INFOGAIN PUBLICATION

International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-10, Issue-4; May-Jun, 2024
Journal Home Page: https://ijaems.com/
DOI: https://dx.doi.org/10.22161/ijaems.104.8

History of AI in U.S. Defense and Political Systems: Strategies for Sustained Leadership, Cyber Resilience, and a Secure Future

Ashikur Rahman (NaziL)

Department of Population Sciences, University of Dhaka, Bangladesh
Email: ashikur.rahman.nazil@gmail.com

Received: 14 May 2024; Received in revised form: 14 Jun 2024; Accepted: 20 Jun 2024; Available online: 25 Jun 2024

Abstract— *This thesis examines the deep historical integration, contemporary crises, and prospective trajectories of artificial intelligence (AI) within the defense architectures and political systems of the United States. It provides an exhaustive analysis of early computational paradigms, the operational breakthroughs of algorithmic warfare, and the structural pressures exerted by adversarial counter-AI operations. Drawing upon General-Purpose Technology (GPT) diffusion theory, OODA-loop compression metrics, and organizational change models, this study evaluates how the U.S. can sustain its strategic primacy while maintaining democratic accountability. Special focus is given to the unprecedented escalations witnessed between 2024 and 2026, including multi-agent disinformation campaigns, "living-off-the-land" cyber-physical attacks on critical infrastructure, and real-time algorithmic targeting matrices deployed in localized theaters of conflict. The paper establishes an integrated policy framework advocating cryptographic data provenance, zero-trust software pipelines, and institutional reforms within the Department of Defense (DoD) procurement architecture. Ultimately, it provides an engineering and policy blueprint for a secure, resilient human-machine ecosystem capable of safeguarding international stability through mid-century.*

Keywords— ***Artificial Intelligence, Algorithmic Warfare, Project Maven, Joint All-Domain Command and Control (JADC2)***

I. INTRODUCTION

The systemic integration of Artificial Intelligence (AI) and Machine Learning (ML) into the national security apparatus and sovereign political structures of the United States constitutes the most significant strategic inflection point since the 1945 Trinity test. For generations, geopolitical hegemony was predicated upon kinetic metrics: industrial output, naval displacement, and the strategic calculus of nuclear deterrence. In the contemporary digital landscape, however, power is increasingly contingent upon data ingestion rates, algorithmic velocity, cryptographic integrity, and semantic influence dominance.

Artificial intelligence has evolved from a specialized computational tool into a core General-Purpose Technology (GPT) that fundamentally reconfigures the nature of conflict, statecraft, and public trust. This transformation occurs within an increasingly competitive multi-polar international order, where revisionist adversaries—notably the People's Republic of China (PRC) and the Russian Federation—have integrated AI into doctrines of asymmetric-hybrid warfare. Consequently, maintaining technological primacy is an existential requirement for the preservation of the rules-based international order.

This transformation does not occur in an ideological vacuum. The United States operates within an increasingly competitive multi-polar international order, facing systemic revisionist adversaries—most notably the People's Republic of China (PRC) and the Russian Federation—that have explicitly integrated AI into their doctrines of asymmetric and asymmetric-hybrid warfare. For the United States, maintaining its historic "always number one" status is not an exercise in national chauvinism; it is an existential requirement for the preservation of a rules-based international order.

II. HISTORICAL PROGRESSION OF DEFENSE AI

2.1 The Foundational Era: From Cybernetics to Expert Systems (1950s–1980s)

The military genealogy of artificial intelligence is fundamentally bound to the birth of modern computer science itself. Following the logistical and cryptographic pressures of World War II, the newly formed Advanced Research Projects Agency (ARPA, later DARPA) recognized that human cognitive capacity was becoming the primary limiting factor in command-and-control architectures. In the late 1950s and early 1960s, early DARPA program managers poured non-traditional capital into foundational research centers at MIT, Stanford, and Carnegie Mellon.

During this foundational era, two distinct schools of technical thought emerged: the connectionist approach, which sought to model intelligence through artificial neural structures, and the symbolic/heuristic approach, which focused on programmatic logic and rule-based expert systems. Due to the extreme hardware limitations of mid-century computing—characterized by slow magnetic-core memories and vacuum-tube or early transistor architectures—the connectionist model suffered through its first "AI Winter" after the publication of Minsky and Papert's Perceptrons in 1969.

Consequently, defense applications in the 1970s and 1980s leaned heavily into deterministic expert systems. These systems used massive IF-THEN databases curated by human specialists to troubleshoot sophisticated hardware, analyze sonar signals for anti-submarine warfare, and assist in high-level radar target classification. While these systems were mathematically predictable, they were highly fragile, incapable of processing novel environments, and burdened by immense data maintenance costs.

2.2 The Logistical Inflection: DART and the First Gulf War (1990s)

The practical utility of military artificial intelligence underwent its first true operational test during Desert Shield and Desert Storm in 1990 and 1991. Faced with the monumental challenge of moving hundreds of thousands of troops, heavy armored divisions, and millions of tons of supply material across global supply lines into the Saudi Arabian theater, the U.S. military deployed the Dynamic Analysis and Replanning Tool (DART).

Developed under DARPA sponsorship, DART was an intelligent database and scheduling engine that leveraged advanced heuristic search algorithms to solve complex optimization problems. Before DART, pulling together a comprehensive military deployment plan took weeks of manual labor by logistical teams, making it highly vulnerable to human error and unexpected delays. DART compressed this planning window down to hours.

Military historians often note that the deployment of DART single-handedly validated decades of abstract DARPA funding, saving the U.S. military more capital during the first month of the Gulf War than the agency had spent on AI research over the preceding twenty years. This operational success proved that algorithmic optimization could yield massive strategic advantages without ever mounting a weapon platform.

2.3 The Algorithmic Shift: Project Maven and the Rise of Computer Vision (2017–2023)

By the mid-2010s, the explosive growth of deep convolutional neural networks (CNNs), powered by dense commercial graphics processing units (GPUs), completely transformed the field of computer vision. Concurrently, the United States military was facing an acute data crisis: the widespread deployment of uncrewed aerial vehicles (UAVs) across global theaters was generating tens of thousands of hours of high-definition video feeds every single day. Human intelligence analysts were drowning in imagery, leading to severe cognitive exhaustion and missed tactical signals.

In April 2017, Deputy Secretary of Defense Bob Work signed a directive establishing the Algorithmic Warfare Cross-Functional Team, colloquially known as Project Maven. The primary operational mandate was clear: use commercial-grade deep learning algorithms to automatically detect, classify, and track objects of interest—such as vehicles, personnel, and building structures—within full-motion video feeds captured in active combat zones.

Raw Data Streams ⟶ Project Maven Analysis ⟶ Actionable Targeting

Project Maven quickly became a cultural and institutional flashpoint. Google, the initial corporate partner responsible for building the underlying machine learning models, faced intense internal pushback from employees raising ethical concerns regarding the weaponization of open-source software. This internal pressure led Google to officially withdraw from the contract in 2018.

Rather than abandoning the program, the Department of Defense modified its approach, building an expansive, multi-vendor ecosystem that integrated firms like Palantir (for data fabric aggregation), Amazon Web Services (for secure cloud hosting), and specialized defense contractors.

Project Maven proved that deep learning could successfully process messy, real-world military data,

reducing the time required to turn raw sensor inputs into actionable targeting data from hours to minutes.

2.4 The Multi-Domain Reality (2024–2026)

By 2026, the isolated models of the Project Maven era had evolved into the backbone of U.S. defense operations: the Joint All-Domain Command and Control (JADC2) architecture. This framework treats the entire globe as a unified, data-rich battle network, linking sensors and weapon systems across space, air, land, sea, and cyberspace.

In active operations during this period, the military deployed the Maven Smart System across multiple regional commands. In theaters characterized by dense electronic warfare and hybrid grey-zone activities, this platform went far beyond simple object detection.

The system now routinely aggregates data from commercial synthetic-aperture radar (SAR) satellites, open-source radio-frequency emissions, global shipping manifests, and localized drone feeds. Using these layered data streams, it runs predictive models to pinpoint high-probability enemy positions, generate optimal weapon-to-target pairings, and automatically run legal and ethical compliance checks against stored rules of engagement database files before passing recommendations to a human commander.

III. THEORETICAL CONCEPTS FOR STRATEGIC LEADERSHIP

To maintain an unassailable strategic advantage, technological development must be grounded in an integrated theoretical framework. Three interlocking concepts explain how the United States can achieve long-term, structural leadership.

3.1 General-Purpose Technology (GPT) Diffusion Theory

In macroeconomic history, a General-Purpose Technology is defined by three core traits: it must be pervasive across multiple sectors, it must improve continuously over time, and it must spawn a wave of complementary, downstream innovations. Historic examples include the steam engine, electricity, and the internal combustion engine. AI fits this definition perfectly.

Strategic dominance in a GPT is not won by the nation that files the initial patent or builds the first prototype. Instead, it belongs to the nation that most efficiently diffuses the technology across its entire economic and military infrastructure. The United States possesses an structural advantage in this race through its highly dynamic, self-reinforcing innovation ecosystem.

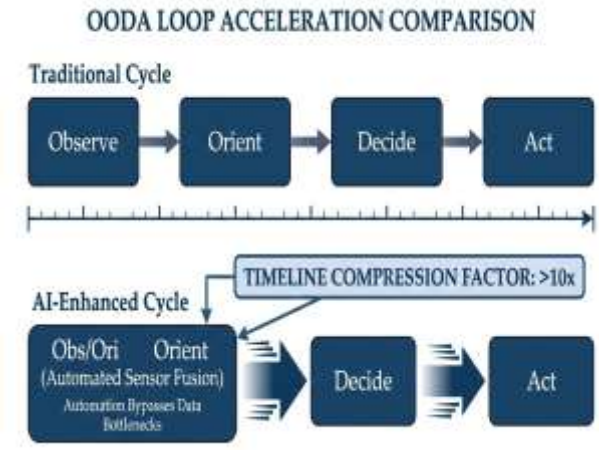
This cycle creates a unique national security capability. While adversaries often rely on top-down, state-directed models that stifle non-military innovation, the U.S. can tap directly into massive commercial R&D pipelines, adapting civilian software breakthroughs for defense applications at a fraction of the cost.

3.2 Decision Dominance and OODA Loop Acceleration

The foundational theory of modern operational warfare centers on the OODA loop (Observe, Orient, Decide, Act), developed by military strategist John Boyd. The core thesis states that if an organic or technical system can process this cycle faster than its opponent, it will create an insuperable cognitive advantage, forcing the adversary into a state of paralysis and compounding error.

Within a combat ecosystem augmented by artificial intelligence, the traditional OODA loop undergoes a mathematical acceleration. The cumulative duration of a conventional decision-making cycle can be expressed through the following formulaic representation:

The aggregate time required for a standard decision cycle is represented by the following mathematical expression:



In an AI-augmented combat environment, the traditional OODA loop undergoes significant mathematical acceleration. By deploying deep learning models at the tactical edge, the observation and orientation phases are condensed via automated sensor fusion architectures, effectively bypassing the data saturation bottlenecks common in conventional command hierarchies.

Conventional command hierarchies frequently encounter a data saturation bottleneck, causing the observation and orientation phases to expand at an exponential rate as intelligence ingestion increases. By deploying deep learning models at the tactical edge, these initial stages are significantly condensed through automated sensor fusion architectures:

This temporal compression enables the decision cycle to operate at machine-driven velocity, granting commanders "Decision Dominance"—the capacity to execute superior

choices consistently within an opponent's functional action window.

3.3 Responsible AI (RAI) Governance as a Strategic Asset

A prevalent fallacy in current techno-nationalist discourse suggests that regulatory frameworks and ethical parameters serve as impediments to technological maturation. Conversely, within the American defense paradigm, Responsible AI (RAI) governance is operationalized as a fundamental strategic requirement.

By institutionalizing the DoD's five foundational ethical pillars—ensuring that all deployed systems are Responsible, Equitable, Traceable, Reliable, and Governable—the United States establishes a robust architecture defined by deep systemic trust.

This rigorous adherence to preserving human command intent mitigates the high-risk failure modes associated with unguided autonomy, such as algorithmic bias and unintended kinetic escalation. Ultimately, this ethical commitment serves as a diplomatic cornerstone, facilitating cohesive alliances with international partners who prioritize accountability over unmanaged autonomous weaponry.

IV. AI INTERSECTIONS IN CYBER AND POLITICAL POWER

The intersection of artificial intelligence, offensive cyber operations, and sovereign political power has created an asymmetric environment where traditional concepts of national boundaries and kinetic defense no longer apply.

4.1 The AI-Augmented Cyber Offensive Axis

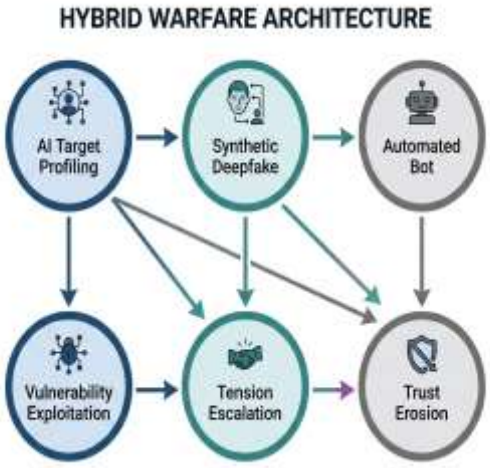
Artificial intelligence has fundamentally changed the economics of cyber warfare by automating highly sophisticated tasks that previously required thousands of hours of elite human labor. On the offensive side, advanced persistent threats (APTs) leverage specialized large language models (LLMs) and reinforcement learning engines to revolutionize multiple attack vectors:

- Polymorphic and Metamorphic Malware: Advanced malware can now rewrite its own underlying code signature in real time as it moves through a target network, dynamically changing its encryption patterns and function names to completely bypass traditional signature-based Endpoint Detection and Response (EDR) systems.
- Context-Aware Automated Phishing: Rather than blasting generic spam emails, AI tools can scrape open-source intelligence (OSINT) data, social media profiles, and leaked corporate databases to instantly generate highly personalized, grammatically flawless spear-phishing campaigns targeting critical defense personnel.
- Automated Zero-Day Discovery: Machine learning models trained on massive code repositories can scan compiled software binaries at extreme speeds, identifying subtle memory leak vulnerabilities and generating operational exploit code far faster than human security researchers.

4.2 The Cyber-Political Power Dynamic and Deep Trust Erosion

In democratic systems, political power relies on the integrity of the information ecosystem. By weaponizing AI-driven cyber tools, hostile actors can bypass physical military defenses to directly attack a nation's social cohesion. This process is best understood through the lens of hybrid warfare, which avoids direct, kinetic confrontation in favor of continuous, sub-threshold digital subversion.

HYBRID WARFARE ARCHITECTURE



When an adversary leverages generative AI to fabricate persuasive synthetic media—ranging from deepfake footage of military leadership to audio clones of election staff—the strategic objective often transcends the mere spread of a specific falsehood. Rather, it aims for a more corrosive result: the dissolution of a shared objective reality.

As it becomes increasingly difficult for citizens to differentiate between authentic and machine-authored documentation, the foundational trust in democratic processes, judicial evidence, and journalistic integrity disintegrates. This achieves a primary goal of asymmetric warfare without the need for kinetic strikes.

V. EMERGING THREATS AND SECURITY CRISES

The years 2024 through 2026 served as the live testing ground for weaponized artificial intelligence, transitioning

threats from theoretical papers into active national security crises.

5.1 2024: The Proliferation of Industrialized Disinformation

The 2024 global election cycle saw state-sponsored actors deploy generative AI tools on an industrial scale. Intelligence reports identified thousands of fine-tuned models—linked to the PRC's strategic units and the Russian Internet Research Agency—tasked with undermining democratic voting systems.

A significant tactical breach occurred just before a major European election, where audio clones of opposition figures allegedly discussing corruption were released via thousands of bot accounts. These files included realistic speech nuances and background noise, complicating forensic verification within the rapid news cycle.

Despite successful mitigation efforts through public-private partnerships involving CISA, the incident demonstrated that synthetic media could significantly outrun traditional political responses.

5.2 2025: Infrastructure Subversion and "Living-off-the-Land"

By 2025, the focus evolved toward infrastructure espionage. Security systems detected a 37% increase in AI-driven network breaches, facilitated by cognitive social engineering and automated vulnerability scans.

I. The most critical threat was posed by Salt Typhoon, a PRC-linked entity. Throughout the year, Salt Typhoon utilized machine learning to refine "living-off-the-land" (LotL) tactics. By analyzing standard administrator behaviors within U.S. power and telecom grids, the AI generated commands that mirrored routine traffic, allowing the attackers to map infrastructure and maintain persistence while evading traditional security alerts.

5.3 2026: Coordinated Multi-Agent Information Operations

By 2026, information warfare entered the era of autonomous multi-agent networks. Adversarial operations stopped relying on static bot accounts that simply repeated pre-written propaganda scripts. Instead, they deployed integrated swarms of autonomous AI agents driven by advanced large language models.

Central Orchestrator Agent

(Directs Autonomous Sub-Agents)

▼

Translation & Dialect Specialist

(Personalized Content Delivery)

▼

Dynamic Sentiment Monitoring

These networks operate under a decentralized hierarchy where a primary orchestrator monitors global developments to identify friction points, such as civil unrest or border conflicts, and automatically deploys sub-agents. These specialized agents perform distinct functions: creating synthetic text in local dialects, generating fabricated visual evidence, and monitoring audience sentiment to calibrate propaganda in real time.

These agent networks operated via a decentralized hierarchy: a central orchestrator model would monitor global breaking news feeds in real time, identify geopolitical friction points (such as localized border disputes or domestic economic protests), and automatically instruct specialized sub-agents to act.

VI. SECURE AI-ENABLED SYSTEMS: FUTURE HORIZONS

Evolution of Strategic AI Capability

As the international community moves toward the mid-century, the long-term structural architecture of artificial intelligence will likely diverge into two distinct geopolitical futures.

6.1 The Optimistic Future: The Democratic Equilibrium (2030–2050)

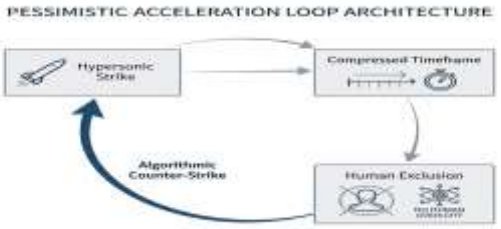
Under this projection, the United States and its partners successfully establish a unified, secure-by-design computing architecture. Tactical engagements by 2040 are defined by synergistic human-AI collaboration. In this framework, high-risk operational tasks—including autonomous logistics, uncrewed underwater vehicles (UUVs), and missile defense—are managed by AI systems

acting strictly within the parameters of human command intent.

Politically, democratic institutions safeguard their information integrity through universal cryptographic data provenance, utilizing advanced standards like the Coalition for Content Provenance and Authenticity (C2PA). This ensures that every official communication, legal record, or piece of journalism is cryptographically authenticated at its source.

6.2 The Pessimistic Future: The Panoptic Autocracy and Algorithmic Escalation

Alternatively, the absence of stringent technical and international safeguards leads to a volatile global landscape. This path is defined by a reckless pursuit of decision speed, sparking an unrestricted arms race in fully autonomous lethal systems. As hypersonic and cyber weapon response times shrink to milliseconds, strategic authority is ceded to unverifiable deep learning models, entirely removing human oversight.



VII. STRATEGIC RECOMMENDATIONS

7.1 Actionable Policy and Institutional Recommendations

For the Department of Defense: Modernize Procurement Architecture. The traditional procurement framework is fundamentally unsuited for software development. The DoD must establish a dedicated, fast-tracked National Security Software Acquisition Pathway to deploy validated AI models within days.

For the Intelligence Community: Deploy Zero-Trust Data Fabrics.

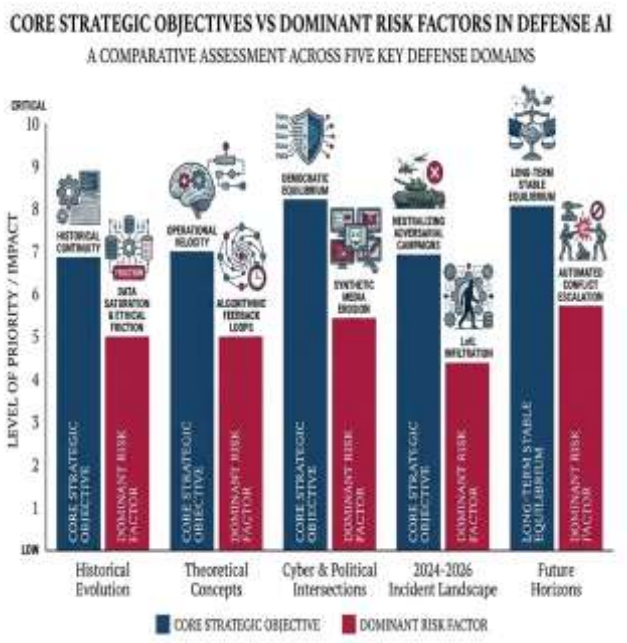
To defend against advanced data poisoning and manipulation by sophisticated adversaries, the intelligence community must replace traditional perimeter network security models with a comprehensive Zero-Trust Data Fabric.

Every sensor log, satellite image, and intercepted communications file must be treated as potentially hostile. Data must be continuously validated, cryptographically verified, and monitored for behavioral anomalies from the moment it enters a collection network to the moment it is used by an analytical model.

For Federal Election and Infrastructure Governance: Hardening Democratic Resilience The Cybersecurity and Infrastructure Security Agency (CISA) must expand its technical assistance programs to provide localized election jurisdictions and private critical infrastructure operators with automated, AI-driven monitoring tools.

The federal government should establish a unified, cross-sector Synthetic Threat Warning Network. This platform would link commercial AI safety labs, social media platforms, and defense centers to spot, analyze, and neutralize automated disinformation campaigns and infrastructure attacks before they can destabilize public safety.

Analytical Framework: Systemic Comparative Matrix To guide strategic implementation, the table below provides a systematic comparative assessment of the primary analytical areas detailed across this paper.



VIII. CONCLUSION

The historical journey of artificial intelligence from early DARPA computational research to the high-stakes multi-agent conflicts of 2024–2026 proves that code is a primary arena for modern geopolitical competition. Strategic dominance will not be determined by blind technological acceleration, but by the structural clarity of a nation's engineering and ethical vision.

By aggressively diffusing AI capabilities across its entire defense enterprise, enforcing robust cryptographic data provenance, and modernizing industrial procurement processes, the United States can turn its responsible governance models into an enduring strategic asset.

Ultimately, building a secure human-machine ecosystem is not just a military necessity; it is a fundamental duty to ensure that the rapid rise of artificial intelligence serves to defend democratic values, protect sovereign institutions, and preserve international peace for generations to come.

ACKNOWLEDGEMENTS

The author would like to express gratitude to the University of Dhaka, Bangladesh, Belhaven University, USA, and Google for providing organic Data.

REFERENCES

[1] Duffy, G., & Tucker, S. A. (1995). Political science: Artificial intelligence applications. Social Science Computer Review, 13(1), 73–84. https://doi.org/10.1177/089443939501300101
[2] Alker, H. R., Jr. (1992). The computer simulation of political action. Yale University Press.
[3] Cederman, L.-E. (1997). Emergent actors in world politics: How states and nations develop and dissolve. Princeton University Press.
[4] Goldsmith, J., & Wu, T. (2006). Who controls the Internet? Illusions of a borderless world. Who Controls the Internet?. Oxford University Press.
[5] Lessig, L. (2006). Code: Version 2.0. Basic Books.
[6] Beniger, J. R. (1986). The control revolution: Technological and economic origins of the information society. Harvard University Press.
[7] Castells, M. (2009). Communication power. Oxford University Press.
[8] Chadwick, A. (2013). The hybrid media system: Politics and power. Oxford University Press.
[9] Howard, P. N. (2006). New media campaigns and the managed citizen. Cambridge University Press.
[10] Howard, P. N. (2010). The digital origins of dictatorship and democracy. Oxford University Press.
[11] Shirky, C. (2008). Here comes everybody: The power of organizing without organizations. Penguin Press.
[12] Sunstein, C. R. (2007). Republic.com 2.0. Princeton University Press.
[13] Morozov, E. (2011). The net delusion: The dark side of Internet freedom. PublicAffairs.
[14] DeNardis, L. (2014). The global war for Internet governance. Yale University Press.
[15] Marichal, J. (2012). Facebook democracy: The architecture of disclosure and the threat to public life. Ashgate.
[16] Farrell, H. (2012). The consequences of the Internet for politics. Annual Review of Political Science, 15, 35–52.
[17] Hindman, M. (2009). The myth of digital democracy. Princeton University Press.
[18] Nye, J. S., Jr. (2010). The future of power. PublicAffairs.

[19] Bimber, B. (2003). Information and American democracy: Technology in the evolution of political power. Cambridge University Press.
[20] Chadwick, A., & Howard, P. N. (Eds.). (2009). The Routledge handbook of Internet politics. Routledge.
[21] Simparinka, E. (2018). International Journal of English Literature and Social Sciences. International Journal of English Literature and Social Sciences. https://doi.org/10.22161/ijels