Defending Japan's Sovereignty in the AI Era: Leveraging Linguistic Uniqueness to Build Sovereign AI

Beyond Muscles: In the AI era, cyberspace and intelligence constitute the very brain and nervous system of the sovereign state.
***Source*:** AI generated by Gemini

Kitamura Shigeru, Former Secretary General of the National Security Secretariat

Until the end of the Cold War, the center of gravity of national security rested primarily on the two pillars of military and diplomatic power. There is no doubt that the quantity and quality of weapon systems, starting with nuclear weapons, along with the expansion of alliances and economic cooperation, served as the primary indicators for gauging a nation's survival and influence. The United States and the Soviet Union, confronting each other across the Iron Curtain, competed to expand their nuclear arsenals and alliance networks, barely maintaining peace upon that precarious balance.

However, now that a quarter of the 21st century has passed, the situation has clearly changed. The elements that determine a nation's true power are no longer limited to kinetic forces or the visible scope of diplomatic activities. They have expanded to include the security of data and networks, the resilience of supply chains in key industries, and the capability to secure advanced technologies—including Artificial Intelligence (AI)—either independently or

in coordination with allies.

In other words, if destroyers, fighter jets, and tanks are the "muscles" of a nation, then cyberspace and AI constitute its "nervous system" and "brain." No matter how robust the muscles may be, if the nervous system is severed and the decision-making functions are paralyzed, the nation will be rendered immobile. Modern security is the endeavor of asking how to protect and fortify this nervous system and brain.

Just as Meiji-era Japan simultaneously developed its military and bureaucracy through the twin pillars of *Fukoku kyohei* (Enrich the Country, Strengthen the Armed Forces) and *Bunmei kaika*" (Civilization and Enlightenment),[1] 21st-century Japan cannot speak of its identity as a sovereign state without forging these new "nervous systems" and "brains": cyber and AI.

Vulnerability of the National "Nervous System"

During the Russian invasion of Ukraine, it was a symbolic occurrence that even before the onset of military aggression, sequential cyberattacks were launched against Ukraine's power plants and government agencies, causing severe disruptions to communications and public services. Before the invading forces crossed the border, the target nation's administrative procedures had already stagnated, and citizens found it difficult to access accurate information. Malware attacks targeting the electrical grid caused temporary blackouts, and disruptions extended to railway and financial systems. Furthermore, interference with satellite communication systems not only disrupted command and control chains on the battlefield but also impacted private enterprises and ordinary civilians. In times of conflict, "chaos" no longer manifests solely through the flash of a bombardment, but in the form of frozen screens and a litany of error codes.

The "NotPetya" ransomware, which struck the world in 2017, spread by exploiting the update function of accounting software used by Ukrainian companies, ultimately paralyzing the systems of Western port operators, logistics firms, and pharmaceutical companies. It is a symbolic case demonstrating that cyberattacks, irrespective of national borders, can halt the global economic cycle through supply chains.

[1] *Fukoku Kyohei* (Enrich the Country, Strengthen the Armed Forces) was a national slogan championed by the Meiji government. In the late 19th century, as various Asian nations were being colonized by Western powers, this guideline represented the urgent necessity for Japan to acquire "economic and military strength comparable to the West" in order to maintain its independence. On the other hand, *Bunmei Kaika* (Civilization and Enlightenment) was a cultural movement that actively embraced Western civilization and revamped social institutions and lifestyles. It was not merely a passing trend, but an essential process for Japan to be recognized as a "modern state" within the international community by introducing modern values, such as liberty, equality, and scientific education.

In that same year, 2017, the "WannaCry" ransomware directly hit the UK's National Health Service (NHS), causing disruptions to hospital booking systems and making medical records inaccessible. Reports indicate some hospitals were forced to stop admitting emergency patients, showing that cyberattacks no longer affect only corporate profits and losses, but can lead to situations directly

impacting human lives. Behind patients filling hospital beds, an invisible attacker binds the decisionmaking capacity of the medical frontline—we must confront this abnormality head-on.

Against the backdrop of such incidents, Japan's endeavor to include individual hospitals within the scope of "Specified Essential Infrastructure Providers" under the Economic Security Promotion Act
(ESPA) can be described as significant progress.[2]

A series of major incidents also occurred in the United States. In the 2021 "Colonial Pipeline cyberattack," parts of the East Coast's gasoline supply network were halted, and images of people rushing to gas stations circled the globe. Although it was a criminal organization, their technical prowess and choice of targets bore a striking resemblance to state-level tactics.
In the 2020 "SolarWinds supply chain attack," malicious code embedded in an update for the company's
IT management software, Orion, silently infiltrated the US Department of Homeland Security and Treasury, as well as the government agencies and corporations of allied nations. The management software at the system's backyard had effectively become a hidden passageway for external forces.

The conflict over oil has extended into cyberspace. In 2012, Saudi Arabia's state-owned oil company, Saudi Aramco, was subjected to an attack by a "wiper"—malware designed to erase HDD data to an unrecoverable level—known as "Shamoon," resulting in destructive damage to over 30,000 computers. It is reported that the attack involved overwriting the display image of the company logo with a skull and crossbones and wiping the contents of hard drives. Since the Gulf War (1990), the struggle over crude oil interests has shifted its stage from battlefield bombardments to the world of malware code.

North Korea utilizes cyberspace as a de facto means of "earning foreign currency." A typical example is the massive fraudulent remittance case from the Bangladesh Central Bank,

[2] Specified Essential Infrastructure Providers: Under the ESPA, the Japanese government designates critical entities across 15 sectors—including electricity, gas, telecommunications, and finance—that are subject to prior screening when installing key equipment to prevent cyberattacks and supply chain risks.
[3] VIVANT, a Sunday Theatre drama series aired on the TBS network in 2023, tells the story of a trading company employee embroiled in a fraudulent remittance scandal who is revealed to be a member of "Beppan," a secret intelligence unit within the Japan Self-Defense Forces, as he pursues the mysteries of an international terrorist organization.

reminiscent of the opening scenes of the popular Japanese drama series *VIVANT*,[3] as well as the outflow of funds due to the hacking of cryptocurrency exchanges. In 2014, the film company Sony Pictures suffered a cyberattack involving large-scale information leaks and operational shutdowns over a film it had produced. Outside the framework of financial transactions that the international community has tightened through sanctions, state activities are being conducted by exploiting highly anonymous digital spaces. It remains true across all times and places that "piracy" is tacitly permitted by some states and used as a means to enrich the national treasury.

Attacks against Taiwan by China have progressed even further. Beyond intruding into government websites, the method of displaying political messages on infrastructure that permeates daily life—such as convenience store displays and railway information systems—represents a new form of warfare that fuses psychological and information warfare.

In 2007, when Estonia relocated a Soviet-era war memorial, the country was subjected to a massive cyberattack, temporarily paralyzing government sites, banks, and the media. This incident, in which the involvement of Russian hackers was pointed out, is positioned as the beginning of diplomatic issues surrounding "historical perception" manifesting as attacks in cyberspace.

The experiences of Taiwan and the Baltic states demonstrate that cyberattacks are evolving into methods that directly interfere with "public opinion." Furthermore, the fact that AI enables the identification of system vulnerabilities at an unprecedented speed is exacerbating the situation.

The "Periphery" Dictates National Security

These international trends are by no means a "fire on the other side of the river" for Japan. Ransomware attacks on entities such as Asahi Group Holdings and ASKUL Corporation have laid bare the fact that disruptions to corporate activities lead directly to the paralysis of economic and social functions. Targeted attacks against defense-related companies, semiconductor manufacturers, universities, research institutions, and telecommunications carriers continue unabated. There have also been incidents where the information systems of local governments were compromised, resulting in the suspension of administrative services. The structure in which terminals used by municipal staff for daily operations, or outsourced system management, become the entry points for attacks illustrates that the "periphery" of our nation's information management can dictate the security of the state as a whole.

The reality that "diverse entities support national functions, and those same diverse entities can serve as entry points for attacks against the state" has already become "common sense" in the international community. During the Second World War, the strategy was to sever logistics by striking enemy munitions factories and ports. In the modern era, this has transformed into targeting the infrastructure embedded in daily life: servers of small and medium-sized enterprises that occupy a corner of the supply chain for strategically important goods, business systems hosted on the cloud, and network equipment supporting the counter services of local governments.

Reflecting this structural change, Japan enacted the ESPA in 2022, establishing frameworks for the stable supply of critical materials, the stable provision of essential infrastructure services, and support for the development of advanced critical technologies. [3] Not only physical resources such as semiconductors, storage batteries, and critical minerals, but also "invisible foundations" such as telecommunications infrastructure and cloud programs, have become subjects of major national security concern.

Furthermore, in 2025, the Active Cyber Defense legal framework was established, marking a shift from conventional passive defense—premised on responding after damage has occurred—to a proactive stance that enables the detection, interception, and neutralization of threats at the pre-attack stage. Additionally, the National Cybersecurity Office was newly established to coordinate authorities and responsibilities previously dispersed across various ministries and agencies, forming the foundation for comprehensive coordination and command and control at the national level.

Behind these measures lies the recognition that the cyber domain is no longer merely a field handled by technical specialized departments, but a national security issue concerning the very foundation of the state's decision-making. Just as the discourse on nuclear deterrence during the Cold War was premised on the awareness of "how to prevent escalation based on misperception," today we are confronted with the question: "To what extent can a state maintain normal judgment while its information systems are paralyzed?" This shift in perception is a major milestone in Japan's security policy and serves as a prerequisite for future policy development.

However, what threatens the heart of the state is not limited to cyberattacks. The discourse surrounding AI has deepened beyond mere issues of industrial competition or productivity improvement into the fundamental challenge of how to secure a nation's information sovereignty.

[3] The Four Pillars of the ESPA (2022): (1) Strengthening supply chains for critical materials; (2) Ensuring the security of essential infrastructure; (3) Supporting the development of advanced critical technologies; and (4) Protecting sensitive patents (non-disclosure of patents).

In the current landscape where generative AI is increasingly being introduced into policymaking, public administration, crisis management, financial regulation, and even the field of defense, it is no longer permissible for a state to regard AI merely as a "convenient tool." Certain AI models are beginning to be utilized for drafting administrative documents, creating outlines for proposed legislation, searching judicial precedents, and organizing examination criteria; however, as long as the decision-making process remains a "black box," the locus of responsibility inevitably becomes ambiguous.

While the European Union (EU) imposes strict discipline on AI utilization in high-risk areas through the Artificial Intelligence Act, individual nations are advancing the cultivation of their own state-led

foundation models—such as Mistralin France and Aleph Alpha in Germany. In the United Kingdom, while efforts to utilize AI in medical imaging diagnostics to improve early cancer detection rates are progressing, debates over the accountability for diagnostic errors are intensifying. Estonia, as a pioneer of e-government, has thoroughly digitalized everything from tax filings and company registrations to the management of court records, and is now stepping into the automation of administrative services through AI. There, administrative tasks—acting as the "limbs" of the state—are gradually being replaced by algorithms.

Turning to Asia, South Korea is deploying NAVER's large-scale language model, "HyperCLOVA X," into the public sector, using it for drafting administrative documents and providing primary responses to resident consultations. Singapore, under its Smart Nation initiative, is introducing AI into urban management, traffic control, and medical services to improve the convenience of civic life, while simultaneously facing the challenge of how to regulate the vast amounts of personal data collected in the background. China is said to be advancing social credit scoring—combining surveillance camera networks, facial recognition technology, and big data analysis—for use in maintaining public order and administrative management. All of these instances testify to the fact that AI is not only a tool for governance but is becoming a foundational technology that redefines "sovereignty."

In the United States, Project Maven by the Department of Defense is symbolic. AI analyzes vast amounts of video data transmitted from unmanned aerial vehicles and satellites to assist in target identification and situational assessment. As these types of systems become more sophisticated, the degree of reliance on algorithms for the gravest of decisions on the

battlefield—"distinguishing friend from foe"—will increase. In Ukraine as well, it is said that AI has supported the prioritization of artillery fire by integrating various drone footage and battlefield information. AI is no longer limited to being a staff officer for commanders; it even harbors the danger of strengthening its role as a "decider" in the future.

The problem extends to the daily lives of citizens. In Japan, the rapid increase in phishing scams and malicious redirects has become a major issue. The Japan Cybercrime Control Center (JC3) and the Consumer Affairs Agency have identified numerous fake shopping sites that sophistically imitate legitimate brands. Furthermore, the Information-technology Promotion Agency (IPA) has issued warnings regarding cases where users are lured to websites masquerading as legitimate interfaces via links disguised as ordinary web page elements, such as "Next Page" buttons.

Moreover, it is extremely difficult for ordinary people to distinguish these from legitimate links, and such deceptive interfaces are increasing at an accelerated pace due to the use of AI. Furthermore, while these issuestend to be overlooked asnon-concernsfornationalsecurity at first glance,the samemethods can be used for the fraudulent acquisition of highly sensitive information, potentially leading to situations that compromise national safety.

Of course, if appropriately utilized AI functions correctly, there is a possibility that simple coding errors could be significantly reduced. There is potential for issues such as troubles arising from mere coding mistakes in cyberspace, or crimes exploiting those vulnerabilities, to be improved through the application of AI.

On the other hand, attackers are also rapidly enhancing their ability to identify vulnerabilities using AI. In other words, the development of all information systems and applications is becoming a battlefield between competing AIs.

In the CrowdStrike incident the year before last, a defect in the company's buggy software occurred deep within the Windows OS, resulting in impacts on many social infrastructures—such as airline and banking systems—and leading to service outages. Continuing to easily open the "heart" of an OS remains a significant risk.

Against this backdrop, interest is growing worldwide in the concept known as "Sovereign AI" (AI developed and operated based on the laws and regulations of a specific country or region). As mentioned previously, France, Germany, and South Korea are advancing the development of their own state-led foundation models to avoid excessive dependence on USled platforms. India is also strategically cultivating a unique AI infrastructure capable of supporting its multilingual environment. In the Middle East, the development of AI models specialized for Arabic is progressing, as they seek to build dialogue systems sensitive to cultural and religious contexts.

Every nation is strengthening its recognition that an AI capable of accurately understanding

its own language, culture, and legal system sits at the very core of its sovereignty

What is the Optimal Choice for Japan?

What direction, then, should Japan take?

Japan's foundation in both security and technology rests upon its alliance with the United States, and the technological dominance held by US cloud and AI enterprises is overwhelming. Ignoring this reality and aiming for a "completely independent" AI sovereignty, as seen in parts of Europe, would not be a realistic path.

On the other hand, continuing to rely entirely on external entities for the nation's core functions carries risks that are unacceptable for a sovereign state. During the Cold War, a fierce competition was waged over the control of communication cables and satellite links; in the modern era, the control of cloud and AI infrastructure has assumed that role.

Based on this premise, the direction Japan should choose is clear.

First, while maintaining a cooperative framework predicated on the Japan-US alliance, Japan must secure its own "space for discretion" within that framework. In doing so, attention must be paid not only to state actors but also to the industrial sector. Specifically, in fields where Japan or the United States holds a technological advantage, there must be strict refrain from pressuring Japanese companies—or those of the allied United States—to excessively disclose technology or intellectual property. Giving such openings to "countries of concern" would result in negative impacts that extend beyond Japanese and US companies to the state actors themselves. The "Act on Promoting Competition for Specified Software Used in Smartphones" is a prime example of this; its enforcement should be restrained, with safety as the top priority.

Second, in domains directly linked to the nation's decision-making capacity—such as administration, legal affairs, healthcare, education, and crisis management—a technological foundation must be established that possesses, at the very least, a certain degree of autonomy.

Third, focus should be placed on fields where Japan has accumulated expertise over many years— such as the Japanese language, an aging society, natural disasters, robotics, material science, and crisis management—to cultivate "sovereign technologies" with high non-substitutability through "selection and concentration." What is particularly crucial here is the uniqueness of the Japanese linguistic environment.

Weaponizing the Uniqueness of the Japanese Language

The Japanese language relies heavily on its high-context nature for semantic interpretation, and honorifics and euphemisms are frequently used. Consequently, the mere application of standardized global models cannot ensure sufficient reliability in domains requiring high

precision and accountability, such as administrative documents, legal systems, and medical records. An AI capable of accurately understanding and processing administrative documents, judicial records, and medical information composed in Japanese is a “sovereign technology” that supports the decision-making capacity of a sovereign state. To entrust this segment solely to the commercial models of other nations is equivalent, in the long term, to depending on external entities for a portion of the nation’s judgment.

The same applies to AI development specialized in technical domains where Japan has maintained high international competitiveness, such as robotics, materials science, medical research, crisis management, and satellite/geospatial information.Itis not thesuperiority of scale orphysicalcapability that matters; rather, the stance of securing a sovereign space for discretion through irreplaceable expertise is paramount. Just as post-war Japan established a “world-best even in niches” status in automobiles, consumer electronics, and semiconductors—thereby increasing its bargaining power in international negotiations—sovereignty in the AI era should be underpinned by a non-substitutable presence in specific domains.

However, no matter how well systems and technologies are developed, they alone do not complete national security. The entities that move the state are people, and human vulnerability remains the greatest risk. It is clear from international cases that information leaks by insiders, unauthorized access, the lackadaisical continued use of legacy systems, and a lack of awareness regarding information management bring about more serious damage than external cyberattacks or information theft. Internal vulnerabilities—such as the massive information leaks from the National Security Agency (NSA) seen in the Snowden incident, the removal of classified US military documents to personal devices, and the dissipation of defenserelated information in various European countries—have often shaken the very foundations of national security.

In 2024, Japan enacted the Act on the Protection and Utilization of Critical Economic Security Information (the “Security Clearance Act”), which, in conjunction with the Act on the Protection of Specially Designated Secrets, established a unified framework for managing access to state secrets and sensitive information. This law includes not only the government but also private enterprises within its scope, clearly identifying the information and technologies that must be protected by the state while granting legal authority and transparency to access privileges. Through these systems, it can be evaluated that Japan has acquired a structural foundation regarding personnel security measures. In an era of economic security where the boundaries between the state and private enterprises are becoming relativized, it is impossible to confine

information security within state institutions alone; a nationwide effort that includes the private sector is indispensable.

The Frontline of "Digital Geopolitics"

Broadening our perspective to Southeast Asia, it becomes apparent that the structure in which the digital infrastructures of both the United States and China coexist is reaching its limits. Traditionally, many countries in the region maintained a certain balance by utilizing Chinese equipment for telecommunications and surveillance systems while relying on US companies for cloud and financial services. However, now that cloud computing and AI have reached a stage where they define national functions themselves, it is overly optimistic to believe that such a "double-edged" posture can be sustained in the long term. On which country's infrastructure should national data be placed? Which cloud will reliably continue to function in times of emergency? Who bears responsibility when a failure occurs? Each of these questions strikes at the very heart of national sovereignty.

Singapore is centralizing information related to national functions into a governmentmanaged cloud, while Indonesia is moving toward prioritizing the security of physical infrastructure by constructing national data centers in cooperation with US companies. In Vietnam and the Philippines, reviews are also underway regarding their degree of dependence on Chinese infrastructure and their cloud service contracts.

Southeast Asia is now becoming the frontline of geopolitical choices in the digital domain. Just as the Middle East became the focal point of geopolitics surrounding oil during the Cold War, Southeast Asia in the 21st century has become the new geopolitical intersection for digital data and AI.

However, it is not appropriate to understand this as Southeast Asian nations being forced into a total tilt toward either the United States or China. A realistic strategy is one that pays attention to different layers: shifting core areas of national security toward trusted partners—namely allies and quasi-allies— while maintaining diversity in the commercial sector and seeking to upgrade domestic technological capabilities.

At the same time, when expanding regulations on specific countries of concern, sufficient care is required to ensure that such measures do not unduly restrict the activities of allied companies and, consequently, weaken one's own industrial base. Discerning the form of regulation that is truly necessary and effective will be a critical challenge for Japan's future diplomacy, security, and economic policies.

The examination of seemingly distinct domains—cyber, AI, human security, and regional order— reveals that the underlying question converges into one: How does a nation maintain its capacity for judgment and its freedom of action?

"Sovereignty" as the "Autonomy of Decision-making"

Cyberattacks seize initiative from the outside; excessive dependence on AI infrastructure renders decision-making processes opaque; and internal misconduct, information leaks, or simple errors in software development erode national foundations—including industrial bases—from within. Meanwhile, shifts in the regional order intensify external pressure on national choices regarding digital service infrastructure. In the face of such complex crises, a nation must not limit itself to isolated, piecemeal responses but must design integrated resilience from a multilateral perspective.

By 2025, through a series of measures—the enforcement of the "Security Clearance Act," the establishment of the Active Cyber Defense legal framework, the creation of the National Cybersecurity Office, and the operation and review of the ESPA—Japan has steadily prepared the foundation for what can be called the "nervous system" of national security. However, what breathes life into these institutional and organizational "vessels" is the will of the state and the understanding of society. Economic security should not be positioned merely as an extension of industrial policy. It should be defined as a redesigning of "sovereignty" in order to hand over the freedom and responsibility of national decision-making to the next generation, while taking into account our alliances.

In an era where uncertainty has become the norm, the core of "sovereignty" lies in the "autonomy of decision-making." How shall we protect and forge anew the foundations of national judgment? The commitment to this challenge will dictate Japan's course hereafter.

Translated from "AI Jidai ni Nihon no Shuken wo Do Mamoruka: 'Nihongo no Tokushusei wo 'Buki' ni shite Dokuji AI wo (Defending Japan's Sovereignty in the AI Era: Leveraging Linguistic Uniqueness to Build Sovereign AI)," Bungeishunju*, February 2026, pp. 126–135. (Courtesy of Bungeishunju, Ltd.)* [March 2026].

KITAMURA Shigeru
Former Secretary General of the National Security Secretariat
President of Kitamura Economic Security Inc.

Born in Tokyo in 1956. Graduated from the Faculty of Law at the University of Tokyo. Joined the National Police Agency (NPA) in 1980. Studied abroad at École nationale d'administration (ENA).

After serving as Director of the NPA Security Division and Foreign Affairs and Intelligence Division, Executive Secretary to the Prime Minister (the first Abe Cabinet), and Senior Counselor at the NPA Commissioner General's Secretariat, Kitamura joined the Noda Cabinet as Director of Cabinet Intelligence. He remained in the post from the second to the fourth Abe Cabinets.

In 2019, he was appointed Secretary General of the National Security Secretariat. Kitamura remained in the position under the Suga Cabinet until his resignation in July 2021.