Korea Internet & Security Agency

Data driven .kr DNS Security Initiative from KISA

Feb 28, 2017

Billy Cheon / Young-Jun Choi

Content

Ⅰ Security Risks with DNS

Ⅱ The Biggest Threat - DDoS

Ⅲ Current .kr DNS Status

Ⅳ .kr DNS Security Initiative

Ⅴ Next Steps

KISA Korea Internet & Security Agency

Ⅰ. Security Risks with DNS

Data Corruption

Threats causing unauthorized change of information in the DNS

- Authority Impersonation
- Authoritative Server Corruption
- Cache Corruption
- Protocol Corruption

.kr DNS Nameservers

DDoS Attacks

Threats preventing Internet users from using the DNS

- Resource Starvation
- Resource Disruption

Information Exposure

Threats causing disclosure of information about Internet users by examination of their DNS traffic

- Domain Front Running
- Cache Snooping
- Zone Walking
- DNS Query Tracking
- NXDomain Redirection

Threats from DNS

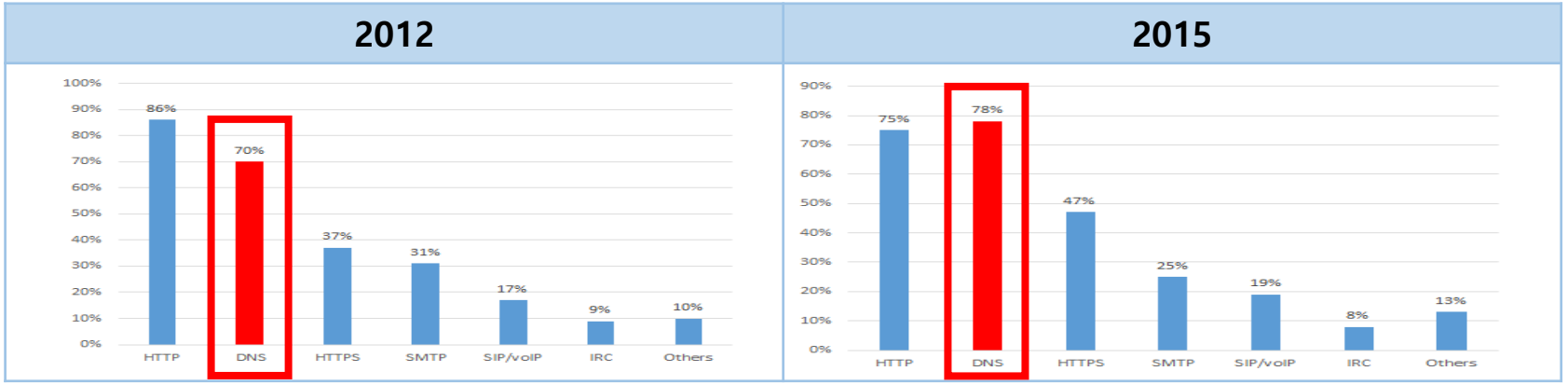
Threats utilizing DNS as a useful tool for attacking 3rd targets

- DNS Amplification Attacks
- Fast Flux DNS
- DNS as a Covert Channel

Ⅱ. The Biggest Threat - DDoS

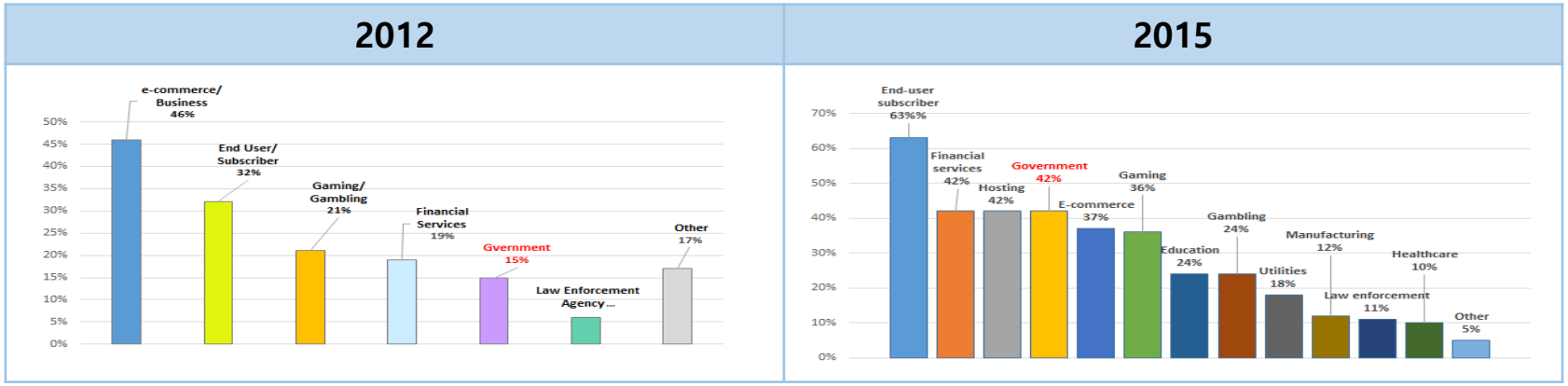
▪ Main Targets of DDoS Attack : DNS, Government

- 2012 → 2015 : DNS(70%→**78%**), Web(HTTP, 86%→75%)



※ Worldwide Infrastructure Security Report / 2012 Volume VIII / ARBOR, 2012, Worldwide Infrastructure Security Report / Volume XI / ARBOR, 2016

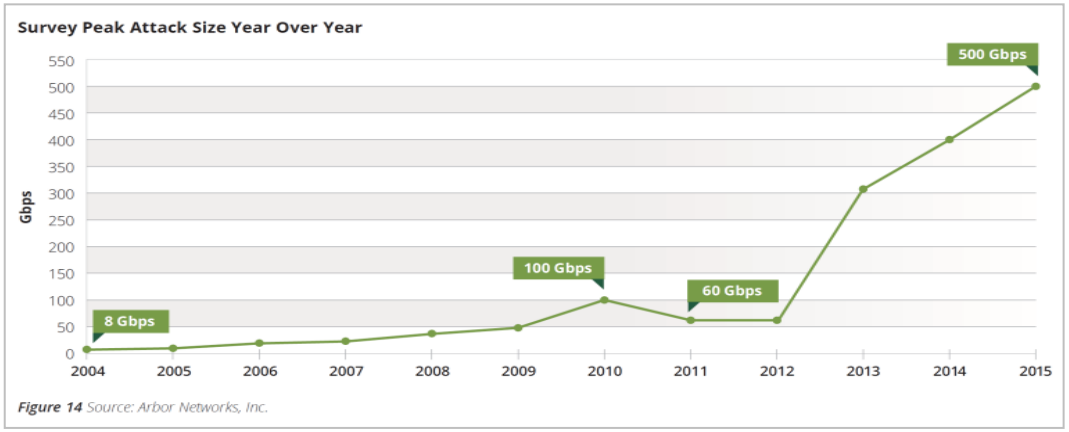
- 2012 → 2015 : Government(15%→**42%**)



※ Worldwide Infrastructure Security Report / 2012 Volume VIII / ARBOR, 2012, Worldwide Infrastructure Security Report / Volume XI / ARBOR, 2016

Ⅱ. The Biggest Threat - DDoS (cont.)

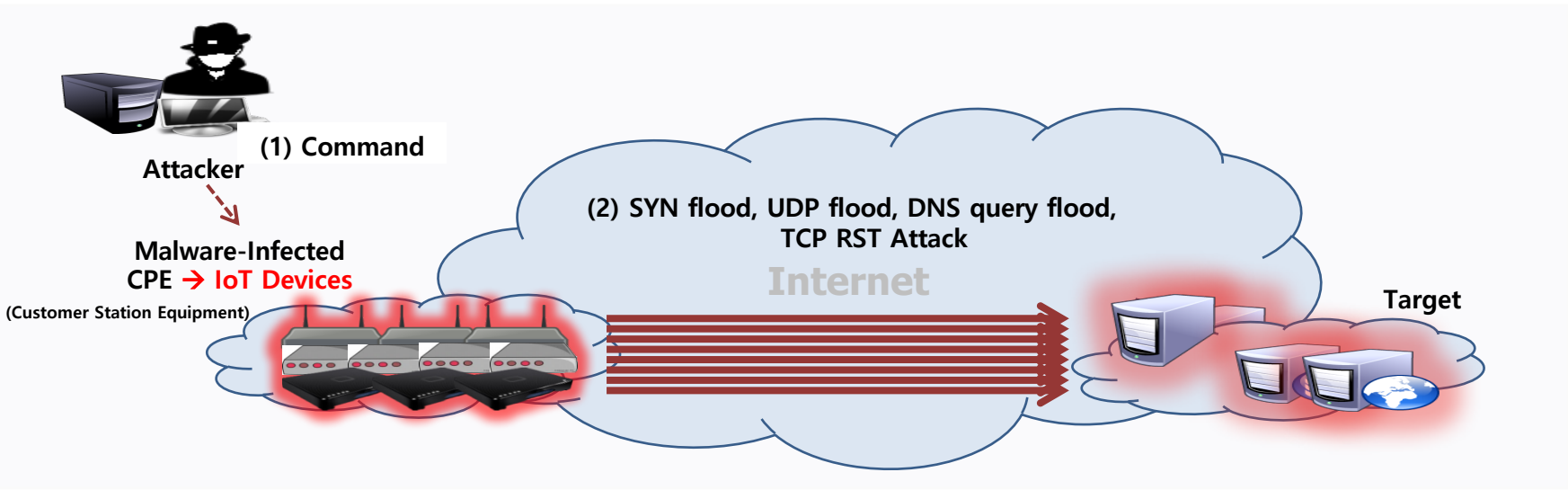
▪ Massive Amount of Traffic Attack through IoT devices



Time	Traffic	Target
'15.12	602Gbps	BBC
'16.09	665Gbps	Krebs On Security
'16.09	~ 1Tbps	France, OVH
'16.10	~ 1.2Tbps	USA, Dyn

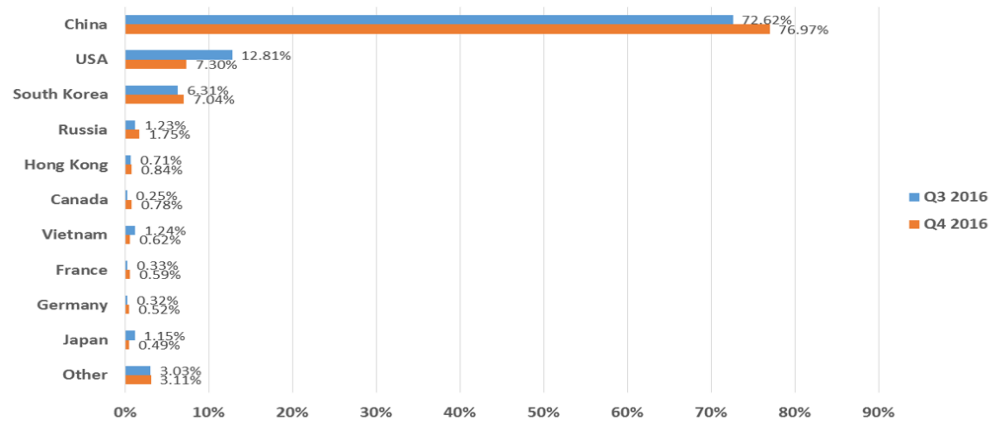
Ref : Worldwide Infrastructure Security Report, 2016년, Arbor Networks, https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

< DDoS Attacks through Malware-infected CPE → IoT devices >



Ⅱ. The Biggest Threat - DDoS (cont.)

▪ Q4 2016 DDoS attack trends

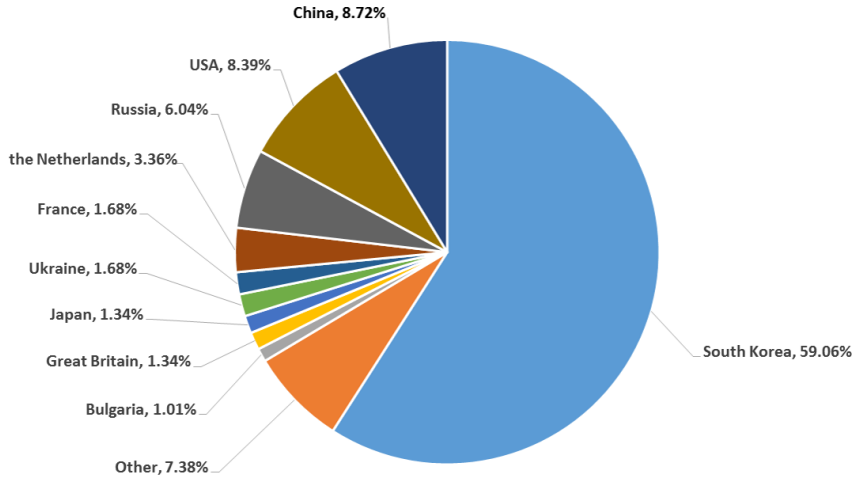


Distribution of DDoS attacks by country, Q3 2016 vs. Q4 2016

Ref : DDoS attacks in Q4 2016 By SECURELIST

In Q4 2016, the geography of DDoS attacks expanded to 80 counties, with China accounting for 76.97% (4.4 p.p. more than the previous quarter). The US (7.3%) and **South Korea (7%)** were once again second and third respectively. The Top 10 most targeted countries accounted for 96.9% of all attacks. Canada (0.8%) appeared in the rating, replacing Italy. Russia (1.75%) moved from fifth to fourth thanks to a 0.6 p.p. decline in Vietnam's share.

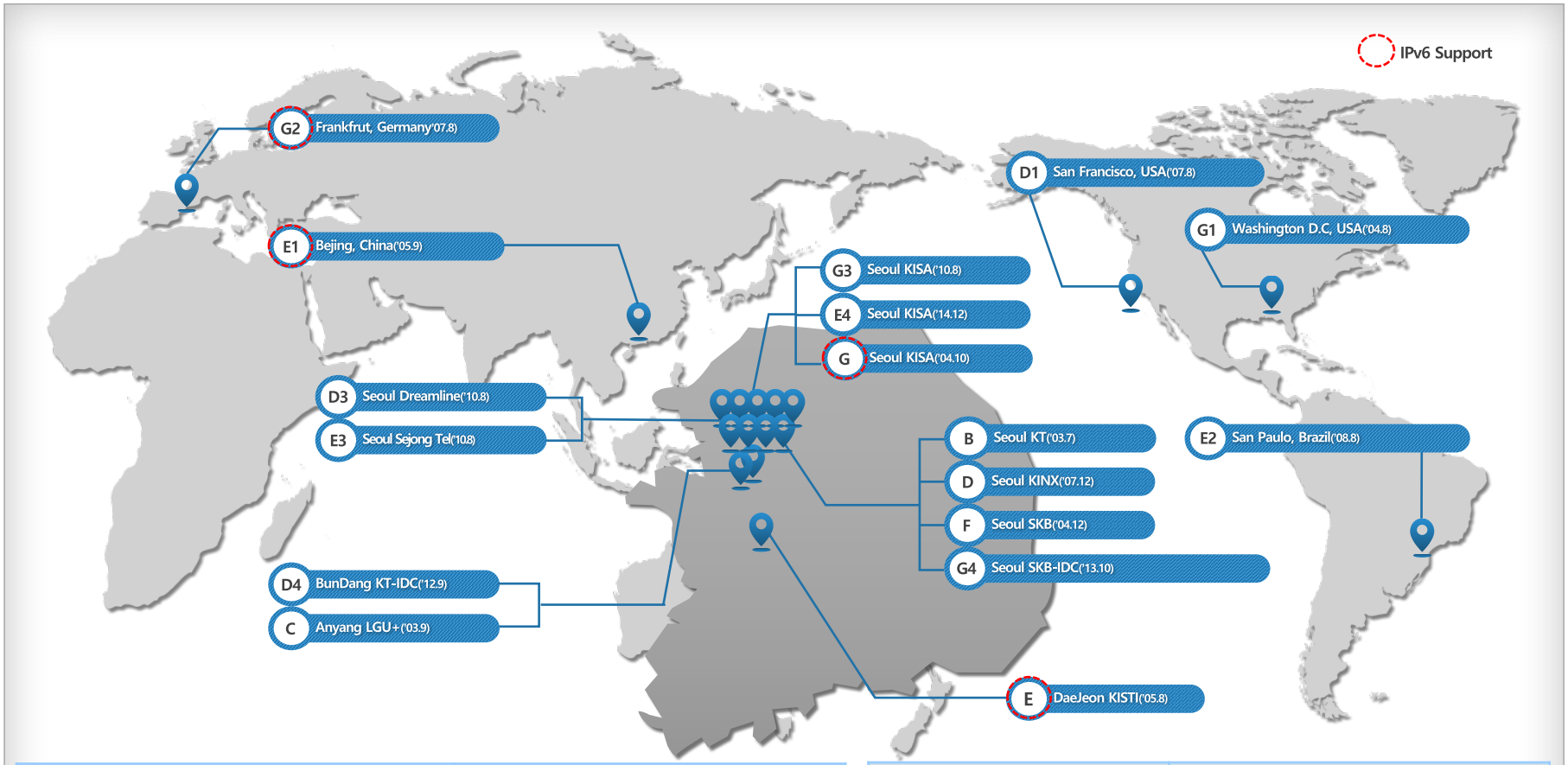
In Q4, the highest number of C&C server (59.06%) was detected in South Korea. Although the country's contribution increased by 13.3 p.p. from the previous quarter, it is must less than in Q2 2016 (69.6%). The top three counties hosting the most C&C servers remained unchanged – South Korea, China (8.72%) and the US (8.39%). Their total share accounted for 76.1% which is an increase of 8.4 p.p. compared to Q3.



Distribution of botnet C&C servers by country in Q4 2016

Ref : DDoS attacks in Q4 2016 By SECURELIST

Ⅲ. Current .kr DNS Status

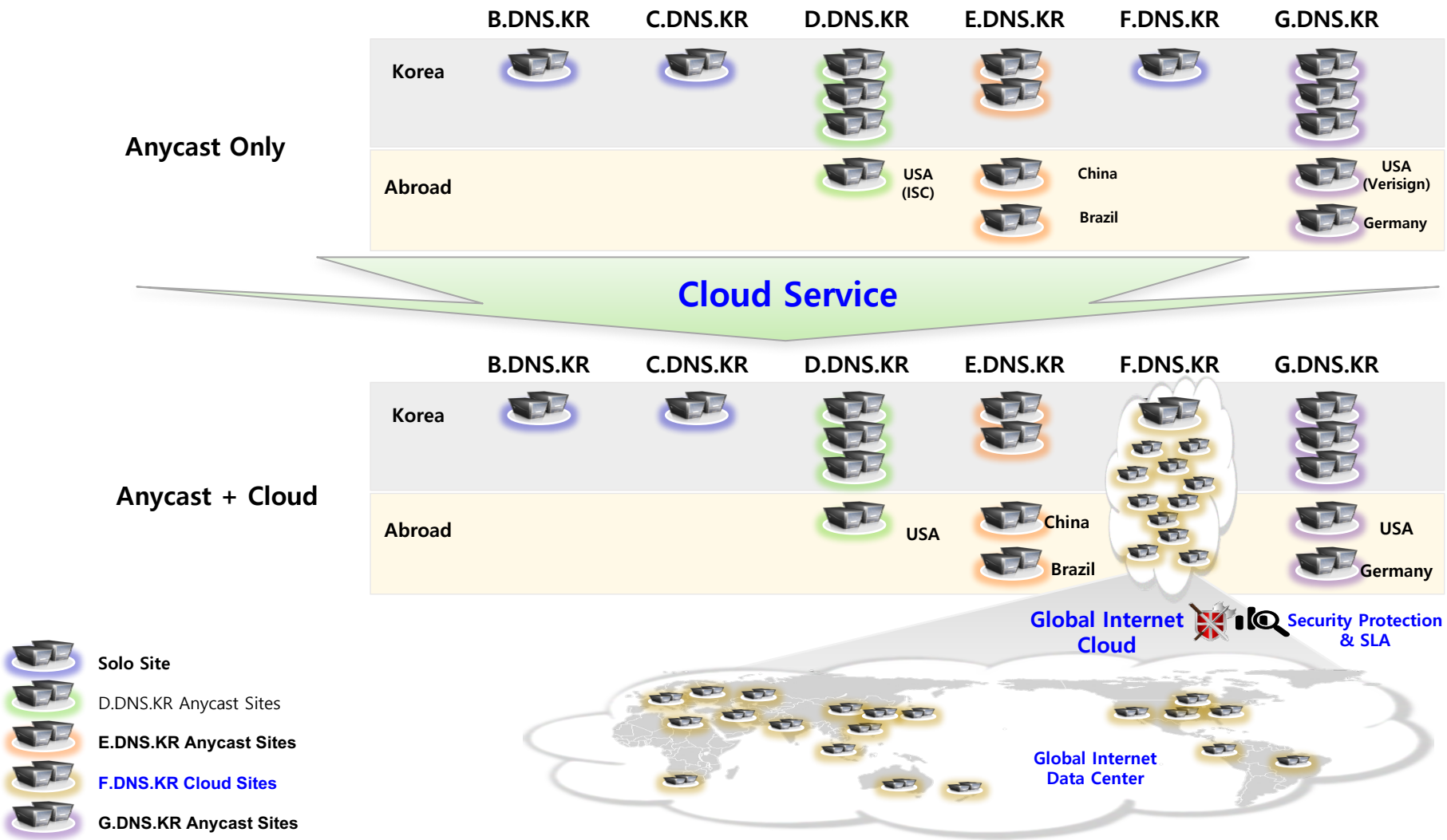


Index		Stat ('16. 10)
Domain	.kr	▪ 1,048,709
	.한국(IDN)	▪ 37,783
IP	IPv4	▪ 112,423,424
	IPv6 /32 prefix	▪ 5,250
ASN	ASN	▪ 1,021

Index		Query & Response	
		Average	Max
krDNS	.kr, .한국 DNS	1.9 Billion / Day	2.3 Billion / Day
	Reverse Domain DNS	0.4 Billion / Day	0.8 Billion / Day
	Total	2.3 Billion / Day	3.1 Billion / Day

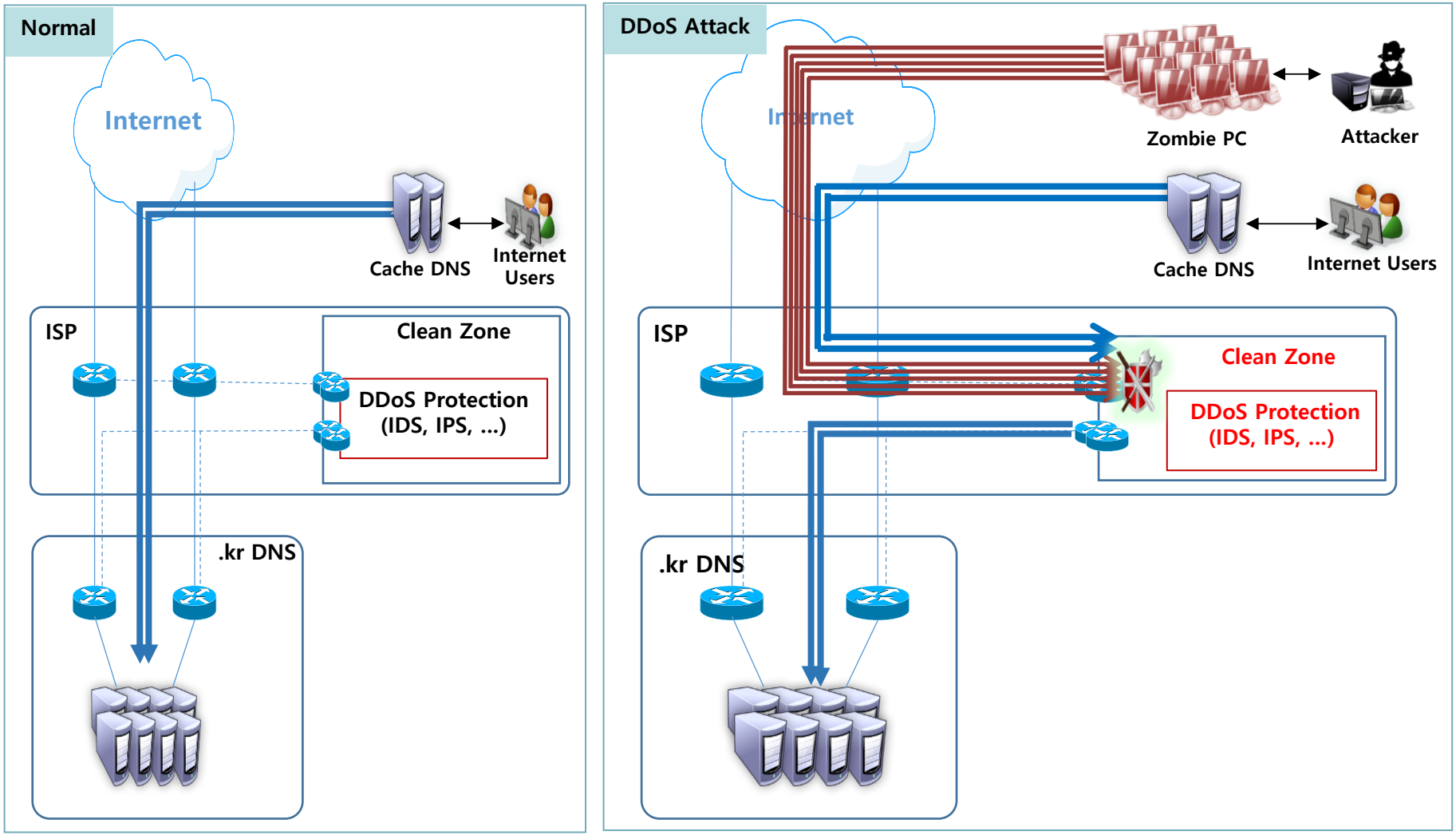
IV. .kr DNS Security Initiative (cont.)

.kr DNS Cloud Service



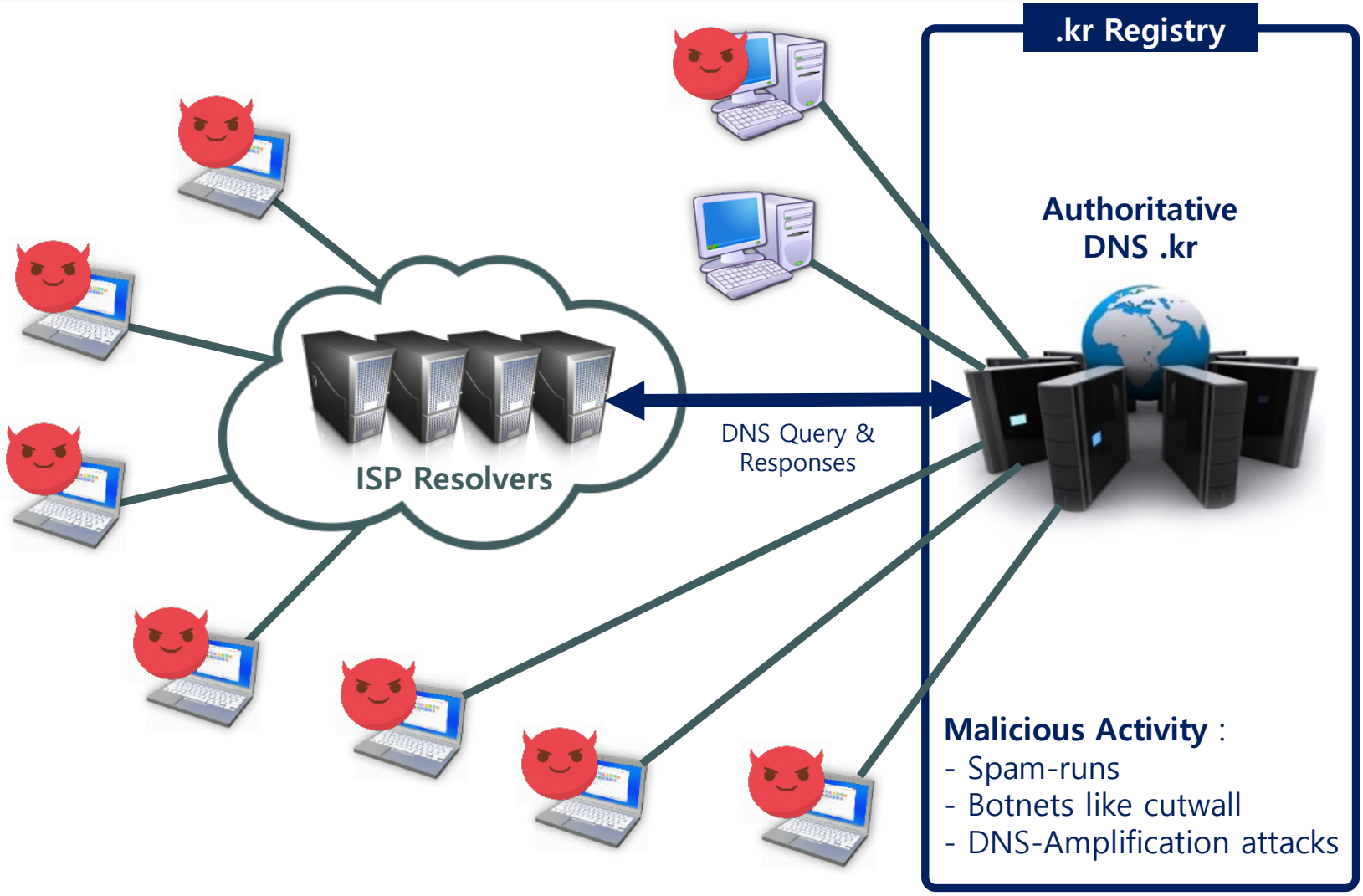
IV. .kr DNS Security Initiative (cont.)

.kr DNS Clean Zone Service



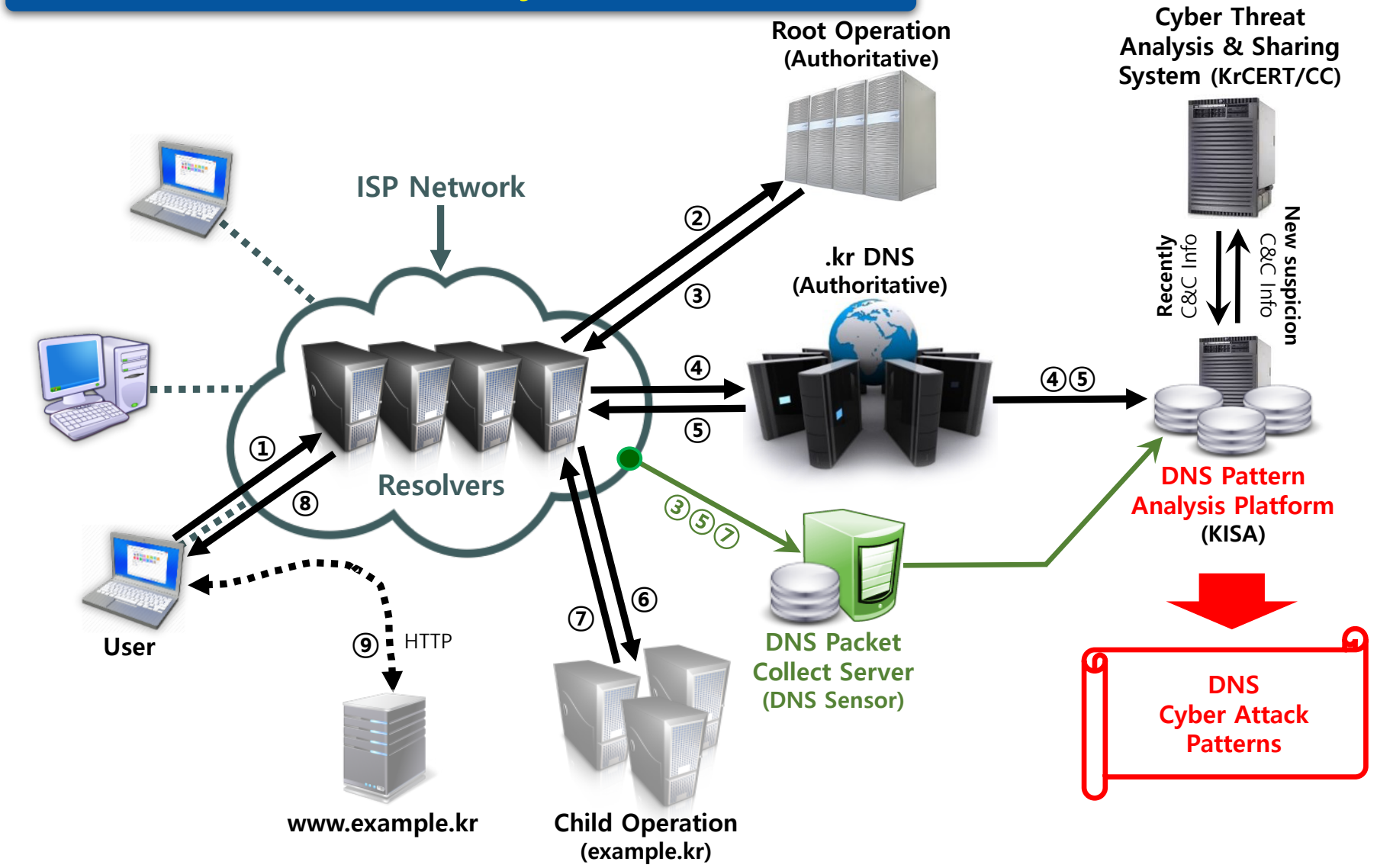
IV. .kr DNS Security Initiative (cont.)

Data driven .kr DNS Security Project Concept

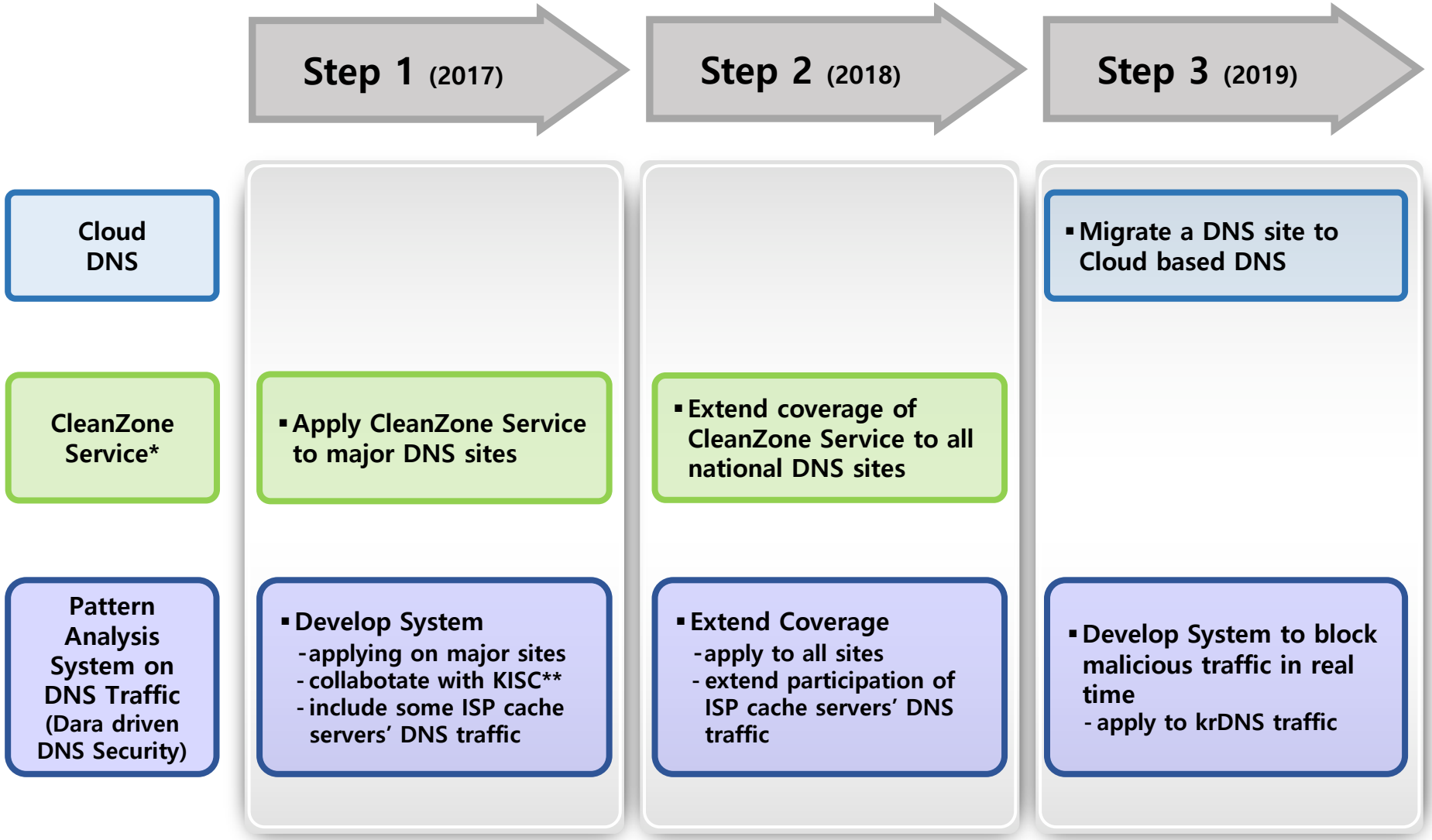


IV. .kr DNS Security Initiative (cont.)

Data driven .kr DNS Project Architecture



V. Next Steps



* "CleanZone Service" : DDoS Protection Services being provided by Korean ISPs
** KISC : Korea Internet Security Center of KISA

KISA Korea Internet & Security Agency

Internet On, Security In!

Thank you!