2025 14th Korea Internet Governance Forum (KrIGF) Results Report

2025. 09.

Korea Internet Governance Forum
Program Committee

KIGA
Korea Internet Governance Alliance

KrIGF
S.KOREA INTERNET GOVERNANCE FORUM

Table of Contents

0. Introduction to the Korea Internet Governance Forum (KrIGF)

The IGF was first held in 2006 in Athens, following Paragraph 72 of the Tunis Agenda, a document resulting from the 2005 World Summit on the Information Society (WSIS). Since then, it has been held annually in various countries.

The IGF facilitates dialogue between governments, businesses, civil society, academia, the technical community, international organizations, and other stakeholders on public policy issues related to the internet. It has been recognized for playing a significant role in raising issues related to the internet and in strengthening the policy capacities of developing countries and new participants.

Moreover, the IGF is increasingly expected to deliver more concrete outcomes, such as "recommendations" on critical internet policy issues.

At the NetMundial meeting held in São Paulo from April 23 to 24, 2014 (a multi-stakeholder meeting on the future of internet governance), participants once again emphasized the need to strengthen the IGF.

The Korea Internet Governance Forum (KrIGF) aims to promote dialogue and discussion among various domestic stakeholders, including governments, businesses, civil society, academia, the technical community, and users, regarding key internet-related public policy issues. In addition, through education and outreach on key internet governance issues, it seeks to enable more citizens to participate in the internet policymaking process.

Furthermore, by strengthening connections with regional and global IGFs, KrIGF aims to facilitate more active participation of Korean stakeholders in regional and global internet governance discussions.

The Korea Internet Governance Forum (KrIGF) has been held annually since 2012, and the 14th event will be held in 2025. Since 2014, a Program Committee composed of multi-stakeholders has been organizing the event. Since 2017, the final report of the event has been published, and KrIGF has been officially registered as a National IGF with the global IGF. The final report for 2025 will also be published following the previous year, and it will be submitted to the global IGF Secretariat.
If you have any comments on this report, please contact us at the details below.

o Contact: KrIGF Secretariat (Tel. 02-3446-5934, E-mail. krigf@kiga.or.kr)

1. Overview of the 2025 14th Korea Internet Governance Forum (KrIGF)

o Theme: “The Future of Internet Governance: The Path We Must Take”

o Date: Thursday, July 3, 2025, 9:00 AM – 6:00 PM

o Venue: Gwanggaeto Hall B1, Sejong University

o Organizer: Korea Internet Governance Alliance (KIGA)

o Co-organizers: Korea Internet & Security Agency (KISA), GABIA, International Meta Media Association, Nanum Vitamin, Able Square Daejeon, Letuin Edu, Rocket Film, PetaFlag, Cyber Security Research Institute, Asia Institute of Social Sciences, Upful, ImpactUs, Open Net, Jungle Studio, Korea Information Society Development Institute (KISDI), Korean Progressive Network Jinbonet, Kakao, True Networks, Korea Game Users Association, Korea Internet Corporations Association (Total: 20 organizations)

o Sponsors: Ministry of Science and ICT (MSIT), GABIA, Cyber Security Research Institute, Kakao, True Networks (Total: 5 organizations)

o Website: www.krigf.kr

o Participants: 157 in total (On-site participants: 121 (77%), YouTube viewers: 36 (23%))

* Breakdown of confirmed 121 stakeholders:

* Technical community: 4 (3%), Industry: 13 (11%), Civil society: 16 (13%), General users: 40 (33%), Public sector: 23 (19%), Academia: 25 (21%)

* Note: YouTube participation was measured by the number of viewers; there may be duplicate participants across sessions.

o Key Results:

- A total of 9 workshop sessions were held within the Artificial Intelligence, Governance, and Digital Responsibility tracks under the theme "The Future of Internet Governance: The Path We Must Take."
- By providing real-time captioning services, accessibility to KrIGF for individuals with hearing impairments was ensured.
- Active online promotion by supporters before and after the event, YouTube channel uploads, and archiving of videos, among other efforts, were systematized for the Korea Internet Governance Forum (KrIGF).

2. Preparation Process

1) Program Committee

o The Korea Internet Governance Forum (KrIGF) is managed by the Program Committee which operates as a working group under the Korea Internet Governance Alliance (KIGA). The current Program Committee consists of participants from various fields, including government, industry, academia, the technical community, and civil society.

o The 2025 Program Committee is composed as follows:

- Oh Kyung-mi (Co-Chair), Open Net, Civil Society
- Lee Soo-young (Co-Chair), Policy and Legislative Research Institute, Civil Society
- Kim Young-gyu, Korea Internet Corporations Association, Industry
- Seo Young-jin, ICTNet, Civil Society
- Oh Byung-il, Korean Progressive Network Jinbonet, Civil Society
- Lee Jin, Cyber Security Research Institute, Civil Society
- Lee Jong-hyun, Asia Venture Philanthropy Network (AVPN), Industry
- Lee Hwa-young, Cyber Security Research Institute, Civil Society
- Jeon Sun-min, Korea Information Society Development Institute (KISDI), Government

- Jeon Young-gyun, Kakao, Industry
- Cho Bu-seung, Korea Institute of Science and Technology Information (KISTI), Technical Community
- Jo Yong-ho, Byeonhyeok Legal Policy Research Institute, Civil Society
- Choi Hyun-ah, Korea Internet & Security Agency (KISA), Government

2) Preparation Process of the Program Committee

o In 2025, the Program Committee held meetings as follows to discuss the event preparations. For detailed discussions and outcomes, please refer to [Attachment 1].

o January 24: First Meeting of the 2025 Program Committee (85th Meeting)

- Adoption of agenda items (KrIGF85-1)
- Review of the previous meeting minutes (KrIGF84-2)
- Confirmation of applications for the 2025 KrIGF Program Committee
  - ▶ Election of Co-Chairs and NRI Coordinator
- Review of the 2024 KrIGF evaluation meeting minutes
- Review of the overall 2025 KrIGF Program Committee schedule
- Other matters

o February 27: Second Meeting of the 2025 Program Committee (86th Meeting)

- Adoption of agenda items (KrIGF86-1)
- Review of the previous meeting minutes (KrIGF85-2)
- Sharing of the proposed venue for the 2025 KrIGF
- Discussion of tracks and session topics for the 2025 KrIGF
- Review of the 2025 KrIGF workshop session call for proposals and evaluation schedule
- Other matters

o March 27: Third Meeting of the 2025 Program Committee (87th Meeting)

- Adoption of agenda items (KrIGF87-1)
- Review of the previous meeting minutes (KrIGF86-2A)
- Sharing of poster session proposals
- Updates on preparation for the WSIS+20 pre-discussion webinar
- Review of the necessity for planning sessions on specific key issues
- Other matters
  - ▸ Sharing of venue-related changes
  - ▸ Scheduling considerations (afternoon vs. full-day)
  - ▸ Sharing of supporter recruitment plan (draft)

o March 21 – April 30: 2025 KrIGF Workshop Session Call for Proposals Period

o April 7 – May 12: 2025 KrIGF Supporters Recruitment Period

o April 11: Webinar on “Trends in International Digital Governance and Korea’s Response Strategies”

o April 11 – May 30: 2025 KrIGF Poster Session Call for Proposals Period

o April 24: Fourth Meeting of the 2025 Program Committee (88th Meeting)

- Adoption of agenda items (KrIGF88-1)

- Review of the previous meeting minutes (KrIGF87-2)
- Discussion on poster session operations
- Sharing of results from the WSIS+20 pre-discussion webinar
- Other matters
  - ▸ Sharing of venue-related changes

o May 22: Fifth Meeting of the 2025 Program Committee (89th Meeting)

- Adoption of agenda items (KrIGF89-1)
- Review of the previous meeting minutes (KrIGF88-2)
- Sharing of updates on 2025 KrIGF workshop session proposals and evaluation results
- Structuring of the overall 2025 KrIGF program
- Discussion of opening remarks and congratulatory messages by stakeholders
- Discussion of the 2025 KrIGF slogan
- Discussion on poster session operations
- Other matters
  - ▸ Sharing of supporter recruitment results
  - ▸ Recommendations for co-organizers and sponsors

o June 11: Sixth Meeting of the 2025 Program Committee (90th Meeting)

- Review of the previous meeting minutes (KrIGF89-2)
- Review of updates to 2025 KrIGF workshop session

proposals and confirmation of panelists

- Final check of opening remarks and congratulatory messages for the 2025 KrIGF
- Sharing of evaluation schedule for the 2025 KrIGF poster session
- Confirmation of live streaming and real-time captioning services, and related budget
- Review of the necessity of a pre-event inspection meeting before the 2025 KrIGF (scheduled for July 3)

3) Secretariat

o The following individuals have diligently worked on the preparation and execution of the 2025 Korea Internet Governance Forum (KrIGF)

- Jeong Gil-won, KOICS
- Park Eun-ha, KOICS
- Kim Hak-jin, KOICS
- Seo Yoon, KOICS
- Kim Jeong-bin, KOICS
- Park Hae-in, KOICS
- Lee Dong-geun, KOICS
- Lee Seo-yoon, KOICS
- Lee Seol-woong, KOICS
- Lee So-jung, KOICS
- Lee Hyo-rim, KOICS

o (Supporters)

- Go Do-won, Kyungpook National University
- Kim Do-yeon, Sookmyung Women's University
- Kim Hyun-jae, Freelancer
- Nam Chul-woo, Yonsei University
- Moon Pil-seop, Graduate School, University of Seoul
- Seong No-a, Hongik University
- Eom Jeong-woo, Sungkyunkwan University
- Lee Hee-ji, Sookmyung Women's University

- Lim Young-jo, Dankook University
- Choi Yeon-jae, Sookmyung Women's University
- Heo Yoon-young, Hankuk University of Foreign Studies

4) Facebook Page

o Although a Facebook group already existed, it was managed under a personal account. Therefore, to strengthen organized promotion through KrIGF's official account, a Facebook page was established in 2019.

o Facebook page : https://www.facebook.com/krigf.kr/

5) YouTube Channel Launch and Systematic Management of KrIGF Videos

o Decided to systematically manage the YouTube channel, including videos filmed in the past.

o YouTube channel : https://www.youtube.com/@2025KrIGF

6) Text interpretation

o It was decided to provide text interpretation to ensure accessibility for people with disabilities and to maintain transcripts for record-keeping.

o The real-time captioning service was provided by AUD, a social cooperative.

3. Program

Track 1	Track 2	Track 3
Artificial Intelligence (AI)	Governance	Digital Responsibility

Time	Content		
13:00 ~13:30	**Opening Ceremony**		
	□ **Host:** Oh Kyung-mi (Co-Chair, KrIGF) □ **Opening Remarks:** Lee Dong-man (Chair, KIGA) □ **Congratulatory Message:** Park Ji-hyun (Director, Ministry of Science and ICT) (Video) Lee Hae-min (Member of the National Assembly, Rebuilding Korea Party)	□ **Opening Address** - **Public Sector:** Park Jung-seop (Center Director, KISA) - **Civil Society**: Oh Byung-il (Representative, Jinbonet – Korean Progressive Network) - **Technical Community:** Kim Jin-soo (Senior Vice President, KISIA) - **Academia**: Lee Dong-man (Chair, KIGA) - **Industry:** Park Sung-ho (President, Korea Internet Corporations Association) – read by Kim Young-gyu (Director of Policy, KICA)	
13:40 ~15:00 (80')	**The Questions Raised by the Boom of Studio Ghibli-style Generative AI Images**	**Discussion on the Policy for Opening Reserved Domain Names**	**The Two Faces and Future of Digital Twin Technology at the Boundary of Innovation and Responsibility**
	■ **Moderator:** Lee Soo-young (Policy and Legislative Research Institute) ■ **Presenter:** Jung Il-jin (17 Jungle Studio) ■ **Discussants:** Jo Yong-ho (Byeonhyeok Legal Policy Research Institute) Jeon Young-gyun (Kakao) Cho Yoon-jae (Shinhan University) Kim Na-young (Root Sound Research Institute) Lee Chang-beom (Yonsei University)	■ **Moderator:** Kang Kyung-ran (Ajou University) ■ **Presenter:** Lee Jung-min (Korea Internet & Security Agency, KISA) ■ **Discussants:** Oh Byung-il (Korean Progressive Network Jinbonet) Lee Myung-soo (Megazone) Lee Ye-jin (Ewha Womans University)	■ **Moderator:** Bae Jeong-cheol (Dong-Eui University) ■ **Presenter:** Lee Ye-rim (Upful) ■ **Discussants:** Yeom Se-kyung (Dongguk University) Min Jae-myung (Korea National Open University) Lee Jin (Cyber Security Research Institute) Yoon Sung-yeol (Cyber Security Policy Youth Research Association)
15:00~ 15:10	Break		
15:10 ~16:30 (80')	**AI Ethics Letter: The Present and Future of Public Discourse on AI Ethics in Korea through Performance Reports**	**Coexistence and ESG Directions of Internet Companies**	**The Evolution of AI-based Voice Phishing and Threats to the Digital Trust System**
	■ **Presenter:** Ko Ah-chim (AI Ethics Letter) ■ Discussants: Kwon Oh-hyun (Parti Social Cooperative) Song Su-yeon (Unmake Lab)	■ **Moderator:** Jeon Young-gyun (Kakao) ■ **Presenter:** Kwon Hyun-ok (Kakao) ■ **Discussants:** Oh Kyung-mi (Open Net) Lee Jung-min (Korea Internet & Security Agency, KISA) Jeon Sun-min (Korea Information Society Development Institute, KISDI) Seong Jeong-mo (Undergraduate, Senior Year, Kwangwoon University)	■ **Moderator:** Kim Min-ji (Sookmyung Women's University) ■ **Presenter:** Lee Ji-hyun (Sookmyung Women's University) ■ **Discussants:** Jung Yong-uk (Cyber Investigation Division, Seoul Metropolitan Police Agency) Kang Dae-gyu (Financial Security Institute) Jung Su-min (Sookmyung Women's University)

			Choi Da-yeon (Sookmyung Women’s University)
16:30~ 16:40	Break		
16:40 ~18:00 (80’)	**Military Artificial Intelligence Threatening Human Rights and Peace: Is This Acceptable?**	**WSIS+20 and Future Directions for Domestic and Global Internet Governance Discussions**	**An Age of Anxiety, Is Your Information Safe? – The SKT USIM Data Breach Incident and Ontological Security**
	■ Moderator: Ko Ah-chim (AI Ethics Letter) ■ Discussants: Kim Yoon-myung (Institute for Digital Policy) Lee Hwa-young (Cyber Security Research Institute) Jeong Ya-ping (Palestine Peace Solidarity) Park Hae-ryong (Korea Internet & Security Agency, KISA) Kim Han Min-young (Amnesty International Korea) Choi Hyo-min (Ph.D. Candidate, Seoul National University) Kate Sim (Tech Workers Coalition)	■ Moderator: Park Min-jung (Korea Information Society Development Institute, KISDI) ■ Presenter: Jeon Sun-min (Korea Information Society Development Institute, KISDI) ■ Discussants: Jeon Young-gyun (Kakao) Oh Byung-il (Korean Progressive Network Jinbonet) Song Hye-in (Korea Internet & Security Agency, KISA) Yang Ji-soo (Ewha Institute for Social Sciences) Jeong Da-hyun (Ewha Womans University)	■ Moderator: Min Byung-won (Professor, Ewha Womans University) ■ Presenters: Kang Se-eun, Kim Ki-young, Kim Ha-eun, Do Ga-young, Lim Gyu-ri (Ewha Womans University) ■ Discussants: Shim Dong-uk (Korea Internet & Security Agency, KISA) Lee Jin-gyu (Naver) Kim Hyun-i (Shin & Kim LLC) Choi Hong-gyu (EBS)

o For detailed workshop session results, please refer to [7. Workshop Session Detailed Contents].

4. Event Evaluation

1) Participant Statistics

o Total Pre-registered Participants: 185, Survey Respondents: 78

o Total Participants: 157 (Pre-registered attendees: 81 (53%), On-site registration: 40 (25%), YouTube participants: approx. 36 (22%))

* A total of 121 confirmed stakeholders

* Technical community: 4 (3%), Industry: 13 (11%), Civil society: 16 (13%), General users: 40 (33%), Public sector: 23 (19%), Academia: 25 (21%)

* YouTube participants were counted based on the number of viewers, and duplicate participation across sessions may have occurred.

2) 만족도 조사결과

1. Survey Participant Distribution (78 respondents in total)	Public Sector (14)	Academia (17)	Industry (10)	Civil Society (7)	Technical Community (3)	Users (27)
	18%	22%	13%	9%	4%	34%

2. Experience in Participating in the Korea Internet Governance Forum	**Participants (42)**	**54%**
	Non-participants (36)	**46%**

3. Workshop Satisfaction (Afternoon Session 1)	**Workshop Session**	**Content Relevance**	**Timing Appropriateness**
	Session1 : The Questions Raised by the Boom of Studio Ghibli-style Generative AI Images (36 responses)	92%	87%
	Session2 : Discussion on the Policy for Opening Reserved Domain Names (19 responses)	95%	88%
	Session3 : The Two Faces and Future of Digital Twin Technology at the Boundary of Innovation and Responsibility (19 responses)	90%	90%

4. Workshop Satisfaction (Afternoon Session 2)	**Session4 : AI Ethics Letter: The Present and Future of Public Discourse on AI Ethics in Korea through Performance Reports (22 responses)**	93%	92%
	Session5 : Coexistence and ESG	92%	91%

	Directions of Internet Companies (25 responses)		
	Session6 : The Evolution of AI-based Voice Phishing and Threats to the Digital Trust System (27 responses)	92%	89%

5. Workshop Satisfaction (Afternoon Session 3)	Session7 : Military Artificial Intelligence Threatening Human Rights and Peace: Is This Acceptable? (22 responses)	89%	90%
	Session8 : WSIS+20 and Future Directions for Domestic and Global Internet Governance Discussions (23 responses)	94%	89%
	Session9 : An Age of Anxiety, Is Your Information Safe? – The SKT USIM Data Breach Incident and Ontological Security (29 responses)	91%	90%
6. Event Venue and Service Satisfaction	Venue Facilities (78 responses)	88%	

7. Other Opinions	- (Civil Society): I participated in Session 5 and gained new insights into corporate ESG activities and efforts to improve internet accessibility. It was a meaningful experience. - (Academia): I attended Session 6, and it was beneficial as both real-world impacts and policy alternatives were presented together. - (Public Sector): The venue pathways were slightly inconvenient, but the guidance and assistance provided were well organized. - (Industry): It would be helpful if a booklet summarizing each session's topics, content, and panel details could be distributed in advance. - (Academia): I appreciated that the materials and videos were uploaded on YouTube after the event, allowing me to revisit the sessions. - (User): I attended Session 9, and the panel was diverse and highly professional, which made the information useful, and the discussions comprehensive. - (Technical Community): Session 9 was particularly refreshing and informative, as it dealt with the topic of AI-based voice phishing. - (Academia): The discussions helped me to once again recognize the risks that may arise if AI technology is misused.
8. Suggested Themes and Venue for Next Year's	- Theme: AI-related ‣ Protection of personal information from AI ‣ AI ethics

KrIGF	‣ AI governance - Theme: Digital Trust and Security ‣ RDAP/RPKI ‣ Information security in the metaverse ‣ Transnational cybersecurity ‣ Embedded software security - Theme: Governance ‣ Algorithm fatigue among the digital youth generation ‣ Digital divide ‣ Corporate ESG activities - Preferred Venue ‣ A hotel or professional exhibition hall in the Seoul metropolitan area, Sangmyung University, Sejong University, Franciscan Education Center, or venues in Cheonan or Daejeon. ‣ A comfortable environment with proper indoor ventilation. (For example, at Sejong University, the air was stuffy and the venue was hot).

3) Program Committee Self-Evaluation

o **2025 KrIGF Program Committee Self-Evaluation and Improvement Suggestions**

- (Oh Byung-il): The Poster Session may require a separate space due to spatial and time constraints. Attendance decreased by about 40–50 people compared to last year, which could be attributed to either the absence of morning sessions or insufficient promotion. However, it was positive that the number of participants was maintained until the end since the event was held only in the afternoon.
- (Jeon Sun-min): All Poster Session presenters should be evaluated at the same time, but improvements in exhibition layout and placement are also needed. Attendance might have declined due to accessibility issues with the venue, though it was still efficient to operate only in the afternoon.
- (Jeon Young-gyun): Personally, I felt this year's KrIGF was the best so far. The afternoon-only schedule helped maintain participants' attention until the end and kept them engaged. The Poster Session was also meaningful. I agree with the concern that the venue environment was somewhat stifling, and I believe environmental conditions should be considered for next year.
- (Cho Bu-seung): Having recently participated in international academic forums, I observed that technical topics are actively discussed abroad. Incorporating discussions on global cooperation in research networks and security into KrIGF sessions would strengthen both

international connectivity and expertise.

- (Lee Hwa-young): The Poster Session provided a new opportunity for student participation, but the operation method needs to be further systematized.
- (Kim Young-gyu): Running the event intensively for half a day felt more impactful and efficient than a full-day schedule. Attendance was higher than expected, which was encouraging. Compared to recent years, there seemed to be fewer tracks dedicated to youth.

o Summary

- Most committee members positively evaluated the afternoon-only schedule.
- The Poster Session requires further systematization and operational improvements.
- To address declining attendance, improvements in promotion and venue accessibility are necessary.

5. KrIGF Event Photos

1) Opening Ceremony

WIFI : SEJONGGUEST PASS : 0234083114 2025년 제14회 한국 인터넷거버넌스 포럼(KrIGF) THE 14TH KOREA INTERNET GOVERNANCE FORUM	2025년 제14회 한국 인터넷거버넌스 포럼(KrIGF) THE 14TH KOREA INTERNET GOVERNANCE FORUM
Oh Kyung-mi, Co-Chair, hosting the opening ceremony	Lee Dong-man, KIGA Chair, delivering the opening remarks
Park Jung-seop, Director of KISA, delivering remarks on behalf of the public sector	Group photo of the opening ceremony at the 2025 KrIGF

2) Track 1

Studio Ghibli-style Generative AI Images Session	AI Ethics Letter Session
Session on Military Artificial Intelligence Threatening Human Rights and Peace	Group photo of the Poster Session Award Ceremony

3) Track 2

Session on the Policy Discussion for Opening Reserved Domain Names

Session on Coexistence and ESG of Internet Companies

WSIS+20 Session

Session Q&A

4) Track 3

Session on the Two Faces and Future of Digital Twin Technology

AI-based Voice Phishing Session

불안의 시대,
당신의 정보는 안녕하십니까?
- SKT 유심 정보 유출 사고와 존재론적 안보

Session on the USIM Data Breach Incident and Ontological Security

Session Q&A

7. Workshop Session Results Report

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Lee Soo-young

Session Title	**The Questions Raised by the Boom of Studio Ghibli-style Generative AI Images**			
Date & Time	July 3, 2025 (Thursday), 13:40 – 15:00		Venue	Gwanggaeto Hall (Rooms 1+2), Sejong University
Participants	Moderator	Lee Soo-young (Chair, Policy and Legislative Research Institute)	Presenter	Jung Il-jin (CEO, 17 Jungle Studio)
	Panelists	Jeon Young-gyun (Senior Manager of Social Cooperation, Kakao)		Cho Yoon-jae (Professor, Shinhan University)
		Kim Na-young (CEO, Root Sound Research Institute)		Lee Chang-beom (Professor, Graduate School of Law, Yonsei University)

	Category	Key Points
Summary	Artistry	Majority opinion emphasized that AI is merely a tool, while creative intent and human planning remain essential.
	Copyright	AI training itself does not constitute copyright infringement, but controversies persist regarding the similarity of outputs.
	Accountability	Responsibility among creators, AI developers, and platforms remains unclear, necessitating institutional improvements.
	Transparency	Generated content should indicate AI involvement (e.g., watermarking).
	Environmental Issues	Concerns were raised about carbon emissions from AI image generation, highlighting the need for ethical use.
	Labor and Creativity	Artists can enhance productivity and focus on creativity through AI, but their rights must be protected.

Topic	Summary of Issues	Panel Opinions
Artistry and Creativity	AI is only a creative tool; artistry depends on human planning and editing.	Broad agreement. However, caution was raised against a culture of simple replication and consumption.
Personal Data / Facial Images	Structural issue of users unconsciously providing facial data.	Need to improve user awareness and strengthen platform responsibility.
Copyright Issues	AI training itself is not infringement; the key issue lies in the similarity of outputs.	Korea is considered overly conservative; flexibility is needed as in the U.S. cases.
Environmental Costs	AI use results in high electricity consumption and carbon emissions.	Ethical education and policy measures are necessary for technology use.
Institutions and Laws	Social ethical standards, platform responsibility, and user self-regulation matter more than law.	A “soft law” approach is preferable over a “hard law” framework.
Job Security for Creators	Will AI replace artists’ jobs?	Rather, AI can grant creators more time and autonomy.

General review

The session “The Questions Raised by the Boom of Studio Ghibli-style Generative AI Images” held at the 14th Korea Internet Governance Forum (KrIGF) on July 3, 2025, provided a meaningful opportunity to examine the multifaceted issues of technology, society, art, law, and the environment in light of the recent boom in AI image generation.

1. **Raising relatable concerns through everyday examples**
   - By addressing the social and cultural phenomenon of the Ghibli-style image boom, the session allowed even ordinary citizens unfamiliar with AI technologies to easily engage with the topic.
   - For example, the opening remark about “parents changing their profile pictures to AI-generated images” effectively drew the audience’s attention and enhanced immersion.
2. **Multidisciplinary perspectives enriching the discussion**
   - The panel included experts from diverse fields such as law, art, platform companies, and policy studies, ensuring both depth and balance in the debate.
   - In particular, Kim Na-young, CEO of Root Sound Research Institute, commented, “AI is not a threat to creators, but a tool that gives back time,” which reflected the spectrum of opinions within the art community and resonated well with participants.

3. **Shifting from a ‘tech trend’ to ‘social reflection’**
   - The discussion moved beyond simple judgments such as “Ghibli-style images are cute or creepy” to broader considerations of the ethical, ecological, and institutional implications of AI image consumption.
   - Professor Cho Yoon-jae’s remark that “We live in an era where GPUs decide everything” served as a striking reminder of the environmental costs of technology consumption.

4. **Inclusion of practical alternatives**
   - Jeon Young-gyun, Senior Manager at Kakao, suggested practical measures for ensuring transparency at the platform level, such as watermarking and tagging AI-generated content. This provided a concrete starting point for follow-up discussions.

Areas for improvement

🕐 Lack of media and youth perspectives

- Generative image content is most actively used by digital-native generations such as teenagers and young adults through YouTube and social media. However, issues related to ethics education and media literacy for these groups were relatively overlooked.
- Future sessions should include user experiences from younger generations and insights from media education experts to provide a more balanced perspective.

🕐 Environmental issues left without structural solutions

- While the problems of GPU use, energy consumption, and carbon emissions were highlighted impressively, the discussion did not extend to concrete solutions (e.g., AI computation optimization, carbon taxes, ethical GPU usage guidelines). The debate therefore remained at the level of problem recognition.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Hwang Hae-ran

Session Title	**Discussion on the Policy for Opening Reserved Domain Names**				
Date & Time	July 3, 2025 (Thursday), 13:40 – 15:00		Venue	Gwanggaeto Hall B1, Sejong University	
Participants	Moderator	Kang Kyung-ran (Professor, Ajou University)	Presenter	Lee Jung-min (Team Leader, Korea Internet & Security Agency, KISA)	
	Panelists	Lee Jung-min (Team Leader, Korea Internet & Security Agency, KISA)		Lee Ye-jin (Student, Ewha Womans University)	
		Oh Byung-il (Representative, Korean Progressive Network Jinbonet)		Lee Myung-soo (Deputy General Manager, Megazone)	

Summary	○ Introduction to Reserved Domain Names - Definition: Protection of domain names expected to be used in the future. - Background: Introduced to serve the public interest, ensure stable operations, and uphold social responsibility and ethical standards. - Current Status: A total of 7,282 reserved names, including common nouns, regional names, profanities, single characters, and public institution-related terms. - Need for Opening: In line with social changes and the registration of ".kr" in Hangul (46,000 cases), there is a need to promote activation. In particular, "Hangul .kr" domains face more restrictions compared to other domains. - Survey Results: 75.6% of respondents support the opening of common noun reserved domain names. ○ Draft Policy for Opening Reserved Domain Names - Scope: 753 common noun reserved words under "Hangul.kr" - Method: First-come, first-served registration - Timeline: To be opened within 2025
General review	While there was general agreement on the need to open reserved domain names, differing views emerged regarding the method of opening and whether to grant priority rights. Oh Byung-il (Representative, Jinbonet) argued for a complete opening of reserved words, stating there is "no real reason to block them," and called for a re-examination of the grounds for maintaining each category.

Lee Myung-soo (Deputy General Manager, Megazone) emphasized the need to provide priority rights to existing registrants or at least advance notice, in order to prevent confusion among current users.

Lee Ye-jin (Student, Ewha Womans University) also expressed concern over potential confusion between domains from the user's perspective, stressing that "protection of registrants and sufficient publicity should go hand in hand."
Attorney Yoon Bok-nam (participant from the floor) highlighted the importance of ensuring consistency across domain policies, beyond simply opening reserved words.

Moderator Kang Kyung-ran (Professor, Ajou University) underlined that "the key issue is not whether to open them, but how to do so." She also noted that most reserved words were designated 20 years ago and that changes in language use and social perceptions across generations require policy-level responses.

Voting results among participants confirmed a consensus in favor of opening reserved words. However, it was also recognized that sensitive categories—such as profanities, single-character names, and regional names—still require cautious handling.

This public hearing served as a starting point for building social consensus on the issue, and it reminded stakeholders of the need to balance public interest, practicality, and fairness in designing future policies.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

작성자 : 이예림

Session Title	**The Two Faces and Future of Digital Twin Technology at the Boundary of Innovation and Responsibility**			
Date & Time	July 3, 2025 (Thursday), 13:40 – 15:00		Venue	Gwanggaeto Hall B1, Sejong University
Participants	Moderator	Bae Jeong-cheol (Adjunct Professor, Pusan National University; Dong-Eui University)	Presenter	Lee Ye-rim (CEO, Upful Co., Ltd.)
	Panelists	Yeom Se-kyung (Professor, Department of Industrial and Systems Engineering, Dongguk University)		Min Jae-myung (Professor, Korea National Open University)
		Lee Jin (Director, Cyber Security Research Institute)		Yoon Sung-yeol (President, Cyber Policy Youth Research Association)

Summary	Under the theme "The Two Faces and Future of Digital Twin Technology at the Boundary of Innovation and Responsibility", this session explored the current state and future directions of digital twin technology, as well as the ethical and legal challenges that accompany it. The discussion emphasized that digital twin technology is not merely a replication tool but one that increasingly influences our lives, policies, and ethical boundaries. The presentation covered how digital twins are currently implemented, the key concepts that warrant attention, and the specific issues that must be addressed to ensure preventive measures. The core elements of digital twin technology were summarized as big data, AI, and 3D modeling simulations. It was explained that AI learns from vast datasets, organizes this information, and converts it into 3D simulations through system modeling — which forms the essence of digital twins. Emerging trends such as spatial intelligence and physical AI were highlighted, including advancements that enable real-time 3D generation from 2D images, as well as applications in robot training and autonomous driving (e.g., Tesla's FSD). However, the session also raised concerns about the limitations and risks underlying these advancements: insufficient data leading to gaps in accident scenario simulations, the potential distortion of reality, and the lack of clear accountability in the event of failures.

General review	- Discussed the current state and future of digital twin technology, as well as the complex legal, social, and ethical challenges it raises, from a multistakeholder perspective. - Highlighted concrete examples to illustrate the negative aspects of digital twin technology, including data insufficiency and the lack of clear accountability, presenting realistic challenges. - Shared perspectives from technical, academic, civil society, and youth stakeholders on issues such as the gap between ethical regulation and technological reality, reflection on the current state of Korea’s technological capacity, and the need for personal data ownership and compensation. - Engaged in in-depth discussion on ways to clarify accountability for predictive decision-making and accidents, ensure transparency in data usage, and safeguard individual control. - Emphasized the importance of building a flexible yet robust governance system that can respond to rapid technological change, including proposals for expanding direct citizen participation in decision-making, shifting toward a “permit first, regulate later” approach, and implementing effective technical measures for data protection. - Reached consensus on recognizing the dual nature of technological advancement, establishing clear accountability structures for unpredictable risks, and the need for social consensus and collaboration to build sustainable digital governance.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Ko Ah-chim

Session Title	**AI Ethics Letter: The Present and Future of Public Discourse on AI Ethics in Korea through Performance Reports**		
Date & Time	July 3, 2025 (Thursday), 15:10 – 16:10	Venue	Gwanggaeto Hall B1, Sejong University
Participants	Moderator& Presenter	Ko Ah-chim (Operating Member, AI Ethics Letter)	
	Panelists	Kwon Oh-hyun (Parti Social Cooperative)	
		Song Su-yeon (Unmake Lab)	

Summary	• Presented the purpose and operational status of the AI Ethics Letter, providing an overview of its activities. • Highlighted major topics and cases covered by the newsletter, including labor exploitation, gender bias, data rights, disinformation, ecological impact, technology governance, cultural influence, and surveillance technologies. • Identified key trends observed while operating the newsletter: the “existential threat” AI hype often obscures real harms, and the spread of AI nationalism and discourse imbalance overly centered on the tech industry. • Noted that although there are significant voices calling for critical alternatives, these remain fragmented. The need was emphasized to connect diverse perspectives, expand technological literacy, and engage in intensive policy and discourse debates within the Korean context. • The panel discussion revolved around keywords such as diversity in technological approaches, formation of critical discourse, and community-centered technology design.
General review	The workshop was proposed as an opportunity to introduce the vision, operational status, objectives, and challenges of the AI Ethics Letter to a general audience, while also clarifying its direction. The contributions of the two panelists added context and depth to the presentation, making a meaningful contribution to the 2025 KrIGF theme, “The Path We Must Take.” From the presenter’s perspective, the outcomes achieved serve as a basis for continued efforts and strategic refinement aimed at connecting and visualizing diverse perspectives, addressing discourse imbalance, and ultimately contributing to real-world improvements. The proposal’s component on “international dialogue and solidarity” could not be covered due to time constraints, but it remains a goal to be pursued in future activities.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Kwon Hyun-ok

Session Title	**Coexistence and ESG Directions of Internet Companies**			
Date & Time	July 3, 2025 (Thursday), 15:10 – 16:30		Venue	Gwanggaeto Hall B1, Sejong University
Participants	Moderator	Jeon Young-gyun (Kakao)	Presenter	Kwon Hyun-ok (Kakao)
	Panelists	Oh Kyung-mi (Open Net)		Seong Jeong-mo (Senior Undergraduate, Department of International Trade, Kwangwoon University)
		Lee Jung-min (Korea Internet & Security Agency, KISA)		Jeon Sun-min (Korea Information Society Development Institute, KISDI)

Summary	This workshop, introduced through the presenter's opening remarks, focused on the social responsibility of internet companies and the ESG directions they should pursue, with a particular emphasis on Kakao's shared growth initiatives. Various programs were presented in which Kakao leverages its technology and platforms to help address the digital divide. Examples included the "Visiting Senior Digital School" for older generations, "Kind Digital World" for children and youth, "Kakao Class" for small business owners, and the "Kakao Tech Campus" and "Kakao Tech Bootcamp" for nurturing young talent. In the subsequent discussion, participants reaffirmed the social value of these initiatives and exchanged suggestions on scalability and sustainability for future development.
General review	This workshop successfully demonstrated how internet companies can enhance digital inclusion and fulfill their social responsibilities through the case of Kakao. By providing tailored programs for different generations and social groups, Kakao's initiatives showed a clear example of how corporate ESG values can be translated into practice, from bridging the digital divide to nurturing future talent. The panel discussion further highlighted key tasks for advancing these programs, such as strengthening publicity, sharing know-how, and improving accessibility. Based on these discussions, it was emphasized that when corporate shared growth initiatives are linked to a virtuous cycle of solving social challenges, the overall sustainability of Korea's internet ecosystem will be further reinforced.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Choi Da-yeon

<table>
<tr><td>Session Title</td><td colspan="4"><b>The Evolution of AI-based Voice Phishing and Threats to the Digital Trust System</b></td></tr>
<tr><td>Date &amp; Time</td><td colspan="2">July 3, 2025 (Thursday),
15:10 – 16:30</td><td>Venue</td><td>Gwanggaeto Hall B1,
Sejong University</td></tr>
<tr><td rowspan="4">Participants</td><td>Moderator</td><td>Kim Min-ji
(Member, EG@IG, Sookmyung Women's University)</td><td>Presenter</td><td>Lee Ji-hyun
(Member, EG@IG, Sookmyung Women's University)</td></tr>
<tr><td rowspan="3">Panelists</td><td colspan="2">Jung Su-min
(AI Security Architect, AWS)</td><td>Jung Dae-gyu
(Principal, Threat Analysis Team, Financial Security Institute)</td></tr>
<tr><td colspan="2">Jung Yong-uk
(Ph.D., Digital Forensics Division, Cyber Investigation Unit, Seoul Metropolitan Police Agency)</td><td>Choi Da-yeon
(Advisor, Europol Cybercrime Centre)</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

Summary

Voice Phishing and Its Social Impact

o **Definition:** Financial fraud using telecommunications (calls, text, messengers).

o **Current Situation:**

- 20,000–30,000 cases annually; daily damages average KRW 2.2 billion.
- While case numbers have decreased, the average loss per case has increased (KRW 17M in 2019 → KRW 25M in 2022).

o **New AI-Driven Methods:** Use of deep voice and deepfake to mimic family or acquaintances, undermining trust.

o **Social Impact:** Extends beyond individual harm to systemic erosion of trust.

AI and Voice Phishing: Key Concepts

o **Deep Voice:** Replicates intonation, breathing, and emotions; enables real-time synthesis.

o **Caller ID Spoofing**: Fakes familiar numbers, making deception almost unavoidable.

o **Deepfake Video**: Fabricated faces used in kidnapping threats or extortion.

o **Overseas Case:** Hong Kong CFO defrauded via deepfake, resulting in KRW 35 billion transfer.

o **Domestic Case:** A daughter's synthesized voice used in extortion calls, nearly indistinguishable from reality.

Psychological Perspective (Choi Da-yeon)

o **Exploitation of Psychological Triggers:**
- Obedience to authority (impersonation of prosecutors/police).
- Urgency triggers (immediate transfer demands).
- Emotional trust (romance scams with cognitive dissonance).
- Similarity effect (deepfake/voice leading to mistaken identity).

o **Secondary Trauma**: Self-blame, stigma, anxiety, reluctance to report, social isolation.

o **International Responses:**
- UK Action Fraud: Combines AI analysis with psychological support; 72% phishing email blocking rate.
- Singapore ScamShield: Real-time suspicious SMS alerts, blacklist sharing, privacy protection.

o **Korea's Status**: Integrated reporting centers and post-support exist, but psychological support remains underdeveloped.

o **Proposals:**
- Real-time psychological alerts ("Possible voice phishing detected — pause before acting")
- faster integration of reporting-analysis-blocking to overcome current 3–7 day delays.

Technological Perspective (Jung Su-min)

o **AI Techniques:**
- SV2TTS, VITS, YourTTS — real-time synthesis with only a few seconds of samples.
- NLP-based smishing generates thousands of credible phishing messages.

o **Domestic Telecom Responses:**
- LG U+: Anti–deep voice detection.
- SKT: Scam Bank Guard (behavior-based detection).
- KT: Real-time call detection and alerts via Whowho app.

o **Challenges:**
- Attackers freely exploit new technologies.
- Defenders lag due to legal and policy constraints.

o **Proposals:**
- Enhance detection and watermarking of synthetic voices
- Strengthen cross-platform/telecom cooperation

	- Enforce labeling of AI-generated content - Expand user security training. **Financial Sector Perspective (Kang Dae-gyu)** o **Role of FSI:** Operates ISAC, issues threat intelligence reports, and coordinates responses. o **Voice Phishing Response:** - Detects phishing sites/malicious apps (linked with KISA) - Anomaly detection via FDS, and runs cooperative information-sharing systems across banks, law enforcement, telecoms, and security firms. o **Threat Intel Cases:** - Shadow Voice (organization tactics) - Operation Black Echo (modular attacks) - Operation Midas (fraudulent trading scams). o **New Fraud Tactics**: NFC relay payment fraud, ATM NFC withdrawal scams. o **Key Message**: While technology and institutional cooperation are critical, the ultimate safeguard is user awareness. **Forensics and Law Enforcement Perspective (Jung Yong-uk)** o **Forensic Experience:** 25 years in digital forensics; recent surge in Telegram investment scams. o **Cases**: Use of forged IDs and company info, long-term investment inducement — losses ranging from tens to hundreds of billions of KRW. o **Challenges:** Recovery and investigations often prolonged (up to 8+ years). o **Cultural Reflection:** Voice phishing groups depicted in popular films (Citizen Duk-hee). o **Legislative Developments:** - EU AI Act: Risk-based regulation, bans in 8 areas. - U.S. AI Bill of Rights (2024). - Korea's AI Basic Act (2025 enactment, 2026 enforcement; details still lacking). o **Proposals:** - Warn against blind trust in AI (risk of inaccurate data/errors) - use predictive policing systems (e.g., Pre-COPS) - ensure institutional management to balance AI's opportunities and risks.
General review	This session was highly significant in shedding light on the real threats posed by AI-driven voice phishing and the resulting challenges to the digital trust system from a multi-dimensional perspective. It was positively noted

	that the discussion went beyond purely technical issues to incorporate insights from psychology, finance, law enforcement, and international cooperation, demonstrating the necessity of a multi-stakeholder approach. In particular, the presentation and panel discussion effectively raised public awareness by providing concrete examples of deep voice and deepfake cases, mechanisms of psychological manipulation, threat intelligence from the financial sector, and the urgent need for institutional responses. It was also noteworthy that, despite being led by students, the session reflected meticulous research and careful preparation. Overall, the session was meaningful in posing the fundamental question of how trust can be redesigned in the age of AI. It is expected that further academic research and follow-up discussions will help develop more concrete and actionable solutions.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Hee-woo (Korean Progressive Network Jinbonet)

Session Title	**Military Artificial Intelligence Threatening Human Rights and Peace: Is This Acceptable?**			
Date & Time	July 3, 2025 (Thursday), 16:20 – 17:50		Venue	Gwanggaeto Hall B1, Sejong University
Participants	Moderator	Ko Ah-chim (AI Ethics Letter)	Format	Open Discussion
	Panelists	Park Hae-ryong (Director, Security Technology Division, Information Security Industry Bureau, KISA)	Jeong Ya-ping (Palestine Peace Solidarity)	
		Kim Yoon-myung (Director, Digital Policy Research Institute)	Kate Sim (Organizer, No Tech for Apartheid campaign; part of the Fired Fifty for Google 416 action in 2024; Organizer, Tech Workers Coalition)	
		Kim Han Min-young (Amnesty International Korea)		

Summary	Session 7 of the 14th Korea Internet Governance Forum (KrIGF) addressed the threats posed by military artificial intelligence (AI) to human rights and peace. It was highlighted that AI applications in the military domain have evolved beyond auxiliary functions to directly engaging in surveillance, target identification, simulations, battlefield command, and even lethal decision-making. Park Hae-ryong (KISA) introduced cases of AI military applications such as autonomous lethal drones, unmanned tanks, and AI-based surveillance and analysis systems, raising concerns about civilian casualties and loss of human control. He emphasized the need for safeguards such as “Meaningful Human Control (MHC)” and civilian-area avoidance algorithms. Kim Yoon-myung (Digital Policy Research Institute) defined the greatest challenge of autonomous weapons as a “responsibility vacuum,” noting that accountability cannot be clearly assigned to developers, commanders, or operators, and criticizing the recurring regulatory exceptions granted under the banner of national security in both domestic and international law. Lee Hwa-young (Cyber Security Research Institute) elaborated on the concept of AI agents and the “Defense Metapower” strategy, citing the Israel–Hamas conflict as an example where reliance on AI intensified civilian massacres. He proposed the establishment of safety measures such as a “cyber AI kill switch” to address malfunctions and hacking risks.

	Kim Han Min-young (Amnesty International Korea) stressed that autonomous weapons directly threaten the rights to life and dignity, calling for a total ban on anti-personnel autonomous weapons and the adoption of binding international treaties. Jeong Ya-ping (Palestine Peace Solidarity) described how Israel has deployed AI programs such as Lavender, Habsora, and Where's Daddy? in its occupation of Palestine, resulting in indiscriminate civilian attacks. She labeled this the "world's first AI-powered genocide" and underscored the complicity of big tech companies. Kate Sim (Tech Workers Coalition) criticized Google and Amazon's Project Nimbus contract with the Israeli government, arguing that big tech firms are directly contributing to occupation and genocide. She also shared how workers' protests led to internal censorship and mass dismissals, calling for international solidarity and resistance. The discussion focused on the effectiveness of "Meaningful Human Control (MHC)," the limitations of international treaties, and the potential role of civil society. It reaffirmed that military AI is not merely a security issue but an urgent challenge that undermines the foundations of human rights, international law, and democracy.
General review	This session clearly revealed that military AI is not merely a technical issue but a complex intersection of international politics, corporate accountability, and human rights realities. The case of Palestine underscored that the risks are not abstract but represent an ongoing "AI-enabled genocide," which heightened the urgency of the discussion. The examples of big tech complicity and internal worker resistance further demonstrated that the problem of military AI extends beyond states, affecting workers and citizens alike. Participants' remarks highlighted how military AI is already being deployed by exploiting gaps in international norms and legal frameworks, reaffirming the pressing need for international solidarity and resistance to safeguard human rights and democracy.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Jeon Sun-min

Session Title	**WSIS+20 and Future Directions for Domestic and Global Internet Governance**			
Date & Time	July 3, 2025 (Thursday), 16:20 – 17:50		Venue	Gwanggaeto Hall B1, Sejong University
Participants	Moderator	Park Min-jung (Korea Information Society Development Institute, KISDI)	Presenter	Jeon Sun-min (Korea Information Society Development Institute, KISDI)
	Panelists	Jeon Young-gyun (Kakao)		Oh Byung-il (Korean Progressive Network Jinbonet)
		Song Hye-in (Korea Internet & Security Agency, KISA)		Yang Ji-su (Institute for Social Sciences, Ewha Womans University)
		Jung Da-hyun (Ewha Womans University)		

Summary	**<WSIS Achievements and Limitations>** o **(Achievements)** -Since the Geneva (2003) and Tunis (2005) summits, WSIS presented the vision of a people-centered, inclusive, and development-oriented information society. -Established 11 action lines that laid the foundation for ICT use, including infrastructure, education, security, cultural diversity, and ethical principles. -Institutionalized multistakeholder dialogue platforms such as the Internet Governance Forum (IGF) and WSIS Forum. -Linked ICT explicitly to the SDGs, positioning it as a key enabler for sustainable development. o **(Limitations)** -Remains bound by frameworks designed in the early 2000s, insufficiently reflecting new agendas such as AI, data governance, and digital public goods. -Lacks enforcement capacity, with consensus-driven structures producing no binding norms or outcomes. -Digital divide efforts remain declaratory, with inadequate financial and capacity-building mechanisms. -While developing countries and civil society are included, they face limits in securing real influence and resources.

	<Key Issues and Challenges> o **(Digital Divide)** One-third of the global population remains offline; shift needed toward “Meaningful Connectivity” beyond basic access. o **(Financial Mechanisms)** Calls for sustainable ICT funds or global financing mechanisms. o **(Governance Structures)** IGF valued as a dynamic space for civil society and emerging issues, yet criticized for lack of concrete outcomes. WSIS provides a cooperative dialogue framework but is slow to adapt to technological change. Ongoing tension between Multistakeholderism (MSM) and Multilateral (government-led) cooperation models. o **(Emerging Technologies)** Increasing need to address AI, data governance, privacy, cybersecurity, and environmental impacts. **<Tasks for Korea>** o **(Strategic Mediator Role)** Korea could position itself as a mediator and agenda-setter within the multistakeholder model. o **(Financial Contributions and ODA Linkages)** Align ODA/KOICA strategies with efforts to bridge the ICT divide, enhancing Korea’s credibility and status internationally. o **(Broader Participation)** - Academia: Develop indicators and evaluation frameworks to contribute substantively. - Civil Society: Raise issues of privacy, AI, and human rights within IGF and WSIS platforms. - Youth: Expand opportunities for Korean youth to participate more actively in global discussions.
General review	o It was noted that while WSIS has provided the fundamental framework for global digital cooperation over the past 20 years, it now faces structural limitations in keeping pace with today’s rapid technological advances and growing competition over digital norms. o The upcoming WSIS+20 review process should therefore go beyond merely assessing past achievements and serve as an opportunity to address pressing issues such as emerging technology governance, bridging the digital divide, and establishing sustainable financial mechanisms. o Korea is expected to strengthen its international influence by positioning itself as a mediator and value-based leader — balancing multistakeholder and intergovernmental cooperation, linking ODA and funding to support developing countries, and expanding the participation of academia, youth, and civil society.

Workshop Session Results Report of the 2025 Korea Internet Governance Forum (KrIGF)

Author: Kim Ki-young, Do Ga-young

Session Title	**In an Age of Anxiety, Is Your Information Safe? – The SKT SIM Data Breach and Ontological Security**			
Date & Time	**July 3, 2025 (Thursday), 16:40 – 18:00**		Venue	**Gwanggaeto Hall B1, Sejong University**
Participants	Moderator	Min Byung-won (Professor, Ewha Womans University / Academia)	Presenters	Kim Ha-eun (Ewha Womans University / Academia) Kang Se-eun (Ewha Womans University / Academia) Kim Ki-young (Ewha Womans University / Academia) Do Ga-young (Ewha Womans University / Academia) Lim Kyu-ri (Ewha Womans University / Academia)
	Panelists	Shim Dong-wook (Director, KISA / Public Sector)		
		Lee Jin-gyu (Executive Director, Naver / Industry)		
		Kim Hyun-yi (Attorney, Shin & Kim LLC / Legal Sector)		

Summary	**1. Concept and Characteristics of Anxiety** In April 2025, SKT experienced a massive leak of subscribers' USIM information. This incident caused psychological shock and anxiety among countless users, and SKT's follow-up response further amplified users' anxiety. Such data-leak incidents continue to occur in Korean society today, inevitably heightening public anxiety. Anxiety is a crisis emotion that appears in the absence of a clear, tangible object, and it is different from fear. Anxiety is characterized by uncertainty and persistence. Because the source of anxiety is unclear and the feeling arises from the mere possibility that something might happen, it is experienced as vague. Anxiety also exists continuously within the flow of time that frames an individual's life and death. A feeling similar to anxiety is fear. Unlike anxiety, however, fear has a clear object—an "enemy." The SKT USIM information leak can be seen as a case where anxiety and fear coexist. The mere fact that USIM information was leaked evokes fear in users—that feeling is fear. At the same time, users also feel anxiety due to the possibility of secondary harm, such as misuse of the leaked information. Even in the absence of secondary harm, the uncertain possibility produces a "fear of fear." The emergence of anxiety is a problem that touches on human existence. Existence refers to our very being and to questions of life and death. To protect this existence, one's personal identity—an account of "who am I?"—plays an important

role. The continuity and stability of identity provide trust and confidence to individuals living unpredictable lives. When that continuity and stability are lacking, individuals feel existential threat, and anxiety is triggered.

2. Identity and Ontological Security

Ontological security is a state in which an individual maintains internal consistency regarding their identity and stably possesses the sense that "I am still myself." When ontological security is secured—i.e., when personal identity is stably maintained and no existential threat is felt—the individual does not feel anxiety. This concept of security differs from the physical security emphasized in society to date. Whereas physical security refers to safety from tangible threats such as weapons, war, and crime, ontological security refers to safety from abstract threats to identity.

Because anxiety has the property of persistence, it cannot be completely eliminated. Accordingly, over the course of life, an individual cannot fully secure ontological security. Rather, the individual resides within a process of continuously pursuing ontological security and managing anxiety. From this perspective, anxiety is not merely an emotion but something that must be continually controlled and managed. Anxiety should be considered not only an individual matter but one that merits attention at the level of society as a whole.

As technology becomes more advanced, personal identity is established not only in the physical world but also in cyberspace. Because information in cyberspace constitutes elements that form personal identity in modern society, the USIM information leaked in the SKT incident can also be seen as part of identity. Therefore, the SKT USIM information leak threatens the stability of identity and, further, represents an existential threat to users and a crisis for ontological security.

3. Analysis of the SKT USIM Information Leak

1) Problems in SKT's Response and the Amplification of Anxiety

At exactly 18:00 on April 18, 2025, anomalous traffic was detected in SKT's HSS at the Network Infrastructure Center. Around 16:40 on April 20, SKT reported the leak to KISA. On the 22nd, SKT officially confirmed the USIM information leak and began its response.

This response process did not relieve users' anxiety; rather, it amplified it. The first problem that heightened anxiety was the more-than-40-hour delay between intrusion detection and reporting to KISA. This violated the legally required 24-hour reporting period and, even if not an intentional cover-up, showed that the organization's crisis-response system was neither swift nor proactive.

The second problem was the vulnerability of the HSS, a core authentication component of the telecommunications network. Given that SKT's network serves a significant portion of the public, SKT's security level and response fell far short of what is expected for telecommunications equipment at the level of national critical infrastructure.

Third was the inadequacy of countermeasures against the USIM information leak. Amid user confusion, SKT did not accurately notify the data subjects whose USIM information had been leaked. The measure prepared to prevent damage—USIM replacement—also proved ineffective due to stock shortages.

Finally, there was a lack of accountability and transparency stemming from insufficient communication about the incident. Although the SKT CEO issued an official apology, users were not clearly informed of the cause of the incident, any disciplinary actions against those responsible, or follow-up measures. Because of these four problems, user trust in SKT declined sharply, and anxiety grew as the response process went on.

2) Analysis from the Perspective of Ontological Security

In the SKT USIM information leak, users experienced existential anxiety and felt confusion about their identity. Left for a long period without clear explanations from SKT or the government regarding whether their information had been leaked, who held their data, or their risk of harm, users lost a sense of control over their very existence—beyond mere inconvenience. The reporting delay undermined users' timely awareness of the situation, eroding trust in companies and institutions. The absence of clear guidance about harm further deepened confusion and anxiety over whether they had been affected and how to respond, leading to feelings of disappointment and betrayal. These emotions manifested in concrete behavioral changes such as lawsuits and service termination.

The SKT incident was a complex event involving both external intrusion (hacking) and structural weaknesses in internal systems. Users first suffered an immediate emotional shock—fear—upon learning that an external hack had occurred. Then, as information about the cause and responsibility was not disclosed, anxiety arose from the recognition that the state, companies, and institutions they trusted had failed to protect "me," producing a second emotional shock. In short, users were exposed to two shocks: the impact of an external attack and the loss of trust in internal systems—going beyond a merely technical breach.

Today, personal identity is composed not only of information such as one's name or photograph but also of fragments stored on the USIM, such as phone numbers, authentication keys, and the IMSI. USIM data goes beyond mere technical data that proves "me" in cyberspace; it is a core element that socially verifies "me" and constitutes everyday identity. However, such information is not held by the individual alone; it is stored within corporate systems. Therefore, if corporate security is compromised, there arises a possibility that others may hold an individual's identity—an impact that goes beyond inconvenience and becomes a shock to one's very existence.

In modern society, identity-linked data fragments are not held exclusively by individuals but depend on corporate information infrastructures. As a result, individuals possess incomplete authority to prove themselves, which leads to a continual loss of control and triggers ontological anxiety stemming from the inability to have one's identity verified. This anxiety further connects to identity confusion and ultimately expands into a crisis of ontological security.

A crisis of ontological security cannot be resolved merely by eliminating physical threats. That is, even if physical security is restored, confusion or loss surrounding personal identity does not automatically disappear. Although SKT took technical and physical measures after the incident to restore and strengthen its security systems, such measures do not relieve users' internal anxiety; the absence of ontological security thus continues. As users' anxiety persists and intensifies, their confidence in their personal identity gradually diminishes, placing ontological security itself in a fundamentally threatened state.

The SKT USIM information leak shows that ontological security is a palpable, real-world crisis in the lives of modern people who depend on digital infrastructure. It also suggests the need for social responses and institutional design that go beyond the restoration of physical security to address crises of human identity.

4. Domestic and International Legal/Institutional Frameworks on Identity

1) Domestic Legal Framework

With respect to identity, Articles 1 and 4 of Korea's Personal Information Protection Act (PIPA) state the Act's purposes and the rights it guarantees, showing on the surface that domestic law considers individual self-determination and dignity. In actual legal proceedings, however, abstract elements such as "dignity," "freedom," and "rights" are not readily apparent.

When determining liability for damages in data-leak cases, legal processes focus on establishing tangible harm and its scope rather than on conceptual elements such as ontological security or anxiety. Criteria for determining a company's liability—such as identifiability of the data subject, the possibility of third-party access, and the extent of data dissemination—are largely grounded in physical facts. Subjective and existential elements—including the data subject's anxiety, threats to identity, and loss of self-control—are either not considered or are difficult to prove and thus are not substantially reflected in legal judgments.

As seen in Supreme Court precedents indicating that mental damages are difficult to recognize solely on the basis of a data leak, emotional and existential harms that are hard to prove as concrete disadvantage or rights violations are, in reality, difficult to recognize as legal damages. In foreign case law on issues similar to domestic data-leak incidents, the United States and Japan tend to recognize anxiety itself as damage more readily than Korea does and show a broader willingness to protect victims' psychological suffering.

2) U.S. Personal Data Protection System

The U.S. operates a decentralized, sector-specific regulatory approach. There is no comprehensive, general law; instead, there are separate regulations by state and by industry. The most representative example is California's Consumer Privacy Act (CCPA), which is being strengthened over time. Even under a fragmented regime, personal data protection functions robustly due to legal, social, and economic factors in the U.S. Civil litigation over rights violations is active, so companies, fearing potentially massive liability and reputational damage, tend to voluntarily operate strict privacy policies. Strong sectoral rules, innovative legislative competition among states, market and consumer pressure, and regulatory enforcement together form multi-layered constraints that powerfully induce companies' "voluntary regulation."

3) European Personal Data Protection System

The European Union regards personal data not merely as "privacy" but as a citizen's right and a condition of democracy, and has developed the strongest protection regime. The representative framework is the GDPR, whose five core principles include purpose limitation, data minimization, clarity of consent, guarantees of access/rectification/erasure/portability, and the right to an explanation regarding automated decisions. The core of European policy is "guaranteeing individuals' control over their data," and GDPR strictly and meticulously regulates such control through clear consent and rights to object to automation.

In France, specifically, the independent authority CNIL enforces GDPR. In 2019, CNIL imposed a €50 million fine on Google and, more recently, has led on algorithmic transparency and biometric regulation in the AI era. Following a 2022 medical-data breach at the French health authority, France enacted a data algorithm transparency law that enshrines citizens' right to explanations of automated decision structures. It also works to raise public awareness through mandatory data-rights education in schools and local bodies and by using citizen panels to shape public policy.

4) Implications

Although Korea's personal data protection framework resembles Europe's, the realization of individual data-control rights remains weak. Korea therefore needs to build a strategy to strengthen the law based on ontological security and identity-protection systems. First, to reflect victims' psychological suffering from data leaks, criteria for recognizing mental damages should be broadened and refined. In addition, social conditions that foster a shift in individuals' self-perception as data owners and that elevate the recognized importance of personal data must be created.

5. Conclusion: The Need for an Integrated Approach to Guarantee Ontological Security

The SKT USIM information leak illustrates a crisis of ontological security triggered by uncertainty and identity anxiety. As seen in the response to this incident, current government and corporate measures focus on physical restoration—security reinforcement and technical upgrades—while paying insufficient attention to victims' existential anxiety and identity damage.

To resolve this crisis, an integrated approach is needed at the levels of individuals,

	companies, and the state. Individuals lack substantive control over the collection, processing, and distribution of their data, and society is poorly prepared, socially and emotionally, to manage identity crises and anxiety. Repeated data-leak incidents have also dulled individuals' sensitivity to leaks. Recognizing the seriousness of data violations is a basic step in response; hence, there is a need to build a socio-cultural environment that recognizes the importance of personal data through curricula for civic education, public campaigns, and platforms for public communication. At the same time, legal and institutional reforms are needed to protect individuals from the perspective of ontological security so that subjective and existential harms can be reflected. Beyond efforts to codify substantive rights for identity restoration, institutionalizing recovery procedures centered on data subjects could achieve identity restoration that purely physical responses cannot. Furthermore, transnational efforts are essential. Because data circulates across borders via the internet, no single country can resolve the crisis of ontological security alone. Therefore, cross-border cooperation is indispensable—concluding and strengthening multilateral/bilateral agreements on personal data protection, expanding the roles of international organizations, and establishing oversight mechanisms for global big-tech companies.
General review	This discussion is positively evaluated for offering a new perspective by using the SKT USIM information leak as a starting point to interpret personal data breaches not merely as technical or security issues but as a crisis of "ontological security." It pointed out that victims' existential anxiety and identity damage cannot be resolved through physical restoration measures alone, and impressively proposed multi-layered responses—integrated action at the levels of individuals, companies, and the state; enhancement of civic awareness; legal and institutional supplementation; and transnational cooperation. Through the panel debate, concrete and practical discussions were also held, including attempts to connect the concept of ontological security to damages and liability in legal systems, reorienting the use of administrative fines, designing UX-based procedures to alleviate anxiety, and emphasizing the importance of social consensus. However, the depth and persuasiveness of the discussion could be further strengthened by adding a more detailed and balanced comparison between foreign and domestic legal regimes. It is expected that this will be supplemented by additional student research going forward.