Cyber & Cyberspace Is A Domain Not Just A Security Function

Dean Marc Co

Field CTO | ZedOptima Enterprises

A paper conducted under:
Birkbeck, University Of London
Business, Poltical Economy & Society

09 September 2023

Summary

This study aims to explore and investigate the contemporary perceptions, understanding, and implicit semantic meanings of cyber and cyberspace. While the concepts from the surface and within common social conversational context seem simple and obvious, deeper investigation of literature and institutional policy doctrines reveals that prevailing definitions have minimal mutual understanding, and that definitions of scope, scale, and semantics are sector specific and minimally transferrable to other contexts. It also overlaps excessively with adjunct conceptual entities like 'digital', 'internet', 'Internet', virtual worlds, metaverse, and others creating ambiguity and conflicts. Additionally, a sub-function of cyber, namely cybersecurity, became the proxy and de facto entity that represents the cyber practice across public policy, private enterprises and investments, and military or institutional domain definitions. Key questions centre around (i) the definition and scope of what cyber and cyberspace are from the perspective of institutions and its people, be it in the public sector or private enterprises; and (ii) how this relates to the direction, maturity, competitiveness, adaptability, trustworthiness, and effectiveness with its organisational purpose. The research process embodied an overarching qualitative grounded theory methodology, using only minimal assumptions as anchor concepts or scaffolds for taxonomy. These conceptual frameworks were mainly based on information systems theory, enterprise architecture paradigms, and prevailing doctrines defined by large institutions like the military and its sovereign state. The assumptions and propositions initially established were enhanced and expanded significantly based on wise feedback and actionable insights that were in fact, already in practice for organisations and functions that have achieved a high level of maturity, regardless of variances in the sophistication it entails. This allows or enables effective and competent delivery of the purpose of the organisation, thus ultimately leading to public trust in institutions, customer satisfaction for private enterprises, and social benefit when waste and needless ambiguity are given clarity.

Table Of Contents

Summary **1**

List Of Figures 4

List Of Tables 5

1. Introduction **6**

1.1. Rationale, Context, And Background 6

1.2. Research Objectives And Questions 7

1.3. Significance 8

2. Critical Review Of Literature **10**

2.1. History 10

2.2. Fundamentals 11

2.3. Information Systems 11

2.4. Cities And Urbanisation Parallels 13

2.5. Business, Political Economy, And Society 14

2.6. Domain For Military And Government Strategy And Operations 15

2.7. Present And Future Workloads 17

2.8. UK Perspective, A Starting Point 19

2.9. Broader Comparative Analysis 20

2.10. Identification Of Gaps In Existing Literature 22

3. Research Methods **24**

3.1. Research Design 24

3.2. Sampling Strategy 25

3.3. Data Collection Methods 26

3.4. Data Analysis Methods 28

3.5. Ethical Considerations 30

4. Findings And Analysis **32**

4.1. Conceptual Framework 32

4.2. Selection Of Specific Case And Context 34

4.3. Presentation Of Findings 36

4.4. Summary Of Research Findings 53

5. Conclusion **56**

5.1. Reflections On The Research Process 56
5.2. Proposed Global Cyber Architecture Model 57
5.3. Description Of The Proposed Model 58
5.4. Justification And Rationale 60
5.5. Potential Implications And Benefits 61
5.6. Limitations And Challenges 62
5.7. Policy Recommendations 62
5.8. Academic Contributions 63
5.9. Suggestions For Further Research 64
6. References 66
7. Bibliography 76
8. Annex 83
8.1 List Of Abbreviations 83

List Of Figures

Figure 3.4.1.	Coding Is An Iterative Process (Mason 2002)
Figure 3.4.2.	Data Analysis In Qualitative Research (Creswell, 2009)
Figure 4.1.1.	The Zachman Framework (Lankhorst et al, 2009; Zachman, 1987)
Figure 4.1.2.	A Conceptual Architecture Of Cyberspace
Figure 4.3.1.	Location Of Respondents
Figure 4.3.2.	Interview Distribution vs Sector Category
Figure 4.3.3.	Interview Distribution vs Sector Category - Detailed
Figure 4.3.4.	Seniority Level Distribution vs Seniority Level Category
Figure 4.3.5.	Lexical Analysis Supporting Code System
Figure 4.3.6.	Interview Responses Word Cloud
Figure 4.3.7.	Code and Perspectives
Figure 4.3.8.	Organisational Cybersecurity Practices
Figure 4.3.9.	Organisational Infrastructure Maturity
Figure 4.3.10.	Organisational Change And Maturity Capability
Figure 4.4.1.	Traditional Layered View Of Cyberspace (Parish & Madahar, 2016)
Figure 5.2.1.	A Conceptual Architecture Of Cyberspace

List Of Tables

Table 3.3.1.	Interview Questionnaire
Table 4.3.1.	Most Common Relevant Work Tokens And Concepts

1. Introduction

1.1. Rationale, Context, And Background

Cyberspace, as a continuously transforming and complex conceptual and notional entity (Caton & Bartholomees, 2012), embodies a multifaceted fusion of technologies, activities, and realms, defying categorisation as a monolithic or isolated construct (Crowther, 2017; Fanelli, 2016). This intricate blend, encompassing domains such as military, governance, commerce, infrastructure, and socio-technical systems, eludes simplified representations in contemporary dialogue and technological methodologies (Choucri, 2015; Crowther, 2017; Dunn Cavelty & Egloff, 2019; US DoD, 2022). In light of this complexity, this research is oriented towards an exploration of the background, semantic evolution, conceptual scope, and functional applicability of terminologies such as cyber, cyberspace, cybersecurity, and cyber maturity.

By employing rigorous scrutiny of scholarly literature, policy papers, and integrating insights from various disciplines and expertise, the study sets out to achieve a thorough but pragmatic examination of prevailing intellectual schools of thought on cyber taxonomy. It will build upon established cyber maturity models and structural designs, synthesising case studies and foundational technical tenets, to devise a renewed and formalised construct of the cyber domain. The objectives extend to uncovering and rectifying gaps within existing literature, accommodating newly arising socio-technological interactions, and broadening the scope of cyber maturity interpretation across diverse fields of study.

With an adherence to resilient and systematic research techniques, in particular studies and engagement with leading experts and practitioners, the research process endeavours to evaluate elements influencing institutional and national cyber maturity within an array of sectors. This analysis will culminate in the identification of a comprehensive taxonomy and architectural blueprint that furthers the assessment of maturity and augments strategic planning within the fluid technological terrain and global political environment.

Subsequently, this study aspires to enhance the broad taxonomy categories with a cohesive, integrative, and ubiquitous global architecture framework that aims to augment, if not supersede the current fragmented, episodic, and siloed perspectives on the cyber domain thinking, strategy, development, application, and operations.

1.2. Research Objectives And Questions

Central to this scholarly exploration are a pair of interlinked enquiries:

> (a) In our evolving digital epoch, how do institutions or organisations — encompassing both the labyrinthine corridors of public governance and the dynamic arenas of private enterprise — articulate and interpret the constructs of 'Cyber' and 'Cyberspace'?
>
> (b) In what manner do these institutional articulations act as navigational beacons, influencing and moulding overarching agendas related to competitiveness, maturity, evolution, trustworthiness, and operational efficacy?

At the base for this research is an in-depth study of the UK's National Cyber Strategy. This document or set of documents and sub-strategy papers, emblematic of a nation's ambition and trajectory in the cyber realm, will be the primary beacon illuminating our understanding of cyber maturity, its inherent resilience, and its ever-evolving capabilities (HM Government, 2022a). To enrich this foundational exploration, we shall traverse the landscape of documentation from an array of UK governmental entities. As elucidated by thinkers like Galston and McElvein (2015), such national strategies are not mere policy papers; they are complex fabrics with threads of technological nuances, political motivations, economic imperatives, and overarching strategic visions — each reflecting and influencing global trajectories.

One of the pivotal underpinnings of this research endeavour is to critically gauge the resonance between the UK's cyber aspirations and the broader envisioning of a "Global Britain" (HM Government, 2021; HM Government 2022). This involves a meticulous dissection

of elements like collaborative frameworks, the symbiotic building of alliances, and the cultivation of trust across institutional boundaries (as expounded by scholars like North, 1991; Savaş and Karataş, 2022). The overarching ambition here is not mere analysis, but the construction of a holistic, inclusive global cyber architecture that's both reflective of and responsive to contemporary challenges.

While the UK emerges as the predominant focal point of our analytical lens, it is imperative to underscore that this choice is not indicative of an insular or restricted viewpoint. The UK, in this context, offers a rich tableau — a baseline from which to extrapolate, compare, and contrast. It serves as a point of departure, enabling us to discern universalities and specificities in the vast tapestry of the cyber domain.

Broadening our horizon, we shall incorporate comparative insights from a global palette, with a marked emphasis on contrasting UK-centric narratives against institutional frameworks from other significant global players, like the United States. Such an approach not only bolsters the depth and breadth of our study but provides a panoramic view of the diverse manifestations of cyber — be it in its technological intricacies, societal ramifications, administrative imperatives, or as a domain with undeniable and escalating utility.

1.3. Significance

Anchored at the nexus of the ever-expanding realm of cyberspace and its geopolitical ramifications, this research casts a discerning eye on institutional perspectives vis-à-vis cyber maturity. In an age where cyberspace is progressively intertwined with global technological, economic, and strategic tenets (Dun Cavelty & Egloff, 2019; Keohane & Nye, 1998), the urgency for cogent cyber paradigms reaches a crescendo. Through this analytical journey, the study underscores the ripple effects engendered by terminological discrepancies within the 'cyber' nomenclature, shedding light on their manifestation in varied policy echelons of nations and organisations (Hathaway 2013; Luiijf et al, 2013).

One cannot overstate the gravity of the study's geopolitical underpinnings. As cyberspace emerges as the modern-day crucible where power structures are both challenged and redefined (Choucri, 2012; Cordesman, 2022; Dunn Cavelty & Egloff, 2019), there emerges an exigency for cyber blueprints that balance the scales of competition with foundational pillars of trust and collaboration. In this evolving schema where cyber instruments often overshadow traditional geopolitical channels (McGuffin & Mitchell, 2014), the quest for robust, encompassing frameworks gains pronounced importance.

Charting a meticulous course, the research embarks on a multi-disciplinary comparative lens, spotlighting governance touchstones emblematic of synergy, fortification of capabilities, and the edifice of trust. Embedded within the granular narrative of an archetypal national cyber strategy, such as the sets of policy documentation and strategy positioning of the United Kingdom (MoD, 2022a; MoD, 2022b), the exploration yields a treasure trove of insights, unearthing both the intricacies and vast horizons germane to cyber maturity roadmap.

From an academic viewpoint, the research introduces a meticulously outlined taxonomy – a confluence of cyber terminologies, maturity yardsticks, and strategic institutional vectors. By harmonising a spectrum of interdisciplinary insights, the endeavour is to sculpt a refined theoretical construct, the intent is to shape a seminal theoretical model; a lighthouse for institutions navigating the unpredictable waters of today's technological zeitgeist.

2. Critical Review Of Literature

2.1. History

Tracing its etymological roots to the Greek word "kybernetes" or steersman, the term "cyber" has undergone a multifarious transformation in its interpretation and application throughout history. The semantic trajectory of "cyber" and "cyberspace" has continued to diversify, evolving in tandem with the varied perspectives and agendas of stakeholders across disciplines (Caton & Bartholomees, 2012; Kreuzer, 2021), the nuances of public discourse, and the shifting paradigms within the technological and sociopolitical landscapes (Choucri, 2015; Beecroft, 2021).

In its embryonic stages, mathematician Norbert Wiener applied the term to the nascent field of cybernetics in 1948, highlighting the self-directed control and regulation inherent within mechanical and biological systems (Wiener, 2019). Subsequently, the term was employed by Danish architects in the 1960s to describe an architectural ethos envisioning open and adaptable sensory environments devoid of technological interference (Lillemose & Kryger, 2015). By the 1980s, the term had permeated the realm of science fiction, with William Gibson conceptualising "cyberspace" as a collective digital repository housing the entirety of human-computer interaction, visually depicted in his works "Burning Chrome" (Gibson, 1988) and "Neuromancer" (Gibson, 1984).

In general, especially in relation to its use in the transactional continuum of private companies and enterprises or its strategic or operational application in governments or the defence domains, the contemporary semantic meanings of "cyber" and "cyberspace" have coalesced around three principal domains: the Physical World, the Logical or Virtual World, and the Social or Human World (Clark, 2010; Gao et al, 2019; Ministry of Defence, 2022b).

Further refinements introduce definition granularity to these foundational layers, (a) distinguishing between Information and Data within the Logical domain; (b) recognising

Personas as distinct from Humans; and (c) demarcating Cyber-Enabled Spaces from purely physical constructs (Ning et al, 2018).

2.2. Fundamentals

The pervasive and extensible reach of cyberspace transcends geographical boundaries (Gao et al, 2019; HM Government, 2022a; Van Haaster, 2016). This, for example, allows for instant global communications among its many other utilities. As a web of interdependent elements by which an action in one area can impact the entire system, the interconnectedness of cyberspace offers benefits to millions and billions of users, but consequently and inherently becomes prone to disruption if key components or entities in the underlying system become faulty (Castell, 2010). As an ever-evolving construct, new technologies, applications, and threats emerge regularly (Demchak, 2020; Libicki, 2021). It entails a vigilance across a multitude of entities and actors within the system to keep the system operating. The ubiquity, virtuality, and decentralisation of cyberspace through the rise of Internet-connected devices such as IoT and smartphones has woven cyber realities into daily physical existence (Choucri, 2012). This facilitation through complex computing systems enables novel interactions like online gaming, digital currencies, online shopping, social media, and other key access to government services (Castell, 2010). This decentralisation enhances the distribution of data and services but implicitly complicates governance (Betz & Stevens, 2011) and oversight as well as introduces further challenges to privacy and identity management.

2.3. Information Systems

Using the perspective of information systems theory, the virtual realm where digital communications occur, the intricate interplay of people, processes, technology, governance (McMullen & Schneider, 1972; Gregor, 2006), and other factors defines the digital landscape (Checkland, 1988; Orlikowski & Robey, 1991). From this vantage point, the theory transitions into practical and tangible constructs. In other words, this global domain ultimately comprises an interconnected network of information technology infrastructures, including the Internet,

telecommunications networks, computer systems, embedded processors, and controllers (Porter & Heppelman, 2014). This becomes a very pragmatic baseline of components that can be itemised in further discourse, highlighting that while abstractions are useful, the underlying physical reality remains a fundamental pillar in the taxonomy of concepts (Greer et al., 2019).

Hardware represents the tangible components of cyberspace, such as computers, servers, routers, cables, satellites, and more, which underpin digital communication (Jazdi, 2014). It encompasses the devices that individuals use daily, as well as the infrastructure that enables worldwide connectivity. Software, consisting of digitally stored data that guides hardware operations, plays a critical role. Ranging from operating systems like Windows or Linux to applications and protocols that facilitate data transmission, software powers the myriad digital interactions that occur daily (Ning et al., 2018). Networks, or interconnected groups of devices, facilitate communication and data transfer. They vary in scale from global structures like the Internet to local networks such as a home Wi-Fi system. These networks enable data transmission and access to digital services worldwide. Data encompasses all digital information created, stored, manipulated, and transmitted across networks. It can take various forms, including text files, images, audio, and video. The exchange of data is integral to the functioning of cyberspace, enabling individuals and organisations to communicate, share, and interact (Choucri, 2012; Choucri, 2015). Devices, which include computers, smartphones, tablets, and smart devices (IoT), serve as gateways to cyberspace. These points of access allow users to engage with the digital world, facilitating activities such as web browsing, communication, and content consumption. Users, consisting of individuals, organisations, and government entities, interact within the digital landscape.

As active participants in cyberspace, users access digital services, conduct transactions, and engage in various online activities. These communication methods play a vital role in global connectivity. Satellites support long-distance and remote-area communication, enabling services like GPS navigation, satellite TV, and internet access. They extend network coverage beyond terrestrial network limits. Governance and regulation of cyberspace involve the establishment and enforcement of rules and policies governing digital interactions (Kissinger et al., 2021; Keohane & Nye, 1998). This includes laws related to privacy,

data protection, cybersecurity, and intellectual property, among others. Effective governance ensures a secure and ethical digital environment.

2.4. Cities And Urbanisation Parallels

At the heart of a city's birth lies its physical and geographic setting. The bounty of a river, the promise of fertile land, or the lure of trade routes – these are the primal calls that summon cities into being (Bettencourt, 2012). In parallel, the birth of cyberspace owes itself to physical environments: the whirring hardware, the humming servers, and the vast web of networks that interlink them. Like cities, cyberspace has its foundation in the physical and the tangible.

As cities grow, they become teeming hubs of humanity, populated by people who navigate a dense forest of objects – buildings, streets, and vehicles. These objects, infused with life and purpose by their inhabitants, come together to create the unique tapestry of a city's culture (Mumford, 1961). Similarly, cyberspace thrives on the interaction between users and digital objects – websites, applications, and data streams (Clarke, 2010; Dunn Cavelty & Egloff, 2019). Together, they form the vibrant, evolving culture of the online world.

But like any living organism, both cities and cyberspace evolve. From humble beginnings as simple settlements or nascent networks, they mature into intricate ecosystems of complexity and diversity (Bettencourt, 2012; Voo et al., 2022). In this process of evolution, they hunger for better infrastructure – the robust skeleton that supports their growing bodies. The sprawling roads of cities echo the high-speed data highways of cyberspace.

With growth comes the need for guidance and governance. Cities find their stewards in local governments, law enforcement, and social institutions that shepherd their inhabitants through the twists and turns of urban life. In cyberspace, the digital shepherds emerge as internet service providers, platform administrators, and online communities, guiding users through the ever-shifting landscape of the internet (Dunn Cavelty & Egloff, 2019).

Cities and cyberspace – the physical and the digital – are twin journeys of humanity, parallel narratives in the story of our civilisation. They share a common origin in the tangible, a mutual evolution towards complexity, and a collective pursuit of sustainable harmony. From this correlation, an analytical guideline drawn from parallel and analogy can be derived.

2.5. Business, Political Economy, And Society

The intricate ecosystem of cyberspace facilitates global connectivity and innovation, fostering new business models and marketplaces akin to the rise of urban commercial centres (Sassen, 1991; Castells, 2010). Examples include the emergence of online marketplaces such as Amazon and Alibaba. However, this increased interconnectedness also accentuates cybersecurity vulnerabilities (IISS, 2021), necessitating robust risk management strategies and the adoption of standardised security protocols (Carr, 2012; Choucri, 2015; Jabbour & Devendorf, 2017). Just as cities drive economic specialisation and diversification (Florida, 2002), cyberspace spurs competitive advantage and differentiation through the adoption of digital technologies (Porter & Heppelmann, 2014).

The digital realm's analogue to cities extends to the political economy, where the management of resources, power dynamics, and regulations shape the contours of the cyber world (Clarke, 2010; Dunn Cavelty, 2013). As governments attempt to exert control over cyberspace through regulatory frameworks, questions of sovereignty, jurisdiction, and transnational cooperation arise (Dunn Cavelty, 2019). The internet's borderless nature and decentralised architecture challenge traditional notions of statehood and territoriality (HM Government, 2022a; HM Government, 2022b). Moreover, the digital economy's role in reshaping labour markets, production, and consumption patterns echoes the transformative effects of urbanisation on economic structures and employment (Florida, 2002; HM Government, 2021).

The sociocultural dimensions of cities and cyberspace converge (Bettencourt, 2012) in their role as platforms for communication, expression, and community-building (HM Government, 2022a; Foucault, 1971). In both environments, the interplay of diverse groups

generates cultural exchanges and the propagation of norms and values (Jenkins, 2006). However, the double-edged sword of connectivity exposes society to misinformation, cyberbullying, and breaches of privacy (Carr, 2012). As in urban centres, the quest for digital equity and inclusion becomes paramount to ensure equitable access to technology and digital literacy (HM Government, 2022a; HM Government, 2022b).

2.6. Domain For Military And Government Strategy And Operations

The emergence of cyber as a domain for military and government strategy and operations can be traced back to the development of the internet in the 1960s (Caton, 2018), initially intended as a way to maintain military communications in the event of a nuclear attack (Castells, 2010; Choucri, 2012). At the centre of this new domain from government and military vantage point is "cyber warfare," defined as the actions by a nation-state or international organisation to attack or defend information and other computer systems in cyberspace (Choucri, 2015; Demchak, 2020).

Cyber as a domain for military and government strategy also involves defensive and offensive operations, including cyber espionage, intelligence gathering, and the development of cyber capabilities for strategic deterrence (Libicki, 2021). The cyber operations of nation-states have included the surveillance of foreign governments and organisations, as well as the theft of intellectual property and sensitive information (Savaş & Karataş, 2022). The cyber domain's role in military operations (Crowther, 2017) is further evidenced by the 2010 Stuxnet attack on Iranian nuclear facilities, a joint operation by the U.S. and Israel that utilised a malicious computer worm to disrupt centrifuge operations (Carr, 2012).

The development of cyber norms, doctrines, and strategies has become an area of focus for governments and international organisations, as countries seek to establish guidelines for responsible behaviour in cyberspace and deter potential aggressors (Nye, 2017). In addition, the concept of "cyber power" has garnered increasing attention within the realms of national security and strategic studies, as digital technologies and cyberspace have become intertwined with the conduct of statecraft (Kissinger et al., 2021; Van Haaster, 2016; Voo et al.,

2022). Defined as the potential and capacity of a state or organisation to exploit cyberspace for its advantage, defend against cyber threats, and influence the behaviour of other actors in the digital realm (Betz, 2011; Jabbour & Devendorf, 2017), cyber power represents a multifaceted construct that extends across multiple domains. Its exploration provides valuable insights into the complexities of geopolitics, strategic competition, and cooperation in the digital age (Choucri, 2012; Kissinger et al., 2021).

Offensive Cyber Power pertains to a state's ability to conduct cyber operations targeting adversaries, encompassing activities such as espionage, data theft, and the sabotage of critical infrastructure (Libicki, 2020; Rid & Buchanan, 2015). These activities which aim to weaken or degrade an opponent's capabilities or extract valuable information (Demchak, 2020), hold the potential to disrupt command and control systems, impede military operations, or inflict economic damage on an adversary.

Encompassing a state's capacity to safeguard its digital assets, networks, and systems against cyberattacks, Defensive Cyber Power necessitates a robust cybersecurity posture that includes intrusion detection, threat analyses, and incident response capabilities (Lin, 2010) as well as the development and implementation of cybersecurity policies, threat intelligence gathering, and the establishment of cyber incident response teams (CIRTs) to mitigate cyberattacks (Libicki, 2020; Dunn Cavelty & Egloff, 2019).

Economic Cyber Power is a reflection of a country's digital economy, technological advancements, and cyber industry. A thriving digital economy, innovation ecosystem, and strong technological industry can provide a country with a competitive edge in the global market (Hathaway, 2013). This also includes the ability to leverage and directly control digital platforms, e-commerce, and fintech ecosystems to foster economic growth and competitiveness (Baller et al., 2016).

Representing the capacity to shape information and narratives in the digital domain, Informational Cyber Power defines a state's capability for cyber-enabled information warfare,

propaganda, and disinformation campaigns (Carr, 2012), as well as efforts to control or censor information within a state's cyberspace (Tucker et al., 2018).

Diplomatic Cyber Power is a proxy for the influence a country wields in shaping international norms, rules, and governance mechanisms for cyberspace. Diplomatic efforts to promote responsible state behaviour, prevent cyber conflict, and foster international cooperation on cybersecurity fall within this domain (Nye, 2011; Nye, 2017).

Navigating the complexities of cyber power involves addressing strategic dilemmas and challenges. The trade-offs between offensive and defensive cyber measures, the balance between digital openness and security, and the pursuit of responsible state behaviour in cyberspace are all critical considerations (Eriksson et al., 2009).

2.7. Present And Future Workloads

In the realm of political economy, cyberspace has reshaped power dynamics, governance, and resource management, prompting questions about sovereignty, jurisdiction, and international cooperation (Nye, 2011; Nye, 2017). At the societal level, cyberspace fosters communication, expression, and community-building while simultaneously exposing society to challenges such as misinformation and privacy breaches (DiResta et al., 2018; Tucker et al., 2018). As cyberspace evolves, it reflects the diverse realities of different countries, regions, and contexts, making its future trajectory complex and multifaceted (Caton, 2018). To navigate this complexity and sustain progress, it is imperative to have foresight that considers the environmental sustainability of cyberspace, addressing issues related to equitability, energy consumption, and potential harm to the natural environment (Greer et al., 2019; Hathaway, 2013).

The global data deluge, driven by the proliferation of digital devices, IoT deployments, and growing user connectivity, has considerably increased the workload of data transmission across cyberspace (Eom et al., 2012). As the volume and velocity of data continue to grow,

efficient routing, increased bandwidth, and high-speed data transmission become critical for managing the data transmission workload (Ning et al., 2018).

The expanding reliance on online services, such as cloud computing, e-commerce, social media, and streaming platforms, further adds to the workload on cyberspace's virtual infrastructure (Tucker et al., 2018). As users demand prompt and dependable access to online services, the capacity to scale resources and ensure service reliability becomes essential (HM Government, 2022a; MoD, 2022b).

Cyberspace also serves as a battlefield for cyber warfare, where nation-states and non-state actors engage in cyber espionage, sabotage, and information warfare (Carr, 2012; Eom et al., 2012; Kreuzer, 2021; Libicki, 2021). The increasing complexity of cyber threats and the escalating cyber arms race necessitate robust cybersecurity postures, threat intelligence gathering, and incident response capabilities (Betz & Stevens, 2011; Lin, 2010; Van Haaster, 2016).

The future of cyberspace is expected to be shaped by emerging technologies, such as artificial intelligence (AI), quantum computing, and blockchain (Clarke, 2010; MoD, 2022a). AI will drive automation and optimisation of cyberspace workloads, while quantum computing promises to revolutionise data processing capabilities (Kissinger et al., 2021). Meanwhile, blockchain technology offers secure and decentralised data management solutions for cyberspace (Baller et al., 2016).

Augmented reality (AR), digital twinning, and space exploration data will also contribute to shaping the future workloads of cyberspace (Lee, 2022). These applications will necessitate greater computational power, data storage, and network connectivity, further extending the notional boundaries of cyberspace beyond Earth (Libicki, 2021).

The future of cyberspace also entails addressing the challenges of establishing norms for responsible state behaviour, fostering international cooperation on cybersecurity, and balancing digital openness and security (Betz & Stevens, 2011; Dunn Cavelty & Egloff, 2019).

The pursuit of digital equity and inclusion will be paramount to ensure equitable access to technology and digital literacy (Nye, 2011; Nye, 2014).

2.8. UK Perspective, A Starting Point

The UK's history in the domain of information sciences and technology is indeed illustrious. From early contributions to digital numerical systems to theoretical machines capable of automating maths operations, the UK has been at the forefront of digital innovation, often in collaboration with experts and scholars worldwide (British Academy, 2022; IISS, 2021). The rise of the UK to technological prominence is analogous to its leadership during the Industrial Revolution. However, the current multipolar evolution of information technology contrasts with the UK's historical imperial ascendancy (House of Lords, 2022; Jazdi, 2014).

Recent literature and reports showcase the UK's sustained influence in various spheres (HM Government, 2021; House of Lords, 2022; Nye, 2011). Key strengths include an open political environment, a developed economy, an advanced education and research ecosystem, and a hub for leading enterprises in Europe. The UK's leadership in addressing challenges such as climate change and its role in global security and diplomacy underscore its influence. Its soft power extends across numerous domains, and its role as a hub for science and technology investment has positioned the UK as a force for innovation across sectors like biotechnology, finance, and energy (House of Lords, 2022; Nye, 2005). The influx of foreign and domestic investments further highlights the UK's leadership in the global economic landscape (HM Government, 2021).

The UK government's Integrated Review in 2020, covering national security, military defence, international development, and foreign policy, demonstrates a recognition of the challenges and threats facing both the UK and the world (HM Government, 2021). The interconnected challenges facing the UK and the world are embodied in the Ministry of Defence’s Global Strategic Trends, including human empowerment, power transitions, information centricity, technical progress, environmental damage, and migration (MoD, 2022a).

These trends represent a confluence of historical legacies and emerging developments, presenting both challenges and opportunities for future progress (MoD, 2022a).

The UK government has launched its National Cyber Strategy to strengthen its cyber capabilities and resilience in the face of rapidly advancing technology and an evolving digital landscape (MoD, 2022b). Built on the National Cyber Security Strategy of 2016, the new strategy aims to keep the UK at the forefront of cyber technology and cybersecurity (DSIT, 2023; MoD, 2022b).

The strategy focuses on five pillars (HM Government, 2022a):

1. Strengthening the UK whole-of-cyber ecosystem.
2. Minimising cyber risks for businesses and citizens, and enhancing data protection and digital confidence.
3. Leading in vital cyber technologies by expanding industrial capacity.
4. Advancing the UK's global leadership and influence.
5. Detecting, disrupting, and deterring adversaries.

Several organisations and initiatives support the strategy, including the National Cyber Security Centre, the National Cyber Force, and the Law Enforcement's National Cyber Crime Network. Additionally, the Cyber Map and the UK Cyber Security Council play essential roles in raising cybersecurity awareness, while the Digital Security by Design initiative contributes to enhancing digital security (HM Government, 2022a). The strategy also highlights the importance of basic cybersecurity in protecting the public sector from ransomware and other cyber threats (MoD, 2022b).

2.9. Broader Comparative Analysis

The UK's approach to cybersecurity and digital strategy is just one perspective in a complex and interconnected global landscape (MoD 2022b). Various states, transnational organisations, and other stakeholders exert their influence in cyberspace, and the actions of one entity often have ripple effects that impact the broader community.

The United States is a dominant force in cyberspace, with a robust cyber ecosystem that encompasses the private sector, government, and academia. The US's National Security Strategy highlights the importance of securing cyberspace as a vital component of its national security efforts (US DoD, 2022; US DoD, 2023). However, the country's decentralised approach has often led to a fragmented cyber policy landscape that is influenced by diverse stakeholders, including technology giants and civil society organisations.

NATO, as a military alliance, has increasingly recognized the significance of cyberspace in warfare and has developed strategies and doctrines to defend against cyber threats (NATO, 2022). The alliance has worked to integrate cyber capabilities into its military operations and has established the Cooperative Cyber Defence Centre of Excellence to promote research and collaboration among member states (NATO, 2022). The European Union has taken significant strides to establish a cohesive approach to cybersecurity. The EU's Cybersecurity Strategy for the Digital Decade aims to build a secure and resilient digital space, protect critical infrastructure, and foster innovation (European Commission, 2020). As part of this strategy, the EU has focused on establishing a robust regulatory framework, as seen in the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive) (European Commission, 2020).

Countries such as Australia, Canada, and Japan have also developed cyber strategies and policies that reflect their unique geopolitical and economic contexts. Australia's Cyber Security Strategy, for instance, emphasises the importance of a strong cybersecurity workforce and promotes partnerships with the private sector and academia (Australian Government, 2022). Canada's National Cyber Security Strategy focuses on the security, resilience, and prosperity of its digital economy (Government of Canada, 2018). Japan's Cybersecurity Strategy, meanwhile, emphasises its commitment to an open, free, and secure cyberspace (Government of Japan, 2015). China's approach to cyberspace stands in contrast to many Western democracies, with the government exerting significant control over its domestic digital ecosystem; its cybersecurity laws focus on the importance of data localization and impose stringent requirements on technology companies operating in China (Raud, 2016).

These challenges impact the ability of nations to fully realise their strategic objectives in cyberspace. Comparing the UK's approach with those of other key players provides valuable insights into the dynamics of the global cyber landscape. The diverse approaches to cyberspace reflect the broader geopolitical and socioeconomic contexts in which they are situated (Caton, 2018). Understanding these complexities is crucial for developing robust and effective cyber and digital strategies.

2.10. Identification Of Gaps In Existing Literature

Scholars have critiqued the inadequacy of current global cyber architectures, emphasising their fragmented technical and policy approaches (Choucri, 2012; Dunn Cavelty & Egloff, 2019). Political economic factors significantly shape cyber strategies, as state-centric paradigms overlook the growing influence of non-state actors and economic interdependence (Keohane & Nye, 1998). Power imbalances persist, particularly through control over digital infrastructure and standards (Betz & Stevens, 2011; Dunn Cavelty, 2021).

Institutional practices often infringe on privacy, rights (Mearsheimer, 1994), and freedoms in cyberspace governance (Cox & Kanji, 2022; Deibert et al., 2008). Examples like China’s censorship and monitoring systems illustrate the risks of prioritising security and surveillance (Gao et al., 2019). Pluralistic governance and participatory policymaking are called for (Chang & Grabosky, 2017).

Nevertheless, the literature reveals gaps. Comprehensive comparisons of national cyber frameworks across public and private sectors are scarce (Cox & Kanji, 2022; Van Haaster, 2016). Despite the UK National Cyber Strategy’s advocacy for unified regulations across sectors (HM Government, 2022a), an integrated international analysis covering legal, technological, governance, and security culture aspects is still lacking.

A broader lens is needed to examine geopolitical dynamics and strategic interests of state and non-state actors through a political economy approach (Carr, 2016; Prince & Sullivan,

2019). The UK strategy recognises cyber capabilities as power shapers, calling for global norms and standards partnerships (HM Government, 2022a). Yet, much of the current literature remains focused on technical dimensions and immediate security threats, neglecting multidimensional and long-term factors influencing global cooperation and equitable cyberspace development.

Additionally, socio-cultural factors such as ethics, privacy, digital rights, identity, and impacts of the global digital divide deserve further exploration (Dunn Cavelty, 2013; Galston & McElvein, 2015). While the UK strategy supports cyber literacy and access for disadvantaged groups, more comparative research on public attitudes and vulnerabilities across demographic divides is essential (HM Government, 2022b). Critical theory can offer valuable insights into dominant values and marginalised voices in global policy discussions (Gorwa, 2019).

3. Research Methods

3.1. Research Design

The objective of detailing the methodology is to provide a clear, comprehensive account of the approach taken to conduct and evaluate the research in a rigorous and systematic manner. As noted by Blumberg et al. (2014), a thorough explanation of the methods used is critical for assessing the reliability, validity, and objectivity of the research findings. By detailing the design, data sources, analysis strategy, and any limitations, this section aims to enhance the reader's understanding of how the investigation was methodically carried out to produce credible, evidence-based insights that address the research objectives.

Ontologically, this study embraces subjectivism, acknowledging that multiple participant realities are influenced by social, political, and economic contexts. This acknowledgement is evident, for instance, in the varying perspectives on data privacy between the private and public sectors. Epistemologically, the study employs an interpretivist perspective, viewing knowledge as contextually situated and generated through insider perspectives rather than external generalisations (Creswell, 2009).

The research methods mirror the interpretivist paradigm, emphasising contextual and naturalistic inquiry. In-depth interviews grant participants the freedom to articulate their experiences and perspectives (Mason, 2002), while surveys offer supplementary data on politico-economic and social aspects of cyber capabilities. Content analysis of institutional reports provides additional insights into strategic priorities and self-assessments of cyber maturity.

By illuminating experiential diversity, this research aims to provide an empirical foundation for the development of inclusive cyber policies that balance security, economic growth, rights, and emerging technologies. The findings aspire to inform models that promote capability building, access, ethics, and cooperation at local and global levels. The analysis

may, for instance, pinpoint priorities for socio-technical frameworks enhancing cyber literacy or intersectoral data-sharing practices that balance innovation, privacy, and societal benefits.

Ultimately, the interpretivist approach allows for the creation of actionable maturity models reflecting the complexities of various institutional and societal contexts (Creswell, 2009; Mason, 2002). The research paradigm aligns with the goal of fostering knowledge on equitable and ethical cyber futures from a grassroots perspective.

3.2. Sampling Strategy

The sampling strategy was informed by a desire to provide a comprehensive and well-rounded perspective on cyber maturity, cybersecurity, and other cyber considerations. In line with recommendations by Mason (2002), it employed a purposive sampling strategy to select key stakeholders from leading businesses, government institutions, and social NGOs, as these individuals and organisations have direct involvement in the development and implementation of cyber policies and strategies. Engaging with these stakeholders allowed us to capture insights from those directly responsible for shaping cyber policies and those affected by these policies (Bell et al., 2022).

To ensure diversity within the sample, we followed the principles of stratified sampling, as outlined by Creswell (2009), by speaking with individuals across various levels of authority, from frontline staff to senior leadership. We also engaged with individuals who have varying levels of subject matter expertise and knowledge, including both cybersecurity specialists and generalists. This approach allowed us to capture a broader range of perspectives and insights, which is essential for understanding the complex and multifaceted nature of cyber maturity issues.

While this had a well-defined sampling strategy in place, we recognized the importance of flexibility in the research process. As Saunders and Lewis (2018) point out, qualitative research often requires a degree of flexibility to respond to emerging insights and unanticipated opportunities. Therefore, we remained open to incorporating insights from individuals or groups

outside of our initial sampling target, provided that their contributions were relevant and valuable to our research objectives.

3.3. Data Collection Methods

The data collection steps include setting the boundaries for the study, collecting information through unstructured or semistructured observations and interviews, documents, and visual materials, as well as establishing the protocol for recording information (Saunders et al., 2019). For the purposes of this study, feedback from diverse groups provides crucial source qualitative data. Experts who were identified and pursued include those working in private or public companies, organisations, businesses, academia, and think tanks focused on implementing cyber, information technology, and other related products.

While field research interviews were largely opportunistic and ad-hoc, expert interviews were carefully scheduled and coordinated with accessible government bodies, industry experts, companies, and professionals. These interviews were conducted either face-to-face or through online methods such as video conferencing or voice calls. In cases where scheduling difficulties arose due to time zone differences or the interviewee's availability, an interview questionnaire was sent via email to allow the interviewee to respond at their convenience. The same questionnaire was used for all interview formats, whether in-person, online, or offline asynchronous interviews. Responses were collected on an online data entry platform, ensuring that the knowledge base was centralised and organised in a consistent manner from the outset, regardless of the mode of conversation.

However, it is important to note that while in-person interviews offer the advantage of being able to explore nuanced conversational cues more deeply (Creswell, 2009), several factors can influence the quality of the discussions. These factors include the interviewee's levels or propensities towards introversion or extroversion, the logistics of the interview (including the time of day and scheduling difficulties), and any subtle cues given by the interviewee. For example, interviewees, even those in leadership positions, may be less open and candid in an office environment compared to a more relaxed setting outside the normal

work environment. This is a critical discovery and consideration that may be intuitively apparent and obvious but is rarely or explicitly addressed in research methodology textbooks (Mason, 2002; Creswell, 2009). Despite the wealth of guidelines on conducting interviews effective, such as preparing properly, engaging politely, and listening intently, and observing alertly, situational contexts inherent in the interview method, research process, and overall circumstances and context of the discussions can still introduce bias into the observations, data collection, and interpretation by the researcher.

The set of questions was developed to capture different perspectives and to provide detailed opinions or thoughts. The second part of the questionnaire is about rating certain cyber practices in their respective organisations. The goal was to understand specific cyber contexts from both specialised and lay viewpoints. Experts provided comparative analytical perspectives given their global experience while their perspectives as citizens or residents were also shared localised attitudes and perceptions. Together, these aim to elucidate multidimensional insights on cyber governance efforts and practices. Open-ended expert interviews allowed additional thoughts beyond the formal questions. This diversity of perspectives enriches analysis.

Interview Questions
Demographic Information
1. Contact / Email / Others (optional)
2. Location. Which city are you in or which location do you currently reside?
3. Occupation? [Student, Professional (Public), Professional (Private), Entrepreneur, Subject-Matter Expert, Homemaker, Other]
4. What is your age?
5. What is your gender? [Male, Female, Prefer Not To Say, Other]
6. What is your educational background?
7. What is your professional experience in the field of cyber?
8. What company, business, organisation or university are you affiliated with?
Questions & Personal Views
1. How would you define cyber maturity at the national level? *

2. In your opinion, what are the key factors that contribute to a nation's cyber maturity? 3. From your perspective, what are the major challenges or barriers that hinder the achievement of cyber maturity at the institutional level? 4. What are the potential risks or limitations associated with implementing a renewed global cyber architecture model? 5. How can governments, organisations, and individuals contribute to the development and implementation of a renewed global cyber architecture model? *
National Cyber Maturity
Please rate the cyber maturity and practices in your country based on the questions below. Scale: 1 = Poor, 5 = Excellent 1. How would you rate your country's level of cyber maturity? 2. How would you assess your country's cybersecurity policies and regulations? 3. How effective do you perceive your country's cybersecurity infrastructure to be? 4. How likely do you think it is for a renewed global cyber architecture model to be successfully implemented and adopted?
Institutional Cyber Maturity
Please rate the cyber maturity and practices in your business or company based on the questions below. Scale: 1 = Poor, 5 = Excellent 1. How would you rate your organisation's level of cyber maturity? 2. How well does your organisation implement cybersecurity best practices? 3. To what extent does your organisation prioritise cybersecurity in its overall strategy and decision-making processes?
Other Notes:

Table 3.3.1.: Interview Questionnaire

The open questionnaires allowed participants to freely share opinions, experiences and perspectives on cyber. Basic demographics were gathered but identities were kept anonymous. This qualitative data was triangulated with expert interviews and secondary literature.

3.4. Data Analysis Methods

Qualitative data analysis involves interpreting complex and nuanced information from sources like interviews and open-ended surveys. It relies heavily on making sense of unstructured human communications and subjective responses. This makes the process inherently intricate.

The operational research activities in this study predominantly focus on the viewpoints and feedback of various stakeholders concerning cyber and cyberspace realities. These stakeholders include government officials, subject matter experts, private sector vendors, academic researchers, professional practitioners, and ordinary citizens or the persona of an ordinary citizen while speaking with experts.

As a supplement to initial samples or contacts for discussions, we also used a combination of snowball sampling to identify additional participants through referrals from initial participants and convenience sampling to select participants based on their availability and willingness to participate. The author was able to engage with these actors within the limitations of the available budget and time resources. The initial plan was not always applicable without changes and adaptation.

Qualitative analysis is also iterative, requiring repeated cycles of reviewing notes, transcribing responses, identifying codes, categorising themes, reorganising material chronologically, and recoding concepts (Creswell, 2009). The data must be continually classified and re-examined as new insights emerge through ongoing immersion.

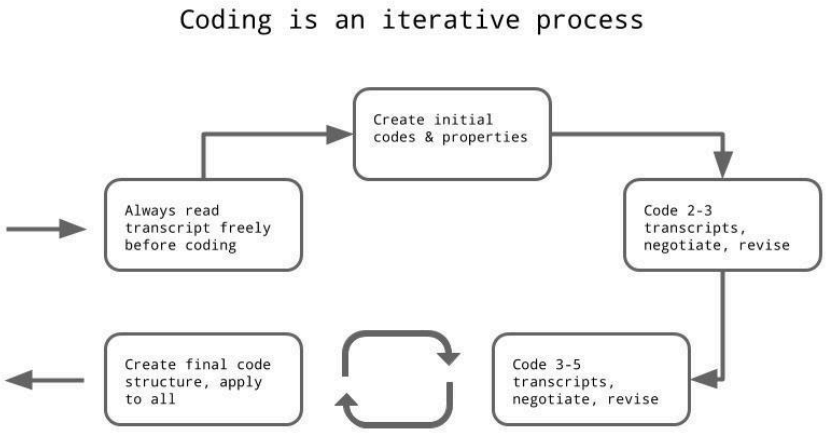


Figure 3.4.1.: Coding Is An Iterative Process (Mason 2002)

Qualitative data analysis involves categorising and characterising people, events, and other elements to uncover meaning. Coding, defined as segmenting textual data into chunks to identify common themes, is done iteratively throughout the analytical process (Creswell, 2009). Organising, coding, and classifying occur in a nonlinear, repetitive manner during qualitative research (Blumberg et al., 2014; Bell et al., 2022). The textual data is broken into portions with related meanings. These codes are consolidated into broader concepts, then re-examined and refined as analysis deepens.

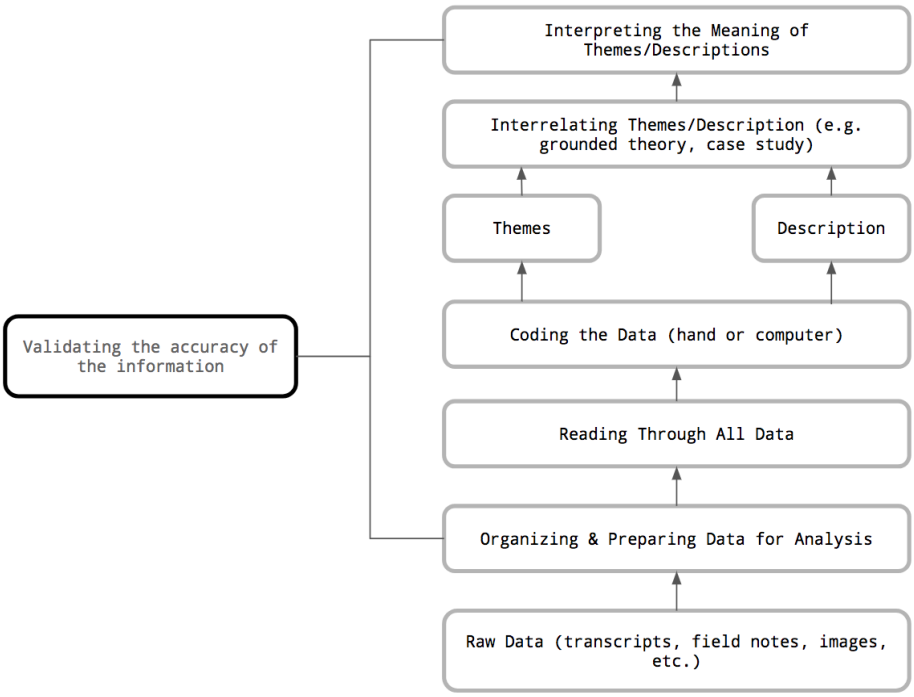


Figure 3.4.2.: Data Analysis In Qualitative Research (Creswell, 2009)

3.5. Ethical Considerations

The research adhered to key ethical principles including voluntary participation, informed consent, anonymity and confidentiality. All questionnaires and interviews explicitly emphasise these standards.

The participants were clearly informed about the study purposes and procedures and they can freely decline to participate or withdraw at any time without repercussion. All

participant identities and responses are also kept anonymous. No identifiable data will be published.

Furthermore, the United Kingdom regulations and guidelines on privacy, data management, and subject protections were followed diligently. Participants can choose to not disclose any business information, sensitive data or government details they prefer to keep confidential. No pressure will be applied regarding disclosure.

4. Findings And Analysis

4.1. Conceptual Framework

This research employed a multi-perspective theoretical framework, synthesising insights from several fields including political science, international relations, organisational design and management, information systems theory, enterprise architecture, and technology governance (Colomb, 2005; Kottemann & Konsynski, 1984). As the subject of cyber maturity is an intricate interplay of social and technical factors, an integrative approach was needed (Gregor, 2006; Jabbour & Devendorf, 2017; Kottemann & Konsysnski, 1984; Matlin & Land O'Lakes, 1979; McMullen & Schneider, 1972).

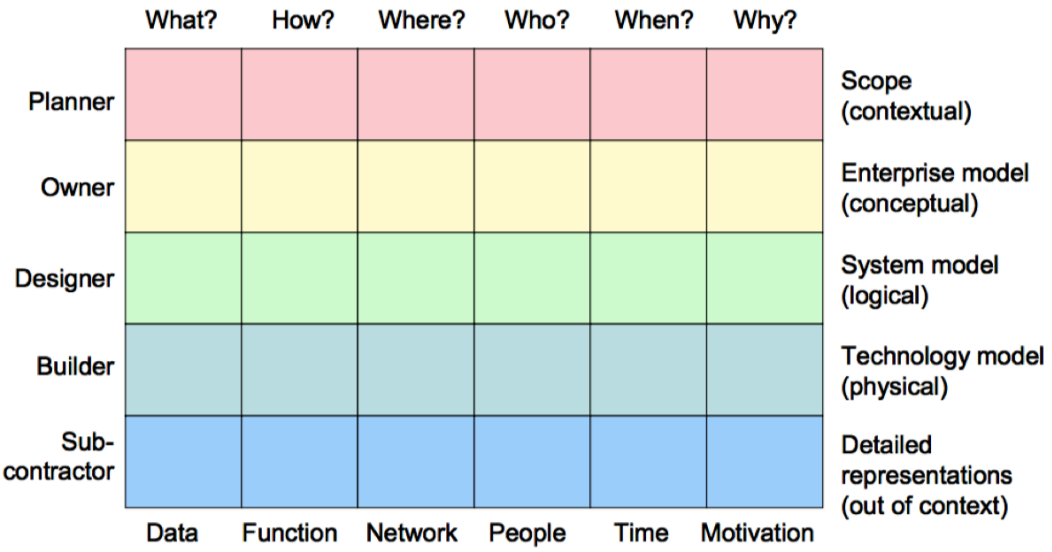


Figure 4.1.1.: The Zachman Framework (Lankhorst et al., 2009; Zachman, 1987)

In the analysis of national cyber strategies, this study leveraged political science and international relations theories that addressed power dynamics, national interests, and competition and cooperation among states (Keohane & Nye, 2011). Rather than adhering strictly to traditional theories such as realism and liberalism (Mearsheimer, 1994), the research

expanded upon these by incorporating constructive and critical perspectives that considered the roles of norms, identity, and discourse in global policy-making (Barnett & Duvall, 2005).

In examining organisations, the study was informed by institutionalism, which provided a framework for understanding governance, culture, capabilities, and strategic orientations within institutions (North, 1991; Peters, 2012). However, this was further enriched by multilevel and social institutionalism (Colomb, 2005; Powell & DiMaggio, 1991) and complemented by theories from organisational psychology and behaviour that explore cognitive processes, motivations, and group dynamics (Peters, 2012).

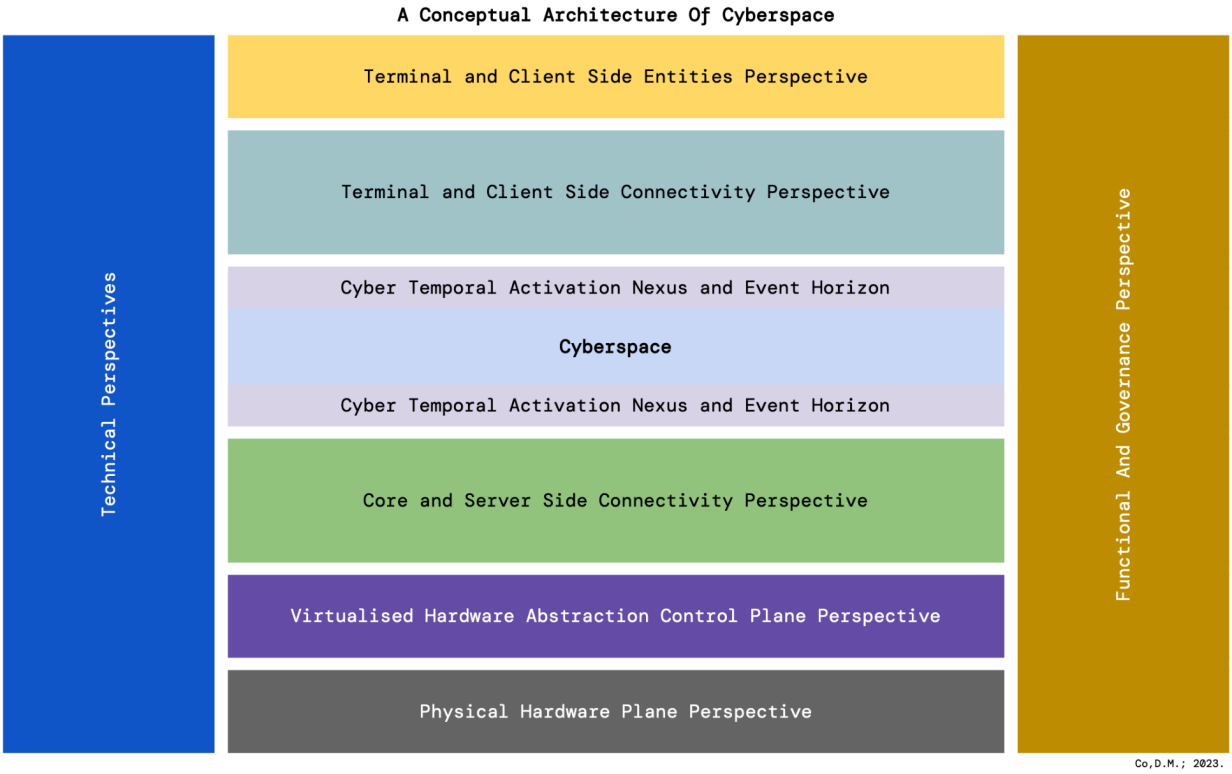


Figure 4.1.2.: A Conceptual Architecture Of Cyberspace

For the consideration of cyber architecture and governance, this study integrated technical perspectives on information sciences, management information systems theories, system complexity, socio-technical interactions, resilience, and standardisation (Chang & Grabosky, 2017; Matlin & Land O'Lakes, 1979; McMullen & Schneider, 1972; Trist, 1981).

These technical viewpoints are balanced by insights from science, technology, and society or STS studies (Jasanoff, 2012), which emphasise the social embeddedness of technological systems and stress the importance of ethical considerations and pluralistic approaches (McMullen & Schneider, 1972; Orlikowski & Robey, 1991).

Before field work commenced, a foundational framework (see Figure 4.1.2) for data was established based on the conceptual framework and taxonomy. This was informed by insights from an in-depth literature review and was iteratively shaped by the initial knowledge amassed during the research inception. With careful mindfulness of excessive confirmation bias, the experience of the author in the technology sector further refined this broad taxonomy scaffold. Given the active participation of the researcher in varied communities, from tech-focused groups to general community circles, a spectrum of different covert and overt observations and perspectives were also utilised for additional grounding and contextualisation. These diverse engagements encouraged a canvas for a richer picture of insights from leaders, managers, and subject matter or domain experts regarding cyber, related organisational initiatives, and their implications. This is reflected in the figure or graphic that represents the broad concerns or anchor perspectives that were used as scaffolding for codes, concepts, and constructs modelled and represented in the interviews and analyses.

4.2. Selection Of Specific Case And Context

This research employed a qualitative approach grounded in an interpretivist paradigm to investigate diverse perceptions of cyber maturity. By utilising semi-structured interviews and surveys, this study sought to gather insights from a broad spectrum of participants, including technology professionals, public administrators, industry leaders, civil society groups, and citizens. This inductive approach enables theories and insights on cyber maturity to emerge naturally from the data, rather than imposing existing hypotheses (Creswell, 2009).

Our exploratory and investigative trajectory sought insights from four broad categories of stakeholders:

(a) Leaders or Managers in public sector entities,

(b) Professionals or Subject Matter Experts in public sector entities,

(c) Leaders or Managers in private enterprises, and

(d) Professionals or Subject Matter Experts in private enterprises,

Their feedback and perceptions were critically analysed against:

(a) The broader cyber landscape,

(b) Cyber architecture or domain paradigms,

(c) Dynamics of cross-sector interactions, and

(d) Other prevalent sentiments and informed perspectives.

Furthermore, open-ended enquiries shed light on possible trajectories for cyber architecture and its potential role in shaping future strategies.

An initial roster of 100 potential interviewees, spanning government and corporate sectors within the cyber, digital, technology, and public governance areas, were identified. Of these, 23 intensive dialogues took place over a span of two months through both face-to-face and digital channels. Some pivotal interactions with key industry figures are still pending but will no longer be included or scoped upon completion of this dissertation.

Consent, anonymity and confidentiality were paramount throughout data collection. No personal data was gathered without express permission and participation was entirely voluntary.

4.3. Presentation Of Findings

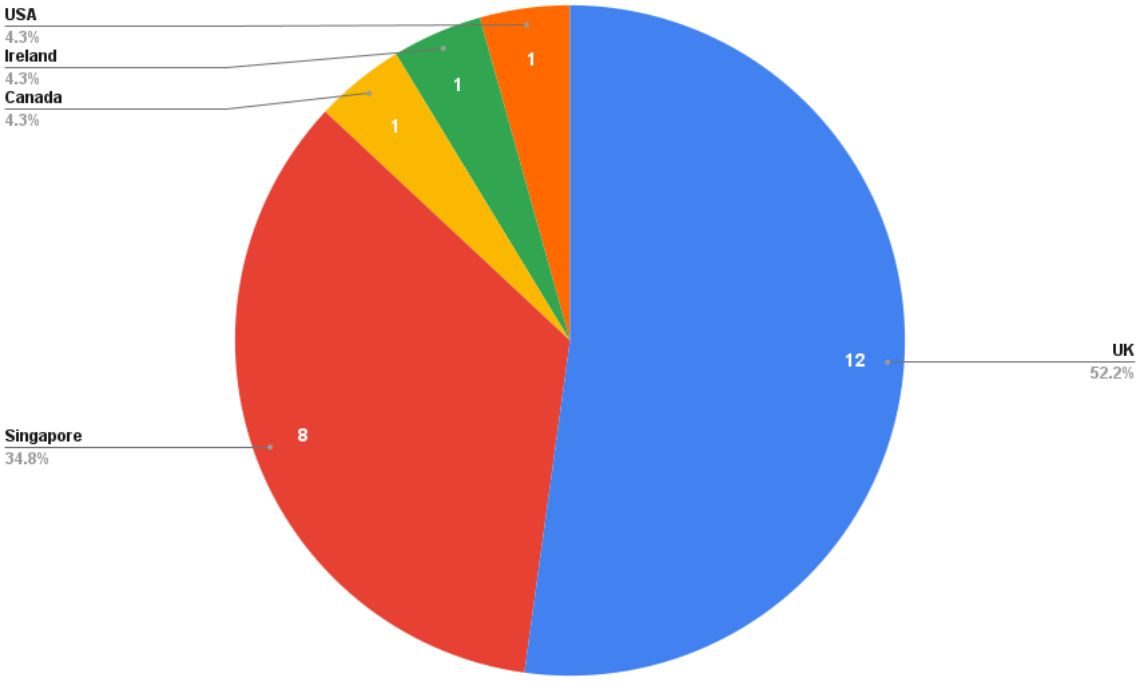


Figure 4.3.1: Location Of Respondents

The research approach, predominantly qualitative in nature, found its grounding in the empirical data derived from extensive expert interactions. Lexical statistics from these dialogues informed and influenced subsequent expert interactions, offering a dynamic and responsive feedback loop.

Logistical assumptions, concerning research location and scheduling, were largely corroborated. Unexpected yet fruitful interactions occasionally emerged during expert liaison, enriching the dataset and broadening the research's purview.

While the author and the process were primarily based in the United Kingdom, the research process transcended and remained liberal with geographical confines. It engaged in

dialogues and gathered data from a wide range of professionals: ranging from leaders and subject matter experts to domain specialists, in both the public and private sectors.

It is noteworthy to highlight the geographical spread of respondents to provide context for the global relevance of our research findings. The highest volume of responses was registered from the following locations, thereby elucidating the primary regions contributing to this dataset:

- United Kingdom: 52.2%
- Singapore: 34.8%
- Canada: 4.3%
- Ireland: 4.3%
- United States of America: 4.3%

This geographical dispersion not only enhances the richness of our dataset but also offers a multifaceted perspective that accounts for regional variability in practices, policies, and perceptions.

While the numbers seem skewed to certain locations that may reduce the validity and reliability even further from a qualitative point of view, the contextual and commercial underpinnings of location sensitive categorisation is often missed. For example, the UK and Singapore are in fact representative of regional and global organisations or ecosystems. This was explicitly mentioned in discussions the research engaged with. The minimal representation of Canada, Ireland, and the United States of America, is partly an administrative limitation as well as a logistics constraint with regards to practical scheduling and coordination.

Part of the aims of the research process was to engage in discourse with leaders of organisations, both from the perspective of domain expertise as well as from managing the organisation itself. These were one of the contrasts and tensions that was being explored to investigate any dissonance or disconnect within organisations or clusters of interrelated organisations within a field or sector. From an information systems perspective as well as an enterprise architecture perspective, the technical aspects of the system of humans or

organisations are rarely the singular driving force in discovery, analysis, prediction, operations, and evolution (Colomb, 2005; Gregor, 2006).

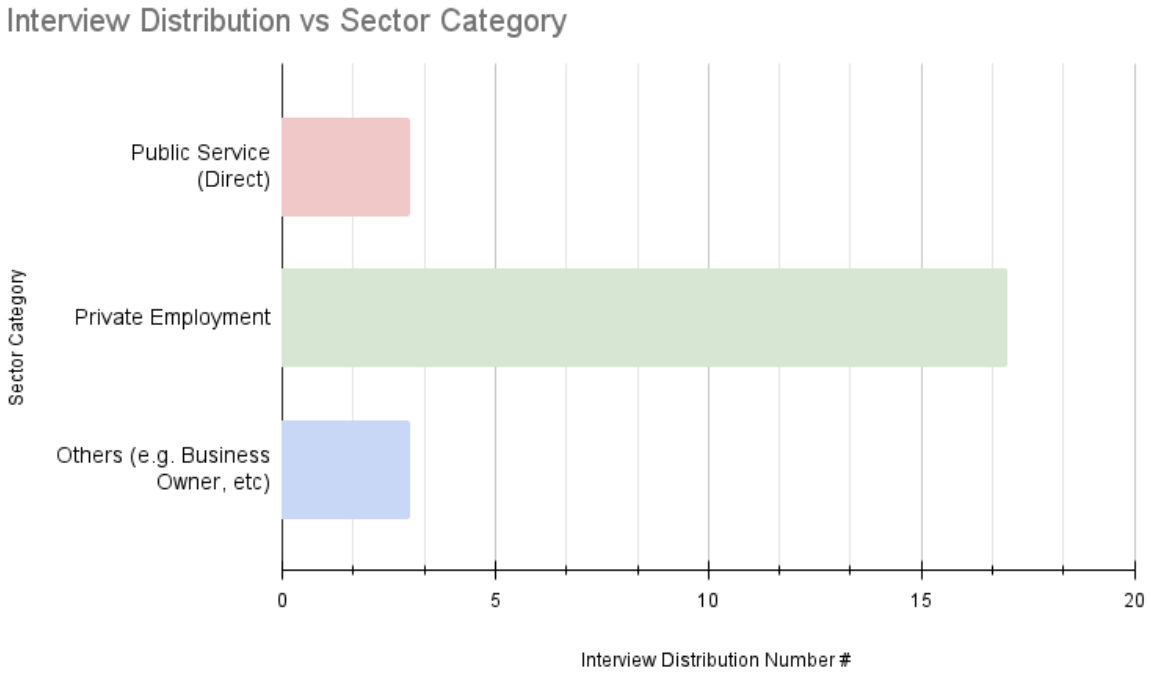


Figure 4.3.2.: Interview Distribution vs Sector Category

The preceding figure represents the distribution of interviews that were actually engaged in. The initial sample segment and targets were distributed equally, but the actual interviews were subject to availability, convenience, and logistical constraints. The raw data points to a predominantly private sector employment of interviews at seventeen (17) people, three (3) people directly employed or contracted with public organisations, and three (3) who were business owners and other categories like NGOs, military, et al.

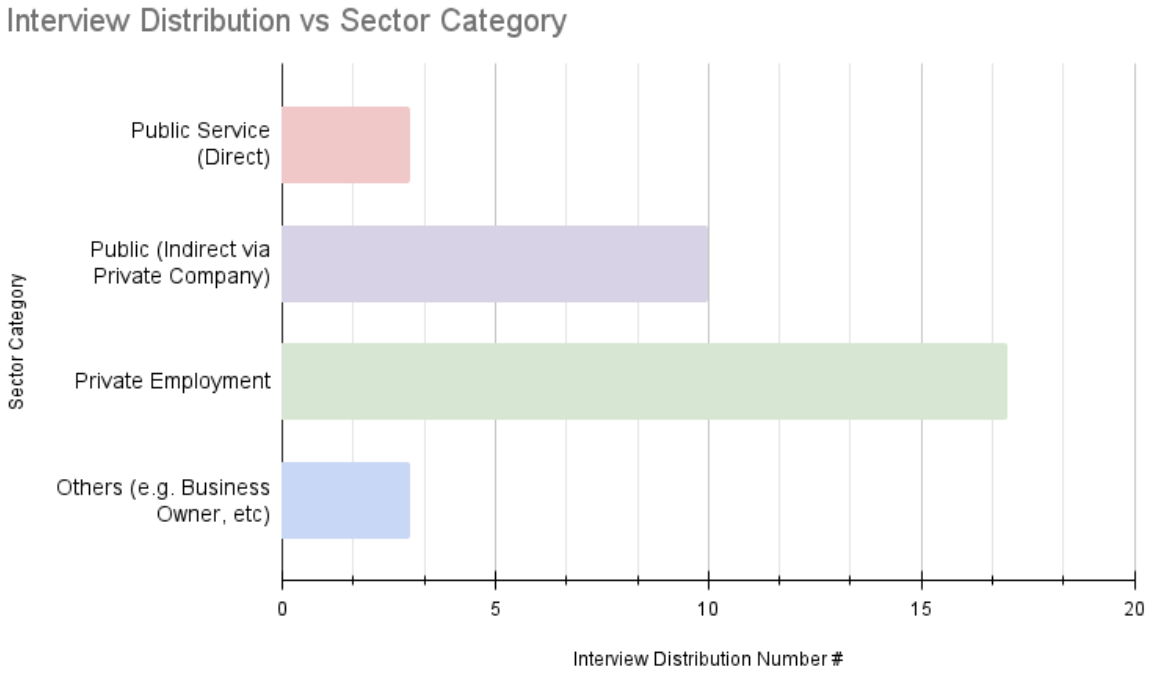


Figure 4.3.3.: Interview Distribution vs Sector Category - Detailed

Upon deeper discussions during interviews and review of the notes, it may be found useful to realise that the representation of relevant public sector domain knowledge and insight is more than initially charted from the raw data. Out of the seventeen (17) privately employed interviewees, ten (10) were directly and exclusively assigned to public organisations, institutions, and bureaucracies; under which they were subject to the same or stricter regime of security clearances and access to and responsibility for relevant information and decisions that is the topic of this research. The differences, as advised by the interviewees, were mainly administrative in nature, plus additional differences in pension management and job security. While seemingly irrelevant, these data points regarding the model of employment represent a source of contention in the incentives and deterrence for certain thinking and activities within key roles and responsibilities (Creswell, 2009).

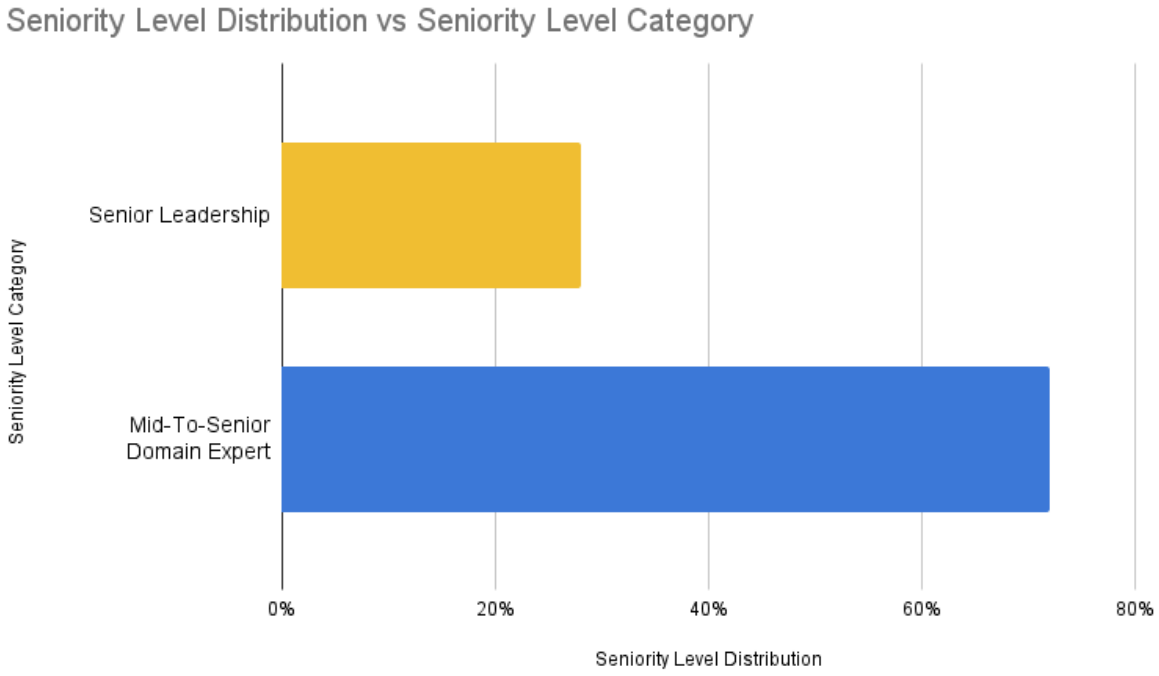


Figure 4.3.4.: Seniority Level Distribution vs Seniority Level Category

As a final highlight among several key attributes that were used to contextualise the research process, segmenting and analysing the viewpoints of different levels within an organisation was tracked. The key difference is that several of senior leadership roles are purely administrative and relatively detached from the nature and purview of the purpose and sector of the organisation. While this is generally considered normal and does not in any way assume incompetence, it always helps to have leaders, managers, governors, and supervisors to have practised or have at least been involved in the sector or the activities of the roles, even indirectly. The research results led to 28% interviewees with senior leadership or management roles while 72% were individual contributors, subject matter experts, or domain experts.

Most Common Relevant Work Tokens And Concepts			
Word	Frequency	Word	Frequency
cyber	57	infrastructure	12
not	32	train	12
cybersecurity	30	good	11
policy	23	model	11

government	22	national	11
nation	21	share	11
IT	20	budget	10
risk	20	business	10
technology	20	digital	10
cooperation	18	international	10
law	18	investment	10
maturity	18	plan	10
people	18	progress	10
think	18	term	10
global	17	capability	9
security	16	citizen	9
standard	16	country	9
system	16	datum	9
technical	16	institution	9
time	16	norm	9
challenge	15	partnership	9
threat	15	robust	9
work	15	collaboration	8
architecture	14	collective	8
practice	14	information	8
skill	14	interest	8
strategy	14	issue	8
lack	13	align	7
regulation	13	aspect	7
change	12	awareness	7

Table 4.3.1.: Most Common Relevant Work Tokens And Concepts

From the raw data, we distilled pivotal terms and statistical nuances to enable detailed analysis. Intriguing patterns and relationships were further reinforced using secondary data sources.

In an endeavour to crystallise the semantic core of our dataset, an exhaustive lexical analysis was undertaken. The purpose of this exercise was not merely to isolate frequently occurring tokens but to delineate the conceptual framework that underpins the discourse in the field. The tabulated representation above enumerates the most prevalent tokens and

associated concepts that surfaced during this analysis. The frequency of each token is also quantified to indicate its prevalence within the dataset.

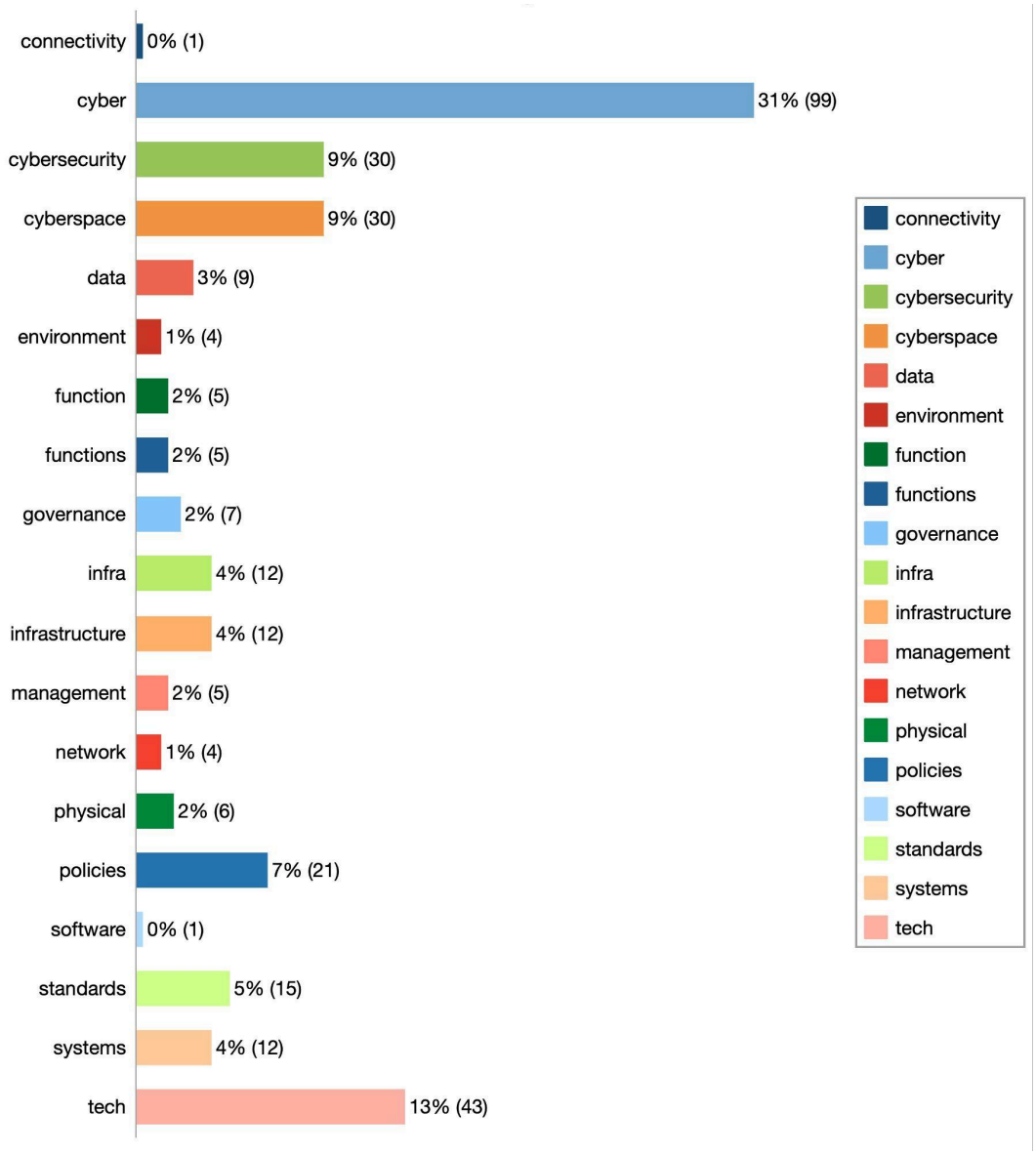


Figure 4.3.5: Lexical Analysis Supporting Code System

The tokens are invaluable pointers towards the prevalent themes, topics, and concerns in the field. For instance, the term 'cyber' and its close derivative 'cybersecurity' together amass a significant portion of the occurrences, indicating the overarching emphasis on these

areas. Similarly, other terms such as 'policy,' 'government,' and 'risk' reflect the multifaceted nature of the topics under discussion.

Although apparent in a straight forward analysis, further contextualisation is required that can only be gleaned with diligence and sense making. For example, in the chart representing percentages of word frequencies, reading it without context may miss a crucial insight, namely that the subject matter experts, domain experts, and the management staff were all clubbing together concepts into representative work tokens as a professional shortcut. As an analogy, if you speak with a civil engineer about infrastructure, the conversations implicitly and semantically mean roads, bridges, buildings, and the necessary components and engineering that it entails. In other words, they do not itemise all the related concepts in every discussion, but simply call them projects or infrastructure builds. Similarly, within the practice of information technology, telecommunications, cyber, and digital, infrastructure is a catch-all term that can be skewed to mean specific products, platforms, and services the sub-sector or the enterprise offers to the market. For example, discussions and topics relating to data centre or hyperscaler cloud facilities that uses the word infrastructure would generally mean the hardware server, the virtualised server hosting capabilities and systems, and the scope and scale of global connectivity within these critical nodes of computing capabilities provided by multinationals (AWS, 2023; Google Cloud, 2023; Mell & Grance, 2011; Microsoft Azure, 2023). In another context, when dealing with major telecommunications providers, whether these are for terrestrial wired networks, cellular-based mobile service networks, and other backbone networks that provide aggregate bandwidth for national and international scale data flow, infrastructure is the coupling of physical network equipments as well as the operating service standards they have to adhere to. As was explained by one of the interviewees, infrastructure is not a generic term for their industry but is a segmented categorisation of capabilities and standards each installation and operated sub-network falls under, e.g. multiple types of land-based broadband network, numerous types of fibre optic based direct connectivity into terminal points like home or business facilities, and the various inter-operable but distinct mobile networks operating within different spectrums like 3G, 4G, 5G, and others.

The gamut of discussions forms a comprehensive perspective on critical research objectives: the shaping and governance of cyber strategies, the integral role -- or lack thereof -- of cyber architecture in strategic planning, the commercial dynamics within this realm, and importantly, the broader public's experience and perspective. Through this lens, we aim to demystify both the tangible impacts of cyber initiatives and the evolving aspirations of those immersed in this digital age.



Figure 4.3.6: Interview Responses Word Cloud

To further elucidate the thematic concentrations present in the qualitative data, a word cloud was generated. The word cloud presented below provides a compelling, data-driven overview of the salient points gleaned from the qualitative material. Utilising specialised data visualisation software, the word cloud was crafted from a corpus of 35414 participant response tokens, filtered to include only nouns and adjectives. In the generated word cloud, the size of each term is directly proportional to its frequency in the dataset, offering a quick yet impactful snapshot of the primary focal points emerging from the qualitative data. The visual representation offered by the word cloud serves to spotlight the recurrence of key terms, thereby signalling predominant themes that warrant further investigation.

Employing foundational elements of lexical studies and an entry-level exploration into the complex field of Natural Language Processing (NLP), the research deployed initial measures such as tokenisation, categorisation, lemmatisation, stemming, syntactic tree construction, and rudimentary semantic scrutiny. These foundational steps are standard entry points and serve as the basis for generating elementary frames of semantics, entity identifications, and modelling of network interactions. This framework subsequently facilitated a more sophisticated second-order semantic interpretation. Ultimately, these techniques helped confirm, extend, and modify the initial scaffolding and anchor concepts at the beginning of the research process, thereby establishing an initial set of codes and perspectives to categorise and understand sub-codes or themes in the interviews and analysis.

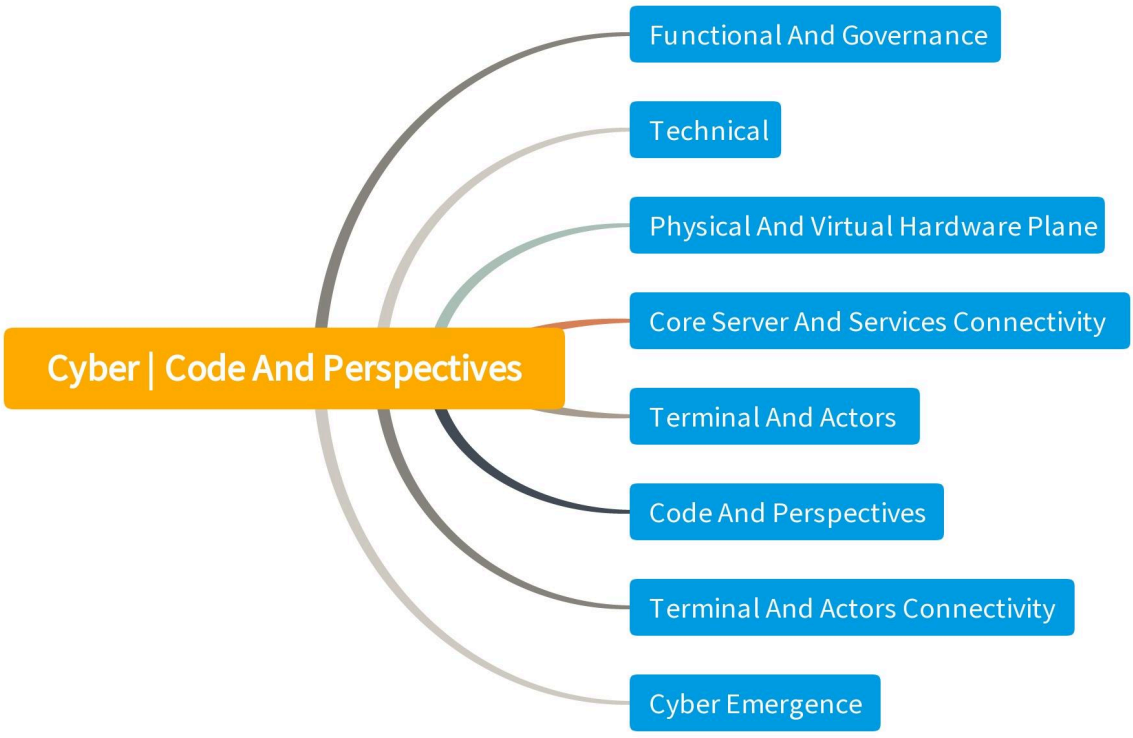


Figure 4.3.7.: Code and Perspectives

Code and Perspectives:

Functional And Governance

Key Themes:

Strategy. Standards. Enterprise. Community. Society. Policies. Processes. Practices. Functions. Geography. Governance. Compliance. Assurance. Certification. Regulations. Value Chain. Logistics. Operations. Intelligence. Security. Education. Qualification. Guilds. Events. Expo.

Relevant Sample Statements:

“A cyber mature nation has developed robust strategies, policies, laws, and governance structures to secure critical infrastructure, businesses, and citizens in the digital domain.”

“Having effective laws, policies, governance and standards to securely manage digital risks and opportunities.”

“We extensively work with other agencies and ministries to aggregate information and transform them into a coherent structure usable in our modeling and forecasting functions.”

“It is about asset management, lifecycle planning, about threat and opportunities analysis, about budgets, about offence and defence, and while military domains and leadership is key, this should be approached as a society.”

“Inability of management to move on and transform due to structural, corporate, and political constraints.”

“Legacy systems and teams that do not collaborate for the goals of the organisation. Difficulty agreeing standardised global policies.”

Code and Perspectives:

Technical

Key Themes:

Hardware. Software. Operating Systems. Runtime Environments. Components. Interface Services. Systems. Utilities. Applications. Data. Schema. Formats. Transit State. Protocols.

Relevant Sample Statements:

“We can think of it in traditional terms like enterprise architecture which is a catch all for all information

systems concerns especially n the aspect business strategy, data strategy, technical strategy, software strategy, security strategy, and governance strategy."

"Technical debt from legacy IT systems poses obstacles for modernization."

"Big tech or governments mishandling data."

"The Internet for example is a force for good but can hurt people when personal data is compromised."

"Old, legacy IT systems are very hard to upgrade, teams not sharing info, and resisting change, lack of skilled people."

"From experience, I can say there are skill gaps in the workforce, legacy systems that impede modernization, poor practices and low threat awareness due to insufficient policies and training, complex regulations. Lack of cooperation due to competing interests, and difficulty standardizing global policies."

Code and Perspectives:

Physical And Virtual Hardware Plane

Key Themes:

Infrastructure. Systems. Compute. Storage. Internal Networks. Services.

Relevant Sample Statements:

"Unlike computer code, you need to get physical infrastructure correct, be it civil works or physical technical works like networks, cabling, signaling systems, centralised operations command, enterprise computer systems, inter-agency data transfers, and all these functions that depend on real physical environments to enable digital work."

"Public and private investment in cybersecurity infrastructure, technology, and training helps strengthen defenses and resiliency."

"Much like how we do it in real civil infrastructure, a good dose of smart planning and thoughtful diligence is needed."

Code and Perspectives:

Core Server And Services Connectivity

Key Themes:

Analog. Digital. Wired. Electromagnetic. Machine Relay. Biological Relay. Internet. Intranets. Operational Networks. Ad Hoc Networks. Personal Networks. Standards. Protocols. Functions. Formats. Lifecycle.

Relevant Sample Statements:

“Legacy IT systems that are difficult to update pose a technical challenge, requiring significant time and investment to modernize.”

“The immense scale of operations requires smart infrastructure for core functions and shared support functions.”

“For example, instead of focusing too much on network coverage, we use measurements critical to network operations and customer satisfaction, the outcomes; e.g. percentage of promised throughput to actual throughput, uptime guarantees, network outage or incident response times, etc.”

Code and Perspectives:

Terminal And Actors

Key Themes:

Entities. Environment. Humans. Other Biological Lifeforms. Things. Software. Actors. Agents. Proxies. Events. Triggers.

Relevant Sample Statements:

“Individuals as citizens can elect policymakers committed to cybersecurity progress and as cyber professionals can contribute technical skills.”

“Resistance to change and people who don't understand the requirements or technology.”

“We have a Smart Nation initiative that now focuses on using ICT for expanding and extending all functions of government.”

Code and Perspectives:

Terminal And Actors Connectivity

Key Themes:

Analog. Digital. Wired. Electromagnetic. Machine Relay. Biological Relay. Internet. Intranets. Operational Networks. Ad Hoc Networks. Personal Networks. Standards. Protocols. Functions. Formats. Lifecycle.

Relevant Sample Statements:

"For example, instead of focusing too much on network coverage, we use measurements critical to network operations and customer satisfaction, the outcomes; e.g. percentage of promised throughput to actual throughput, uptime guarantees, network outage or incident response times, etc."

"The immense scale of operations requires smart infrastructure for core functions and shared support functions."

"From experience, I can say there are skill gaps in the workforce, legacy systems that impede modernization, poor practices and low threat awareness due to insufficient policies and training, complex regulations. Lack of cooperation due to competing interests, difficulty standardizing global policies."

Code and Perspectives:

Cyber Emergence

Key Themes:

Domain. Commons. Notional. Kinetic. Temporal Activation Nexus. Event Horizon. Stimulus. Emergence. Social. Digital Twins. Cyber Physical Systems. Enablement.

Relevant Sample Statements:

"I agree with you that cybersecurity is not the important aspect of cyber."

"Governments can foster international dialogue and negotiate agreements that outline collective norms, principles, and technical standards to form the backbone of a new cyber architecture."

"Additionally, arriving at standardized global technical standards and policies will be challenging with divergent perspectives."

"Fundamentally, cyber maturity requires the government to make resilience a strategic priority integral to our national security, economic prosperity and technological development."

"It means digital practices at the national level is governed well and just happen to make use of transformational technologies we have nowadays."

“Governments must act quick enough to keep pace with technology.”

“Resistance to new technologies and processes hinders agility.”

“Maturity is having the wisdom and ability to have gone through or leap frog through various stages of developing capabilities, capacity, and consistency in supporting legacy, current, and future needs of the digital and cyber platforms and infrastructure of a nation.”

“Cyber maturity refers to a nation's preparedness and capabilities in managing risks and leveraging opportunities within cyberspace.”

Further to these qualitatively analysed statements, a set of subjective rating questions gathered from participants (Figure 4.3.8., Figure 4.3.9., and Figure 4.3.10.) portrayed the impression and message that while key areas of cybersecurity policies seems to already receive ample attentions and resources for the implementation and enforcement of good policies and practices, there is marked shift towards lack of investments in other underlying aspects of the overall enterprise or overall system of governing certain scopes or units of society, be it in small communities, private companies, or larger public institutions and bodies of governments. This leads to an overall impression and historical legacy of carrying too much technical debts or mistakes from the past that simply had to be endured towards the future. As a consequence of (a) consistent overinvestments in ‘cherry-picked low hanging fruits’ a phrase several of the respondents seem to use a lot; (b) constant oversimplification in communications of weight and consequence to convince leadership and management; (c) declining effective state of underinvested areas of cyber and cyberspace like core underlying infrastructure, interdisciplinary education, simple but consistent system upgrades, and global cooperation; (d) misconceptions and ambiguity of concepts leading to policy waste and overlapping bloated bureaucracy; and (e) lack of maturity, process for improving maturity, and a clear framework encompassing enough concerns in an evolving sea of considerations to ‘move the needle’, which was a phrase mentioned numerous times to represent the simple ability of organisations or programmes to enact useful change. While it is an idiom not unbeknownst to the researcher, it reflects the challenge at hand, that a small tick in the great measure of things is considered huge progress; and yet, there was a marked change of tone of optimism whenever change,

improvements, and maturity became the topic of conversation reflecting a sentiment of cynicism in the current state of affairs.



Figure 4.3.8.: Organisational Cybersecurity Practices

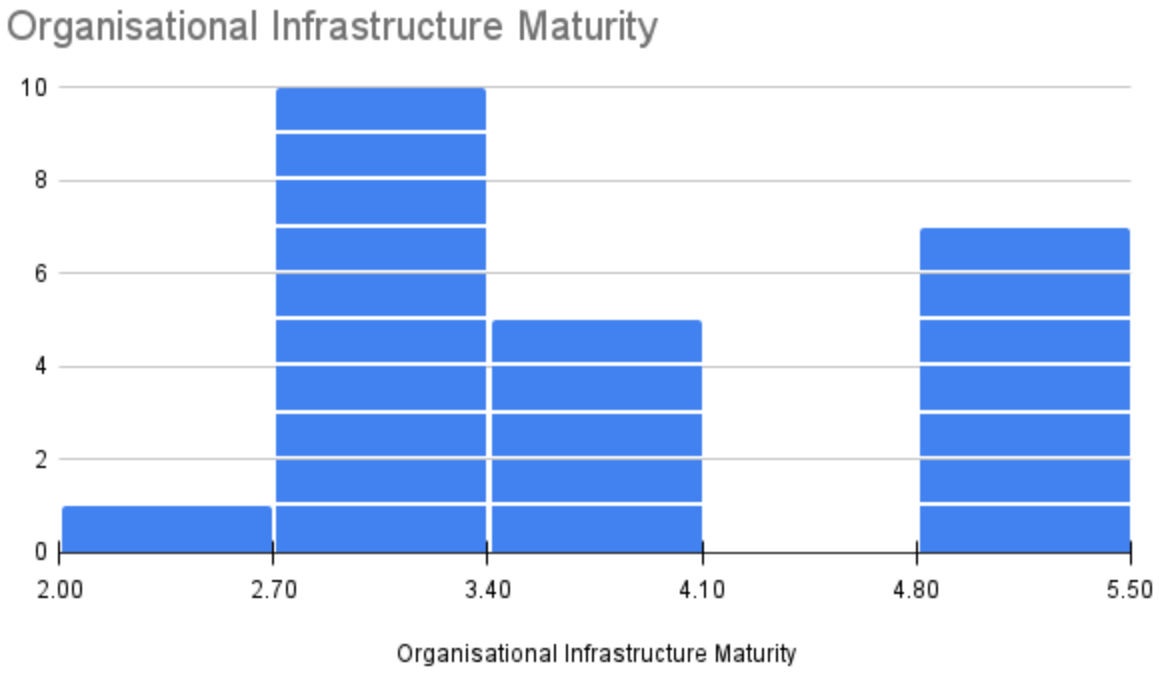


Figure 4.3.9.: Organisational Infrastructure Maturity

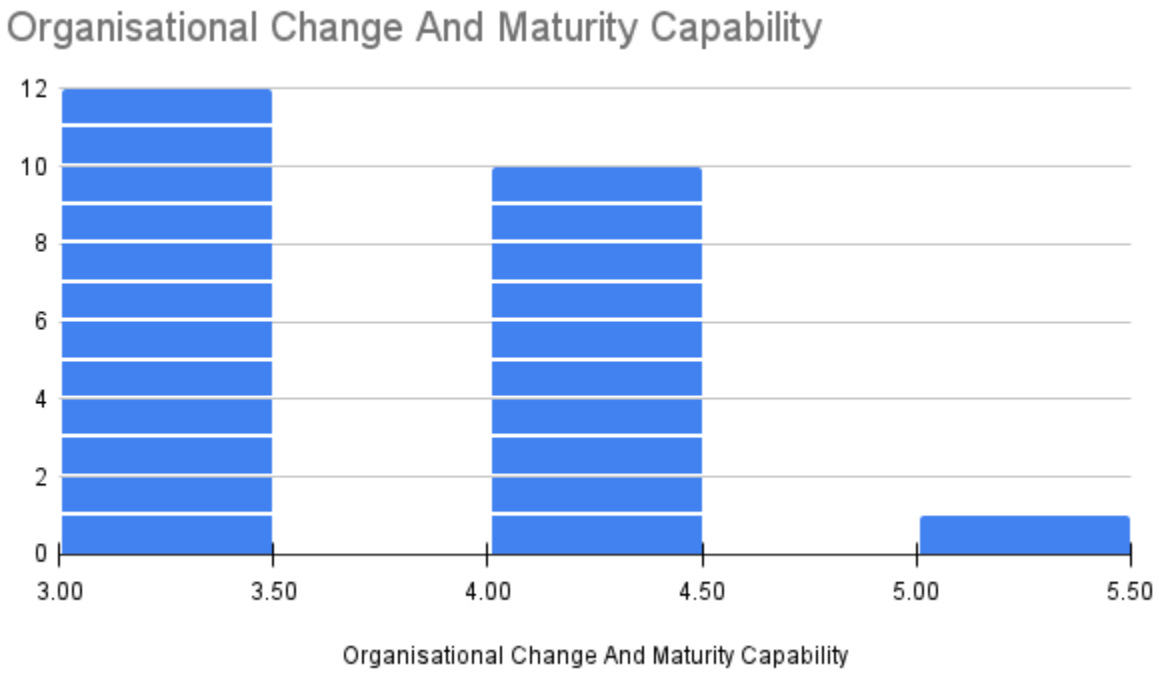


Figure 4.3.10.: Organisational Change And Maturity Capability

4.4. Summary Of Research Findings

It was a key pillar of the activity to take into account basic historical meaning drifts as the concept of cyber has been used and evolved in various contexts. The interviews, surveys, and analysis enacted worked toward a balanced population of subject matter experts, domain experts, organisational management, and other administrative leadership involved in the public and private sphere.

Cyber, a term often confined to specific domains, is more aptly understood as a ubiquitous field that seamlessly integrates with and enhances all human and machine-operated domains. In line with contemporary discourse and research (Choucri, 2015; Clarke, 2010; Wren, 2015), these definitions have incorporated operational considerations (Maurer & Morgus, 2014) reflective of the real-world industry, encompassing emerging communication protocols beyond Transmission Control Protocol over Internet Protocol (TCP/IP) such as (a) Supervisory Control And Data Acquisition or SCADA; (b) Cyber-Physical Systems or CPS, and Internet-of-Things or IoT (Ning et al., 2018). Additionally, it also includes hardware resilience mechanisms embedded within systems and software itself, the architecture of networks and subnetworks, access nodes, and the integral role of data (Greer, et al., 2019; Prince & Sullivan, 2019).

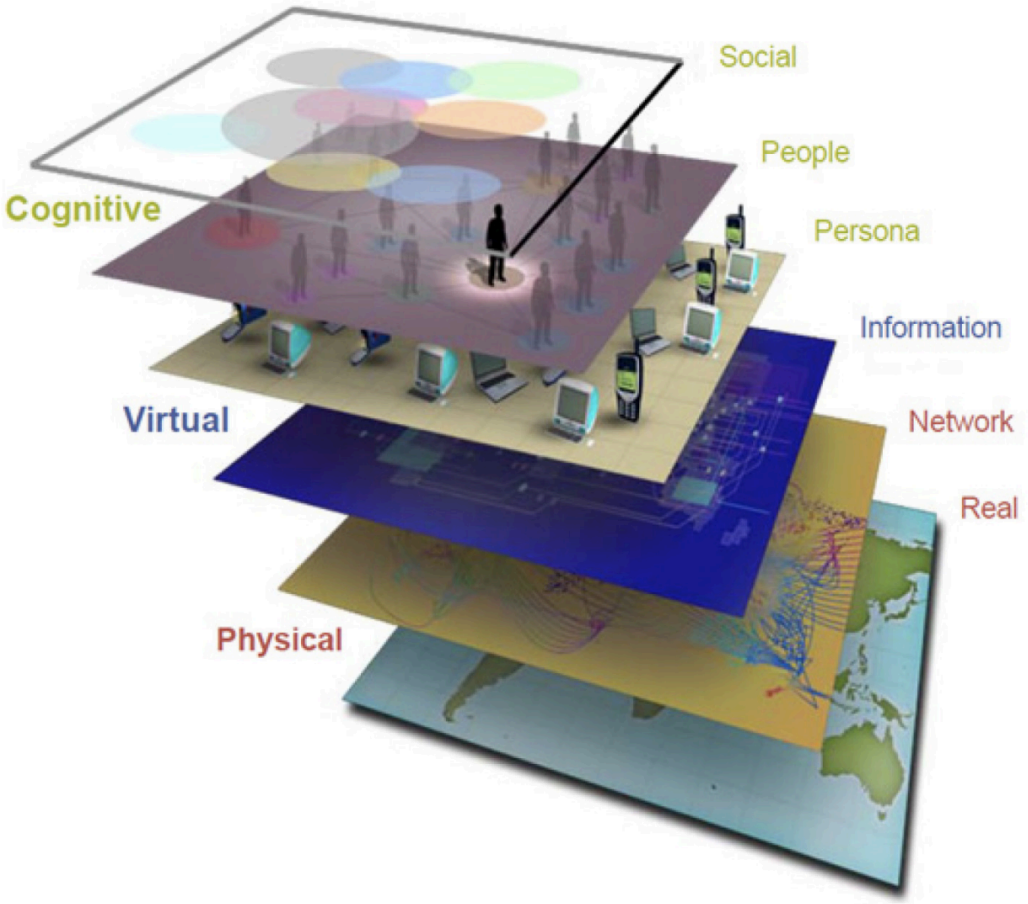


Figure 4.4.1.: Traditional Layered View Of Cyberspace (Parish & Madahar, 2016)

The discussions and analysis of feedback from experts, practitioners, and researchers almost unanimously agreed that traditional conceptual theories and taxonomy of concepts currently utilised create confusion and incorrect assumptions, in particular, towards political bureaucracy, strategic planning, financial engineering, investments, operations, and maintenance of key infrastructures, services, and human capital development. Additionally, typical presentation and conception of simple abstraction layers along one dimension or axis creates an oversimplified model for strategy, planning, operations, and evolution of complex functions that are cross-disciplinary in nature.

Consequently, these inconsistencies create a taxonomy and cross-section of concerns leading to fragile organisational purviews, ambiguous political jurisdictions, misappropriation of funding, and incorrect or imbalanced development of skills or competencies for short term operational effectiveness and long term strategic competitiveness.

5. Conclusion

5.1. Reflections On The Research Process

Outside role-specific sub-functions like cybersecurity, facilities security, or end-user equipment operations, interviewees agreed that the industry and institutions creating policies including major consultancies promote an oversimplification of terms, concepts, and frameworks in the interest of an ‘easy sell’ as one of the domain experts in the telecommunications industry mentioned or as a ‘layman’s version’ of crucial components of processes and procedures to ‘cut through the bureaucracies or to deal with overly incompetent management’ as mentioned by one of the department heads for a government agency in the UK. The research process avoided generalising from individual statements; but it must not discount sincerely provided and consistently competent insights provided by people with authority, subject matter expertise, and integrity, as far as the research can assume. This is echoed in the private sector and in investment circles, where certain sub-functions or ‘feature slices’ instead of complete products or value propositions are highlighted as simplicity even at the expense of coherence gains more attention in the capital markets. This is dangerous in general for society -- even if profitable for small portions of society who benefit despite incompetence, corruption, or parasitic opportunism -- for misappropriated resources is detrimental to the system as a whole.

5.2. Proposed Global Cyber Architecture Model



Figure 5.2.1.: A Conceptual Architecture Of Cyberspace

5.3. Description Of The Proposed Model

Central to the proposed architectural paradigm is an intricate, layered stack that progresses from the foundational core physical infrastructure upwards to a more evolved virtualised platform and, ultimately, to an intricate web of connectivity and networking essential for diverse computing requirements.

At the top are terminals and actors. They are representative of diverse interaction points, extending beyond the conventional human-machine interfaces to encapsulate entities such as environmental sensors and adaptive urban infrastructures. Despite their diversity, these nodes converge on a framework of connectivity, encompassing all communication protocols, from conventional ones like Wi-Fi and Bluetooth to niche mechanisms like legacy radio frequency or RF and Internet-of-Things or IoT based protocols.

A novel feature of this conceptualisation is the dynamic entity of 'Cyberspace'. Contrary to traditional definitions that envision cyberspace as a mere digital continuum or domain, our model posits it as a vibrant conduit of data interactions. Particularly, the introduction of the Cyber Temporal Activation Nexus and Event Horizon reiterates the importance of transitional state of data. The transformation from static 'data-at-rest' to kinetic 'data-in-transit' animates this conceptualisation of cyberspace. It draws parallels with biological circulatory systems in its significance and function. In other words, the key aspect of life or the complex emergence of life stems partly from energy in motion, not just ingredients of life in stasis. Similarly, cyberspace is not a space or a domain in a dimensional sense, but is the sum total reality of all data in motion. A gap in the literature, apart from the concept of cyber enabled physical systems, is the concept of the temporal activation nexus and event horizon. This is a crucial aspect of this conceptualisation.

Breaking this concept down, temporal activation nexus means a time-bound activation or presence of data flow within cyberspace; in addition, the event horizon is the moment latent or potentiality becomes kinetic within physical or virtualised infrastructures and networks. As a practical example, imagine a mobile device that is not linked to the internet by means and

standards available to it. In this state, at this abstraction, where all data resides locally, the mobile device is operational and still fulfils some of its features and functions as a computing device, albeit, in isolation. Upon establishment of connectivity, as soon as data flows from the device and initiates interaction with the various layers of the complex networks and infrastructure, it becomes part of cyberspace. Another similar example that perhaps vastly expands the reach of cyberspace is with interplanetary communications and beyond. In this context, if a satellite, even using legacy and obscure communications protocols, sends information back to earth, and this data flow has reached beyond the initial event horizon, whether through further human processing or machines relaying radio data across the internet, then the satellite becomes, in essence, part of cyber. This has operational and strategic implications in how cyber is viewed, not just a geographical domain sovereign states or merely sub-functions of cyber 'security'.

Flanking the central construct are two pivotal pillars, encapsulating the overarching considerations impinging on every stratum. To the left, the emphasis is on technical intricacies, seamlessly integrating facets of data logistics, system utilities, component interfacing, and the foundational bedrock of operating environments. This harmoniously transitions to the hardware-software nexus, elucidating the seamless interplay between tangible devices and intangible codes.

In juxtaposition, the right pillar illuminates the functional and governance viewpoints. Initiating with grassroots educational strategies and transitioning through intelligence frameworks and security protocols, this segment culminates in a broader governance perspective. Herein, compliance benchmarks, certification routes, and regulatory constructs are outlined, situating them within the broader trajectory of strategic planning and societal integration.

The hallmark of this framework is its holistic approach to understanding cyberspace. Eschewing the conventional layered view, it proposes an ecosystemic perspective, characterised by diverse entities, stochastic interactions, and the persistent influence of technical and socio-cultural determinants.

5.4. Justification And Rationale

This research culminated by proposing an integrative conceptual model to enhance global cyber maturity through coherent policymaking, cooperative implementation regulations, and socio-technical integration. The architecture synthesises empirical insights from comparative analysis of institutional cyber perspectives across public, private, and civil society sectors in both developed and emerging economies.

Findings revealed (a) ineffective bureaucracy, (b) incompetent management, (c) technical and process fragmentation, (d) capability asymmetries, and (e) lack of cooperation as key barriers to improving maturity (Brooks, 1995). While progress has occurred in silos, an interconnected global cyber ecosystem demands greater coherence across national boundaries and competing interests (Checkland, 1988; Choucri, 2012; IISS, 2021).

As such, the proposed multi-level and multi-perspective model provides a unifying taxonomy spanning core technical perspectives, functional perspectives, governance perspectives, physical and virtualised infrastructure perspective, terminal and client side perspective, education, professional or guild associations, and comprehensive definitions of partaking and belonging within the construct of cyber domain (Chang & Grabosky, 2017).

In transcending traditional and limited purview of a technical environment, a military domain, or cybersecurity function, this approach allows standardising foundational elements while retaining flexibility for contextualising based on local political, economic, cultural, and developmental priorities. The conceptual framework balances security, growth, rights, and capabilities as interdependent goals requiring holistic advancement and practical planning and roadmap phasing.

It must be disclaimed that it is not the goal to replace existing standards outright, to assume superiority over the same matter; but rather, the objective is to expand, to scale, and to be as inclusive as possible in terms of considerations and attributes along a path premised on

continuous collective progress. This is not naivete, it is simply revealing the inherent global nature of cyber, and as such must be regarded beyond the confines of national realist or economic enterprise thought processes.

5.5. Potential Implications And Benefits

Critical dimensions will emergently emphasise (a) public-private and multi-stakeholder partnerships as distinctions are unified; (b) transparency on threats and vulnerabilities as analysis and response are liberated from siloed priorities; (c) interoperability mechanisms are democratised and expanded as clearer abstraction layers and maturity aware strategies allow for continuous progress (Kottemann & Konsynski, 1984) than top-down large-scale alignment with technical and political hegemony monopolising acceptable progress; and (d) explicit sharing contemporary and emerging good practices that promotes the most good sustainably, rather than adherence to highly contextual best practices that may easily change at points in time. For instance, the model may encourage regional cooperation platforms for coordinating policy and combating cybercrime across borders as a supplement to global multilateralism. Global certification schemes would help improve baseline maturity of small and medium enterprises worldwide.

The conceptual architecture outlines potential initiatives to significantly improve access, education, technology justice in the digital divide, and youth engagement across the global south. Tools like specialised maturity assessments and incentives aim to motivate continuous improvement fitting localised needs. Tailored training programs and relevant structured policy exercises to aid capacity building in developing countries can be envisioned as sophistication and global standards achievement in cybersecurity or military capability is not the primary goal in and of itself but gradual and sustainable progress in cyber, digital, and literacy skills become more paramount.

By proposing an integrative policy and implementation architecture, this research contributes original recommendations and a roadmap tailored to incrementally cultivating cyber maturity from the organisational to the global level. The model synthesises empirical insights on

addressing systemic gaps hampering security, innovation, cooperation and digitally-inclusive sustainable development worldwide.

5.6. Limitations And Challenges

This study navigated through several inherent limitations. Predominantly anchored in the United Kingdom, international interactions were channelled exclusively via online platforms, which may have nuanced the diversity of global insights and limited deeper meaning that may be gleaned through more conversational methods. The 12-week time frame, though intense, curtailed the breadth of exploration possible. The constraints in both coverage and capacity meant that intricate cultural nuances, intricate political contexts tied to budgetary decisions, and extensive longitudinal evaluations were not as comprehensively addressed. Moreover, the detailed cross-disciplinary considerations of such vast domains may not have been fully captured due to the temporal constraints. Operating on a self-funded model also introduced certain resource-related challenges, potentially impacting the depth and expanse of the enquiries. These factors highlight the avenues ripe for deeper investigation in subsequent studies.

5.7. Policy Recommendations

The interplay between cities and cyberspace offers a compelling analogy, a conduit to elucidate the multilayered complexities of the evolving digital landscape and its impact on business, political economy, and society. A careful examination of this relationship reveals striking parallels in their physical, logical, virtual, and social structures, as well as the emergence of governance mechanisms and institutional hierarchies that guide their progression.

These commonalities serve as a valuable analytical lens to understand the far-reaching consequences of cyber activities. Companies must navigate the rapidly evolving digital landscape to remain agile and responsive to shifting market dynamics. Political actors must grapple with the socioeconomic repercussions of the digital revolution, including the

redistribution of wealth, income inequality, and social mobility. Policymakers, stakeholders, and civil society must forge a collective vision to address the challenges and harness the opportunities presented by the digital transformation.

The convergence of cities and cyberspace presents a multifaceted abstraction for understanding the ripple effects of cyber activities across various domains. The interdependencies and commonalities embedded in their evolution illuminate the intricate web of factors shaping the digital age's trajectory. Navigating this intricate landscape requires a holistic perspective that considers the interplay between the physical, virtual, and social realms. The lessons drawn from the analogue between cities and cyberspace can inform policies, strategies, and actions that foster a more inclusive, secure, and sustainable digital future.

It is essential to consider that the implementation of these strategies and policies is shaped by broader challenges such as bureaucracy, politics, corruption, budgetary constraints, social unrest, economic turmoil, and environmental degradation.

5.8. Academic Contributions

By reframing our understanding of cyber, several pivotal outcomes can be realised: (a) it can liberate unprecedented or stifled innovations and opportunities for differentiating strategies in creative value across numerous sectors and ventures; (b) it can reshape the discourse on the political economy of cyber, allowing us to move beyond traditional military domain delineation, limited cyber security purview, and commercial network of electronic exchange (Caton & Bartholomees, 2012); and (c) it can significantly broaden and variegate the horizon for policy planning, governance institutionalisation, protocol establishment, operational design management, product ideation and development, capability building, lifelong learning, multi-sector innovation, and venture capital investment.

5.9. Suggestions For Further Research

National cyber frameworks, spanning both public and private sectors, often escape systematic comparative scrutiny (Hathway, 2013; IISS, 2021). Notably, the UK National Cyber Strategy (HM Government, 2022a) underscores the urgency for integrated oversight across diverse realms. A comprehensive exploration of international variances in governance structures, legal landscapes, technological mechanisms, and security culture dynamics is paramount. Neglecting this comprehensive perspective risks fragmented strategies and misses the potential to learn vital lessons about resilience and partnership-building.

Existing scholarship frequently gravitates toward the mechanistic aspects of cyber maturity, sidelining the intricate web of geopolitical forces, economic ties, and strategic inclinations of state and non-state players (Carr, 2016; Savaş & Karataş, 2022). Broadening the analytical gaze to capture this multifaceted interplay could guide more cohesive, stable, and inclusive digital futures.

Prominent tech corporations and globally influential states wield significant power in shaping digital norms and infrastructure (KPMG, 2023). Yet, their overarching influence might overshadow the essential needs of the developing regions (Porter, 1980; Porter, 1990). Coupled with nationally siloed stances on technological governance, there emerges a pressing requirement for a harmonised approach to fortify cyber security, bolster network resilience, and counteract cyber espionage threats (Choucri, 2012; Choucri, 2015).

Beyond technical and geopolitical dimensions, the realm of cyberspace beckons exploration of its deeper sociocultural layers. Themes encompassing ethics, privacy, and digital rights demand attention. Comprehensive studies dissecting global predispositions, inherent vulnerabilities, and biases woven into demographic fabrics are indispensable (Dunn Cavelty, 2013). This includes illuminating the existing power disequilibria and ensuring that global dialogues are both equitable and diverse (Betz & Stevens, 2011; Gorwa, 2019).

While much of the prevailing literature anchors itself in institutional narratives, there's a palpable shift toward evaluative approaches steeped in critical theory. Such perspectives unearth concealed power dynamics and disparities (Nye, 2011) lurking within mainstream

maturity frameworks (Savaş & Karataş, 2022; Zachman, 1987). It prompts us to question if current cyber strategies genuinely resonate with their proclaimed ideals or skew towards a paradigm emphasising control and surveillance, often at personal freedom's expense (Castell, 2010).

In reflecting on our exploration into the realms of cyber and cyberspace, we recognise the vast landscape yet to be charted. Our study has anchored its focus on certain dimensions, but the breadth of cyberspace intersects various territories—be it the uncharted waters of new technological frontiers like quantum computing, or the societal undercurrents influenced by digital norms (Kissinger et al., 2021). Opportunities abound in comparative analysis, longitudinal tracking, and policy evaluation. There's also a call to decode the economic cost of cyber incidents and to gauge the pulse of public perception. By venturing into these diverse terrains, future research endeavours can sculpt a more robust, comprehensive map of the digital realm, enriching our strategies and illuminating our path forward in the cyber reality.

6. References

Australian Government. (2022). *2023-2030 Australian Cyber Security Strategy - Discussion Paper*. Available from: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper (Accessed 02 August 2023)

AWS (2023). *Cloud Computing with AWS*. Available from: https://aws.amazon.com/what-is-aws/ (Accessed 05 September 2023)

Baller, S., Dutta, S., & Lanvin, B. (2016). *The Global Information Technology Report 2016: Innovating in the Digital Economy*. World Economic Forum.

Barnet, M. & Duvall, R. (2005). Power in International Politics. *International Organization, 59*(1) (Winter, 2005), pp. 39-75. http://www.jstor.org/stable/3877878 .

Beecroft, N. (2021). *The UK's Cyber Strategy Is No Longer Just About Security*. Available from: https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037 (Accessed 20 December 2022)

Bell, E., Bryman, A., & Harley, B. (2022). *Business Research Methods (6th ed)*. Oxford: Oxford University Press.

Berkun, S. (2005). *The Art of Project Management.* Sebastopol: O'Reilly Media, Inc.

Bettencourt, L. (2012). *The Origins Of Scaling In Cities*. Santa Fe: Santa Fe Institute.

Betz, D. J. & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge.

Blumberg, B., Cooper, D. & Schindler, P. (2014). *Business Research Methods (4th ed)*. Maidenhead: McGraw-Hill Education.

British Academy. (2022). *British Academy response to the House of Lords Science and Technology Committee Inquiry on Delivering a UK Science and Technology Strategy*. Available from: https://www.thebritishacademy.ac.uk/documents/3740/British-Academy-Response-to-Delivering-a-UK-ST-Strategy_IcKJIbV.pdf (Accessed 18 December 2023)

Brooks Jr., F. (1995). *The Mythical Man-Month: Essays on Software Engineering, Anniversary Edition*. Crawfordsville: Addison-Wesley.

Carr, J. (2012). *Inside Cyber Warfare (2nd Ed)*. Sebastopol, CA: O'Reilly Media Inc.

Castells, M. (2010). *The Rise of the Network Society (2nd ed)*. West Sussex: Wiley-Blackwell Blackwell Publishers.

Caton, J. L. & Bartholomees, J. B. (2012). On The Theory Of Cyberspace. In Volume 1: Theory Of War And Strategy, pp. 325–344. Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep12116.26

Caton, J. L. (2018). The Land, Space, and Cyberspace Nexus: Evolution Of The Oldest Military Operations In *The Newest Military Domains*. Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep17662

Chang, L. Y., & Grabosky, P. (2017). The governance of cyberspace. In P. Drahos (Ed.), *Regulatory Theory: Foundations and Applications*, pp. 533–552. ANU Press. http://www.jstor.org/stable/j.ctt1q1crtm.42

Checkland, P. (1988). Information Systems and Systems Thinking: Time to Unite? *International Journal of Information Management, 8*(1988), pp. 239-248.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge MA: MIT Press.

Choucri, N. (2015). *Explorations in Cyber International Relations*. Available from: https://ecir.mit.edu/sites/default/files/documents/ECIR%20Final%20Report.pdf (Accessed 21 December 2022)

Clark, D. (2010). *Characterizing Cyberspace: Past, Present and Future*. MIT CSIL. Available from: https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf (Accessed 03 January 2023)

Cobb, A. (2012). *Leading Project Teams*. Thousand Oaks: SAGE Publications.

Colomb, R. M. (2005). Information systems technology grounded on institutional facts. In D. N. Hart & S. D. Gregor (Eds.). *Information Systems Foundations: Constructing and Criticising*. pp. 77–86. ANU Press. http://www.jstor.org/stable/j.ctt2jbj4x.10

Cordesman, A. (2022). The New U.S. National Defense Strategy for 2022. *Center for Strategic & Internatinoal Studies*. Available from: https://www.csis.org/analysis/new-us-national-defense-strategy-2022 (Accessed 05 January 2023)

Cox, O. & Kanji, H. (2022). *Building Effective Cybersecurity Governance*. Available from: https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/ (Accessed 09 February 2023)

Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Thousand Oaks, California: SAGE Publications Inc.

Crowther, G. A. (2017). The Cyber Domain. *The Cyber Defense Review, 2*(3), 63–78. http://www.jstor.org/stable/26267386

DCMS. (2022). *UK Cyber Security Sectoral Analysis 2022*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf (Accessed 28 December 2022)

Deibert, R. J., Palfrey, J., Rohozinski, R. & Zittrain, J. (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge MA: MIT Press.

Demchak, C.C. (2020). *Cybered Conflict, Hybrid War, and Informatization Wars*. UK: Routledge

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, K., & Johnson, B. (2018). *The Tactics & Tropes of the Internet Research Agency*. Austin, TX: New Knowledge (White Paper).

Department for Science, Innovation and Technology. (2023). *UK Cyber Security Sectoral Analysis 2023*. Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2023/uk-cyber-security-sectoral-analysis-2023 (Accessed 22 July 2023)

Dunn Cavelty, M. & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St. Anthony's International Review, 15*(1), pp. 37-57.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(1), 105–122. http://www.jstor.org/stable/24033170

Eom, J. H., Kim, N. U., Kim, S. H., & Chung, T. M. (2012). Cyber military strategy for cyberspace superiority in cyber warfare. Proceedings Title: *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Kuala Lumpur, Malaysia, 2012, pp. 295-299, doi: 10.1109/CyberSec.2012.6246114.

Eriksson, J., Giacomello, G., Salhi, H., Cavelty, M. D., Singh, J. P., & Franklin, M. I. (2009). Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State. *International Studies Review, 11*(1), 205–230. http://www.jstor.org/stable/25482060

European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018

Fanelli, R. (2016). Cyberspace Offense and Defense. *Journal of Information Warfare, 15(*2), 53–65. https://www.jstor.org/stable/26487531

Florida, R. (2002). *The Rise of the Creative Class: And How It's Transforming Work, Leisure, Community and Everyday Life*. New York: Basic Books.

Foucault, M. (1971). *The Order of Things*. New York: Vintage Books. ISBN 978-0-679-75335-3.

Galston, W. & McElvein, E. (2015). *Institutional innovation: How it happens and why it matters*. Available from: https://www.brookings.edu/research/institutional-innovation-how-it-happens-and-why-it-matters/ (Accessed 09 February 2023)

Gao, C., Guo, Q., Jiang, D., Wang, Z., Fang, C., & Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. *Journal of Geographical Sciences, 29*(1949–1964). https://doi.org/10.1007/s11442-019-1698-7

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Gibson, W. (1988). *Burning Chrome*. Glasgow: Harper Voyager.

Google Cloud (2023). *What is Cloud Computing?* Available from: https://cloud.google.com/learn/what-is-cloud-computing (Accessed 05 September 2023)

Gorwa, R. (2019). What is Platform Governance? *Information, Communication & Society, 22*(6), pp. 854-871.

Government of Canada. (2018). *National Cyber Security Strategy*. Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (Accessed 02 August 2023)

Government of Japan. (2015). *Cybersecurity Strategy.* Available from: https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf (Accessed 02 August 2023)

Graham, M. (2013). Geography/Internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal, 179*(2), pp. 177–182. doi:10.1111/geoj.12009

Greer, C., Burns, M., Wollman, D. & Griffor, E. (2019). *Cyber-Physical Systems and Internet of Things*. Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927259 (Accessed 31 December 2022)

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly, 30*(3), pp. 611–642. https://doi.org/10.2307/25148742

Hathaway, M. (2013). *Cyber Readiness Index 1.0*. Available from: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-readiness-index-1point0.pdf (Accessed 18 August 2023)

HM Government. (2021). *Global Britain In A Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*. Available from: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy (Accessed 21 November 2022)

HM Government. (2022a). *National Cyber Strategy 2022*. Available from: https://www.gov.uk/government/publications/national-cyber-strategy-2022 (Accessed 21 November 2022)

HM Government. (2022b). *Government Cyber Security Strategy*. Available from: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 (Accessed 12 June 2023)

House of Lords. (2022). *“Science and Technology Superpower”: More than a slogan?* Available from: https://publications.parliament.uk/pa/ld5803/ldselect/ldsctech/47/47.pdf (Accessed 20 December 2022).

IISS. (2021). *Cyber Capabilities and National Power: A Net Assessment.* Available from: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (Accessed 28 December 2022)

Jabbour, K. T. & Devendorf, E. (2017). Cyber Threat Characterization. *The Cyber Defense Review, 2*(3), 79–94. http://www.jstor.org/stable/26267387

Jasanoff, S. (2012). Genealogies of STS. *Social Studies of Science, 42*(3), 435–441. https://doi.org/10.1177/0306312712440174

Jazdi, N. (2014). Cyber physical systems in the context of Industry 4.0. *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, pp. 1-4, doi: 10.1109/AQTR.2014.6857843

Jenkins, H. (2006). *Convergence Culture: Where Old and New Media Collide*. New York: NYU Press.

Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs, 77*(5), pp. 81–94. https://doi.org/10.2307/20049052

Kissinger, H., Schmidt, E., & Huttenlocher, D. (2021). *The Age of AI: And Our Human Future*. London: John Murray Publishers.

Kottemann, J. E., & Konsynski, B. R. (1984). Information Systems Planning and Development: Strategie Postures and Methodologies. *Journal of Management Information Systems, 1*(2), pp. 45–63. http://www.jstor.org/stable/40397791

KPMG. (2023). *Cybersecurity Considerations 2023*. Available from: https://kpmg.com/xx/en/home/insights/2023/02/cybersecurity-considerations-2023.html (Accessed 21 August 2023)

Kreuzer, M. P. (2021). *Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age*. Available from: https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age (Accessed 21 December 2022)

Lankhorst, M. (2009). *Enterprise Architecture at Work - Modelling Communication & Analysis.* Berlin: Springer-Verlag.

Lee, L. H. (2022). The Digital Big Bang in the Metaverse Era. *2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, Singapore, Singapore, 2022, pp. 55-55, doi: 10.1109/ISMAR-Adjunct57072.2022.00020.

Libicki, M. (2021). *Cyberspace in Peace and War (2nd ed)*. Annapolis MD: Naval Institute Press.

Lillemose, J. & Kryger, M. (2015). *The (Re)invention of Cyberspace*. Available from: https://kunstkritikk.com/the-reinvention-of-cyberspace/ (Accessed 21 December 2022)

Lowy Institute. (2021). *Lowy Institute Global Diplomacy Index 2021*. Available from: https://globaldiplomacyindex.lowyinstitute.org/ (Accessed 02 January 2023)

Martin, A. & Helmerson, K. (2014). *Emergence: The Remarkable Simplicity of Complexity*. Available from: https://theconversation.com/emergence-the-remarkable-simplicity-of-complexity-30973 (Accessed 22 December 2022)

Mason, J. (2002). *Qualitative Researching*. London: SAGE Publications Ltd.

Matlin, G., & Land O'Lakes, Inc. (1979). What Is the Value of Investment in Information Systems? *MIS Quarterly, 3*(3), 5–34. https://doi.org/10.2307/248786

Maurer, T. & Morgus, R. (2014). SPACE. In Compilation of Existing Cybersecurity and Information Security Related Definitions (pp. 18–24). *New America*. http://www.jstor.org/stable/resrep10487.5

McGuffin, C., & Mitchell, P. (2014). On Domains: Cyber and the practice of warfare. *International Journal, 69*(3), 394–412. http://www.jstor.org/stable/24709325

McMullen, R. M., & Schneider, J. H. (1972). Information Systems. *Science, 175*(4019), 256–258. http://www.jstor.org/stable/1733475

Mearsheimer, J. J. (1994). The False Promise of International Institutions. *International Security, 19*(3), pp. 5–49. https://doi.org/10.2307/2539078

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing*. NIST US Department Of Commerce.

Microsoft Azure. (2023). *What is cloud computing? A beginner's guide.* Available from: https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-cloud-computing#:~:text=Most%20cloud%20computing%20services%20fall,on%20top%20of%20one%20another. (Accessed 05 September 2023)

Ministry of Defence. (2022b). *Cyber Primer*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1115061/Cyber_Primer_Edition_3.pdf (Accessed 23 December 2022)

Ministry of Defence. (2022a). *Global Strategic Trends - The Future Starts Today (6th ed)*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1075981/GST_the_future_starts_today.pdf (Accessed 24 December 2022)

Mumford, L. (1961). *The City In History*. New York: Harcourt, Inc.

NATO. (2022). *NATO 2022 Strategic Concept*. Available at: https://www.nato.int/strategic-concept/ (Accessed 23 July 2023).

Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *IEEE Internet of Things Journal, 5*(3), pp. 1843-1856. doi: 10.1109/JIOT.2018.2815535.

North, D. (1991). Institutions. *Journal of Economic Perspectives, 5*(1), pp.97-112.

Nye, J. S. (2011). *The Future of Power*. New York: PublicAffairs.

Nye, J.S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), pp.44-71.

Parish. B. R. & Madahar, B. K. (2016). *Understanding Cyberspace Through Cyber Situational Awarenes*s. DSTL Cyber and Information Systems Division.

Olofsson, A., Lindberg, O., Pedersen, A. Y., Arstorp, A., Dalsgaard, C., Einum, E., Caviglia, F., Ilomäki, L., Veermans, M., Päivi, H., & Willermark, S. (2021). Digital competence across boundaries - beyond a common Nordic model of the digitalisation of K-12 schools?. *Education Inquiry, 12*(4), pp. 317-328, doi:10.1080/20004508.2021.1976454

Orlikowski, W. J. & Robey, D. (1991). Information Technology and the Structuring of Organisations. *Information Systems Research, 2*(2), pp. 143-169.

Peters, B.G. (2012). *Institutional Theory in Political Science: The New Institutionalism*. New York: Continuum.

Porter, M. E. & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming competition. *Harvard Business Review, 92*(11), pp. 64-88.

Porter, M. E. (1980). *Competitive Strategy: Techniques For Analyzing Industries And Competition*. New York, NY: Free Press.

Porter, M. (1990). *The Competitive Advantage of Nations*. https://hbr.org/1990/03/the-competitive-advantage-of-nations. Accessed 07 June 2017.

Porter, M. (1998). Clusters & The New Economics Of Competition. *Harvard Business Review, November-December 1998*, pp. 77-90.

Powell, W. & DiMaggio, P. (eds) (1991). *The New Institutionalism in Organizational Analysis*. Chicago: University of Chicago Press.

Prince, C. & Sullivan, J. (2019). *The UK Cyber Strategy: Challenges for the Next Phase*. Available from: https://rusi.org/explore-our-research/publications/briefing-papers/uk-cyber-strategy-challenges-next-phase (Accessed 28 November 2022)

Raud, M. (2016). *China and Cyber: Attitudes, Strategies, Organisation*. Tallin: NATO CCDCOE. https://ccdcoe.org/library/publications/china-and-cyber-attitudes-strategies-organisation/

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38*(1–2), pp. 4–37.

Sassen, S. (1991). *The Global City: New York, London, Tokyo*. Princeton, NJ: Princeton University Press.

Saunders, M. & Lewis, P. (2018). *Doing Research In Business & Management: An Essential Guide To Planning Your Project (2nd ed)*. Harlow, England: Pearson Education Limited.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods For Business Students (8th ed)*. Harlow, England: Pearson Education Limited.

Savaş S. & Karataş S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *Int. Cybersecurity Law Rev. 3*(1), pp.7–34. doi: 10.1365/s43439-021-00045-4.

Stevens, T. & O'Brien, K. (2019). Brexit and Cyber Security. *The RUSI Journal, 164*(3), pp. 22-30. DOI: 10.1080/03071847.2019.1643256

Trist, E. (1981). *The Evolution of Socio-Technical Systems*. Occasional Paper No. 2, Ontario Quality of Working Life Centre, June 1981.

Tucker, J., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D. & Nyhan, B. (2018). *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*. Available at SSRN: https://ssrn.com/abstract=3144139 or http://dx.doi.org/10.2139/ssrn.3144139

US Department Of Defense. (2022). *2022 National Defense Strategy Of The United States Of America*. Available at: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF (Accessed 05 January 2023)

US Department of Defense. (2023). *2023 National Defense Science and Technology Strategy*. Available at: https://media.defense.gov/2023/May/09/2003218877/-1/-1/0/NDSTS-FINAL-WEB-VERSION.PDF (Accessed 22 July 2023)

Van Haaster, J. (2016). *Assessing Cyber Power. 2016 8th International Conference on Cyber Conflict Cyber Power* in N. Pissanidis, H.Rõigas, M .Veenendaal (Eds.) 2016 © NATO CCD COE Publications, Tallinn.

Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022*. Belfer Center for Science and International Affairs. Available from: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (Accessed 05 January 2023)

Wiener, N. (2019). *Cybernetics or Control and Communication in the Animal and the Machine, Reissue Of The 1961 Second Edition*. Cambridge MA: MIT Press.

Wren, G. (2015). *MIT Cybersecurity Seminar [Seminar]*. MIT.

Zachman, J. (1987). A Framework for Information Systems Architecture. *IBM Systems Journal, 26*(3), pp. 276-292.

7. Bibliography

Anholt, S. (2020). *Good Country Equation: How We Can Repair the World in One Generation*. Oakland. Berret-Koehler Publishers, Inc.

Beecroft, N. (2021). *The UK's Cyber Strategy Is No Longer Just About Security*. Available from: https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037 (Accessed 20 December 2022)

Berkun, S. (2005). *The Art of Project Management.* Sebastopol: O'Reilly Media, Inc.

Bentley, C. (2010). *PRINCE2: A Practical Handbook (3rd ed)*. Burlington, MA: Elsevier.

Bjørnskov, C. (2010). How does social trust lead to better governance? An attempt to separate electoral and bureaucratic mechanisms. *Public Choice, 144(*1/2), 323–346. http://www.jstor.org/stable/40661062

Bloom, J. (2021). *The tech firm whose fate shows the flaws of Global Britain*. Available from: https://www.theneweuropean.co.uk/arm-holdings-technology-brexit/ (Accessed 03 January 2023)

Blumberg, B., Cooper, D. & Schindler, P. (2014). *Business Research Methods, 4th ed*. Maidenhead: McGraw-Hill Education.

Brand Finance. (2022). *Global Soft Power Index 2022: USA Bounces Back Better To Top Of Nation Brand Ranking*. Available from: https://brandfinance.com/press-releases/global-soft-power-index-2022-usa-bounces-back-better-to-top-of-nation-brand-ranking (Accessed 31 December 2022)

Bussell, J. (2013). *cyberspace*. Encyclopedia Britannica. Available from: https://www.britannica.com/topic/cyberspace (Accessed 20 December 2022)

Cai, K. (2023). *The AI 50 2023*. Available from: https://www.forbes.com/lists/ai50/?sh=3c521acd290f (Accessed 12 April 2023)

CERN. (2016). *The Impact of CERN*. Available from: https://home.cern/sites/default/files/2018-07/CERN-Brochure-2016-005-Eng.pdf (Accessed 02 January 2023)

CERN. (2019). *30th Anniversary of the World Wide Web*. Available from: https://web30.web.cern.ch/ (Accessed 03 January 2023)

Chang, H. J. (2003). *Kicking Away the Ladder: The "Real" History of Free Trade*. Foreign Policy In Focus. Silver City, NM: Interhemispheric Resource Center.

CMS.gov. (2023). *Federal Enterprise Architecture Framework*. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/EnterpriseArchitecture/FEAF.html. Accessed 29 July 2023.

Conway, M. (1968). How Do Committees Invent. *Datamation*: 28–31.

Cook, C., Butchard, R., Holderness, A., & Sanders, G. (2022). *Pathways to Implementing Comprehensive and Collaborative JADC2*. Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220927_Cook_Pathways_ImplementingJADC2_0.pdf?UZ5C9IjGtH0RMITUk0wJBuToEei92zGJ (Accessed 03 January 2023)

Cordesman, A. (2022). *The New U.S. National Defense Strategy for 2022*. Center for Strategic & International Studies. Available from: https://www.csis.org/analysis/new-us-national-defense-strategy-2022 (Accessed 05 January 2023)

Cyberpogo (2023). *The US has announced its National Cyber Security Strategy: Here's what you need to know*. Available from: https://cyberpogo.com/2023/03/15/the-us-has-announced-its-national-cybersecurity-strategy-heres-what-you-need-to-know/ (Accessed 21 August 2023)

Dedehayir, O. & Steinert, M. (2016). The hype cycle model: A review and future directions. *Technological Forecasting and Social Change, 108*(2016), 28-41. https://doi.org/10.1016/j.techfore.2016.04.005.

Department of Defense. (2022). *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*. Available from: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF (Accessed 01 January 2023)

Dunn Cavelty, M. (2014). *'Cybersecurity in Switzerland'*. Cham: Springer.

Dunn Cavelty, M. & Jaeger, M. D. (2015). '(In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous'. *International Political Sociology 9*(2), pp. 176-194.

Dunn Cavelty, M, & Wenger, A. (eds.) (2022). *'Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation'*. London: Routledge.

Edwards, C. (2021). How Wealth Fuels Growth: The Role of Angel Investment. *Policy Analysis 921*. Cato Institute, Washington, DC, September 29, 2021. https://doi.org/10.36009/PA.921.

Eger, A. & Drukker, J. W. (2010). Phases of Product Development: A Qualitative Complement to the Product Life Cycle. *Design Issues 26*(2). 47–58. doi: https://doi.org/10.1162/DESI_a_00004

Elmaghraby, A. & Losavio, M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advance Research, 5*(2014), 491-497. http://dx.doi.org/10.1016/j.jare.2014.02.006

Fawcett, M. (2004). *Political Economy For Beginners*. New York: Barnes & Noble.

Federation of Enterprise Architecture Professional Organizations (FEAPO). (2013). A Common Perspective on Enterprise Architecture. *Architecture & Governance, 9*(4), 11-17.

Fukuyama, F. (2001). Social Capital, Civil Society and Development. *Third World Quarterly, 22*(1), 7–20. http://www.jstor.org/stable/3993342

Gilpin, R. & Gilpin, J. (2001). *Global Political Economy: Understanding The International Economic Order*. NJ: Princeton University Press.

Google Trends. (2023). *cyber*. Available from: https://trends.google.com/trends/explore?q=cyber,cybersecurity&hl=en (Accessed 28 August 2023)

Green, M., Harmacek, J., Htitich, M., & Krylova, P. (2022). *2022 Social Progress Index*. Available from: https://www.socialprogress.org/static/8a62f3f612c8d40b09b3103a70bdacab/2022%20Social%20Progress%20Index%20Executive%20Summary_4.pdf (Accessed 05 January 2023)

Hardin, R. (2002). *Trust & Trustworthiness*. New York: Russell Sage Foundation

Helmke, G. & Levitsky, S. (2004). Informal Institutions and Comparative Politics: A Research Agenda. *Perspectives on Politics, 2*(4), 725-740

Hern, A. (2015). *ARM: Britain's most successful tech company you've never heard of*. Available from: https://www.theguardian.com/technology/2015/nov/29/arm-cambridge-britain-tech-company-iphone (Accessed 18 December 2022)

Holmes, C. (2022). *Delivering a UK Science and Technology Strategy.* Available from: https://www.foundation.org.uk/Blog/2022/Delivering-a-UK-Science-and-Technology-Strategy (Accessed 29 December 2022)

Iacono, J. Brown, A. & Holtham, C. (2009). Research Methods – a Case Example of Participant Observation. *The Electronic Journal of Business Research Methods, 7*(1), 39 - 46.

ICO. (2022). *'Biggest cyber risk is complacency, not hackers' - UK Information Commissioner issues warning as construction company fined £4.4 million*. Available from: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/biggest-cyber-risk-is-complacency-not-hackers/ (Accessed 20 December 2022)

Jensen, M. & Meckling, W. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Capital Structure. *Journal of Financial Economics, 3*(4), 305–360.

Jessop, B. (1998), The Rise of Governance and the Risks of Failure: The Case of Economic Development. *International Social Science Journal, 50*(155), 29–45.

Jessop, B. (2002). *The Future of the Capitalist State*. Cambridge: Polity Press.

Jordan, D., Kiras, J., Lonsdale, D., Speller, I., Tuck, C. & Walton, D. (2016). *Understanding Modern Warfare (2nd ed)*. Cambridge: Cambridge University Press.

Karzel, D., Marginean, H., & Tran, T. (2023). *A Reference Architecture for the Internet of Things.* Available from https://www.infoq.com/articles/internet-of-things-reference-architecture (Accessed 21 July 2023)

Kugler, R. (1994). *U.S. Military Strategy and Force Posture for the 21st Century: Capabilities and Requirements*. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/monograph_reports/MR328.html. (Accessed 28 December 2022)

Landes, D. S. (1999) *The Wealth and Poverty of Nations: Why Some are So Rich and Some are So Poor.* New York: Norton, W. W. & Company.

Lloyds Bank. (2021). *Essential Digital Skills Report 2021.* Available from: https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/211109-lloyds-essential-digital-skills-report-2021.pdf (Accessed 21 December 2022)

Mack, N., Woodsong, C., MacQueen, K., Guest, G., & Namey, E. (2005). *Qualitative Research Methods: A Data Collector's Field Guide*. Durham: Family Health International.

Maney, K., Hamm, S., & O'Brien, J. (2011). *Making The World Work Better: The Ideas That Shaped a Century and a Company*. Crawfordsville: IBM Press.

Myers, M.D. (1997). Qualitative Research in Information Systems. *MIS Quarterly, 21*(2), 241-242.

Myers, M.D. (1999). Investigating Information Systems with Ethnographic Research. *Communications of the AIS, 2*(23), 1-20.

Myers, M.D. & Avison, D. (Eds.). (2002). *Qualitative Research in Information Systems*. London: Sage.

NCS. (2023). National Cyber Security Index. Available from: https://ncsi.ega.ee/methodology/ (Accessed 02 August 2023)

Orlikowski, W. (1993). CASE Tools as Organization Change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly, 17*(3), 309-340.

Orlikowski, W.J., & Robey, D. (1991). Information Technology and the Structuring of Organisations. *Information Systems Research, 2(*2), 143-169.

Pettigrew, A. (1987). Context and Action in the Transformation of the Firm. J*ournal of Management Studies, 24*(6), 649–670.

Porter, M. (2001). *Strategy and the Internet*. Available from https://hbr.org/2001/03/strategy-and-the-internet (Accessed 15 June 2023)

Reuters. (2023). U.S. and China wage war beneath the waves – over internet cables - A Reuters Special Report. Available from: https://www.reuters.com/investigates/special-report/us-china-tech-cables/ (Accessed 02 July 2023)

Rosemont, H. (2021). *Private Sector Engagement After the Integrated Review*. Available from: https://www.kcl.ac.uk/private-sector-engagement-after-the-integrated-review (Accessed 03 January 2023)

Roubini, N. (2022a). *Megathreats: The ten trends that imperil our future, and how to survive them*. London: John Murray Press.

Roubini, N. (2022b). *The Age of Megathreats*. Available from: https://www.project-syndicate.org/onpoint/age-of-megathreats-war-climate-debt-inflation-technology-by-nouriel-roubini-2022-11 (Accessed 19 December 2022)

Sessions, R. (2008). *Simple Architectures For Complex Enterprises*. Redmond: Microsoft Press.

Software Engineering Institute. (2023). *Software Architecture Glossary*. http://www.sei.cmu.edu/architecture/start/glossary/. Accessed 31 July 2023.

Steed, D. (2021). *The UK's Integrated Review and the future of cyber*. Available from: https://www.realinstitutoelcano.org/en/analyses/the-uks-integrated-review-and-the-future-of-cyber/ (Accessed 02 January 2023)

Sutterfield, S., Friday-Stroud, S., & Shivers-Blackwell, S. (2006). A case study of project and stakeholder management failures: Lessons learned. *Project Management Journal, 37*(5), 26-35.

The Open Group. (2010). *World-Class Enterprise Architecture*. San Francisco: The Open Group.

The Open Group. (2011a). *TOGAF® Version 9.1, an Open Group Standard - Introduction*. http://pubs.opengroup.org/architecture/togaf9-doc/arch/. Accessed 29 July 2023.

Thies, C., & Baum, C. (2020). *The Effect of War on Economic Growth*. Available from: https://www.cato.org/cato-journal/winter-2020/effect-war-economic-growth (Accessed 15 November 2022)

The Open Group. (2011b). *TOGAF® Standard Courseware V9.1 Edition - Module 1 Management Overview*. San Francisco: The Open Group.

Tian, N., Kuimova, A., Da Silva, D. L., Wezeman, P. D., & Wezeman, S. T. (2020). Trends In World Military Expenditure, 2019. *Stockholm International Peace Research Institute*. http://www.jstor.org/stable/resrep24438

Transparency International. (2022). *Corruption Perceptions Index 2022*. Berlin: Transparency International.

Turner, O. (2019). 'Global Britain and the narrative of empire'. *The Political Quarterly, 90*(4), pp. 727-734. https://doi.org/10.1111/1467-923X.12739

US Federal Government. (2023). *Federal Enterprise Architecture Framework*. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf. Accessed 29 July 2023.

Von Clausewitz. (2021). *On War*. Ottawa: East India Publishing Company.

Whitney, K. & Daniels, C. (2013). The Root Cause of Failure in Complex IT Projects: Complexity Itself. *Procedia Computer Science, 20*(2013), 325-330.

Whittemore, A. (2014). Practitioners Theorize, Too: Reaffirming Planning Theory in a Survey of Practitioners' Theories. *Journal of Planning Education and Research, 35*(1), 76-86. https://doi.org/10.1177/0739456X14563144

World Bank. (2002). Political Institutions and Governance. *World Development Report 2002*, pp. 99-116.

Zachman, J. (2016). *The Framework for Enterprise Architecture: Background, Description and Utility*. https://www.zachman.com/resources/ea-articles-reference/327-the-framework-for-enterprise-architecture-background-description-and-utility-by-john-a-zachman#EN1. Accessed 30 July 2017.

Zietsma, C. & Lawrence, T. (2010). Institutional Work in the Transformation of an Organizational Field: The Interplay of Boundary Work and Practice Work. *Administrative Science Quarterly, 55*(2010), 189–221.

8. Annex

8.1 List Of Abbreviations

ACD	Active Cyber Defence
AI	Artificial Intelligence
APT	Advanced Persistent Threat
BEIS	Department for Business, Energy & Industrial Strategy
BYOD	Bring Your Own Device
CAF	Cyber Assessment Framework
CBO	Congressional Budget Office
CBRN	Chemical, Biological, Radiological and Nuclear
CERN	European Centre for Nuclear Research / Conseil Européen pour la Recherche Nucléaire
CIA	Central Intelligence Agency
CISO	Chief Information Security Officer
CJEF	Combined Joint Expeditionary Force
CK	Crypt-Key
CNI	Critical National Infrastructure
CO	Cabinet Office
COBR	Cabinet Office Briefing Rooms
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CPS	Cyber-physical system
CNI	Critical national infrastructure
CS	Cyberspace
CT	Counter-terrorism
CTOC	Counter Terrorism Operations Centre

CyBOK	Cyber Security Body of Knowledge
DARPA	US Defence Advanced Research Projects Agency
DCMS	Department for Digital, Culture, Media & Sport
DDaT	Digital, Data and Tehnology
DDoS	Distributed Denial of Service
DNS	Domain Name System
DSTL	Defence Science and Technology Laboratory
EU	European Union
FCAS	Future combat air system
FCDO	Foreign, Commonwealth & Development Office
FPDA	Five Power Defence Arrangements
FSCCC	Financial Sector Cyber Collaboration Centre
GAO	Government Accountability Office (US government auditors)
GC	General Cyberspace
GCASE	Government Cyber Adversary Simulation Exercise
GCCC	Government Cyber Coordination Centre
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
GPS	Global Positioning System
HBC	Host Based Capability
HO	Home Office
IAEA	International Atomic Energy Agency
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control Systems
ICT	Information and communications technology

IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JFCyG	Joint Forces Cyber Group
ML	Machine Learning
MoD	UK Ministry of Defence
NATO	North Atlantic Treaty Organisation
NCA	National Crime Agency
NCF	National Cyber Force
NCSC	National Cyber Security Centre
NCSP	National Cyber Security Programme
NCSS	National Cyber Security Strategy
NECC	National Economic Crime Centre
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NOCP	National Offensive Cyber Programme
NSC	National Security Council
NSRA	National Security Risk Assessment
ODA	Official Development Assistance
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe
OT	Operational Technology
PaaS	Platform as a Service
PII	Personally Identifiable Information
RAF	Royal Air Force
R&D	Research and Development

SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SDGs	Sustainable Development Goals
SIEM	Security Information and Event Management
SIS	Secret Intelligene Service - also known as MI6
SNS	Social Network Services
SOC	Security Operations Centre
SSH	Secure Shell
S&T	Science and Technology
TLS	Transport Layer Security
UN	United Nations