

A Review of the Book: “Department of Information and Communication Technology in the Khilafah Rashidah (Rightly Guided Caliphate)”

(Translated)

General Introduction and Overview:

Hizb ut Tahrir published the book “Department of Information and Communication Technology in the Khilafah Rashidah (Rightly Guided Caliphate)” in March 2026. This serves as another building block in the towering edifice the party has been constructing since its inception—an endeavor driven by the goal of resuming the Islamic way of life. The Hizb has released numerous publications regarding the Caliphate State—such as **“The Ruling System in Islam,” “Introduction to the Constitution,” “Institutions of the Khilafah State in Ruling and Administration,”** and **“Funds in the Khilafah State”**—to form a clear, detailed picture of what the future Khilafah (Caliphate) State by the Permission of Allah (swt) should look like, given that the Khilafah is a unique state, distinct from the forms of governance currently existing in the world.

This book is not a manual on computer engineering or programming. Instead, it is an intellectual and political project that outlines a vision for the role of information technology in managing state affairs. It comes in response to the profound impact of information and communication technology (ICT). In recent decades, ICT has become one of the most influential technologies in the lives of individuals, societies, and nations, evolving into the very infrastructure that drives most economic, administrative, security, and military activities in the modern world. Technology is no longer limited to computers, phones, and communication tools; it has become an integrated system that manages information flow, interconnects institutions, plays a role in decision-making autonomy, and constitutes a key element of state power and influence in the digital age.

In light of these profound transformations, it was essential to present a comprehensive vision regarding the role of ICT within the state. It is viewed as a strategic sector that transcends mere technical application to become an integral part of the regime’s governing control, security, administration, and development. Thus, the study is not limited to defining the technology and its components. Instead, it addresses the public policies that should govern its development, management, and protection, as well as its role in supporting state institutions and enhancing their capacity to perform their various functions.

The Central Theme of the Book:

The book proceeds from the premise that ICT is no longer merely a secondary technical sector. Instead, it has become a fundamental pillar upon which modern states rely for administration, the economy, security, warfare, media, and all other aspects of life. Consequently, possessing this technology and controlling its infrastructure has evolved beyond a mere technical or service-related matter into an issue directly linked to power, control, and liberation.

Thus, for states seeking to safeguard their interests and enhance their capacity to manage their affairs, relying on technologies produced by others is insufficient. Instead, they must build indigenous capabilities that enable them to advance and manage technology, as well as protect their data and information landscape. The various topics and principles discussed in the book stem from this perspective, offering practical approaches to achieving this objective.

The success of this independent vision for ICT depends primarily on the state’s ability to successfully navigate the transitional phase, break the global monopoly on chip supply

chains and other critical components, retain specialized expertise and skilled talent, and strike a balance between security imperatives and the protection of citizens' legitimate rights.

Technology and Revival:

Historically, the revival of Muslims and the source of their strength did not stem from science, industry, or wealth alone. Instead, that revival—past and future—was driven by intellectual advancement grounded in a spiritual foundation; specifically, the intellectual framework upon which the state and the nation were built. The scientific, administrative, and military achievements of Islamic history were the fruits of that revival, not its cause. The Ummah's decline began when it lost the foundation upon which its civilization rested; consequently, science, industry, wealth, power, and unity declined alongside it.

Based on this understanding, technology serves as a tool and a means for managing state affairs and serving the people. It does not constitute the intellectual or political foundation of the state's existence. Thus, the objective is to demonstrate how the information technology sector must be managed within a rising state, recognizing it as an essential tool for administration, control, and influence.

It is worth noting that theoretical sciences provide the Ummah with knowledge and scientific principles; applied sciences transform this knowledge into engineering solutions and designs; and technology subsequently embodies these designs into practical devices, systems, and products that serve the state and society. Therefore, building technological power is not achieved merely by importing technology. Instead, it requires possessing a scientific, engineering, and industrial base capable of producing and advancing technology.

We must never lose sight of the fact that the technology sector emerged and developed under the auspices of Western nations—specifically those holding a worldview contrary to Islam—who utilized it as an instrument of destruction and corruption. They transformed it into a colonial weapon used to plunder wealth, project influence, manipulate minds, cultivate collaborators, and impose the capitalist lifestyle—rendering the impact of technology even more devastating than that of military weaponry. Consequently, the Khilafah State must formulate a general policy rooted in its ideology and rebuild this sector from the ground up, ensuring it is founded upon the Islamic viewpoint towards life.

The true value of information and communication technology does not stem from the technology itself—as it is inherently a neutral tool—but instead derives from the civilizational and political project it serves. However, its importance should neither be underestimated, nor should it be viewed merely as an administrative tool. Instead, it must be seen as a significant instrument of power and authority. A state that relies on importing biotechnology remains vulnerable to dependency and external influence, whereas possessing the technology grants it greater independence and control over its resources and decisions, while bolstering its ability to safeguard its interests and achieve its objectives.

The Digital Revolution and Cyber Warfare:

In recent decades, the world has undergone a radical transformation driven by the digital revolution; information now travels at immense speeds, and computers, networks, and telecommunications have permeated nearly every aspect of life. The scope has expanded far beyond mere data storage and retrieval; digital technology and computerized software now drive a vast array of production processes, machinery, power plants—including nuclear and electrical facilities—water utilities, and more.

This massive development in information systems, computing, telecommunications, and networking has made most vital civilian and military facilities dependent on digital technology. Its impact extends to sectors such as the economy, education, administration, media,

security, and warfare. Given the capacity of these technologies to breach systems and enable the remote, cross-border control and management of facilities, states have recognized the potential threat to their independence, security, and control over critical infrastructure. Consequently, they have moved to safeguard their digital domains and counter attempts at cyber intrusion.

Information technology has also redefined the concept of military power. While military strength was traditionally rooted in conventional armies, energy sources, and natural resources, it now increasingly relies on technical and informational capabilities. Major powers are better able to project influence by dominating the electronics, software, operating systems, telecommunications networks, data, information, and military technology sectors.

Furthermore, this technology has transformed the nature of military operations themselves; unmanned aerial vehicles (UAVs), guided missiles, command-and-control systems, and surveillance and reconnaissance tools now rely heavily on computers, communications, and software. Thus, they have become integral components of military power instead of merely auxiliary tools. As a result of these factors—and the entry of technology into the arena of political, economic, and military conflict between nations—major powers have formulated specific security and military strategies for the cyber domain. This gave rise to the concept of cyber warfare: a silent strategic conflict waged in digital space, where traditional weaponry is replaced by software-based arms—such as malicious code, control and self-destruct viruses, exploits targeting undiscovered security vulnerabilities, and electronic jamming. These digital battles aim to breach an adversary's critical systems, paralyze their command-and-control networks, or disable air defense systems, power plants, water facilities, and airports. The result is near-total administrative and military paralysis, achieved without the need to cross borders or fire a single shot.

Consequently, the ICT sector must be regulated in alignment with the state's overarching policy of protecting its citizens and safeguarding their interests. This is achieved through two fundamental approaches: first, by building an industrial and technological base capable of producing the hardware and equipment that underpin digital systems—such as the manufacture of microchips and integrated circuits; and second, by establishing a clear policy for technology management and usage regulation. This entails managing communication networks, securing systems, controlling connectivity with the outside world, and gaining a deep understanding of operating systems and the mechanisms by which devices and machines communicate.

Furthermore, the emergence of cyber warfare as a modern theater of conflict between nations requires Muslims to develop the necessary technical and digital capabilities—as part of the broader effort to amass a force that deters the enemy. In this context, cyber warfare becomes an element of *Jihad* aimed at protecting the state and its interests, while supporting efforts to carry and propagate the Islamic message.

The Need for a Central ICT Department:

ICT has become an integral part of a state's operations and vital facilities, transcending the role of mere support tools. Administration, security, the economy, warfare, and public services all rely on it. Furthermore, it plays a fundamental role in preserving data and records, facilitating communication between state agencies, operating military and security systems, and managing critical infrastructure. As ICT has become the lifeblood of the modern state—intertwined with various state affairs—any malfunction directly impacts the performance of state agencies and national interests. This underscores the urgent need to establish a specialized, central ICT department.

Leaving this sector fragmented and distributed across multiple departments—without unified management and integrated coordination—creates dangerous vulnerabilities and entry points. Adversaries could exploit these to compromise state facilities or breach vital systems, potentially weakening the state, paralyzing certain functions, or disrupting the interests of the citizenry. Consequently, this department is tasked with the state's technical planning, regulating the telecommunications sector, managing digital infrastructure, protecting systems and networks, coordinating technical operations across various agencies, and bolstering the state's strategic capabilities.

The ICT department maintains close ties with key state entities—foremost among them the Office of the Caliphate, the provinces (Wilayat), the courts, the Department of War, the Department of Industry and Internal Security, and the state's administrative apparatus. It is viewed as an enabling entity that provides the technical tools, systems, and software required by these agencies and departments to carry out their functions. It must be directly linked to the Khilafah centrally, as its impact extends to the majority of decision-making autonomy, administrative, and security-related functions. It is not merely an ordinary service department but an entity with a direct influence on the conduct of state affairs, domestic security, foreign relations, military capabilities, and economic strength.

Key Components of ICT:

ICT is not a singular entity but an interconnected system comprising several layers. It is essential to highlight the fundamental components upon which this system rests, as follows:

First: Electronic chips, devices, and equipment, which constitute the physical foundation of the entire technology. Computers, phones, communication devices, servers, and modern military hardware all rely on electronic circuits and microchips to function.

Second: Operating systems, software, and applications, which enable these devices to operate. Electronic hardware alone performs no function without the software and operating systems that control and manage its various operations. Software represents the logical or operational aspect of technology.

Third: Communication technology, comprising the means that allow devices to exchange information. The mere existence of computers and software is insufficient; there must also be mechanisms to transmit data between individuals and various devices.

Fourth: Networks and the Internet, which form the infrastructure connecting devices to one another, whether within a single facility or on a global scale. The Internet is the largest global network, linking millions of devices and systems and enabling the near-instantaneous exchange of information and services. Network control and management represent a crucial aspect of a state's technological sovereignty.

Fifth: Electronic warfare, which is one of the most significant facets of modern conflict. Conflict between nations is no longer confined to conventional weaponry; it now encompasses system breaches, intelligence gathering, cyber-espionage, signal jamming, service disruption, and the protection of digital infrastructure. Consequently, control over cyberspace has become an integral component of modern military and security capabilities.

Modern technology, therefore, is not merely a matter of computers or phones; rather, it is an integrated ecosystem—ranging from microchips to global networks and cyber warfare—where each component relies upon and complements the others. The mission of the ICT department is to build indigenous capabilities for hardware and software production, thereby achieving self-sufficiency and complete digital sovereignty for the state.

ICT Management Policy:

The ICT sector must be governed by a general policy. The competent department is responsible for formulating the state's general policy for this sector, devising strategic plans, and overseeing their implementation. This department is tasked with building and developing the electronics industry and the software sector, digitizing government operations to ensure fast, accessible, and highly efficient service delivery, providing high-quality, rapid communication services, and supplying the necessary technology to various sectors.

Principles of the ICT Policy:

A system for managing the ICT policy in the Khilafah State must be established. As a foundation for this, a set of ICT policy principles has been formulated; the book outlines nineteen such principles, accompanied by their respective Shariah evidences. While this context does not permit a detailed presentation of these principles and their evidences, we will provide an overview, categorizing them into three major conceptual frameworks or pillars: technical independence, information independence, and strategic administration.

Technical independence refers to the state's ability to control the fundamental architecture of the technology upon which it relies. Rather than merely consuming technologies produced by others, the state possesses the industrial and scientific capabilities to develop the systems, devices, and digital infrastructure it requires. This pillar encompasses principles related to the ICT industry, the development of inventions and technical devices, the establishment of public data centers, the management of digital infrastructure, the regulation of wireless waves and frequencies, and the protection of the State's digital space.

Information independence relates to controlling information and data, which have become among the most significant sources of power and influence. Data is no longer merely a set of records stored within departments; it has become a strategic resource enabling the management of societies, the economy, military forces, and various state apparatuses. This pillar encompasses regulations regarding cybersecurity, the monitoring of external threats, the protection of networks and systems, the preservation of individual privacy, the safeguarding of confidential state data, and the regulation of connectivity to the internet and the outside world.

Administrative and strategic independence, meanwhile, concerns how technology is utilized to serve the state and achieve its overarching goals. The objective is not to boast of technological advancement, but instead to harness these capabilities to improve the management of state institutions, enhance public services, boost performance efficiency, and strengthen planning and decision-making capacities. This pillar covers regulations concerning electronic documents, digital signatures, electronic payments, digital systems, remote judicial proceedings, and the application of artificial intelligence in administrative tasks, as well as the regulation of the relationship between the Information Technology Department and other state bodies.

The book provides specific details regarding Rule 19—which addresses information and communication technology policy in relation to the departments and agencies of the Khilafah—that merit mention: the department's general policy regarding these entities is founded on establishing and managing local data centers; protecting systems and networks; overseeing the production and development of software and security hardware; safeguarding the state's confidential and sensitive information; providing official communication channels and digital systems for all state agencies; and coordinating with various state bodies to develop artificial intelligence and modern technologies and their applications.

Secondly, the department focuses more on the services and systems it provides to the various state departments and agencies than on formulating new policies. It demonstrates

the enabling role the Department plays in supporting the office of the Khilafah; the departments of War, Internal Security, Foreign Affairs, and Industry; and the state's administrative apparatus—including its various components such as the administrations for Health, Education and Curricula, Masajid, Citizenship, and Hajj and Umrah—as well as other government bodies. This support is provided by supplying the systems, software, communication networks, databases, and digital infrastructure required for them to perform their functions. Furthermore, the Department is responsible for upgrading, maintaining, and securing these systems, while ensuring their integration and the secure, organized exchange of information among them; this contributes to enhancing operational efficiency, improving the management of State affairs, and strengthening the State's capacity for planning, decision-making, and the realization of its supreme interests.

Conclusion:

The book concludes that ICT has become a pivotal element of power and sovereignty in the modern era, transcending its status as merely a technical sector or a set of supporting service tools. Consequently, possessing this technology and controlling its infrastructure is a strategic necessity for ensuring the state's liberation (تحرير tahrir) from colonial influence and safeguarding its interests.

The book emphasizes that establishing technological independence requires developing indigenous capabilities in electronics, software, telecommunications, data centers, and cybersecurity, alongside managing the information domain. It also highlights the importance of leveraging technology to serve various state institutions, enhance administrative efficiency, improve services, support decision-making, and utilize modern technologies—particularly artificial intelligence—while maintaining human accountability in tasks and decisions that carry sovereign implications.

Thus, the book's core message is that the state requires an integrated system combining the development of indigenous technical capabilities, the protection of the information domain, and the harnessing of technology to serve administration, security, and development. In this way, ICT becomes a strategic pillar for bolstering state power and independence, as well as the state's ability to utilize digital technology to achieve its objectives.

Finally, this book—like those preceding it—underscores the seriousness and dedication of the advocates calling for the establishment of the Khilafah. It demonstrates the clarity of their political and intellectual vision and their commitment to formulating the practical frameworks necessary for managing the state's various affairs. It also reflects their tireless efforts to cultivate public support for this project within the Ummah by offering detailed approaches to contemporary issues and highlighting Islam's capacity to organize the affairs of life and the state. This effort reveals the awareness and sincerity inherent in the Islamic project, as well as its proponents' possession of an intellectual and political vision aimed at building a genuine state—one that bears and disseminates the message of Islam as a civilizational project addressing the problems of the individual, society, and the state. May Allah (swt) grant success; in Him we place our trust.