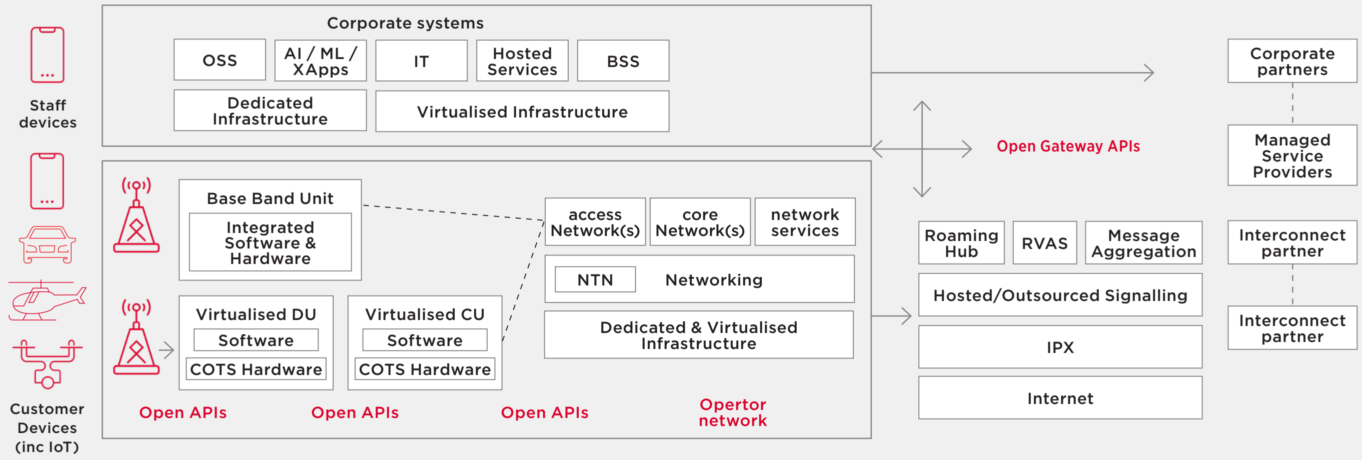
3.0 Attacks on Operators

In order to establish and operate effective security defences, it is necessary to understand the assets that make up the network's attack surface. This includes all the systems (development and operational), people and processes used to operate, design and maintain the network. Network attack surfaces are expanding. There are increasing numbers of connected devices (for example, connected vehicles and IoT equipment), new 5G standalone cores, network application programming interfaces (APIs), open-radio access network (RAN) architectures and new artificial intelligence-enabled services. The diagram below, which illustrates a high-level view of a typical mobile network, provides context for the following sections of this report.

Figure 3



The operational attack surface is wide and complex. Attacks can be launched at many different points externally and from within the network. Mobile network operators (MNOs) have been targeted for many years and these attacks continued in 2023. We can group these attacks into eight types:

- Data breaches
- Ransomware attacks
- Supply chain attacks
- Reconnaissance and initial access
- Direct attacks on service delivery
- DDOS attacks
- Social engineering
- Compromising 'the edge'

A significant number of attacks have primarily targeted customer and staff data that can be further exploited, sold or leveraged. Ransomware attacks can impact access to essential network resources and data, internal servers and communications systems and can result in the unauthorised extraction of data from IT systems. Direct attacks[8], including DDoS attempts, can compromise the availability of services on a temporary or prolonged basis[9]. Operators' employees have been targeted and manipulated into giving attackers access to sensitive systems. Threat actors also seek to compromise 'the edge' of enabling systems (see more on this later). As MNOs have strengthened network security controls and improved end-point detection and response, attackers have pivoted to target devices that support the underlying network infrastructure[10].

Analysis

The attractiveness of both customer and staff data and information makes it an obvious ongoing target for prospective attackers. Other attacks seek to obtain reconnaissance information or an initial network access from which to launch later attacks or gain further access through privilege escalation and lateral movement (in fact the full range of MITRE ATT&CK® adversary tactics[11]).

DDoS attacks[12] aim to overwhelm internet services with more traffic than they can handle, with the goal to disrupt them and make them unavailable to legitimate users. Such attacks have been launched (often with high frequency and large bandwidths[13]) against MNOs[14]. DDoS attacks can be launched via a variety of protocols, including the application layer, network layers, such as IP, transport layers, such as UDP, and via signalling routes. Services are emerging that seek to make launching a DDoS attack easier[15]. Defensive DDoS tools form an important part of network defence and should keep pace with the increasing range and methods of attacks. A common defensive control is to drop packets by routing them to a 'sinkhole' (i.e. the traffic routing is changed such that the packets are dropped rather than allowing onward connection to the target network).

Security controls, such as customisation of defensive tools and proactive security testing, can all play an important role in mounting a successful defence. Attacks via third parties highlight the need to consider the total attack surface for both insourced and outsourced products and services.

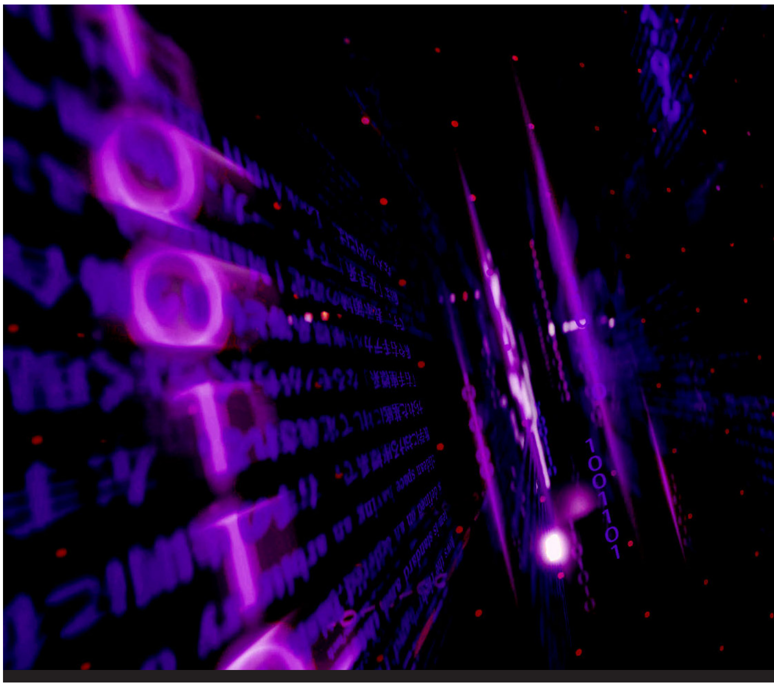
[8] Eg https://www.euractiv.com/section/europe-s-east/news/russian-hackers-were-inside-ukraine-telecoms-giant-for-months-cyber-spy-chief/
[9] For example, the French Cybersecurity agency ANSSI observed an "increase in compromises affecting equipment, particularly routers at the core of operators' networks. These attacks, of a high level of sophistication, are often carried out over a long period of time and are difficult to detect." See full report at https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-010.pdf
[10] Explored more fully in https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02
[11] MITRE ATT&CK®
[12] https://www.imperva.com/resources/resource-library/reports/ddos-threat-landscape-report-2023/
[13] DDoS threat report for 2023 Q3 (cloudflare.com)
[14] For example Ukraine's biggest mobile operator suffers massive hacker attack -statement (msn.com)
[15] German Police Raid DDoS-Friendly Host 'FlyHosting' – Krebs on Security

The extended supply chain continues to be an attractive target (as discussed in a later section) for those intent on inflicting damage.

Attacks that seek to compromise 'the edge' can involve targeting devices such as VPNs, firewalls, Citrix environments, 'jump' boxes, load balancers, proxies, end-points and out-of-band server management interfaces; especially where their management interfaces are connected directly to publicly accessible internet connectivity. These attack types highlight the ongoing need to build strong security defences, including supporting infrastructure and those provided by third parties and managed service providers, and across the whole attack surface and service inventory.

It is vital to build and maintain an accurate and complete inventory of assets and services in order to defend the full attack surface. Resources, such as the Cybersecurity & Infrastructure Agency (CISA) Known Exploited Vulnerability Catalogue[16], can provide useful intelligence on attack vectors that have actually been exploited, rather than more theoretical attack methods.

More broadly, there are extensive existing security defence guidelines available from the GSMA's Fraud and Security Group (FASG). The GSMA has recently comprehensively updated its baseline controls document FS.31[17], which describes a set of effective and proven security controls that have been developed by GSMA members.
More broadly, some interesting new tools can help design the security defence posture. For example, MITRE has released[18] a 'Navigator' tool to assist in the design of cyber resilient systems and the 'Decider' tool to help analysts map adversary behaviour to the MITRE ATT&CK framework.



[16] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[17] GSMA | FS.31 GSMA Baseline Security Controls - Security
[18] MITRE Releases Tool to Design Cyber-Resilient Systems (darkreading.com) & https://crefnavigator.mitre.org/navigator