Legislative Reform Directions for Building a Security-Based Society and Becoming a Security Power in the AI Era

1. Introduction

The rapid advancement of AI brings both unprecedented opportunities and serious security threats. AI now serves as essential infrastructure across all aspects of life, powering information search, translation, creation, and system operations. It also extends human physical and cognitive capabilities. However, these advancements inevitably increase cybersecurity risks. Without proper legal and institutional frameworks, such risks could have severe consequences at the national and societal level. Thus, in the AI era, legislative reform and the establishment of a security-based society are indispensable.

---

2. The AI Era and Technological Development

AI functions like a highway system that no one can avoid using. It is embedded across nearly every domain—information retrieval, translation, creative production, system management, and physical robotics—leaving no area untouched.

Scientific and technological progress is extending the human body and mind, compensating for weaknesses, and even supporting psychological well-being. AI is not merely a technological singularity; it represents a transformative shift in human existence and societal organization.

---

3. The Escalating Cybersecurity Crisis

The spread of AI coincides with the normalization, diversification, and large-scale escalation of cyber threats. Emerging attacks include cryptocurrency theft, AI-driven ransomware, and AI-enabled phishing. Criminals are increasingly using AI to refine their tactics and expand their reach.

Even large corporations with advanced defenses have proven vulnerable. Cyberattacks often spread beyond the initial victim, causing cascading harm to partners and customers. New forms of attacks—such as deepfakes, synthesized voices, and AI-generated malicious code—are particularly difficult to counter with legacy security systems.

---

4. Paradigm Shift: No AI Without Cybersecurity

AI introduces unique risks: black-box deep learning models, accidents during normal operations, uncertain causality, contagion and cascading impacts, and difficulties in recovery. Security is no longer a cost item but a core component of AI service delivery.

Cybersecurity must address both external threats and internal risks inherent to AI's autonomous nature. Moreover, it must be capable of handling not only known threats but also novel and emerging ones. In this sense, cybersecurity must evolve as a "living organism" that continuously adapts to dynamic environments.

---

5. Integrating Traditional and AI Security

Traditional security systems are reliable and well-tested but limited against new attack methods and malware variants. AI security, by contrast, excels at real-time detection and response through large-scale data analysis but risks malfunction if data or algorithms are insufficient.

The path forward requires integrating traditional and AI security to create a resilient, adaptive ecosystem. This must be reinforced by legal and regulatory frameworks to ensure effective governance.

---

6. Legislative Directions for a Security Power

1. **Establishing a Security-Based Society**
   - Lifelong security education, financial support for security costs, regular evaluations, and everyday consulting must become part of daily life.
   - Security should be treated as essential social infrastructure, requiring active participation from every citizen.
2. **Fostering Mega Security Enterprises**
   - Relying solely on individual companies' internal security capacity creates vulnerabilities.
   - Large-scale security enterprises must be cultivated through mergers, acquisitions, and strong R&D investment, making cybersecurity a primary business sector.
3. **Reforming the Legal Framework**
   - Korea currently operates with fragmented laws (e.g., Network Act, Personal Information Protection Act, AI Development Act), which lack systemic coherence.
   - A comprehensive "Basic Information and Communication Security Act" should be enacted, integrating defense, reporting, and response mechanisms into a unified framework.
4. **Strengthening Cybersecurity Governance**
   - A national-level governance system linking government, industry, and academia is needed.
   - Only coordinated, ecosystem-based defense efforts can provide effective protection against evolving threats.

---

7. Global Legislative Trends

- **Japan**: Cybersecurity Basic Act defining national principles and institutional responsibilities.
- **EU**: NIS2 Directive, Cyber Resilience Act (CRA), and common certification systems to harmonize security standards.

- **US**: No single basic law; relies on executive orders, procurement rules, and sector-specific regulations.
- **Others**: UK, Canada, Australia, and Singapore are strengthening laws on IoT security and critical infrastructure protection.

These global efforts demonstrate the need for Korea to move beyond fragmented sectoral laws toward a comprehensive and coherent national cybersecurity framework.

---

8. Conclusion

The AI era is one of simultaneous technological progress and escalating cyber threats. Cybersecurity is not optional—it is the core infrastructure that enables AI's safe and sustainable development.

To transform into a true security power, Korea must:

- Establish a **security-based society** where cybersecurity is a way of life,
- Foster **mega security enterprises** with global competitiveness,
- Enact a comprehensive **Basic Information and Communication Security Act**, and
- Build a robust **national cybersecurity governance system**.

Beyond abstract AI ethics, the identity of cybersecurity must be rooted in purpose and existence—defining what it stands for and why it matters. Only then can Korea secure its place as a global leader in both AI and cybersecurity.