US DNI resigns as expected, sees results from naming Russia in election hacking. Insider credentials used to breach UK mobile firm Three. China says its Internet controls are just bringing their wisdom to cyberspace.

US Director of National Intelligence Clapper, submitting his resignation (as as he's long intended to do—it will take effect at the change in Presidential administrations) also says that Russian cyber operations against US-election-related targets slowed after the US Intelligence Community took formal, public notice of them. Whether any such curtailment was a win for naming-and-shaming or for threatened retaliation is unknown.

Those interested in seeing what an insider threat looks like in action may find a good (by which we mean bad) example in UK mobile phone provider Three. Three, which has 8.8 million customers, had noticed an increase in handset fraud in recent months. This week the company disclosed that about six million customers' personal information had been breached by hackers using employee login credentials—that information includes

name, phone number, address, and date-of-birth. (For a sense of scale, the 2015 TalkTalk breach affected roughly 157,000 accounts.) How the hackers got the employee credentials is unclear, but once in, effectively they operated as insiders. Three arrests have been made, according to the National Crime Authority: "a 48-year old man from Orpington, Kent and a 39-year old man from Ashton-under-Lyne, Manchester on suspicion of computer misuse offences, and a 35-year old man from Moston, Manchester on suspicion of attempting to pervert the course of justice."

Chinese authorities make the case for their new Internet controls at the Wuzhen World Internet Conference as "fair and equitable," and also as bringing "Chinese wisdom" to cyberspace, which is one way of looking at it.