Network Security and Resilience Risks: The Korean Case

Seongcheol Kim, Ph.D

Professor, School of Media and Communication
Director, Center for ICT and Society
Director, Smart Media Service Research Center

Today's agenda

Center for ICT & Society
KOREA UNIVERSITY

Four important questions

1. **Why network security and resilience risks matter in Korea?**
2. **What happened in (South) Korea?**
3. **How has Korea responded to the critical events?**
4. **So what? What can Canada and others learn from the Korean case?**

Center for ICT & Society
KOREA UNIVERSITY

1. Why network security and resilience risks matter in Korea?

Korea is a divided nation

Korea has been divided into North and South since 1945.
The Korean War was fought between North Korea and South Korea from 1950 to 1953.

- While the fighting ended, **technically the Korean War never ended. There is no formal peace treaty.**
- **Continuous conflicts from the division**
  - **Military tension**: The ongoing military standoff between North and South Korea consistently **poses a security threat.**
  - **Cybersecurity threats**: **North Korea possesses substantial cyber-attack capabilities.** These attacks threaten national information security systems and can cause economic and social disruptions.
  - **Political instability**: **The division can lead to domestic and international political instability**. Sudden policy shifts or leadership changes in North Korea can directly impact inter-Korean relations.

(Source: https://www.scienceabc.com/social-science/how-did-japan-losing-world-war-ii-contribute-to-the-split-of-korea.html)

Korea’s geopolitics is unique

Korea's geopolitical significance is profoundly influenced by its strategic location, surrounded by major powers such as China, Russia, and Japan.

- Being located at the crossroad of a continent and an ocean, **geopolitics for Korea has been the source of both blessings and curses.**
- **South Korea is currently facing growing rivalry between China and the United States.**
- **Proximity to key players**: **South Korea's proximity to China, Russia, and Japan places it in a unique position** to influence and be influenced by the political and economic dynamics in the region.
- **Economic interdependencies**: South Korea is deeply integrated into the regional economy, particularly through trade and technology exchanges with China and Japan.

(Source: https://asiasociety.org/switzerland/events/korean-peninsula-and-changing-global-security-landscape-Zurich)

Korea is one of ICT powerhouses

South Korea is one of the global ICT leaders with most advanced digital infrastructures.

Households with Broadband Internet Access at Home (2022)

1st	Korea	99.96%
2	Norway	99.01
3	Netherlands	98.28
4	Luxembourg	97.64
5	Finland	97.59
6	Spain	96.08
7	Denmark	95.16
8	Belgium	94.44
9	Sweden	94.33

High-Speed Internet Penetration Rate (2022)
*Based on fiber-optic cable

1st	Korea	87.31%
2	Japan	83.99
3	Spain	81.22
4	Sweden	79.56
11	Finland	61.73
14	France	51.36
28	Canada	25.94
29	Australia	23.97
32	US	19.89
35	UK	8.60

ICT Infrastructure (2022)

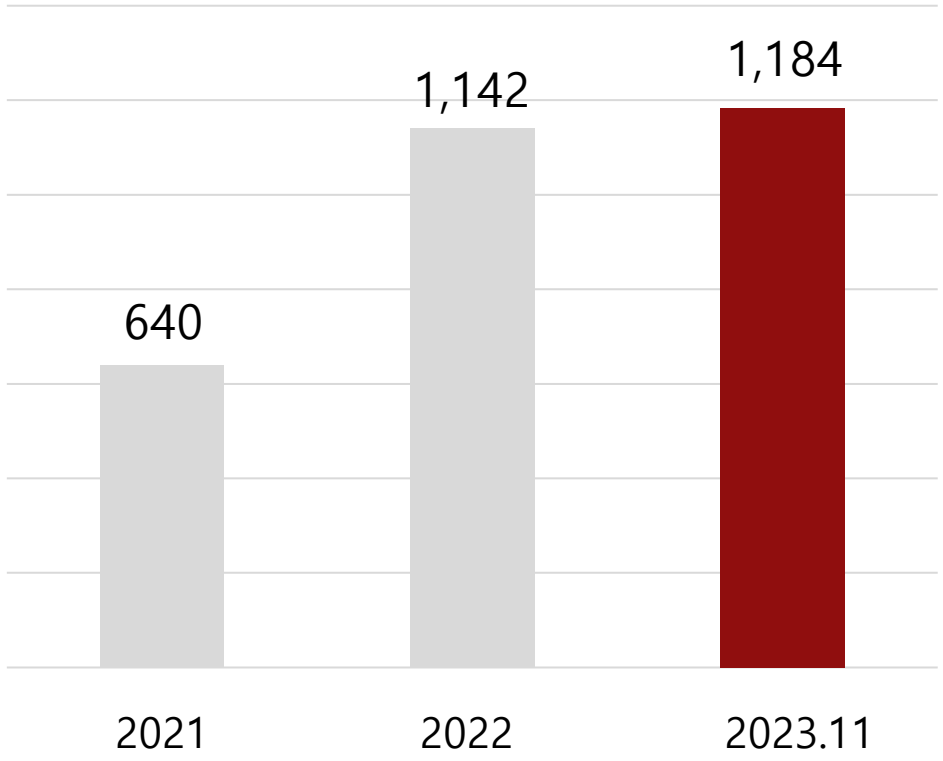
1st	Korea
2	UK
3	Denmark
5	Finland
6	Singapore
7	US
13	UAE
14	Japan
18	France
20	China

(Source: https://www.investkorea.org/ik-en/cntnts/i-299/web.do;
Households with Broadband Internet Access at Home (OECD, 2022); ICT Infrastructure (WIPO The Global Innovation Index 2022)

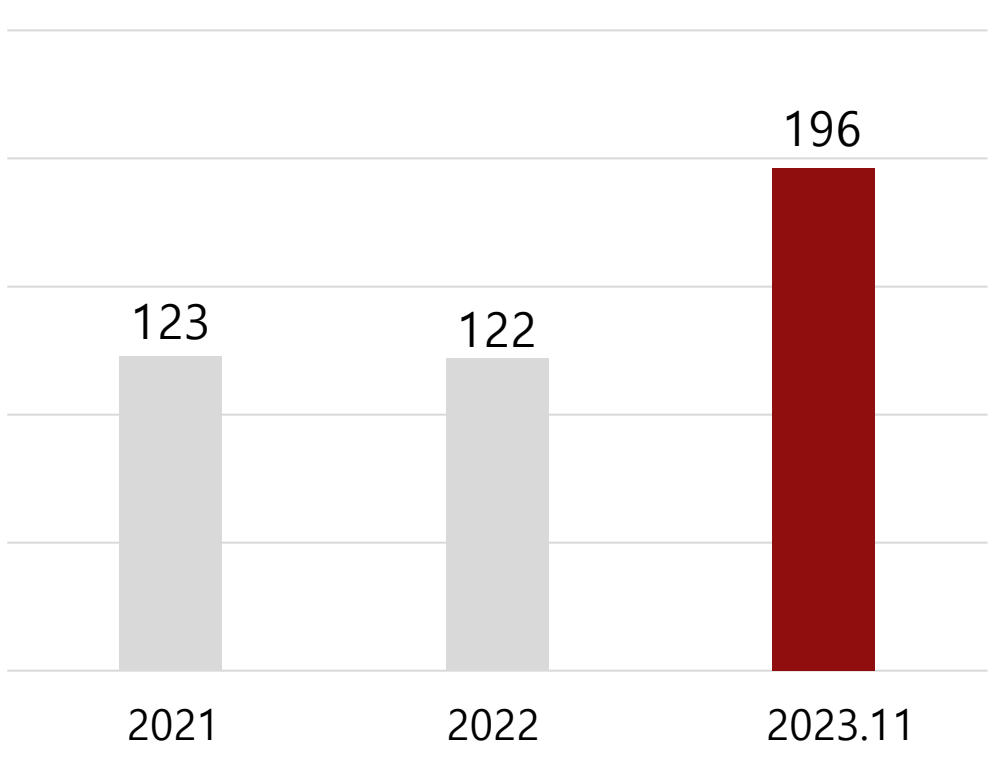
The cyber threats are significant in Korea

Number of cyber incidents against South Korea have been growing.

Number of breach reports in South Korea



Number of DDos attack reports in South Korea

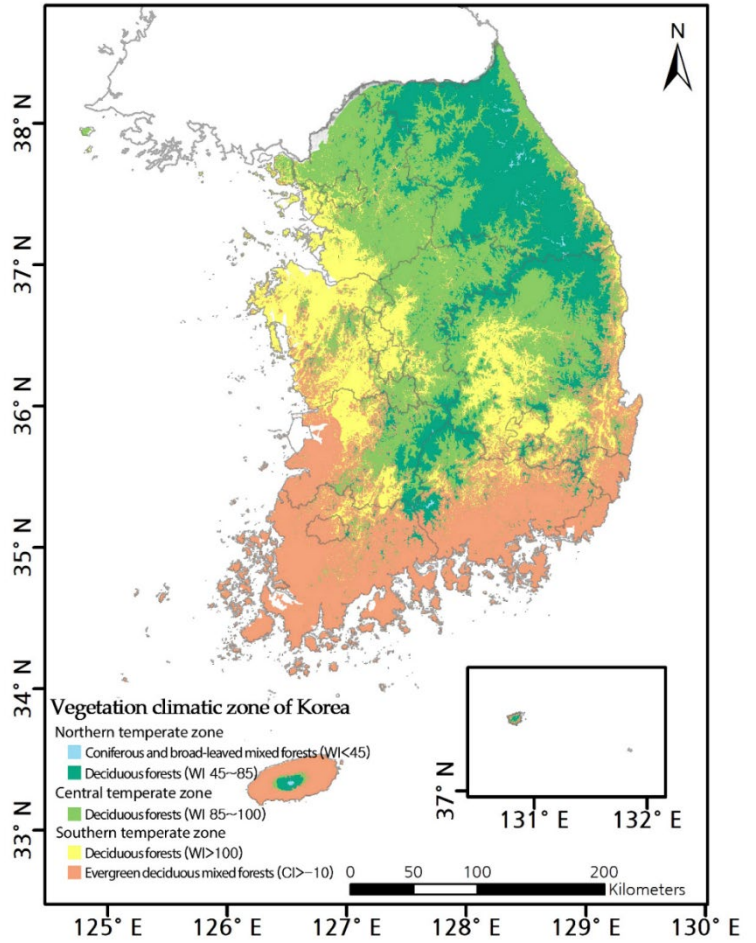


(Source: Cyber threat trends report 2023 / Second half (KISA: Korea Internet & Security Agency, 2024)

Korea is vulnerable to the impacts of climate change

South Korea is already experiencing the effects of climate change, including rising temperatures, more extreme weather events, and rising sea levels.

- With more than **60% of South Korea's land covered by forests**, Korea experiences frequent forest fires, with **562 forest fire events** burning an average of 1863 hectare annually **over the last 5 years**.
- **Warm monsoon climate leads to great seasonal climate variation.**
  - The wind blowing from the north-east continent becomes very dry as it passes over the mountain range, causing **large-scale wildfires** in the east coastal region.
- **Dry weather continues from winter to spring.**
  - While more than 60% of the 1200 mm of annual precipitation occurs during the hot rainy summer season.

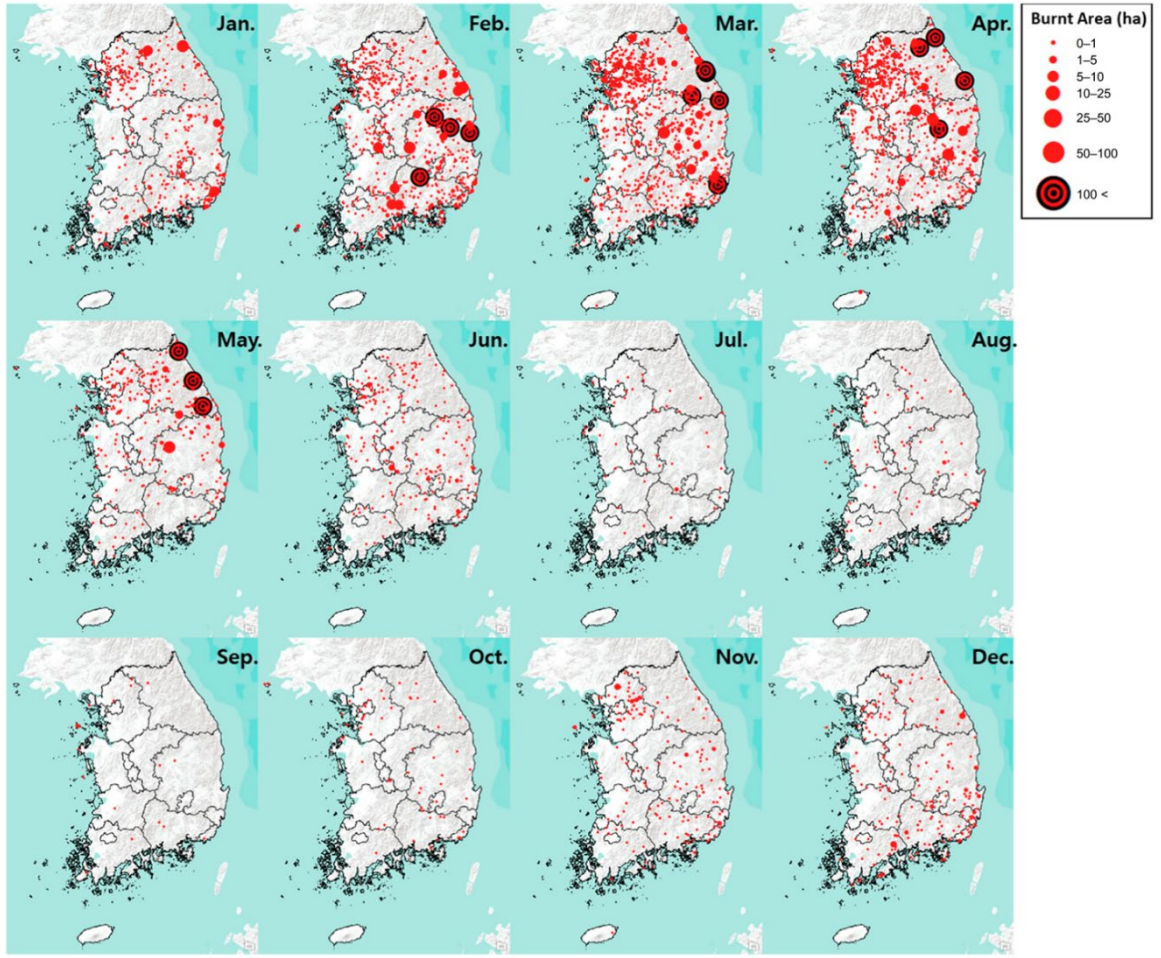


(Source: Jo, H. W., Krasovskiy, A., Hong, M., Corning, S., Kim, W., Kraxner, F., & Lee, W. K. (2023). Modeling Historical and Future Forest Fires in South Korea: The FLAM Optimization Approach. *Remote Sensing, 15*(5), 1446.)

Fires in Korea are increasing

The frequency and scale of forest fires in South Korea are expected to increase due to climate change.

- In South Korea, **most forest fires occur from February to April due to a combination of climate (dry, warm weather) and human factors**, especially **near the Seoul** and south-eastern metropolitan areas.
- The figure displays the frequency and scale of forest fires in South Korea from January 2016 to March 2022.



(Source: Jo, H. W., Krasovskiy, A., Hong, M., Corning, S., Kim, W., Kraxner, F., & Lee, W. K. (2023). Modeling Historical and Future Forest Fires in South Korea: The FLAM Optimization Approach. *Remote Sensing, 15*(5), 1446.)

Center for ICT & Society
KOREA UNIVERSITY

2. What happened in (South) Korea?

More attempts of cyber attacks by foreign sources

North Korea accounted for 80% of those attacks, and China, 5%.

- According to the National Intelligence Service**, cyber attacks against the public sector increased by 36% overall 2023 compared to 2022.**
  - **Chinese attacks tended to inflict more severe damage than North Korean ones.**
  - One survey, conducted in 2023 by cybersecurity firm Humanize Security, paints **a picture of North Korea's cyberwarfare capabilities. The North came in 7th.** The U.S. topped the ranking, followed by China, Russia and the United Kingdom. South Korea is not included in the world's top 10 countries list with the most powerful cyberwarfare capabilities. The survey is based on the National Cyber Power Index.
- **North Korea appears to be behind the hacking of a presidential official's email account in November 2023**
- **The Korea Satellite Operations Center was hacked in December 2023**
  - A breach of the Korean Satellite Operations Center **by North Korean operatives** could endanger a wide range of sensitive data, including security, economic, and environmental information, gathered by South Korea's Multipurpose Satellites.
- **North Korea-linked hacking groups are increasing their use of Russia-based exchanges known to launder illicit crypto assets. This convergence raises national security concerns.**

Cyberattack targeted the 2018 Pyeongchang Winter Olympics

A cyberattack targeted the 2018 Pyeongchang Winter Olympics' critical IT infrastructure

- **On February 9, 2018, at 8:00 PM, during the Pyeongchang Olympics' opening ceremony, a cyberattack targeted the event's critical IT infrastructure to cause widespread disruption.**
- **The organizing committee recovered within 12 hours**. Evidence suggested that a Russian hacking group was behind the attack, possibly motivated by a doping scandal that led to restrictions on Russian athletes. Russia denied any involvement.
- Despite suspicions of Russia's cyberattack before the opening of the 2018 Pyeongchang Winter Olympics, **South Korea reportedly did not participate in public attribution or criticism**, despite demands from allies such as the U.S. and the U.K.

The leak of LGU+ customer information

LGU+, a Korean telecom company, suffered a cyber hack that leaked the personal information of 290,000 customers and DDoS attack.

The leak of LGU+ customer information	
November 2022	• The Customer Authentication System (CAS) was hacked. • Mobile phone numbers, names, addresses, dates of birth, email addresses, IDs, USIM numbers, and 26 other data items were leaked.
10 January 2023	• LGU+ noticed the leaks from **the posts on the dark web selling customer data**. • LGU+ announced that 180,000 customers' data were leaked.
3 February 2023	• LGU+ announced a corrected **total of 290,000 were leaked** (with an additional 110,000).

Timeline and duration of disruption from DDoS attack		
29 January 2023	• 02:00 • 17:00 • 23:00	63 minutes
4 February 2023	• 16:57 ~ 17:40 • 18:07 ~ 18:23	59 minutes

- **Insufficient investment in information security in LGU+** was pointed out as the major cause of the problem.

Fire breaks out at Kakao's data center (hosted by SK C&C)

Major services, including the messaging app (KakaoTalk) most widely used in Korea, experienced service disruptions that lasted 127.5 hours before being fully restored.

(15:30, 15 Oct) Kakao's key services have been down.

- **KakaoTalk (Messenger) / MAU (in 2022): 45 million**
- Daum (Portal)
- Kakao mobility (Map/ Navigation / Taxi-hailing etc.)
- Kakaopay (Payment)
- Kakaobank (Bank/Finance)
- Kakaopage/Piccoma (Webtoon)
- Melon (Music streaming)
- Kakaogames (Online game)
- Kakostyle (Shopping)

(15:52, 15 Oct) Initial notification of service down

- First notification from official twitter account

(21:30, 15 Oct) Issue an apology statement

- By Co-CEO Hong Eun-taek & Namkoong Whon

(1:30, 16 Oct) Partial recovery of KakaoTalk

- Notification from official twitter account at AM 2:20

(8:00 16 Oct) Partial recovery of other services

- Kakaopay (Payment)
- Kakao mobility (Map/ Navigation / Taxi-hailing etc.)

Outage at KT' Ahyeon branch in Seoul

The fire started at approximately 11:13 am on November 24, 2018 in an optical cable in an underground tunnel at KT's Ahyeon branch in Seoul, and resulted in a widespread outage of mobile, internet, and IPTV services.

Cause	• **A fire, caused by electrical overheating**, broke out in a small utility tunnel (2m wide, 2.3m high, 112m long) used for installing cables.
Damage	• (Est. material damage) $36.08 million • **210,000 households lost mobile, cable internet, and IPTV services.** • **Police stations faced disruptions in 112 emergency systems and phone services.** • **Hospitals experienced delays contacting the National Health Insurance Service and had telephone issues.** • **13,500 small merchants were vulnerable due to non-functional electronic security systems.** • KT users were anxious, disconnected, and unable to access information or make purchases. • Residents used public phone booths and paid in cash or bank transfers due to system failures. • **20-30% of delivery drivers couldn't work, significantly impacting sales.**
Restore	• Although the fire was extinguished within 10 hours, **it took a week to fully restore communication services.**

Wildfire in Gangwon

A forest fire broke out in Gangwon (Goseong, Gangneung, Injae) in April 2019, consuming at least 235 buildings and forcing over 4,000 people to evacuate from their homes.

- **The fires damaged some cellular base stations and cables belonging to SKT (2G, 3G, LTE) and KT (3G and LTE).**
  - LG U+ had damage to its 2G base stations
- **This damage led to communication service disruptions for customers in certain affected areas.**

(Source: https://english.hani.co.kr/arti/english_edition/e_national/888917)

Wildfire in Uljin and Samcheok in March 2022

The Korean government declared a national disaster.
A total of 305 mobile communication base stations and 1,067 wired internet lines were damaged.

- **The fire** spread across more than 6,000 hectares (14,800 acres), **destroyed at least 159 homes and 46 other buildings and prompted the evacuation of more than 6,200 people**.
- **The cables of SKT and the relay stations of LG U+ were damaged.**
  - ➢ KT's facilities did not suffer any significant damage.

(Source: https://www.chosun.com/national/regional/yeongnam/2022/03/04/5O2LF5UJYVACFNFUBTI6NHUSVM/)

Center for ICT & Society
KOREA UNIVERSITY

3. How has Korea responded to the critical events?

Post-Pyeongchang response

Korea founded the National Security Research Institute (NSRI) in 2000.

- **South Korea has not publicly responded to Cyberattack targeted the 2018 Pyeongchang Winter Olympics.**
- **However, Korea urged to bolster defense against evolving cyber threat from outside**
- **Key functions of the NSRI**
  - To research and develop the national security system
  - To research and develop national cyber safety technology
  - To study the national security infrastructure technology
  - To provide technical support for national security
  - To provide technology policy establishment support, train manpower, commercialize technology, and implement projects necessary
- **NSRI has proposed a detailed categorization of response measures to cyberattacks based on the target.**

NSRI's response measures to cyberattacks by target

Target of the response	Response Type	Measures		
Country	Political, economic, and diplomatic response	Military response	Invoking the right of self-defense	
		Counter measures	Non-compliance with obligations under treaties and agreements	
			sanctions conflicting with treaties and agreements	
			cyber operations as countermeasures	
		Retaliatory measures	Severance of normal diplomatic relations	
			economic sanctions	asset freezing
				export and import controls
				remittance regulations
				additional tariffs
				boycotts
				prohibition of international ship insurance
			Travel bans	
			Suspension and blockage of aid	
			Suspension of visa exemptions	

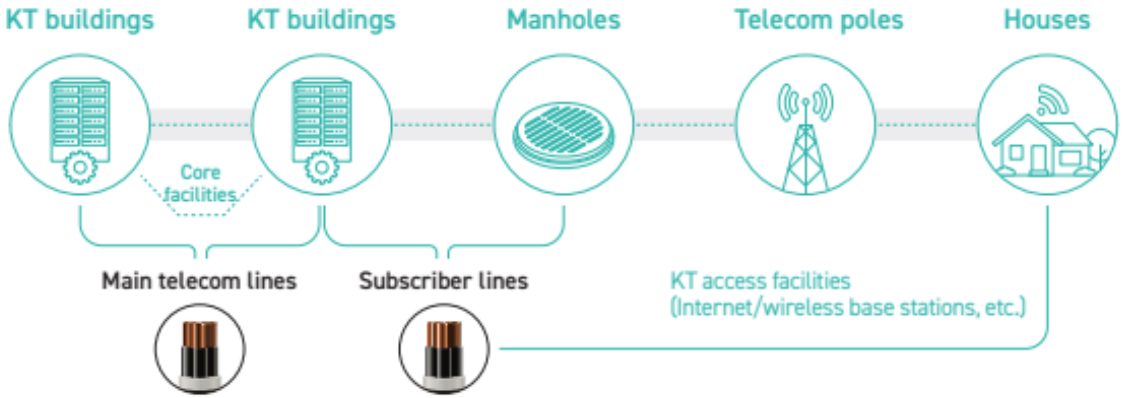
NSRI's response measures to cyberattacks by target

Target of the response	Response Type	Measures	
Country	Political, economic, and diplomatic response	Demanding state responsibility	Cessation and non-repetition of wrongful acts
			compensation
		Other diplomatic measures	Criticism and statements through the media
			official statements by high-ranking government officials
			conclusion of international agreements
			official statements by allied countries
			statements by international organizations
			requests for joint investigations
			political talks
			summoning of diplomats
	Technical response	**Counter-hacking**	gathering information on attackers and attack sites
			measures to stop or interrupt attacks
			measures to neutralize remote access
			measures to destroy leaked information
			infiltrating the attacker's network to delete leaked information
Individuals and groups			Prosecution under domestic law
			Entry ban
			Deportation
			Freezing assets of individuals and groups within the victim country
			Counter-hacking
Countries through which attacks are routed			Request for joint investigation
			Promise to prevent recurrence - Request for capacity building

KT case: Overview

KT, the leading telecom company in Korea, has operated very extensive telecommunication networks.

Status of Communications Facilities



Category	Wireless	Internet	Transmission	Switchboard
Quantity	999,847	591,949	184,953	236,429

Wireless	1,920 5G/LTE/3G core and 997,927 access(DU, RU, relays)
Internet	783 IP core(Kornet, premium, 5G backbone), 591,166 access(OLT, switch)
Transmission	7,320 telecom transmission (WDM, POTN), 177,633 subscriber transmission(MSPP, PTN, etc.)
Switchboard	Switchboard, BcN, VoIP

OSP Facilities

	OSP Facilities				
Telecom buildings	Copper cable	Optical cable	Tunnels	Poles	Manholes
375 stations	321,000 km	917,000 km	280 km	4.83 million	810,000

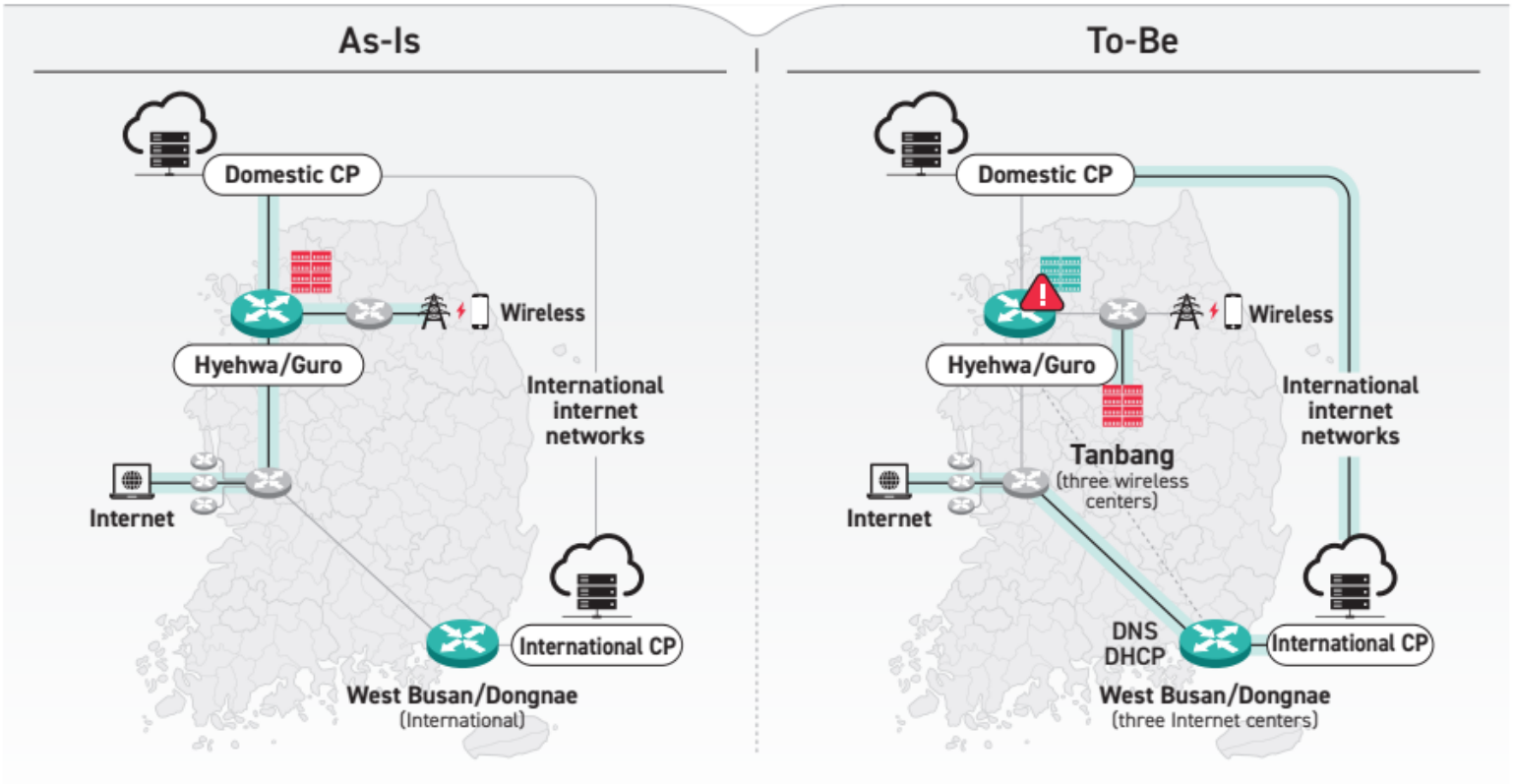
OSP(Out Side Plant) facilities
Basic communications infrastructure such as cable tunnels, poles and manholes, other than communications equipment like base stations, servers, etc.

(Source: KT 2023 ESG report)

KT case: Improvements of network stability

To provide customers with uninterrupted communication services even in the event of a disaster in the Seoul metropolitan area, KT is building three wired and wireless centers in non-metropolitan areas.

Improvements to the Telecommunication Network Structure



*
DNS(Domain Name System) : A system that allows you to translate domain names into IP addresses
DHCP(Dynamic Host Configuration Protocol) : A protocol that provides an IP address to a terminal

(Source: KT 2023 ESG report)

KT case: Telecommunications disaster response system

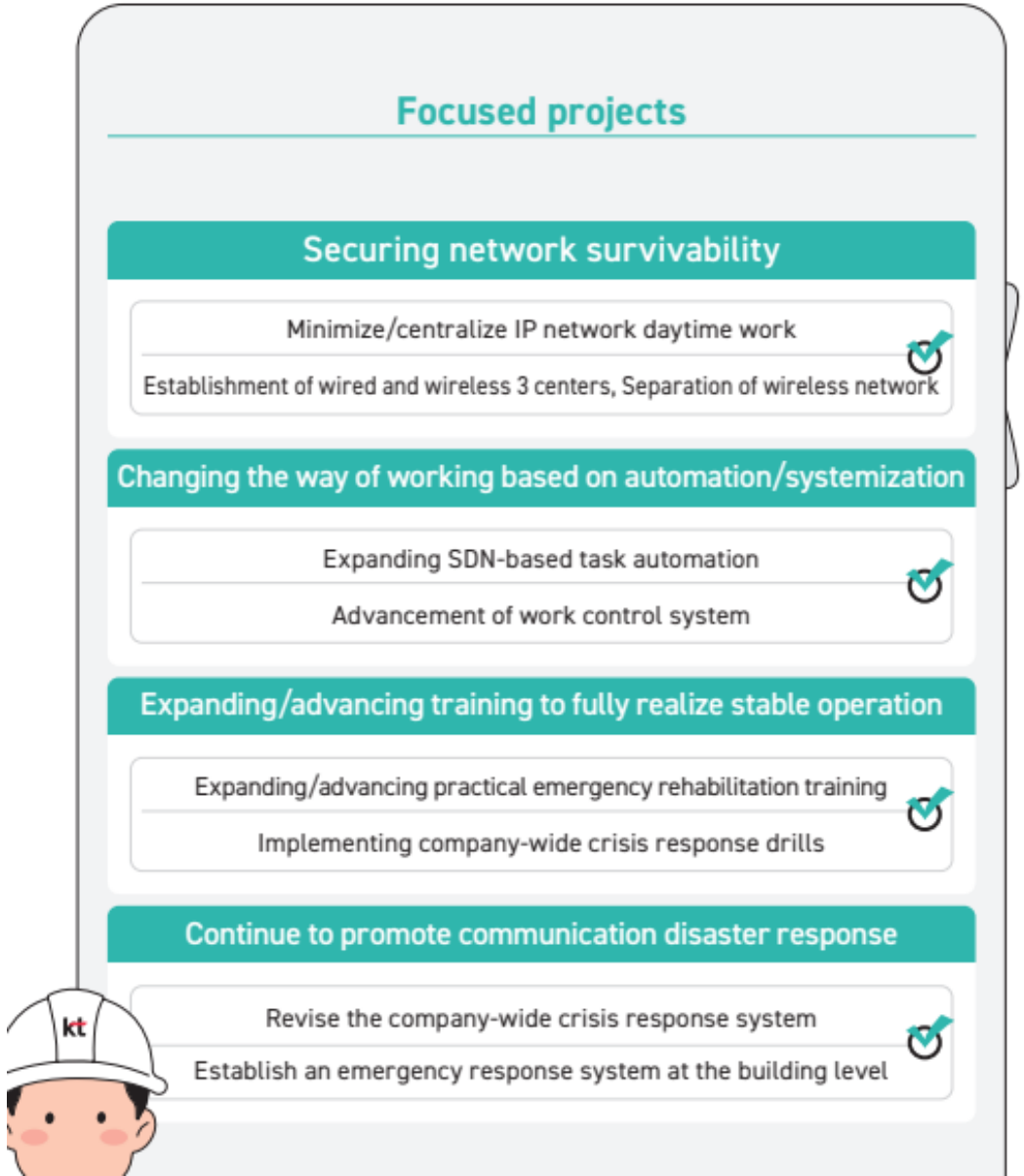
KT operates a company-wide crisis response system.

- **In case of telecommunication disaster or outage, KT should report to the Ministry of Science and ICT within 10 minutes**
- **The Crisis Management Committee is led by CEO.**
- **KT compensates network failures based on the existing terms and conditions.**
  - Mobile, Internet: compensation is applied only for failures that occur for two consecutive hours.
  - Fixed-line, IPTV: compensation is applied only for failures that occur for three consecutive hours.
- **Technical solutions**
  - Emergency roaming service in 30 minutes
  - Public WiFi Emergency in 10 minutes
  - 5G Optical Line Terminal and Moving base stations
  - Smartphone-based USB-tethering payment solution for SME
  - LTE routers
- **ESG activities**

KT case: Company-wide internalization of ‘Basics Must’

The Starting from 2019, KT has been identifying, expanding, and promoting the basics every year since the 2018 Ahyeon fire through the 'Basics First' project

- From 2022, the company-wide 'Basics Must' project has been promoted to ensure that principles take precedence over practices in order to make changes that customers can notice and realize zero accidents.
- In 2023, KT has been continuing its efforts to embody 'Basics Must' to the full extent and realize a year that raises stability, safety, and customer-centricity to the next level.



KT case: Focus on countering DDoS attacks

KT conducts various activities to protect the network-based infrastructure

- KT is the first Korean telecom company to **deploy security equipment in 100% of overseas interconnection network sections** to preemptively block abnormal traffic from both domestic and international sources.
- KT has also **established cyber shelters** to provide seamless and stable services to major domestic companies and national institutions.
- In addition, KT **commercialized the SOAR system to prevent intelligent cyber attacks**, by enabling **the automatic detection of harmful information** using our security infrastructure.
- KT also **conducts diagnoses of security vulnerabilities and hacking simulations** for all infrastructure equipment **on a regular basis**.

Center for ICT & Society
KOREA UNIVERSITY

4. So what? What can Canada and others learn from the Korean case?

Call for “Resilience literacy”

Telecommunication networks are vulnerable. They are not fault-tolerant. They are even exposed to lots of risks.

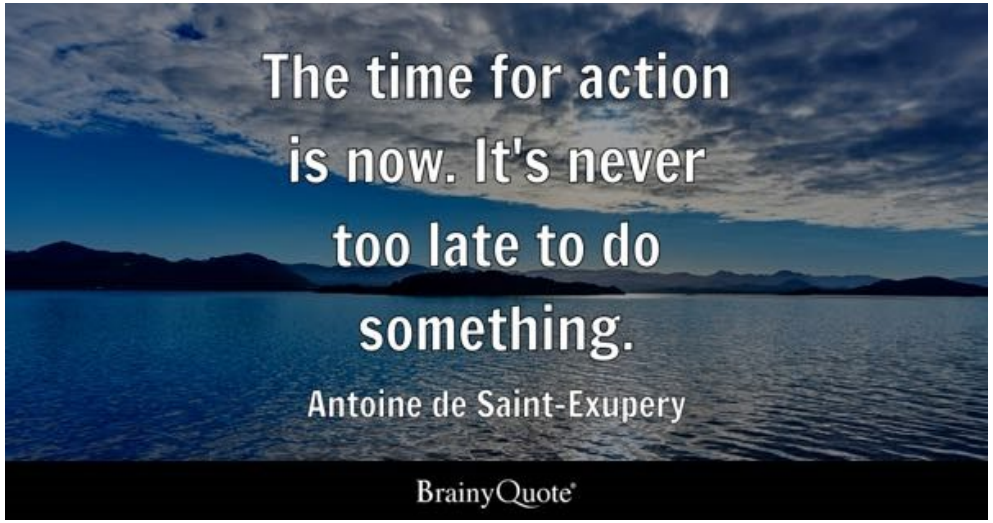
- **Digital infrastructure, in particular telecommunication networks are indispensable.**
- **However, they have become more vulnerable because of**
  - Cyber attacks
  - Man-made accidents and automatic outages
  - Natural disasters
- And then**, do the governments, telecom companies and users recognize the significance of network security and resilience? Not actually.**
- **So, it is time for making a call for “Resilience literacy”.**

Genie?

So what?

What about South Korea? Is this country doing well?

- **South Korea**
  - Korea is a divided nation
  - Korea's geopolitics is unique
  - Korea is one of ICT powerhouses
  - The cyber threats are significant in Korea
  - Korea is vulnerable to the impacts of climate change
- Though Korean governments (MSIT and more) and telecom companies have done much**, they alone can not cope with "Network Security and Resilience Risks".**
- So, it is necessary **for all stakeholders to work together** to develop solutions to defend against cyber attacks and natural disasters.
- In particular, we need to **enhance cooperation with international allies in cyber defense for a "step ahead for global security and resilience."**



(Source: https://www.brainyquote.com/quotes/antoine_de_saintexupery_119056)