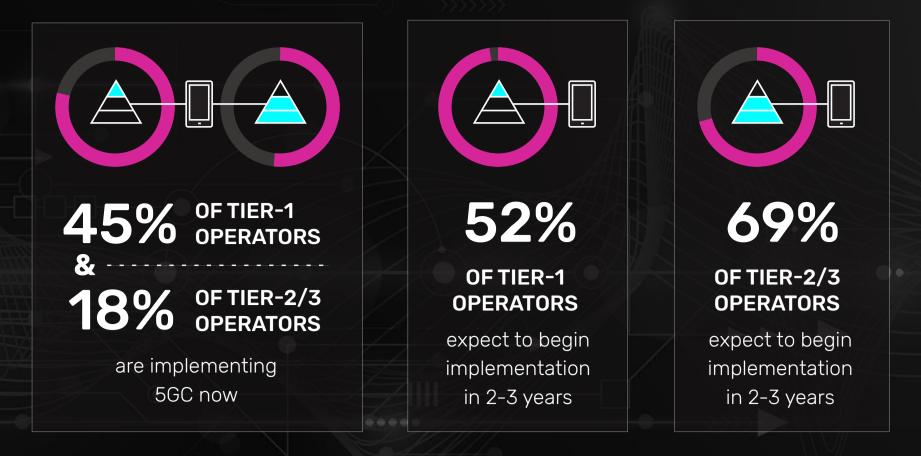# WHAT 5G CORE SECURITY MEANS FOR OPERATORS —AND CYBERCRIMINALS

Mobile operators are excited about the transition to 5G. So are cybercriminals. Here's why.
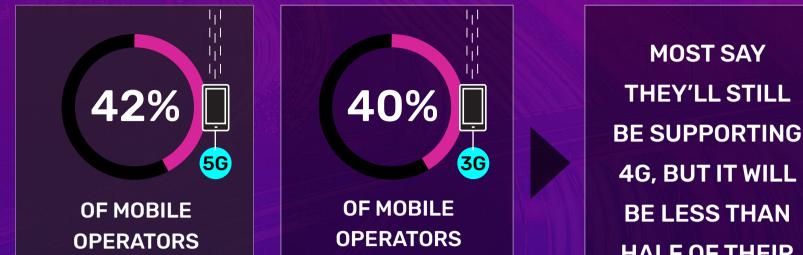

5G CORE

Large and small mobile operators are committed to 5GC—with 93% implementation expected within 3 years.

45% OF TIER-1 OPERATORS & **18%** OF TIER-2/3 OPERATORS are implementing 5GC now

52% OF TIER-1 OPERATORS expect to begin implementation in 2-3 years

69% OF TIER-2/3 OPERATORS expect to begin implementation in 2-3 years

All operators see a steady progression towards 5GC

THE NEW MULTI-GENERATIONAL REALITY INCREASES VULNERABILITY

5G isn't going to replace 3G/4G all at once. **By 2025:**

42% OF MOBILE OPERATORS say most traffic will be 5G

40% OF MOBILE OPERATORS say they'll still be supporting 3G

MOST SAY THEY'LL STILL BE SUPPORTING 4G, BUT IT WILL BE LESS THAN HALF OF THEIR TRAFFIC

3G/4G VULNERABILITIES + 5G VULNERABILITIES = MORE NUMEROUS AND DISPERSED ATTACK POINTS

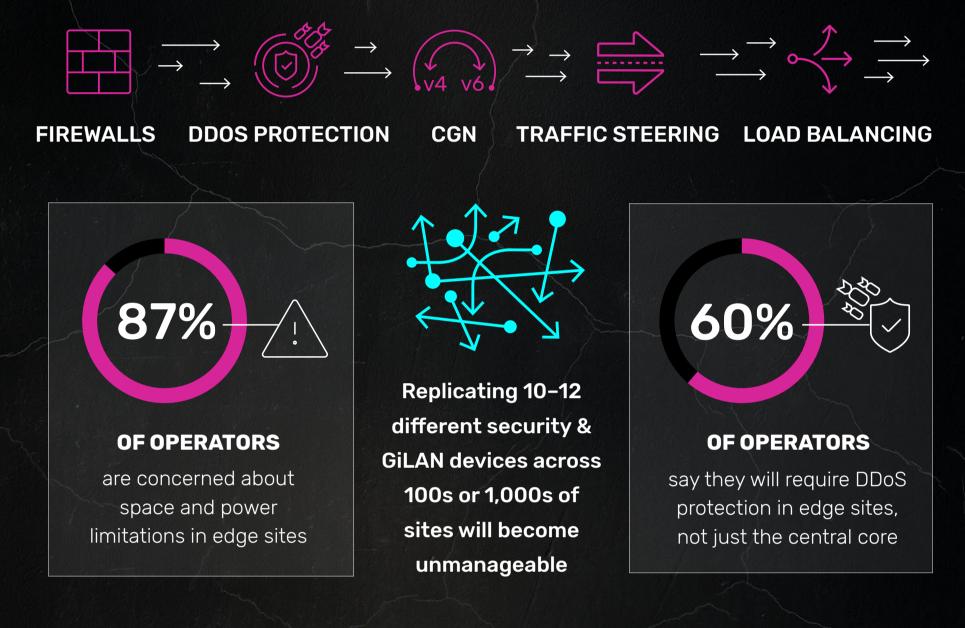**Carrier-grade networking (CGN)** will play a key role in the transition.

80% OF MOBILE OPERATORS expect to need CGN by 2023 to bridge network generations

16% will support CGNAT in container-based functions in a 5G standalone core

Mobile edge compute (MEC) will move slowly as well. In 2025:

73% OF MOBILE OPERATORS will have deployed a MEC architecture

<25% of traffic will be carried through MEC nodes

FRAGMENTED SECURITY MUST INTEGRATE IN MEC

Previously centralized functions are moving to the network edge:

FIREWALLS → DDOS PROTECTION → CGN → TRAFFIC STEERING → LOAD BALANCING

87% OF OPERATORS are concerned about space and power limitations in edge sites

Replicating 10-12 different security & GiLAN devices across 100s or 1,000s of sites will become unmanageable

60% OF OPERATORS say they will require DDoS protection in edge sites, not just the central core

IOT, BOTS, & AUTOMATION RUN WILD
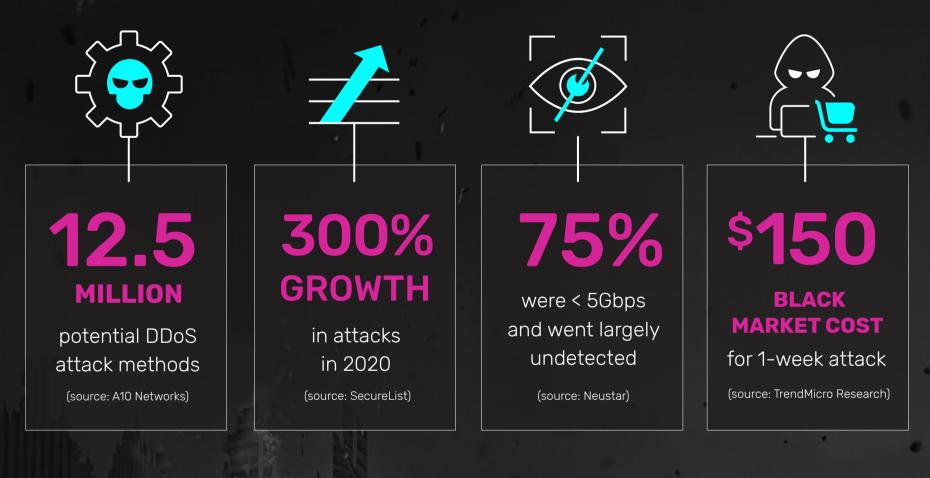
Hackers will use smartphones and stupid devices to plant malware—and recruit them into botnet armies. By 2025:

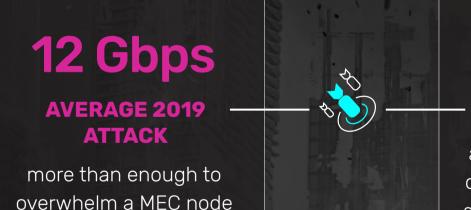**24 BILLION** CONNECTED IOT DEVICES —many highly vulnerable

&

7.5 BILLION SMARTPHONES 85% of mobile subscriptions

Source: Ericsson Mobility Report, June 2020.

DDOS GETS MORE EFFECTIVE —AND POTENTIALLY LETHAL

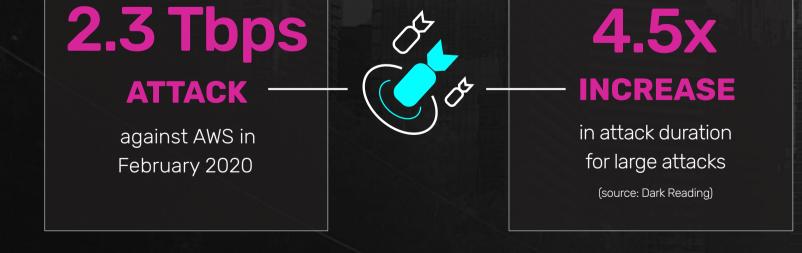DDoS attacks are getting more frequent, harder to detect, and all too affordable.

12.5 MILLION potential DDoS attack methods (source: A10 Networks)

300% GROWTH in attacks since 2019 (source: SecureList)

75% were < 5Gbps and went largely undetected (source: Neustar)

$150 BLACK MARKET COST for 1-week attack (source: TrendMicro Research)

Even small attacks can be devastating

12 Gbps AVERAGE 2019 ATTACK more than enough to overwhelm a MEC node

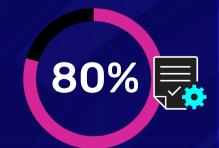**5 Gbps** COULD DEVASTATE an enterprise and disrupt critical services for public security and telemedicine

Meanwhile large attacks are getting larger & lasting longer

2.3 Tbps ATTACK against AWS in February 2020

4.5x INCREASE in attack duration for large attacks (source: Defi Research)

THE 80-20 PROBLEM

Not all DDoS attacks pose the same dangers or challenges

80% use just five protocols—easy to detect and mitigate

HIGH-VOLUME HIGH-IMPACT ATTACKS defend with blackholing, rate limiting, IP blocking by destination

LOW-VOLUME LOW-IMPACT ATTACKS defend with rate limiting, anomaly checks, protocol misuse

Problem lies in the middle

— Multi-vector attacks
— Less common protocols
— Smaller attacks targeting subscribers, not just networks
— Harder to distinguish malicious from legitimate traffic

More sophisticated, surgical defenses needed to respond quickly and accurately

— Pattern recognition
— L4 – 7 countermeasures
— Zero-day automation
— Complex multi-stage mitigation rules
— Stop bad traffic without stopping good traffic

A10