'Development The Power of Numbers: A Critical Review of Millennium Development Goal Targets for Human Development and Human Rights' (2014) 15 Journal of Human Development and Capabilities 105 <https://www.tandfonline.com/action/journalInformation?journalCode=cjhd20> accessed 24 January 2021

Gabay C and Death C, 'Building States and Civil Societies in Africa: Liberal Interventions and Global Governmentality' (2012) 6 Journal of Intervention and Statebuilding

Gamreklidze E, 'Cyber Security in Developing Countries, a Digital Divide Issue' (2014) 20 Journal of International Communication 200

Gill JH, *The Tacit Mode: Michael Polanyi's Postmodern Philosophy* (State University of New York Press 2000)

Global Cyber Security Capacity Centre, 'Cybersecurity Capacity Maturity Model for Nations (CMM)' (2016)

Golder B, *Foucault and the Politics of Rights* (Stanford University Press 2015) <http://ebookcentral.proquest.com/lib/lancaster/detail.action?docID=3568975>

Goodwin S, 'Analysing Policy as Discourse: Methodological Advances in Policy Analysis' in Lina Markauskaite, Peter Freebody and Jude Irwin (eds), *Methodological Choice and Design* (Springer 2011)

Government of the United Kingdom, 'National Cyber Security Strategy 2016-2021' (2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>

Griffith G, 'Minister Griffith Speaks on Cyber Security Agency Bill 2014 | Trinidad and Tobago Government' (*gov.tt*) <http://www.news.gov.tt/content/minister-griffith-speaks-cyber-security-agency-bill-2014> accessed 14 September 2021

Grondin D and de Larrinaga M, 'Securing Prosperity or Making Securitization Prosper?' (2009) 64 International Journal: Canada's Journal of Global Policy Analysis 667

Guillén MF and Suárez SL, 'Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use' (2005) 84 Social Forces 681 <https://academic.oup.com/sf/article/84/2/681/2235280> accessed 9 September 2020

Hameiri S, 'Capacity and Its Fallacies: International State Building as State Transformation' (2009) 38 Journal of International Studies 55

Hansen L and Nissenbaum H, 'Digital Disaster, Cyber Security, and the Copenhagen School' [2009] International Studies Quarterly

Harcourt B, *EXPOSED: Desire and Disobedience in the Digital Age* (Harvard University Press 2015)

Herz JH, 'Idealist Internationalism and the Security Dilemma' (1950) 2 World Politics 157

Hilbert M, 'When Is Cheap, Cheap Enough to Bridge the Digital Divide? Modeling Income Related Structural Challenges of Technology Diffusion in Latin America' (2009) 38 World Development <http://www.elsevier.com/locate/worlddev>

——, 'The Bad News Is That the Digital Access Divide Is Here to Stay: Domestically Installed Bandwidths among 172 Countries for 1986–2014' (2016) 40 Telecommunications Policy

HM Government, '2010 to 2015 Government Policy: Cyber Security' (*gov.uk*, 2015) <https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security> accessed 26 August 2021

——, 'Global Britain in a Competitive Age' (2021) <www.gov.uk/official-documents> accessed 10 September 2022

——, 'National Cyber Strategy 2022 Pioneering a Cyber Future with the Whole of the UK' (2022)

Homburger Z, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace' (2019) 0826 Global Society 224

https://www.bbc.com, 'NHS 111 Software Outage Confirmed as Cyber-

Attack - BBC News' (*https://www.bbc.com/*, 6 August 2022) <https://www.bbc.com/news/uk-wales-62442127> accessed 26 August 2022

Hycner RH, 'Some Guidelines for the Phenomenological Analysis of Interview Data' [1985] Human Studies

International Security Programme, 'The Commonwealth Cyber Declaration: Achievements and Way Forward', vol 44 (2020) <www.chathamhouse.org> accessed 27 September 2021

International Telecommunication Union, 'Measuring the Information Society Report 2014' (2014)

——, *Global Cybersecurity Index (GCI)* (ITU Publications 2020) <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf>

International Telecommunication Union (ITU), 'Measuring the Information Society The ICT Development Index' (2009)

——, *Capacity Building in a Changing ICT Environment* (Suella Hansen ed, 2018th edn, International Telecommunication Union 2018) <https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.01-2018-PDF-E.pdf>

——, 'Global Cybersecurity Index (GCI) 2018' (2019)

Internet Society and African Union, 'Internet Infrastructure Security Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union' <https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/> accessed 12 October 2021

Itu and Abi Research, 'Global Cybersecurity Index and Wellness Profiles' (ITU Publications 2015) <www.itu.int> accessed 18 April 2021

ITU, *Measuring Digital Development Facts and Figures 2022* (2022)

ITU, Schjølberg S and ITU, 'ITU Global Cybersecurity Agenda: Framework for International Cooperation in Cybersecurity' (2007)

Jamil Z and Council of Europe, 'Cybercrime Model Laws: Discussion Paper Prepared for the Cybercrime Convention Committee' (2014) Version 9

Jovanovic B and Rob R, 'The Growth and Diffusion of Knowledge' (1989) 56 The Review of Economic Studies, Oxford Journals 569 <https://about.jstor.org/terms> accessed 25 January 2021

Kaldor M, Martin M and Selchow S, 'Human Security: A New Strategic Narrative for Europe' (2007) 83 International Affairs 273

KELLO L, *The Virtual Weapon and International Order* (Yale University

Press 2017)

Kenkel KM and Martins MT, 'Emerging Powers and the Notion of International Responsibility: Moral Duty or Shifting Goalpost?' (2016) 10 Brazilian Political Science Review 10 <http://dx.doi.org/10.1590/1981-38212016000100003> accessed 30 December 2020

Kiersey NJ, 'Scale, Security, and Political Economy: Debating the Biopolitics of the Global War on Terror' (2009) 31 New Political Science 27

Koenders B, 'TALLINN MANUAL Launch (2017) The Hague'

Koopman C, 'Genealogical Pragmatism: Problematization and Reconstruction' [2011] SSRN Electronic Journal

——, *Genealogy as Critique: Foucault and the Problems of Modernity* (Indiana University Press 2013)

Koopman C and Matza T, 'Putting Foucault to Work: Analytic and Concept in Foucaultian Inquiry' [2013] Critical Inquiry

Koopman C and Prado C., 'Two Uses of Genealogy: Michel Foucault and Bernard Williams', *foucaault's legacy* (Bloomsbury Publishing 2009)

Kshetri N, 'Diffusion and Effects of Cyber-Crime in Developing Economies' (2010) 31 Third World Quarterly 1057

——, 'Cybercrime and Cybersecurity in Africa' (2019) 22 Journal of Global Information Technology Management 77 <https://www.tandfonline.com/action/journalInformation?journalCode=ugit20>

Lai J and Widmar NO, 'Revisiting the Digital Divide in the COVID-19 Era' (2021) 43 Applied Economic Perspectives and Policy 458 </pmc/articles/PMC7675734/> accessed 15 April 2021

Latour B, 'The Powers of Association' (1984) 32 Sociological Review 264

——, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press 2005)

Lemke T, 'Foucault, Governmentality, and Critique' (2002) 14 Rethinking Marxism 49 <https://www.tandfonline.com/action/journalInformation?journalCode=rrmx20>

——, *Biopolitics: An Advanced Introduction.* (Monica J Casper and Lisa Jean Moore eds, NYU Press 2011)

Lévinas E, *Totality and Infinity : An Essay on Exteriority* (M Nijhoff Publishers ; distribution for the US and Canada, Kluwer Boston 1979)

Leye V, 'UNESCO, ICT Corporations and the Passion of ICT for Development: Modernization Resurrected' (2007) 29 Media, Culture and Society

Loader B, *The Governance of Cyberspace : Politics, Technology and Global Restructuring* (Routledge 1997)

Lubbock R, 'Development and Imperialism: Rethinking Old Concepts for a New Age' in G Honor Fagan and Ronaldo Munck (ed), *Handbook on Development and Social Change* (2018)

Mackinnon R, 'Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom', *Liberation Technology in Authoritarian Regimes* (iis-db.stanford.edu 2010)

Madhok S, *Rethinking Agency : Developmentalism, Gender and Rights* (Routledge 2013)

Majia Holmer Nadesan, *Governmentality, Biopower, and Everyday Life* (Routledge 2008)

Makarov V, Schandera S and Simon J, 'The ICT Landscape in BRICS Countries' (2012) 87 Digiworld Economic Journal

Maurer T, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2019) 12 Hague Journal on the Rule of Law 283

Mayntz R, 'From Government to Governance: Political Steering in Modern Societies' in Dirk Scheer and Frieder Rubik (eds), *Governance of Integrated Product Policy: In Search of Sustainable Production and Consumption* (1st edn, Routledge 2006)

Mccarthy DR, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (Palgrave Macmillan 2015)

McChesney RW, *Rich Media, Poor Democracy : Communication Politics in Dubious Times* ([New] ed / with a., New Press 2000)

Mezzadra S, Reid J and Samaddar R, *The Biopolitics of Development: Reading Michel Foucault in the Postcolonial Present* (2014)

Michael V. H, *Playing to the Edge : American Intelligence in the Age of Terror.* (Penguin Books 2016)

Miller P, 'Governing by Numbers: Why Calculative Practices Matter' (2001) 68 Social Research 379

Miller P and Miller BYP, 'Governing by Numbers: Why Calculative Practices Matter' (2001) 68 Social Research 379

Miller P and Rose N, 'Governing Economic Life' (1990) 19 Economy and

Society 1 <https://doi.org/10.1080/03085149000000001>

——, *Governing the Present. Administering Economic, Social and Personal Life* (Nikolas Rose and Peter Miller eds, Polity Press 2008)

Milton L. M, *Ruling the Root : Internet Governance and the Taming of Cyberspace.* (Paperback, The MIT Press 2004)

Ministry of National Security, 'Eighth Meeting of the REMJA Working Group on Cyber-Crime (Washington D.C. - Feb 27 & 28, 2014)'

Mol A, 'Ontological Politics. A Word and Some Questions' in John Law and John Hassard (eds), *Actor Network Theory and After*, vol 47 (1st edn, Blackwell Publishers 1999)

Morse JM, 'Emerging from the Data: The Cognitive Processes of Analysis in Qualitative Inquiry'

Mosco V, *The Political Economy of Communication : Rethinking and Renewal* (Sage Publications 1996)

Mueller M and others, 'Net Neutrality as Global Principle for Internet Governance Drafter: Concurring' (2007) <http://www.fcc.gov/ATT_FINALMergerCommitments12-28.pdf> accessed 25 May 2021

Mueller M, Schmidt A and Kuerbis B, 'Internet Security and Networked Governance in International Relations' (2013) 15 International Studies Review 86

Mueller ML, *Networks and States: The Global Politics of Internet Governance*, vol 48 (MIT Press 2010)

Müller T, 'Customary Transnational Law: Attacking the Last Resort of State Sovereignty' (2008) 15 Indiana Journal of Global Legal Studies 19

Murphy H and Kellow A, 'Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Arenas' (2013) 4 Global Policy 139

National Cyber Security Centre, 'CYBERUK 2019 Gallery - NCSC.GOV.UK' (*www.ncsc.gov.uk*, May 2019) <https://www.ncsc.gov.uk/section/cyberuk/2019-gallery> accessed 7 December 2022

Negroponte N, *Being Digital* (Coronet Books 1996)

Nicholls C, 'Coopration Against Cybercrime', *OCTOPUS CONFERENCE 2013 - Workshop 1 : Policies , activities and initiatives on cybercrime of international organisations* (The commonwealth secretariat 2013)

Noman H and York JC, 'West Censoring East The Use of Western

Technologies by Middle East Censors' (2010) <http://opennet.net.>

Norris P, *Digital Divide : Civic Engagement, Information Poverty, and the Internet Worldwide* (Cambridge University Press 2001)

Nye J, 'How Will New Cybersecurity Norms Develop?' [2018] Project Syndicate

Nye JS, 'Cyber Power' in Joseph S Nye (ed), *The Future of Power in the 21st Century* (Public Affairs Press 2010) <http://belfercenter.org> accessed 27 October 2021

——, 'The Regime Complex for Managing Global Cyber Activities' (2014) 1

O'Malley P, 'Risk and Responsibility' in Andrew Barry, Thomas Osborne and Nikolas Rose (eds), *Foucault and Political Reason, Liberalism, Neoliberalism and Rationalities of Governmentality* (The University of Chicago Press 1996)

O Donovan D, 'Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls', *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016)

Office C, 'National Cyber Security Strategy 2016-2021 - Progress Report' <http://www.nationalarchives.gov.uk/doc/open-> accessed 5 August 2021

Organization for Economic Co-operation and Development, 'Understanding the Digital Divide' (2001)

Ortis C and Evans P, 'The Pacific Review The Internet and Asia-Pacific Security: Old Conflicts and New Behaviour' <https://www.tandfonline.com/action/journalInformation?journalCode=rpre20>

Owusu-ekuful U, 'Ghana Will Get African Countries to Accede to Budapest Convention' (2019)

Palfrey J, 'The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed' (2004) 17 Harvard Journal of Law & Technology 409 <http://jolt.law.harvard.edu/articles/pdf/v17/17HarvJLTech409.pdf> accessed 1 August 2021

Patryk P and others, 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity' (2017) 2 Journal of Cyber Policy 123

Pawlak P, 'Riding the Digital Wave The Impact of Cyber Capacity Building on Human Development', vol 21 (2014)

——, 'Capacity Building in Cyberspace as an Instrument of Foreign Policy' (2016) 7 Global Policy 83

Pheko TG, ‘Speech by the Chief Executive Botswana Communications Regulatory Authority’

Philips SU, ‘Language and Social Inequality’ in Alessandro Duranti (ed), *A Companion to Linguistic Anthropology* (John Wiley and Sons Inc 2007)

Porter D, Isser D and Berg LA, ‘The Justice-Security-Development Nexus: Theory and Practice in Fragile and Conflict-Affected States’ (2013) 5 Hague Journal on the Rule of Law 310

Pranggono B and Arabo A, ‘COVID -19 Pandemic Cybersecurity Issues’ (2021) 4 Internet Technology Letters

Pritchett L, ‘Divergence, Big Time’, vol 11 (1997)

Pritchett L, Woolcock M and Andrews M, ‘Capability Traps? The Mechanisms of Persistent Implementation Failure’ [2012] SSRN Electronic Journal <https://papers.ssrn.com/abstract=1824519> accessed 18 April 2021

Raab D, ‘CYBERUK Conference 2021 : Foreign Secretary ’ s Speech’, *How the UK will lead internationally in protecting the most vulnerable countries* (National Cyber Security Centre 2021)

Raab D, Foreign Commonwealth and Development and National Cyber Security Centre, ‘CYBERUK Conference 2021: Foreign Secretary’s Speech - GOV.UK’ (*gove.uk*, 12 May 2021) <https://www.gov.uk/government/speeches/cyberuk-conference-2021-foreign-secretarys-speech> accessed 4 September 2022

Rabinow P, *The Foucault Reader* (1984)

——, *The Accompaniment: Assembling the Contemporary* (University of Chicago Press 2011)

Rabinow P and Rose N, ‘Biopower Today’ (2006) 1 BioSocieties 195

Raymond M, ‘Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot’ (2016) 10 Strategic Studies Quarterly 123

Reid J, ‘Interrogating the Neoliberal Biopolitics of the Sustainable Development-Resilience Nexus’ in Sandro Mezzadra, Julian Reid and Ranabir Samaddar (eds), *The Biopolitics of Development: Reading Michel Foucault in the Postcolonial Present* (Springer 2013)

Renaud K and others, ‘Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China’ (2020) 80 Public administration review 577

Republic of Ghana Ministry ofCommunications, ‘National Cyber Security Policy & Strategy’

Researcher, 'Interview with SJ - Canadian Centre for Cyber Security CyberUK'

Reyes A, 'Strategies of Legitimization in Political Discourse: From Words to Actions Introduction: Legitimization in Discourse' (2011) 22 Discourse & Society

Rojo LM, 'Division and Rejection: From the Personification of the Gulf Conflict to the Demonization of Saddam Hussein' (1995) 6 Discourse & Society 49

Rojo LM and Van Dijk TA, '"There Was a Problem, and It Was Solved!": Legitimating the Expulsion of "illegal" Migrants in Spanish Parliamentary Discourse' (1997) 8 Discourse & society 523

Rose N, *Powers of Freedom: Reframing Political Thought* (Cambridge University Press 1999)

——, *The Politics of Life Itself* (Princeton University Press 2007)

——, 'The Politics of Life Itself': (2016) 18 http://dx.doi.org.ezproxy.lancs.ac.uk/10.1177/02632760122052020 1 <https://journals-sagepub-com.ezproxy.lancs.ac.uk/doi/abs/10.1177/02632760122052020> accessed 18 August 2022

Rose N and Miller P, 'Political Power beyond the State: Problematics of Government' (1992) 43 The British Journal of Sociology 173

Rose N, O'malley P and Valverde M, 'Governmentality' (2006) 2 Annual Review of Law and Social Science 83 <www.annualreviews.org>

Rose NS, *Governing the Soul : The Shaping of the Private Self.* (2nd ed., Free Association Books 1999)

Rosenau JN and Czempiel E-O, *Governance without Government: Order and Change in World Politics* (James N Rosenau and Ernst-Otto Czempiel eds, Cambridge University Press 1992) <https://www.cambridge.org/core/terms.https://doi.org/10.1017/CBO9780511521775Downloadedfromhttps://www.cambridge.org/core>

Rovner J and Moore T, 'Does the Internet Need a Hegemon?' (2017) 2 Journal of Global Security Studies 184

Rugumamu SM, 'Capacity Development in Fragile Environments: Insights from Parliaments in Africa' (2011) 7 World Journal of Entrepreneurship, Management and Sustainable Development 113

Sadek J, 'EU Cyber Resilience for Development Project Launch Address by Ambassador Jan Sadek'

Saith A, 'From Universal Values to Millennium Development Goals: Lost in Translation' 37 Development and change 1167

Sandoval C, *Methodology of the Oppressed* (University of Minnesota Press 2000)

Sartre J-PP, *Being and Nothingness: An Essay in Phenomenological Ontology* (Mary Warnock and Hazel Estella Barnes eds, Methuen 1958)

Schia NN, 'The Cyber Frontier and Digital Pitfalls in the Global South The Cyber Frontier and Digital Pitfalls in the Global South' (2018) 6597 Third World Quarterly 1 <http://doi.org/10.1080/01436597.2017.1408403>

Schjølberg S, 'ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)' (2008) <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html> accessed 26 October 2021

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N Schmitt ed, Cambridge University Press 2017) <http://ebooks.cambridge.org/ref/id/CBO9781316822524>

securityweek.com, 'UK Foreign Secretary Calls for Cooperation on Cybersecurity | SecurityWeek.Com' <https://www.securityweek.com/uk-foreign-secretary-calls-cooperation-cybersecurity>

Skaletsky M and others, 'Exploring the Predictors of the International Digital Divide' (2016) 19 Journal of Global Information Technology Management 44 <https://www.tandfonline.com/action/journalInformation?journalCode=ugit20>

Snyder J, Komaitis K and Robachevsky A, 'The History of IANA: An Extended Timeline with Citations and Commentary' (2017) <internetsociety.org> accessed 7 June 2021

Sørensen E and Triantafillou P, *The Politics of Self-Governance* (Eva Sørensen and Peter Triantafillou eds, 1st edn, Routledge 2009)

Spivak GC, *The Post-Colonial Critic : Interviews, Strategies, Dialogues* (Sarah Harasym ed, Routledge 1990)

Stancu AI, 'Evolution of the International Regulations Regarding Cybercrime' (2016) 18 Public Administration & Regional Studies

Stevens T, 'Cyberweapons: Power and the Governance of the Invisible' (2018) 55 International Politics 482

Sylvia P, 'The Performance of Security as a Site of Biopolitical Struggle' (2014) 14 Cultural Studies ↔ Critical MethodologiesCritical Methodologies 451

Symantec and African Union Commission, 'Cyber Crime and Cyber

Security: Trends in Africa' (2016) <https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf> accessed 12 November 2021

Tapscott D and Caston A, *Paradigm Shift : The New Promise of Information Technology* (Art Caston ed, McGraw-Hill 1993)

The Commonwealth, *Promoting IT Enabled Services*, vol 3 (Nikhil Treebhoohun ed, Commonwealth Secretariat 2011)

——, 'The State of the Digital Economy in the Commonwealth' (The commonwealth secretariat 2020)

The Commonwealth Heads of Government, 'Commonwealth Cyber Declaration' (The commonwealth secretariat 2018)

The commonwealth secretariat, 'Cybersecurity for Elections: A Commonwealth Guide on Best Practice' (2020) <https://books.thecommonwealth.org/>

The Commonwealth Telecommunications Organisation, 'COMMONWEALTH APPROACH FOR DEVELOPING NATIONAL CYBERSECURITY STRATEGIES: A Guide to Creating a Cohesive and Inclusive Approach to Delivering a Safe, Secure and Resilient Cyberspace' (2015)

'The Internet' (*clintonwhitehouse4.archives.gov*) <https://clintonwhitehouse4.archives.gov/WH/EOP/OVP/24hours/internet.html> accessed 22 August 2022

The Researcher, 'Interview Conducted on the 22 of May 2019 with Senior Government Official - Ghana'

The World Bank and United Nations, *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies* (Creative C, The World Bank Group 2017)

thecommonwealth.org, 'About Us | Commonwealth' (*thecommonwealth.org*) <https://thecommonwealth.org/about-us> accessed 21 November 2019

Triantafillou P, *New Forms of Governing* (Palgrave Macmillan 2012)

United Nations, 'The Millennium Development Goals Report' (2015)

US Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command' (US Cyber Command 2018) <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf> accessed 18 January 2020

Villadsen K and Dean M, 'State-Phobia, Civil Society, and a Certain Vitalism' (2012) 9 Constellations

<https://onlinelibrary.wiley.com/doi/10.1111/cons.12006> accessed 1 December 2022

Villadsen K and Wahlberg A, 'The Government of Life: Managing Populations, Health and Scarcity' (2015) 44 Economy and Society 1 <https://www.tandfonline.com/action/journalInformation?journalCode=reso20> accessed 23 November 2021

Villeneuve N, 'The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace' (2006) 11 First Monday

von Heinegg WH, 'The Tallinn Manual and International Cyber Security Law' in Terry D Gill and others (eds), *Yearbook of International Humanitarian Law*, vol 15 (Cambridge University Press 2012)

Wade RH, 'Bridging the Digital Divide: New Route to Development or New Form of Dependency?' (2002) 8 Global Governance 443

Wallerstein I, 'The Inter-State Structure of the Modern World-System' in Steve Smith, Ken Booth and Marysia Zalewski (eds), *International theory: Positivism and Beyond* (10th edn, Cambridge University Press 2008)

Walters W, *Governmentality : Critical Encounters* (Routledge 2012)

Wang S, 'Pulling the Plug: A Technical Review of the Internet Shutdown in Burma' <http://www.irrawaddy.org/article.php?art_id=8705.> accessed 7 June 2021

Warner M, 'Cybersecurity: A Pre-History' (2012) 27 Intelligence and National Security 781

Warschauer M, *Technology and Social Inclusion: Rethinking the Digital Divide* (The MIT Press 2019)

Watch HR, 'False Freedom Online Censorship in the Middle East and North Africa' (2005)

Weinberg J, 'ICANN and the Problem of Legitimacy' (2000) 50 Source: Duke Law Journal 187

Wellman B and others, 'Does the Internet Increase, Decrease, or Supplement Social Capital? Social Networks, Participation, and Community Commitment' (2001)

World Economic Forum, 'The Global Risks Report 2023 (18.ª)' (2023) <https://www.weforum.org/reports/global-risks-report-2023>

Wright J, 'Cyber and International Law in the 21st Century' (2018) 2018 Chatham House Speech 19 <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>

Wynn E and Katz JE, 'Hyperbole over Cyberspace: Self-Presentation and Social Boundaries in Internet Home Pages and Discourse' (1997) 13 The Information Society

Yoo IT, 'New Wine into Old Wineskins? Regime Diffusion by the Powerful from International Trade into Cyberspace' (2017) 32 Pacific Focus

Zeng J, Stevens T and Chen Y, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"' (2017) 45 Politics and Policy

Zizek S, 'Why Does The Law Need An Obscene Supplement' in Peter Goodrich and David Gray Carlson (eds), *Law and the Postmodern Mind: Essays on Psychoanalysis and Jurisprudence* (University of Michigan Press 1998)

Zuckerman E, 'Intermediary Censorship' in Ronald Deibert and others (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (The MIT Press 2010) <https://doi.org/10.7551/mitpress/8551.003.0010>

AFILIAS DOMAINS NO 3 LIMITED v INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS [2001] ICDR IRP

Cyber Security Agency HR Bill 2015 (TT)

African Union Convention on cyber security and personal data protection in Africa 2014 (African Union Convention) 0

Charter of the Commonwealth 2012 (Charter of the Commonwealth)

Convention on Cybercrime 2001 (European Treaty Series - No 185) 6

Declaration on the Commonwealth Connectivity Agenda for Trade and Investment

Appendix A. List of empirical materials

Document Title	**Document Groups**
18 Act 29-06-2018 - CYBERCRIME AND COMPUTER RELATED CRIMES ACT, 2018 No. 18	Botswana
31 Act 10-08-2017-ELECTRONIC COMMUNICATIONS AND TRANSACTIONS (AMENDMENT) ACT, 2018	Botswana
32 Act 10-08-2018 - DATA PROTECTION ACT, 2018	Botswana
BOCRA WEBSITE APPLICATION SECURITY GUIDELINES	Botswana
Development of National Broadband Strategy Legal and Regulatory Review	Botswana
Development of National Broadband Strategy Policy Objectives_0	Botswana
Email Security Guidelines - BOCRA	Botswana
EU Cyber Resilience for Development Project: Launch Address by Ambassador Jan Sadek	Botswana
EU Cyber Resilience for Development Project	Botswana
Mr Thari G. PHEKO: Speech at ITU eGovenence convention - S Korea, 2014	Botswana
National Broadband Strategy FINAL(June2018)	Botswana
Press Realease SADC ICT Ministers Meeting - model framework draft - 2012	Botswana
Press Release - ITU-EC Project: Harmonized ICT Policies in the ACP countries (2011)	Botswana
Approved Botswana National Cybersecurity Strategy	Botswana
Cybersecurity and Cybercrime Laws in the SADC Region.indd	Botswana

Botswana_2020-02-12_ncsi.ega.ee: National cybersecurity index	Botswana
Cybersecurity and Cybercrime Laws in the SADC Region.indd	Botswana
Cybersecurity Act 2020 (Act 1038) - Ghana	Ghana
Interview transcript - Ghana- Official	Ghana
Ghana 2014 National Cybersecurity Policy Strategy Final Draft 2014	Ghana
Minister for Communication - Council of Europe Speech - Ghana will get African countries to accede to Budapest Convention	Ghana
Government of Ghana - Press Release: LEGISLATION ON CYBERSECURITY WILL ADDRESS WEAKNESSES IN OUR CYBERCRIME LAWS	Ghana
Hon-MinisterSpeech-at-National-Girls-in-ICT-Day-Celebration-2018	Ghana
Minister Speech - Ghana-PP-22-High-Level-Policy-Statement	Ghana
Speech-for-Minister-for-Communications-October-1-2020-1	Ghana
Data-Protection-Act-2012-Act-843	Ghana
Directive_CII	Ghana
Electronic_transactions_act-2008-act_772	Ghana
UNCITRAL - Model law - international commercial arbitration	ITU & InterOrg
ITU - Virtual consultation of councillors, 8-18 June 2021 Report by the Secretary-General	ITU & InterOrg
ITU Report - Are African countries doing enough to ensure cybersecurity and Internet safety	ITU & InterOrg
ITU Publication - Capacity building Assistance to devpng countries	ITU & InterOrg
ITU - Commonwealth ICT leaders summit - Global	ITU & InterOrg

Trends and Future Growth, 2012	
Commonwealth Working Group on Cybercrime - opening remarks	ITU & InterOrg
Conference on Cyberspace budapest - 2012 speech	ITU & InterOrg
ITU CYBLDC ConceptNote 2013 - Enhancing Cybersecurity in Least Developed Countries	ITU & InterOrg
ITU - Capacity Building in a Changing ICT Environment	ITU & InterOrg
ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) - Chairman Report	ITU & InterOrg
Global cybersecurity index 2015	ITU & InterOrg
Global cybersecurity index 2020	ITU & InterOrg
Global-Cybersecurity-Agenda-itu-17-may-2007	ITU & InterOrg
GUIDELINES FOR UTILIZATION OF THE GLOBAL CYBERSECURITY AGENDA	ITU & InterOrg
ITU- some history	ITU & InterOrg
itu-j-f_le_bihan-presentation_general_du_projet-en	ITU & InterOrg
ITU - Empowering Development Initiative Report, 2018	ITU & InterOrg
Message from the BDT Director 0- SADC	ITU & InterOrg
Message from the ITU Secretary-General SADC	ITU & InterOrg
Press Release_ ITU statistics symposium debates access to ICTs for sustainable development	ITU & InterOrg
Worldbank-toolkit - Combatting Cybercrime:Tools and Capacity Building for Emerging Economies	ITU & InterOrg
African Union and Internet Society - African Internet Infrastructure Security Guidelines May 2017	ITU & InterOrg
final Report-bsg-elac-cyber due diligence in international law	ITU & InterOrg
UN “In progress” - Reflections on the UN	ITU & InterOrg

discussions on state behaviour in cyberspace	The UK & the west
Cybercrime Model Laws	The Commonwealth
Bill-AN ACT to provide for the creation of offences related	The Commonwealth
CCI presentation	The Commonwealth
Charter of the Commonwealth 20113	The Commonwealth
Commonwealth Cyber Declaration	The Commonwealth
Commonwealth Cybergovernance Model	The Commonwealth
Commonwealth heads of government meeting Perth 2011	The Commonwealth
Commonwealth Declarations	The Commonwealth
Commonwealth Heads of Government Interim Report	The Commonwealth
Commonwealth - Small States Digest - Connectivity and ICT in the pacific 2017	The Commonwealth
CoE - Cyber crime legislation of Commonwealth Countries 2013	The Commonwealth
Cyber Governance in the Commonwealth - Towards Stability and Responsible State Behaviour in Cyberspace	The Commonwealth
Cybersecurity in the Commonwealth - building the foundation of effective national responses in the Caribbean	The Commonwealth
cybersecurity in the commonwealth - supporting economic and social development and rights online	The Commonwealth
Cybersecurity for Elections : A Commonwealth Guide on Best Practice	The Commonwealth
Declaration-Commonwealth-Connectivity-Agenda	The Commonwealth
Digital Connectivity Report - The state of the digital economy in the commonwealth	The Commonwealth
Commonwealth 12th Internet Governance Forum 2018	The Commonwealth

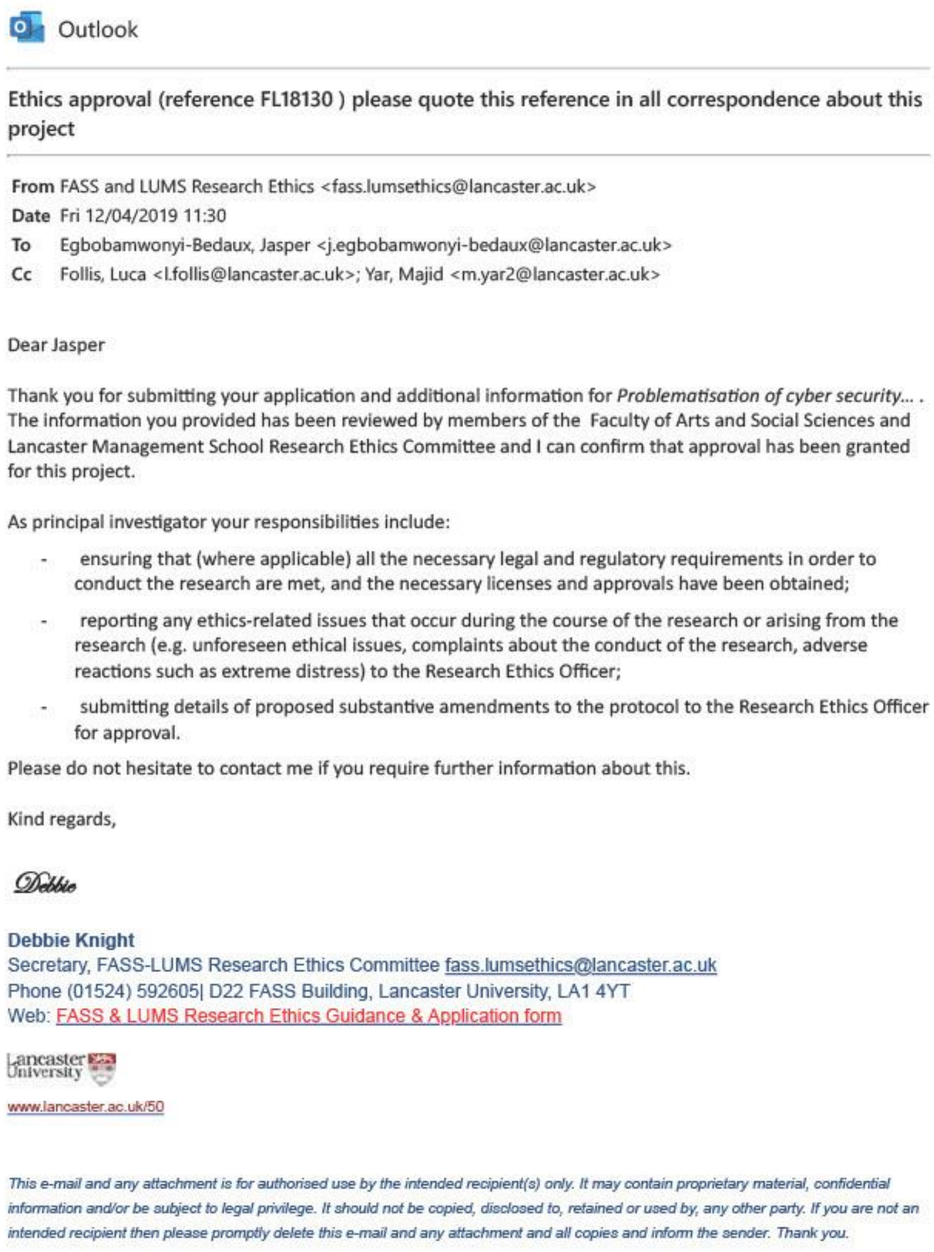
Commonwealth - Problems and Prospects for Commonwealth Developing Countries	The Commonwealth
Interview transcript – CCI Adviser – Commonwealth Secreteriat	The Commonwealth
Law reform in the commonwealth 1992 5th ed	The Commonwealth
Lessons from the commonwealth - Promoting IT services	The Commonwealth
Model Law Computer Related Crime	The Commonwealth
NATIONAL CYBERSECURITY STRATEGY - Kenya	The Commonwealth
Octopus Conference Presentation - Colin Nicholls QC - The Commonwealth Working Group of Experts on Cybercrime and the Commonwealth Cybercrime Initiative	The Commonwealth
Report of the Commonwealth Working Group of Experts on Cybercrime May_2014	The Commonwealth
small state digital transformation	The Commonwealth
Interview transcript - Legal Adviser - CCI projects	The Commonwealth
The Commonwealth Cyber Declaration - Achievements and Way Forward 1	The Commonwealth
THE COMMONWEALTH HEADS OF GOVERNMENT MEETING 2018 REPORT	The Commonwealth
Trade & Technology beyond COVID-19	The Commonwealth
eCommonwealth - Press Release	The Commonwealth
Abdul Minty interview	The Commonwealth
Cybercrime Model Laws	The Commonwealth
Interview with Billie Miller	The Commonwealth
Wtiness serminal - Britain in the commonwealth	The Commonwealth
GOV.UK - 2010 to 2015 government policy - cybersecurity	The UK, Int. Org & the west
GOV.UK - African Cyber Experts Fellowship lessons learnt report 2020	The UK, Int. Org & the west

UK Gov - Application of international law to states conduct in cyberspace uk statement	The UK, Int. Org & the west
BIS-Information security breaches survey 2014 executive summary revision1	The UK, Int. Org & the west
Britain, cybersecurity and the world	The UK, Int. Org & the west
Cyber and International Law in the 21st Century - UK's position on applying international law to cyberspace	The UK, Int. Org & the west
Cyber Governance in the Commonwealth - Towards Stability and Responsible State Behaviour in Cyberspace_2	The UK, Int. Org & the west
FCO - cyber securirty awareness in the commonwealth of nations	The UK, Int. Org & the west
Cybersecurity in the Commonwealth - building the foundation for effective national response	The UK, Int. Org & the west
Cybersecurity in the Commonwealth - supporting economic and social development	The UK, Int. Org & the west
UK Parliament - cybersecurity workshop report final 2020	The UK, Int. Org & the west
CYBERUK conference 2021: Foreign Secretary's speech	The UK, Int. Org & the west
Cybersecurity Considerations the Caribbean Process for for the Democratic Latin America and the Caribbean	The UK, Int. Org & the west
FACT SHEET_ U.S.-United Kingdom Cybersecurity Cooperation	The UK, Int. Org & the west
COMMONWEALTH 18 – 20 FUND INDEPENDENT ASSESSMENT Case Study 2 | 3 of Cybersecurity Programme	The UK, Int. Org & the west
Human rights in the digital age - state of play in the commonwealth pacific	The UK, Int. Org & the west
The Commonwealth Cyber Declaration - Achievements and Way Forward	The UK, Int. Org & the west
The United Kingdom's New Vision of Cyber Power	The UK, Int. Org & the west

UK foreign secretary - calls for cooperation on cybersecurity	The UK, Int. Org & the west
FCO Press release - UK pledges £22 million to support cyber capacity building in vulnerable countries	The UK, Int. Org & the west
UK Commonwealth Cybersecurity Programme - six case studies	The UK, Int. Org & the west
European Convention - INTERNATIONAL CYBER CAPACITY BUILDING: GLOBAL TRENDS AND SCENARIOS - Notes on Cyber Capacity Building Funders	The UK, Int. Org & the west
Commonwealth ncsirt Capacity Building Program - self help guide	The UK, Int. Org & the west
Cybersecurity Considerations the Caribbean Process for for the Democratic Latin America	The UK, Int. Org & the west
COMMONWEALTH 18 – 20 FUND INDEPENDENT ASSESSMENT Case Study 2 | 3 of Cybersecurity Programme 2	The UK, Int. Org & the west
USIP_United_Kingdom_Capabilities_for_Capacity_Building	The UK, Int. Org & the west
Global Britain in a competitive age - The Integrated Review of Security, Defence, Development and Foreign Policy 2021	The UK, Int. Org & the west
Computer misuse act 1990	The UK, Int. Org & the west
Regulation of Investigatory Act 2000	The UK, Int. Org & the west
8th meeting Working Group on Cyber-Crime bill session proceeding	Trinidad
8th meeting Working Group on Cyber-Crime	Trinidad
ACTIVITIES ON STRENGTHENING	Trinidad
AN ACT to provide for the establishment of the tt cybersecurity agency - essentials	Trinidad
AN ACT to provide for the establishment of the Trinidd and Tobago cybersecurity agency	Trinidad
HIPCAR - Cybercrime -e-Crimes - model policy and	Trinidad

xlegislative tex	
NATSEC Report- Joint Commitee on National Security	Trinidad
Report on inquiry into dna sampling	Trinidad
ELECTRONIC TRANSACTIONS ACT 2011	Trinidad
ELECTRONIC TRANSFER OF FUNDS CRIME ACT 2000	Trinidad
INTERCEPTION OF COMMUNICATIONS ACT 2010	Trinidad
The Computer misuse act 2000	Trinidad
Trinidad and Tobago_2021-03-02_ncsi.ega.ee national cybersecurity index	Trinidad

Appendix B. Ethics approval



Outlook

Ethics approval (reference FL18130) please quote this reference in all correspondence about this project

From FASS and LUMS Research Ethics <fass.lumsethics@lancaster.ac.uk>
Date Fri 12/04/2019 11:30
To Egbobamwonyi-Bedaux, Jasper <j.egbobamwonyi-bedaux@lancaster.ac.uk>
Cc Follis, Luca <l.follis@lancaster.ac.uk>; Yar, Majid <m.yar2@lancaster.ac.uk>

Dear Jasper

Thank you for submitting your application and additional information for *Problematisation of cyber security…* . The information you provided has been reviewed by members of the Faculty of Arts and Social Sciences and Lancaster Management School Research Ethics Committee and I can confirm that approval has been granted for this project.

As principal investigator your responsibilities include:

- ensuring that (where applicable) all the necessary legal and regulatory requirements in order to conduct the research are met, and the necessary licenses and approvals have been obtained;
- reporting any ethics-related issues that occur during the course of the research or arising from the research (e.g. unforeseen ethical issues, complaints about the conduct of the research, adverse reactions such as extreme distress) to the Research Ethics Officer;
- submitting details of proposed substantive amendments to the protocol to the Research Ethics Officer for approval.

Please do not hesitate to contact me if you require further information about this.

Kind regards,

Debbie

Debbie Knight
Secretary, FASS-LUMS Research Ethics Committee fass.lumsethics@lancaster.ac.uk
Phone (01524) 592605| D22 FASS Building, Lancaster University, LA1 4YT
Web: FASS & LUMS Research Ethics Guidance & Application form

Lancaster University

www.lancaster.ac.uk/50

This e-mail and any attachment is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and/or be subject to legal privilege. It should not be copied, disclosed to, retained or used by, any other party. If you are not an intended recipient then please promptly delete this e-mail and any attachment and all copies and inform the sender. Thank you.