KISA Korea Internet & Security Agency

Data driven .kr DNS Security Initiative from KISA

Sep. 10, 2018

KRNIC

Content

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

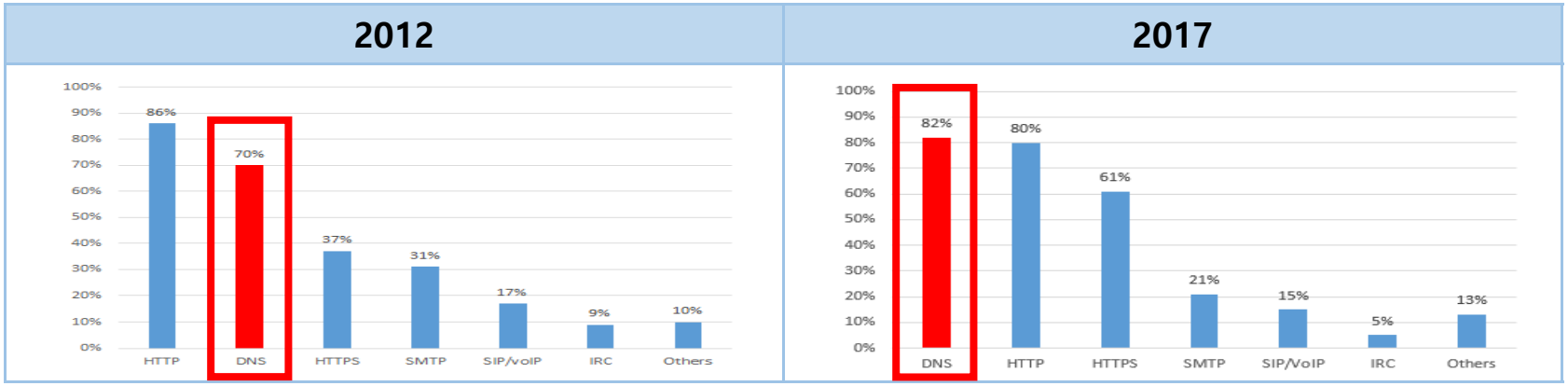
Threats utilizing DNS as a useful tool for attacking 3rd targets

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

Ⅱ. The Biggest Threat - DDoS

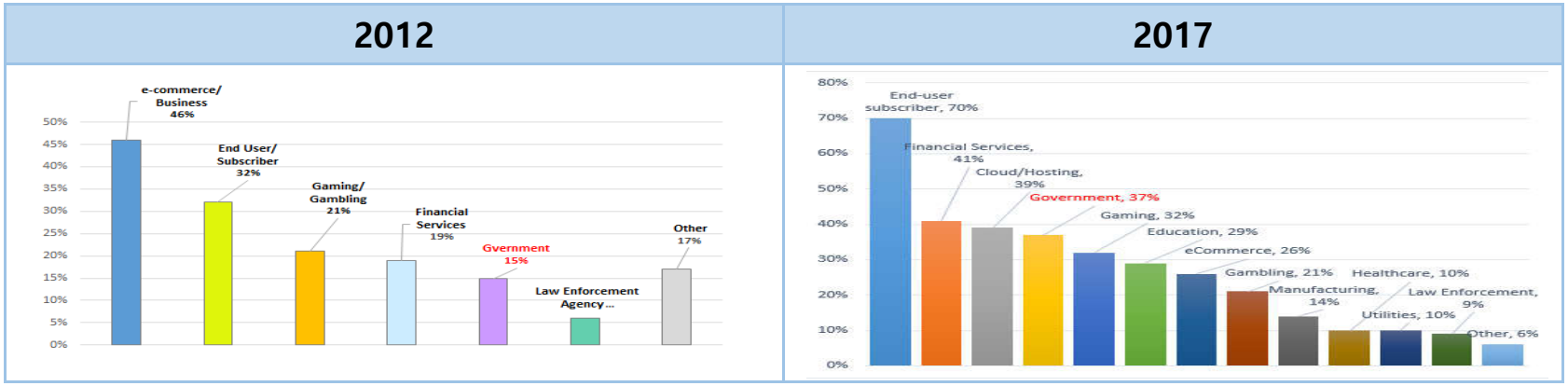
▪ Main Targets of DDoS Attack : DNS, Government

- 2012 → 2017 : DNS(70%→**82%**), Web(HTTP, 86%→80%)



※ Worldwide Infrastructure Security Report / 2012 Volume VIII / ARBOR, 2012, 13th Worldwide Infrastructure Security Report / ARBOR, 2018

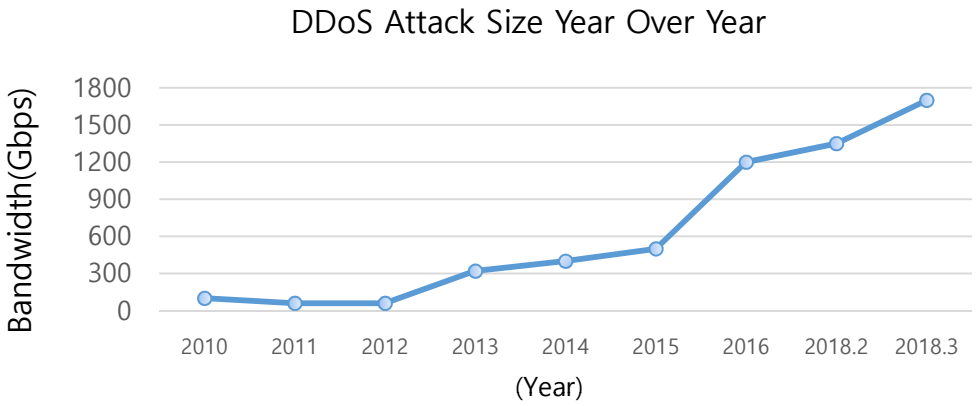
- 2012 → 2017 : Government(15%→**37%**)



※ Worldwide Infrastructure Security Report / 2012 Volume VIII / ARBOR, 2012, 13th Worldwide Infrastructure Security Report / ARBOR, 2018

Ⅱ. The Biggest Threat - DDoS (cont.)

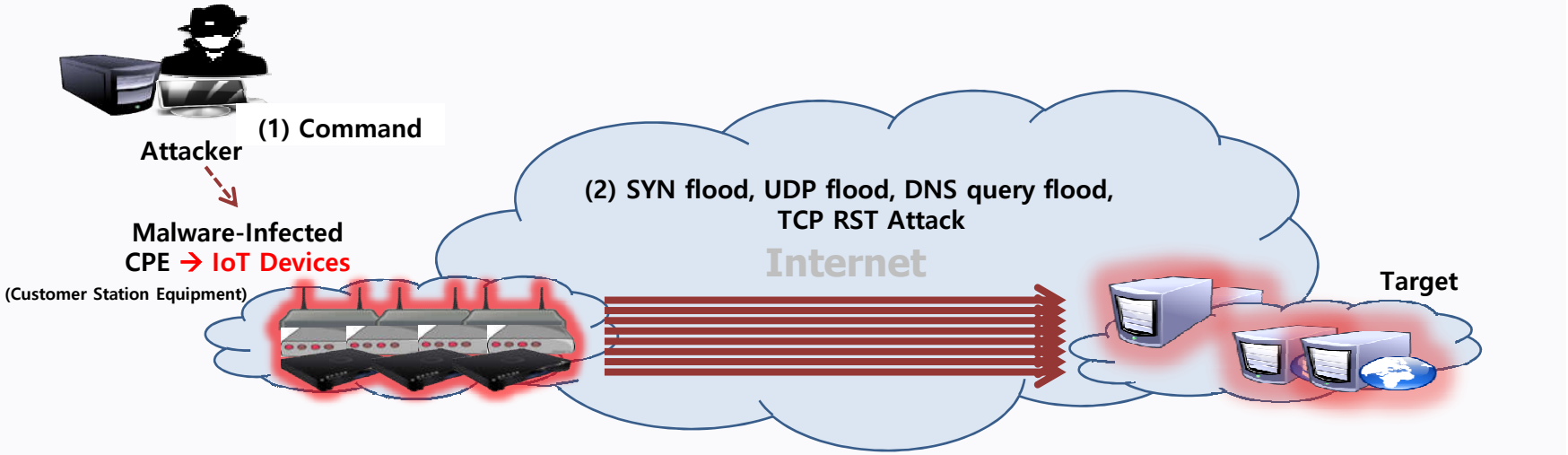
▪ Massive Amount of Traffic Attack through IoT devices



Ref : blog.haltdos.com/2017/02/22/busuinesses-india-can-learn-recent-ddos-attacks/

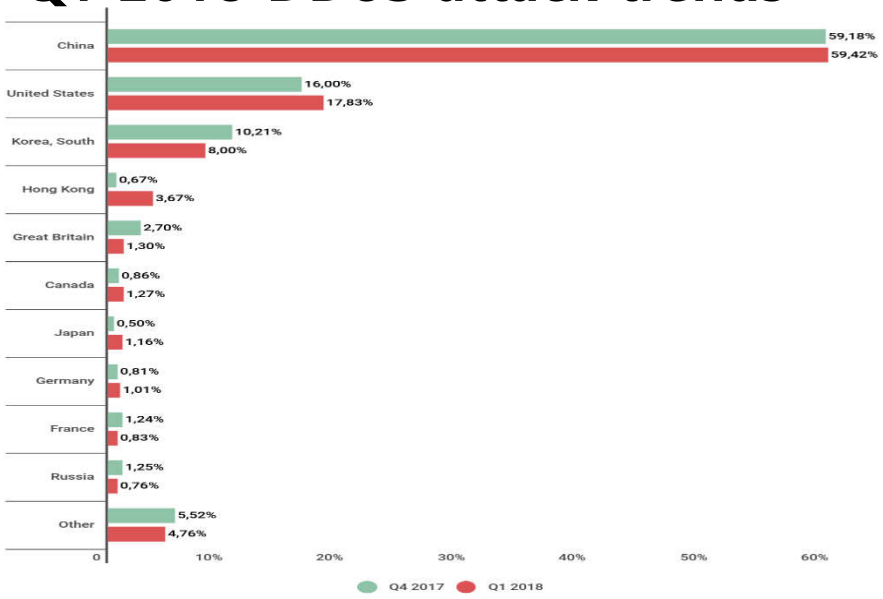
Time	Traffic	Target
'15.12	602Gbps	BBC (UK)
'16.09	665Gbps	Krebs On Security (US)
'16.09	~ 1Tbps	OVH (France)
'16.10	~ 1.2Tbps	Dyn (US)
'18.2	~ 1.35Tbps	Github (US)
'18.3	~ 1.7Tbps	One of Arbor's Customers (US)

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



Ⅱ. The Biggest Threat - DDoS (cont.)

▪ Q1 2018 DDoS attack trends



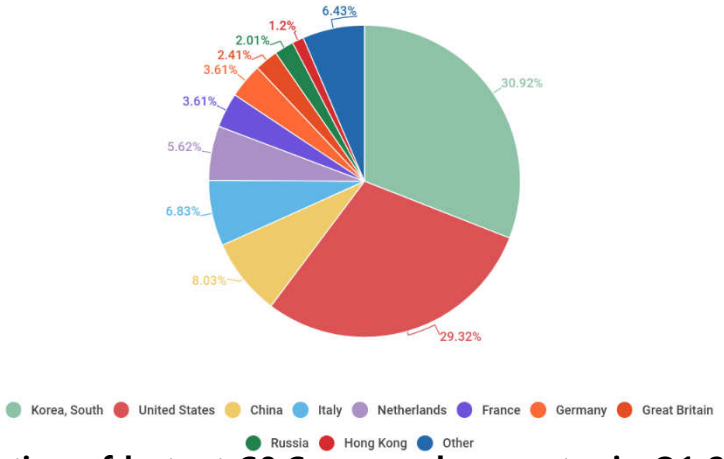
Distribution of DDoS attacks by country, Q4 2017 vs. Q1 2018

Ref : DDoS attacks in Q1 2018 By SECURELIST

China easily retained pole position by number of attacks: its share remained almost unchanged, up from 59.18% to 59.42%. The US share (17.83%), the second largest, increased by a more noticeable 1.83%. South Korea again took bronze, but its share fell by more than 2%, from 10.21% to 8%.

Britain (1.30%) moved from fourth to fifth. Tenth place in Q1 2018 went to Russia, whose share decreased from 1.25% to 0.76%. The Netherlands and Vietnam dropped out of the top ten, but Hong Kong (with a solid 3.67% against 0.67% in Q4 2017) and Japan (1.16%) reappeared.

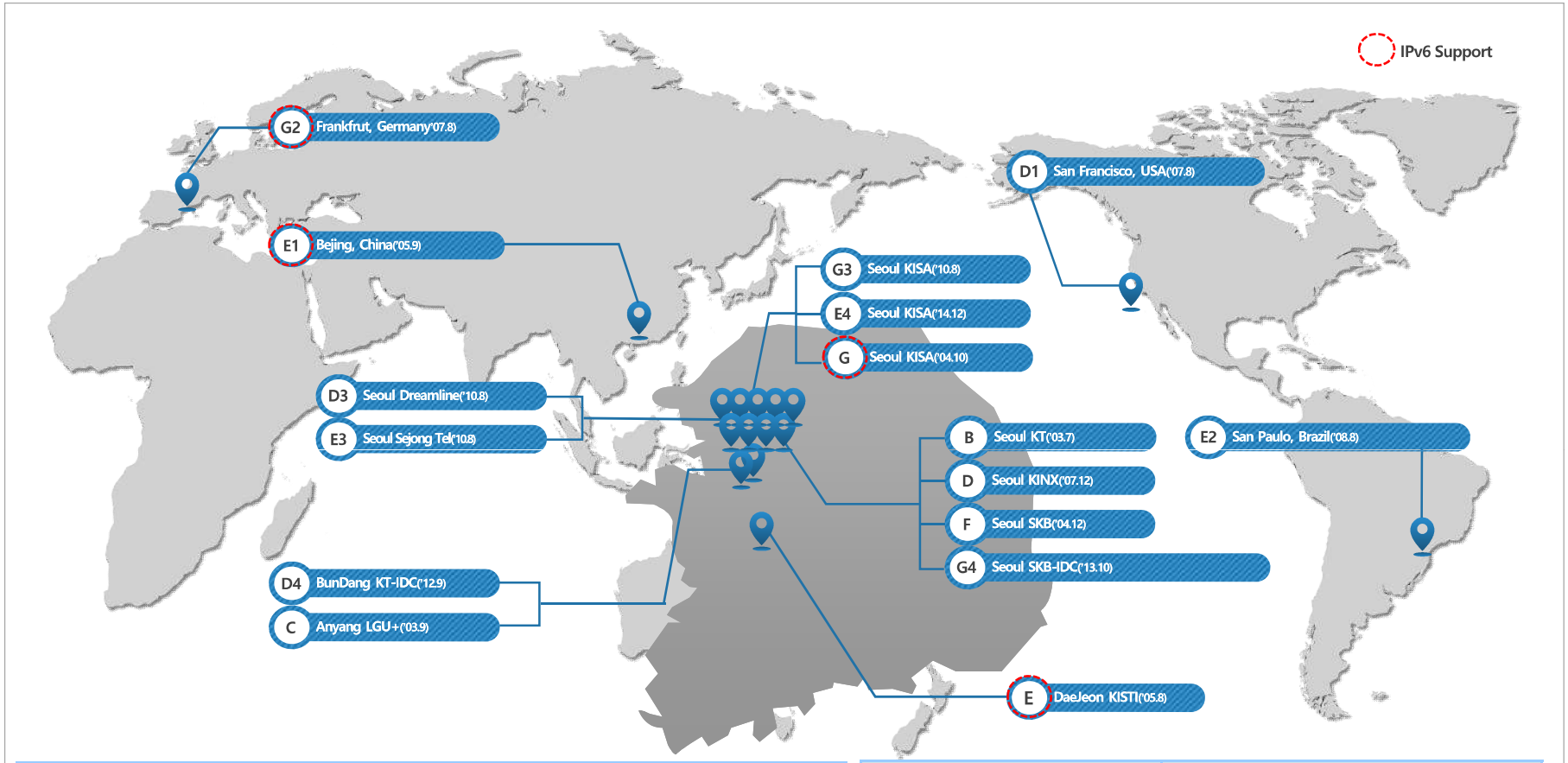
The top ten countries by number of C&C servers last quarter underwent a major reshuffle: Canada, Turkey, Lithuania, and Denmark dropped out, while Italy, Hong Kong, Germany, and Britain climbed upwards. The top three remained practically unchanged: South Korea (30.92%), the US (29.32%), China (8.03%). Only Russia (2.01%), having shared bronze with China in late 2017, slid down to ninth place.



Distribution of botnet C&C servers by country in Q1 2018

Ref : DDoS attacks in Q1 2018 By SECURELIST

Ⅲ. Current .kr DNS Status

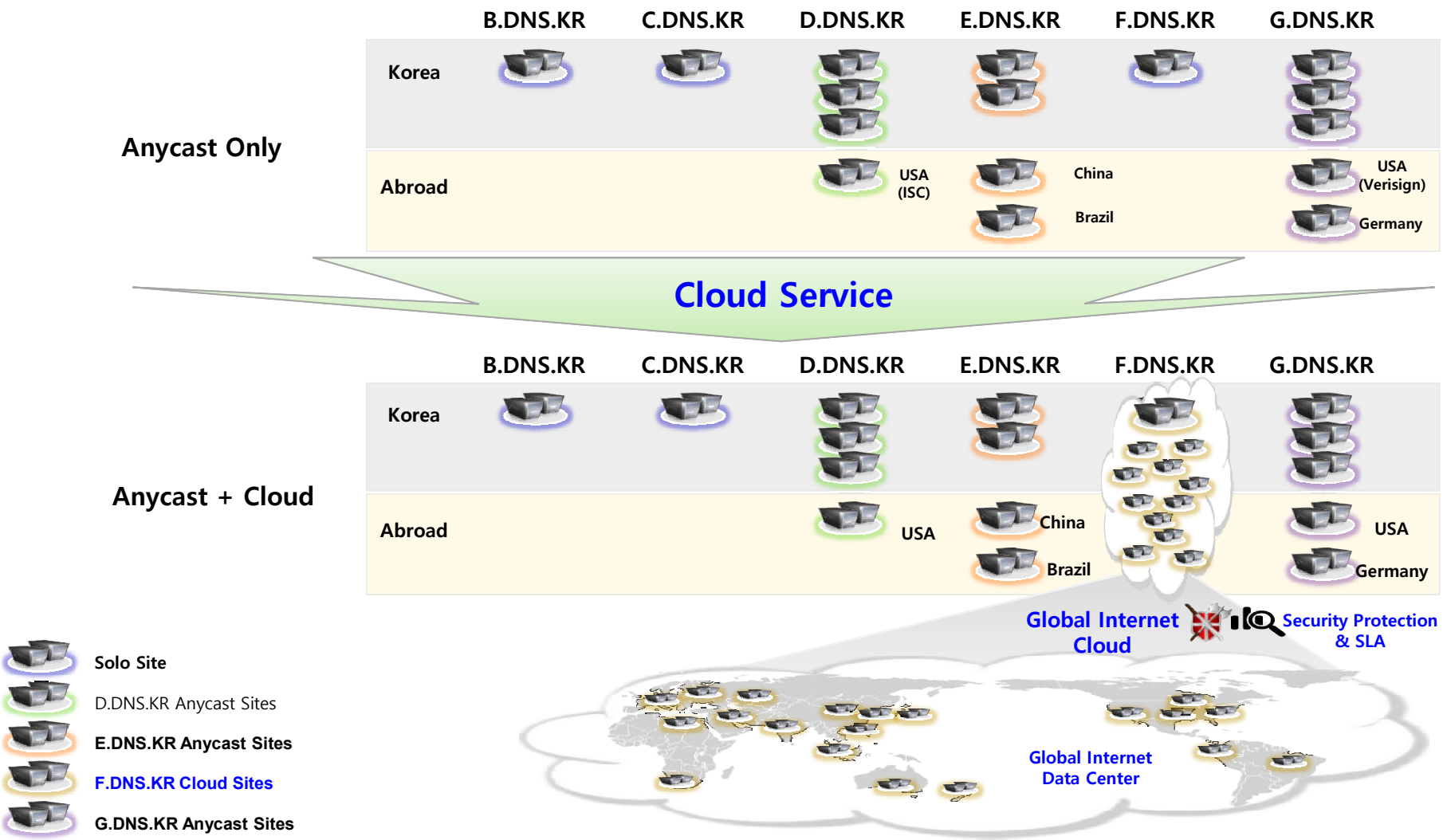


Index		Stat ('18. 4.)
Domain	.kr	▪ 1,046,953
	.한국(IDN)	▪ 30,179
IP	IPv4	▪ 112,389,888
	IPv6 (/32)	▪ 5,253
ASN	ASN	▪ 1,024

Index		Query & Response	
		Average	Max
krDNS	.kr, .한국 DNS	-	-

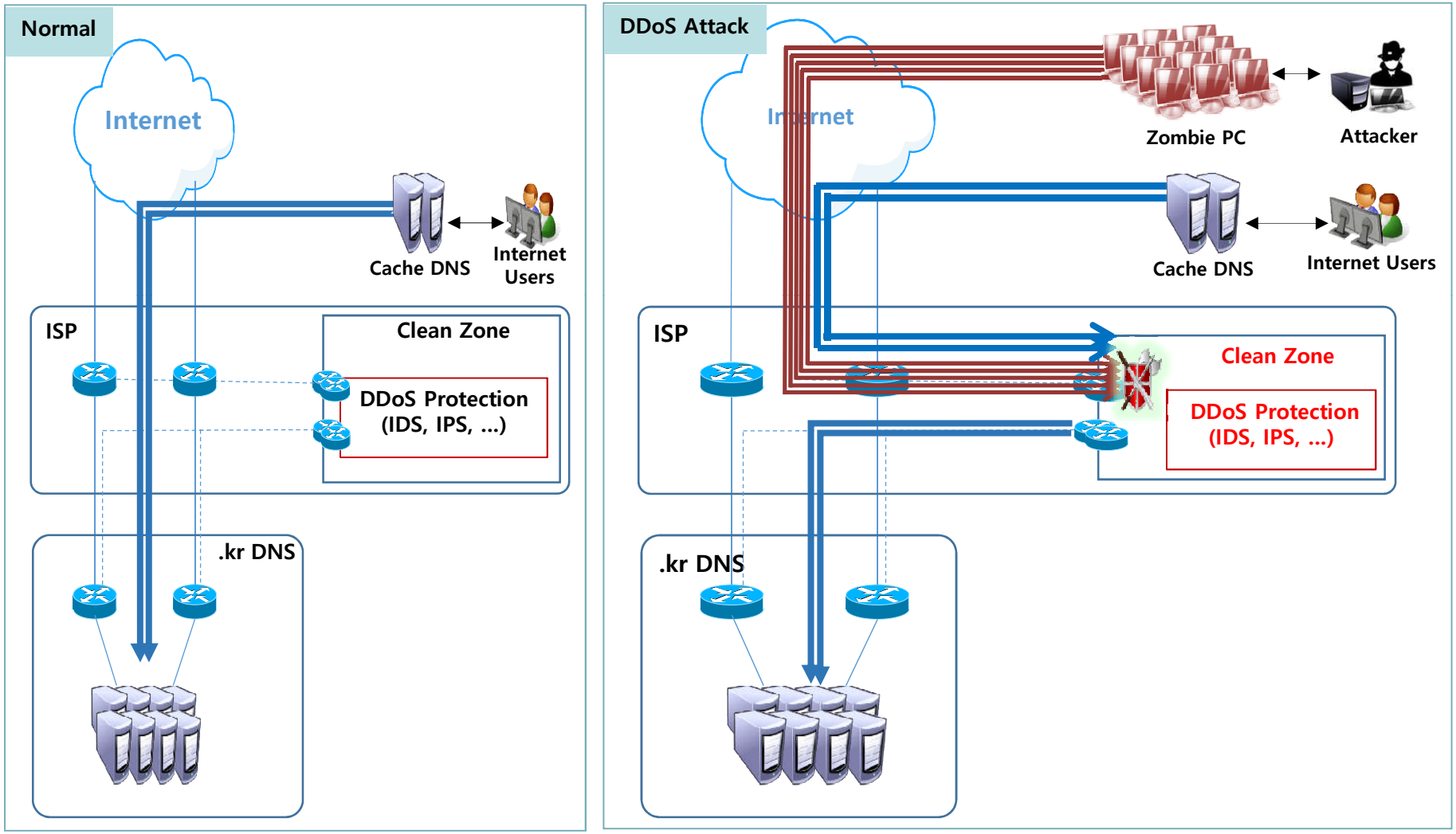
IV. .kr DNS Security Initiative

.kr DNS Cloud Service



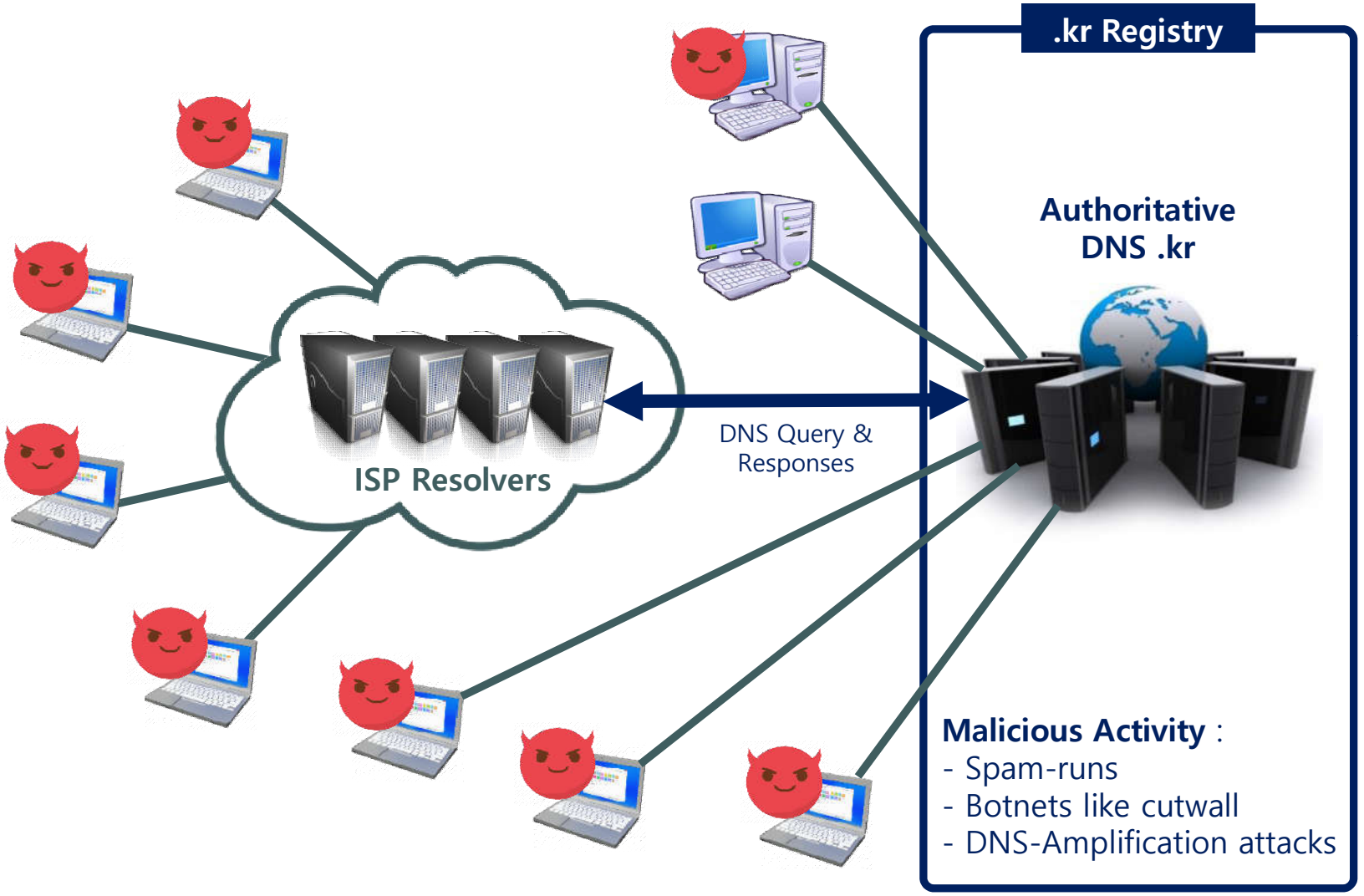
IV. .kr DNS Security Initiative (cont.)

.kr DNS Clean Zone Service



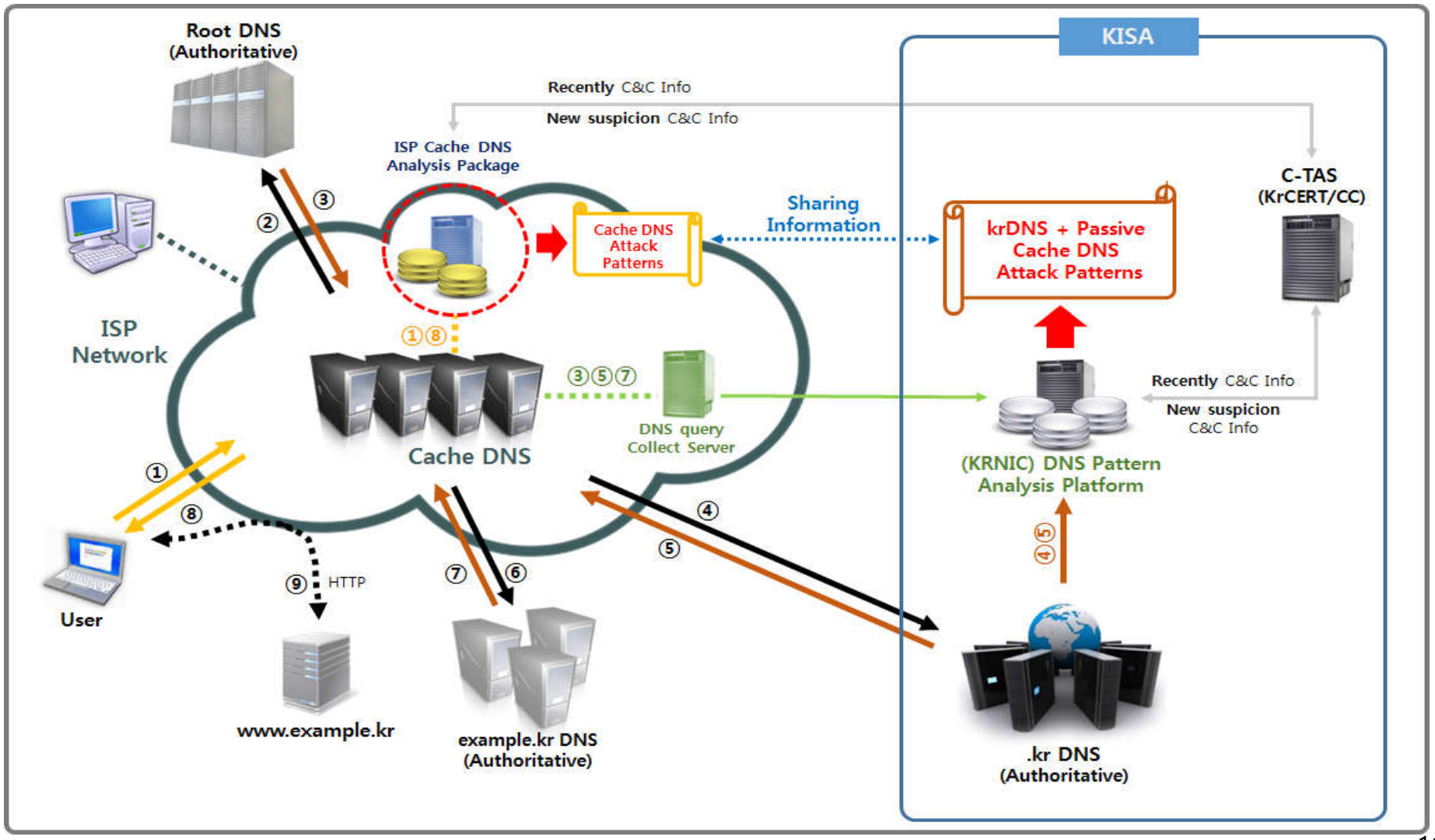
IV. .kr DNS Security Initiative (cont.)

Data driven .kr DNS Security Project Concept



IV. .kr DNS Security Initiative (cont.)

Data driven .kr DNS Project Architecture(concept)



KISA Korea Internet & Security Agency

Internet On, Security In!

Thank you!