RELIABLE NETWORK
SAFE WORLD
TOPSEC

5G 安全威胁技战术研究报告

天融信阿尔法实验室

目录：

一、综述

1.1 5G 发展现状

“互联网+”时代，多样化信息技术长足发展促使互联网产业与普通产业的渗透与融合，多样化的终端接入导致大量的新兴业务场景产生也对通信系统带来的压力呈指数级增长。5G 技术的出现给通信技术带来了新的突破，随着 5G 设备基建的逐渐完善，人们对 5G 的应用前景也在逐渐乐观。5G 不仅满足了人对更高效通信的渴求，也带来了更多的可靠性保证。在大规模的核心设备间的通信过程中，5G 可构建高速、低延时、高质量的网络链接，提高对自主系统和边缘设备的访问效率。在工业上，5G 直接推动了工业 4.0 时代的到来，是制造业、IoT 行业、能源业、医疗业的支撑型产业，是国家层面重要战略支撑点。经 Ericsson 专家组预测，预计到 2024 年为止，将有 15 亿的用户使用 5G 网络，覆盖范围将达到世界人口的 40%以上[1]。5G 技术的长足发展，也带来了边缘节点过载、虚拟化主机资源滥用、恶意利用网络编排器等新的安全威胁。

安全性上，5G 的脆弱性必须在设计最初就加以考虑，新的技术必定会带来新的威胁。在 1G 移动通讯中，面临的是伪基站问题，大量的非法基站非法伪装充斥着 1G 网络。在 2G 中，网络面临的问题是大量的虚假诈骗短信以及大量的营销广播类信息。在 3G 时代，由于终端设备被分配了独立的 IP，使得设备大量暴露在外网，于是设备将面临大量的传统的互联网网络安全问题。在 4G 时代，由于更快更稳定的网速，大量的文本、声音、视频、网络应用等流量出现在移动领域，这导致了移动安全特有的安全问题出现，如针对 IOS 与 Android 设备的入侵、针对指定 APP 的入侵、针对 LTE 设备的入侵等等。

在 5G 时代，网络安全面临的威胁将继续增大。基于 5G 的城市服务设备与工业设备将逐渐增多，如智能家居、车联网等。随着社会进程的推动，直接对接 5G 的设备也将逐渐增多，这些设备的网络安全问题也将逐渐暴露出来。需指出部分 5G 通讯设备和数据是从 4G 或者 3G 中集成过来的，这些被继承的设备和数据其中一些已经暴露出去，与 4G 相比，这些数据可能对 5G 通信造成更大的安全

隐患，比如从 4G 继承过来的数据库密码登录密码、继承的一些服务漏洞等等。同时 5G 通信基建本身也引入了许多新的设备与技术：虚拟化技术、SDN/NFV、切片技术、移动边缘计算等新技术，这些引入的新技术与设备同样会带来新的安全挑战。

1.2 技战术综述

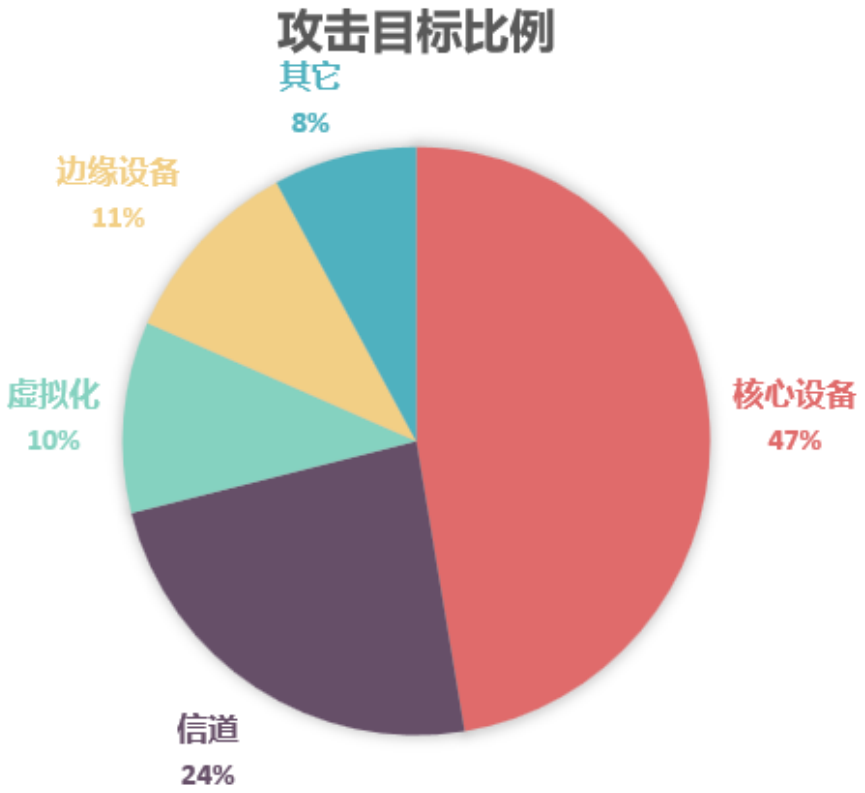
为了更好应对 5G 发展中的新安全风险，天融信阿尔法实验室特编写了本报告。报告介绍了在 5G 场景下一些新引入的 5G 体系结构，并针对这些新体系结构在不同的场景下可能面临的网络安全威胁，进行了技术战术总结。为了能够更好的理解这些安全威胁，需要对新引入的这些体系结构进行介绍。在此基础上，阿尔法实验室对这些信息体系结构进行特有的安全威胁评估，并对评估结果进行技战术（ATT&CK）总结。

i	Technology_Lv2	Technology_Lv1	Tactics	Affect	Aims
0	内存抓取	操作系统凭证转储	凭证窃取	个人用户	核心设备
1	虚假或流氓MEC网关	中间人	凭证窃取;收集	企业级	边缘设备
2	恶意网络功能注册	恶意利用信任关系	初始接入	企业级	核心设备
3	基于UICC格式攻击	利用面向公众的应用程序	初始接入	个人用户	其他
4	虚拟化主机资源滥用	端点设备拒绝服务	影响	企业级	虚拟化
5	恶意修改硬件设备	供应链威胁	初始接入	企业级	其他
6	恶意修改网络配置数据	中间人	凭证窃取;收集	企业级	信道
7	虚假的网络节点	中间人	凭证窃取;收集	企业级	信道
8	测通道攻击	获取已流失凭证	凭证窃取	企业级	核心设备
9	审计工具的恶意利用	审计工具的恶意利用	收集	国家级	核心设备
10	用户身份验证/授权数据的恶意使用	恶意利用储备的身份验证资料	防御规避;横向移动;初始接入	企业级	核心设备
11	恶意远程访问	外部远程服务	持久性控制;初始接入	企业级	核心设备
12	共享资源利用	有效账号	权限提升;持久性控制;初始接入;防御规避	企业级	核心设备
13	地址解析协议(ARP)欺骗	中间人	凭证窃取;收集	个人用户	信道
14	恶意使用数据中心互连(DCI)协议	外部远程服务	持久性控制;初始接入	企业级	虚拟化
15	IMSI捕获攻击	IMSI捕获攻击	收集	个人用户	信道
16	边缘节点过载	端点设备拒绝服务	影响	企业级	边缘设备
17	绕过网络虚拟化	恶意使用权限管理机制	权限提升;防御规避	企业级	虚拟化
18	恶意利用网络资源编排器	恶意使用权限管理机制	权限提升;防御规避	企业级	核心设备
19	利用不安全的用户设备	利用面向公众的应用程序	初始接入	个人用户	其他
20	恶意修改网络流量	数据处理	影响	国家级	核心设备
21	利用配置不当的系统/网络	利用面向公众的应用程序	初始接入	企业级	核心设备
22	漫游身份数据的利用	恶意利用储备的身份验证资料	防御规避;横向移动;初始接入	企业级	核心设备
23	身份验证流量峰值	干扰或拒绝服务	信道威胁	企业级	核心设备
24	流量嗅探	流量嗅探	凭证窃取;发现	个人用户	核心设备
25	MAC欺骗	中间人	凭证窃取;收集	个人用户	信道
26	云计算资源的滥用	端点设备拒绝服务	影响	企业级	虚拟化
27	无线电干扰	干扰或拒绝服务	信道威胁	国家级	信道
28	利用合法的监管功能	外部远程服务	持久性控制;初始接入	国家级	核心设备
29	利用应用程序编程接口(API)	恶意利用信任关系	初始接入	企业级	核心设备、边缘设备
30	操纵网络核心设备配置数据	事件触发执行	权限提升;持久性控制	企业级	核心设备
31	洪水攻击	端点设备拒绝服务	影响	国家级	核心设备、边缘设备、信道
32	利用设计不良的体系结构	利用面向公众的应用程序	初始接入	企业级	核心设备
33	恶意利用频谱资源	干扰或拒绝服务	信道威胁	国家级	信道
34	无线电流量操纵	无线电流量操纵	信道威胁	国家级	信道

如图所示，阿尔法实验室一共总结了 35 个攻击手法，每个攻击技术分别对应着一个或多个战术用途，这些攻击技术细节将在第三部分展开讨论。

1.2.1 威胁集中在 5G 核心网络

5G 具有快速稳定、低延迟、边缘计算等特点，为了支持这些新特点，5G 网络必须对外暴露更多的设备接口与服务接口。正是这些暴露在外的设备与服务接口，导致了这 35 种攻击的出现：



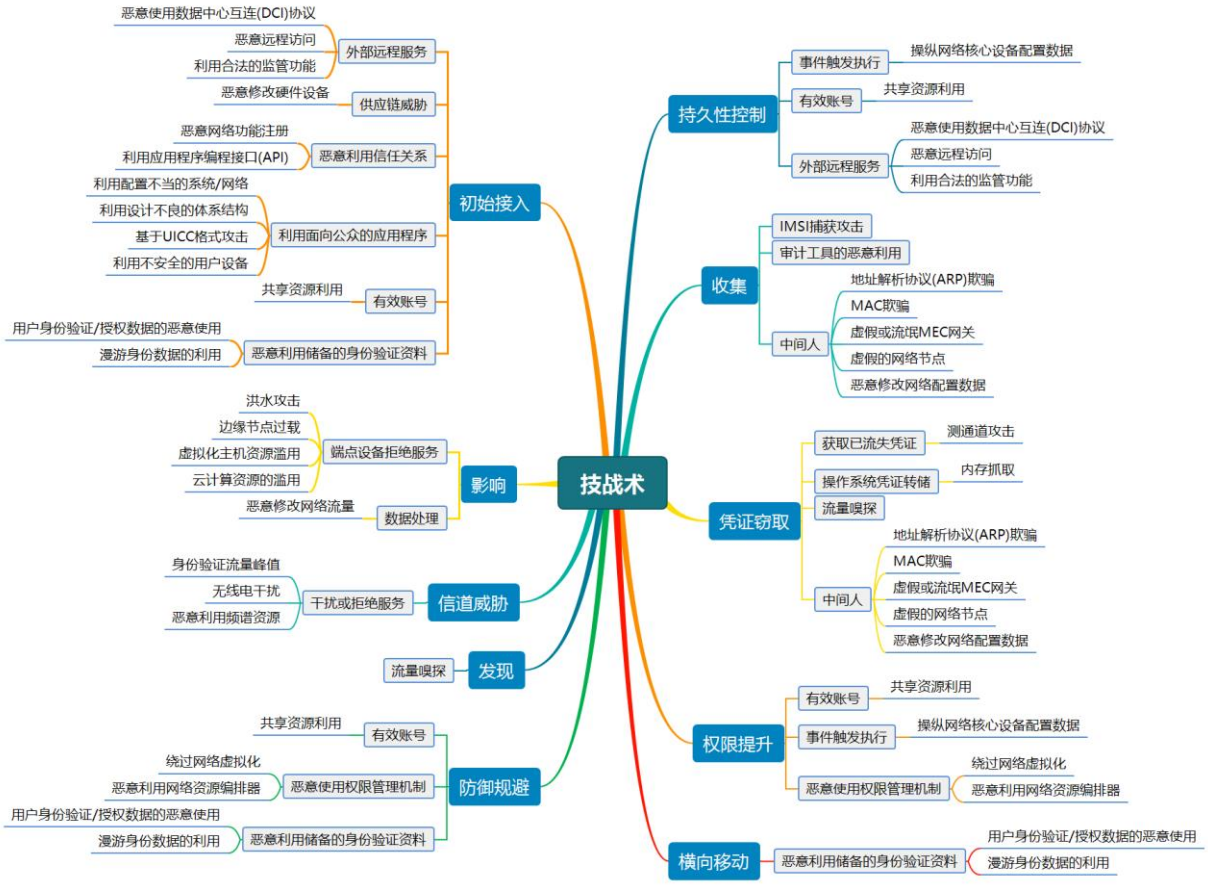
在这些攻击的 5G 设备目标技术手段中，有 11%的攻击手法面向的是边缘计算设备，10%的攻击方式是面向虚拟化设备，24%是针对信道的攻击，47%是面向 5G 的核心网络通信设备。可见在 5G 网络安全的初始阶段，核心网络设备必将成为网络攻击的重灾区。

相较于传统，设备边缘计算、虚拟化设备等是新的设备载体，所以要考虑到未知网络安全问题存在的可能性。诸如在 2005 年英特尔开发 UEFI 规范用于取代 BIOS 的限制，在 10 多年的时间里 UEFI 逐渐得到普及，于 2018 年 APT28 利用操作系统的驱动程序权限漏洞，成功的将 UERI Rootkit 写入 UEFI，用于做到无感知的持久性控制[2]。于此类似，基于 5G 的新功能将会逐渐普及，随着人们对 5G 技术的不断熟悉，对这种未知的威胁的感知也要与时俱进。所以不仅要关注于基

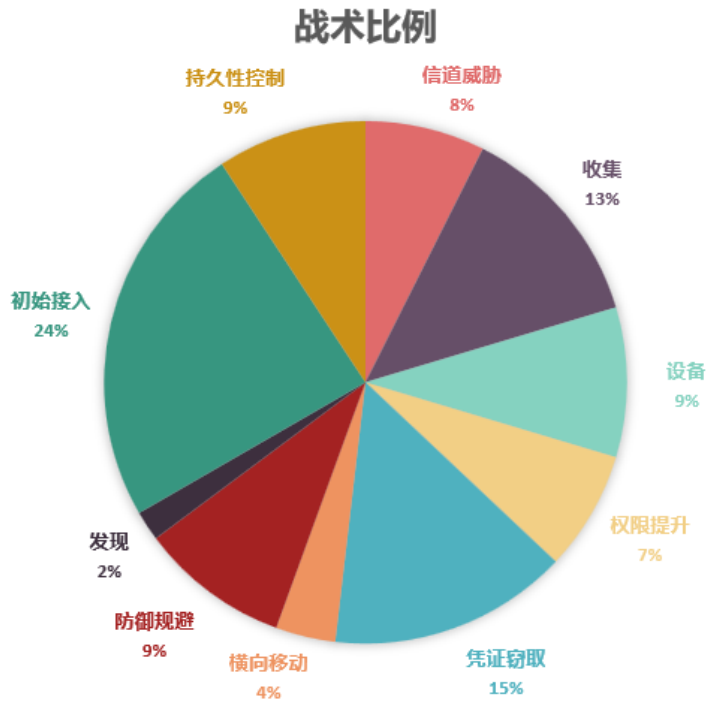
于 4G 网络发展而来的核心设备的安全问题，也要正视新加入的设备安全问题。

1.2.2 初始接入阶段的攻击手段变多

对适用于 5G 环境下的攻击手段进行技战术分类，分类结果如下图所示：



图中这些适用于 5G 环境的攻击手段，被归类在 10 个战术类别中，分别是：初始接入、持久控制、凭证窃取、横向移动、权限提升、防御规避、发现、收集、信道威胁、设备影响。由于存在着单一技术对应多种战术的情况，所以在这 10 个战术分类下技术会出现重复的情况。经过统计，其类别分布如下：

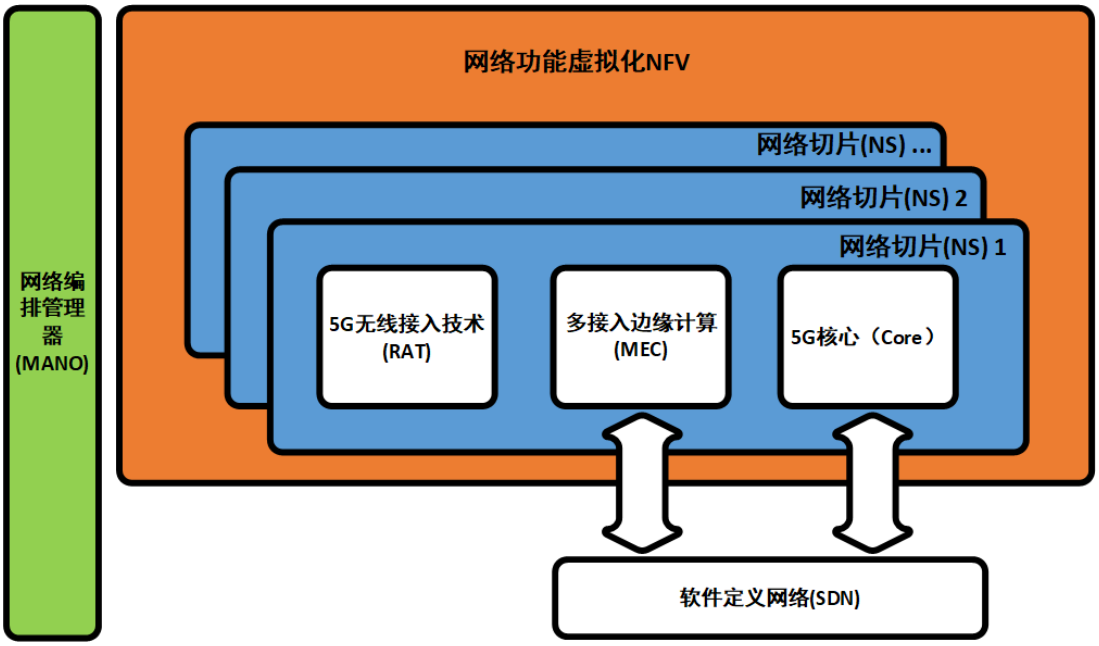


如图所示，适用于初始接入阶段的技术比例为 24%，适用于凭证窃取的比例为 15%，适用于收集的比例为 13%。初始接入阶段占了总比重的四分之一，即是说未来 5G 用户普及后，黑客们在初始入侵的时候可供选择的手段变多了，在入侵之后，可供进行凭证窃取的手段也变多了。所以接下来的防御重点应该放在如何防御初始接入和如何防御凭证窃取上。

二、体系结构

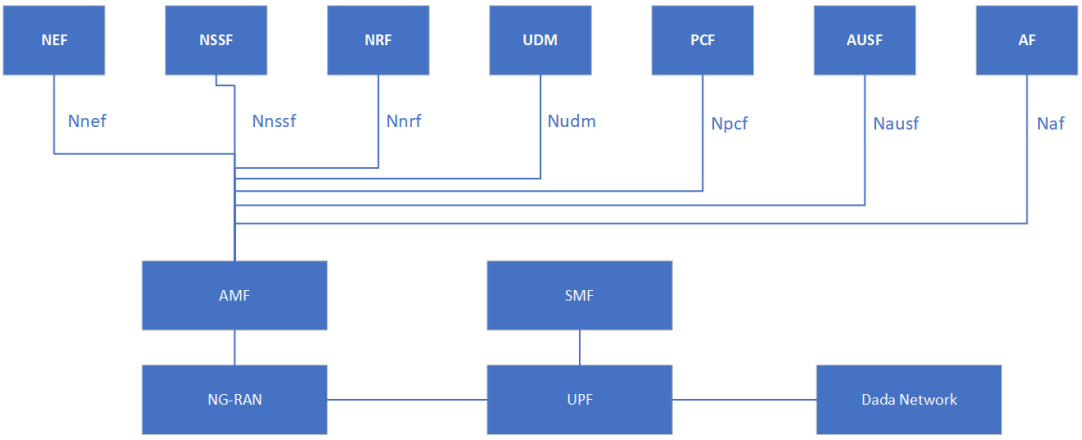
2.1 通用的 5g 体系结构

3GPP 定义的 5G 系统框架是基于服务的[3]，这意味着每一个在 5G 系统框架内的网络功能都将被服务化。每一个服务会对外开放接口，外部程序可以利用基于通用框架的接口与特定服务通讯，用以实现特定的网络功能。在系统框架内的每一个模块，都可以通过网络存储功能（Network Repository Function，NRF）发现其他功能模块提供的服务。5G 体系结构是模块化的，这种模块化的构架设计有利于部署最新的虚拟化软件技术。整个 5G 通用框架如下：



重要的组件包括核心网络（5G Core）、网络功能虚拟化（NFV）、网络切片（NS）、软件定义网络（SDN）、多访问边缘计算（MEC）、无线电接入网络（RAN）、网络编排管理器（MANO）、安全体系结构（SA）。从上图可看出，整个 5G 构架，以网络功能虚拟化技术为基础，使用虚拟化技术模拟与集成 5G 中所使用的组件，并使用 SDN，在 MEC 与核心网络之间进行数据分类传输。

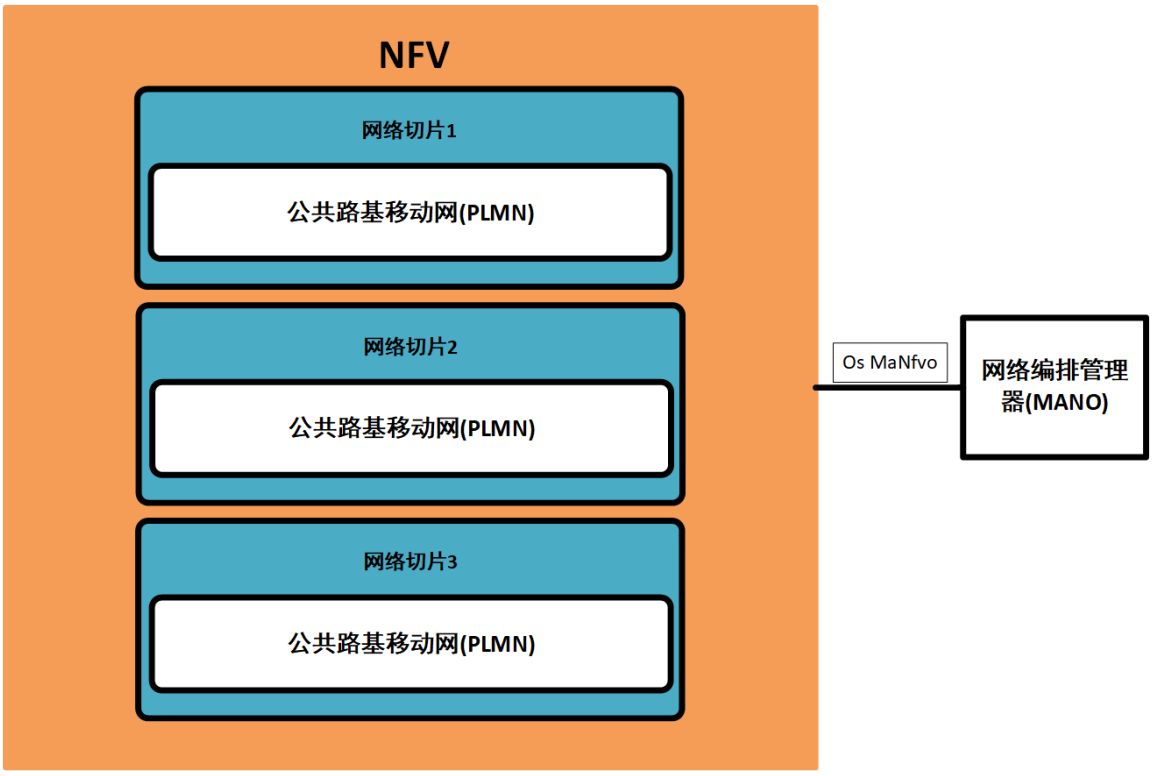
2.2 核心网络体系结构



5G 核心网络，是为了支持更高吞吐量而建立的，是 5G 构架的核心关键系统。3GPP 规定，5G 核心必须采用 SBA 架构来支持云服务。5G 核心的主要功能是负责

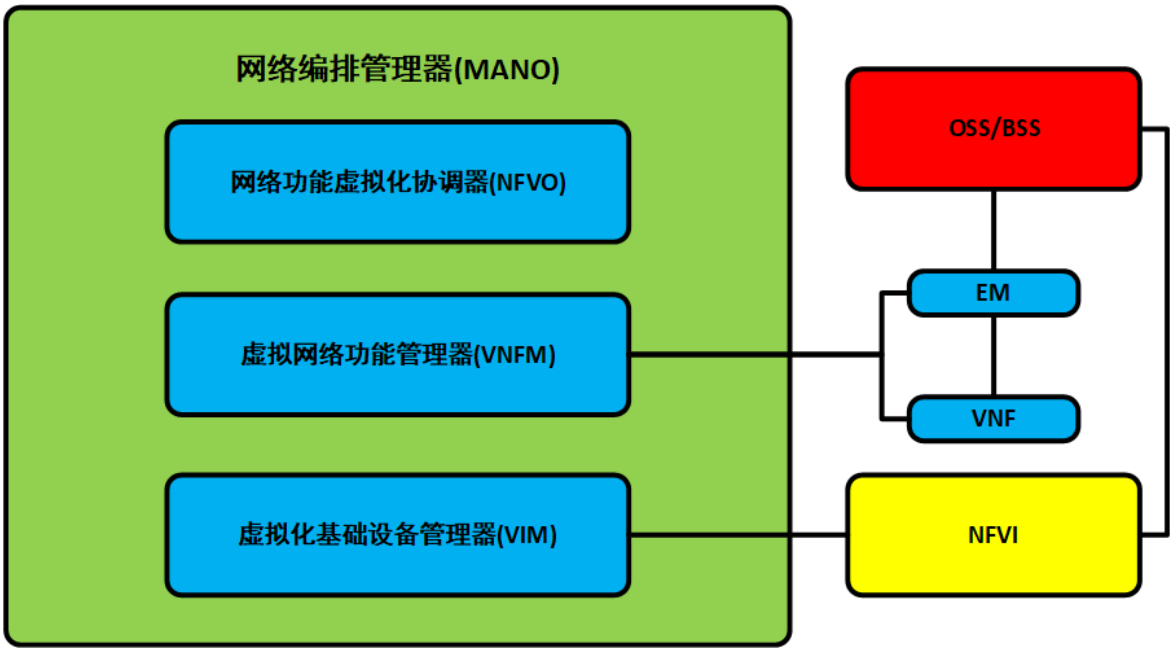
与组件交互，他参与了 5G 的大多数流程，如会话管理、身份验证、通信安全、中断设备流量的聚合、数据同一存储、安全边缘保护代理、密钥管理等。

2.3 网络切片(NS)



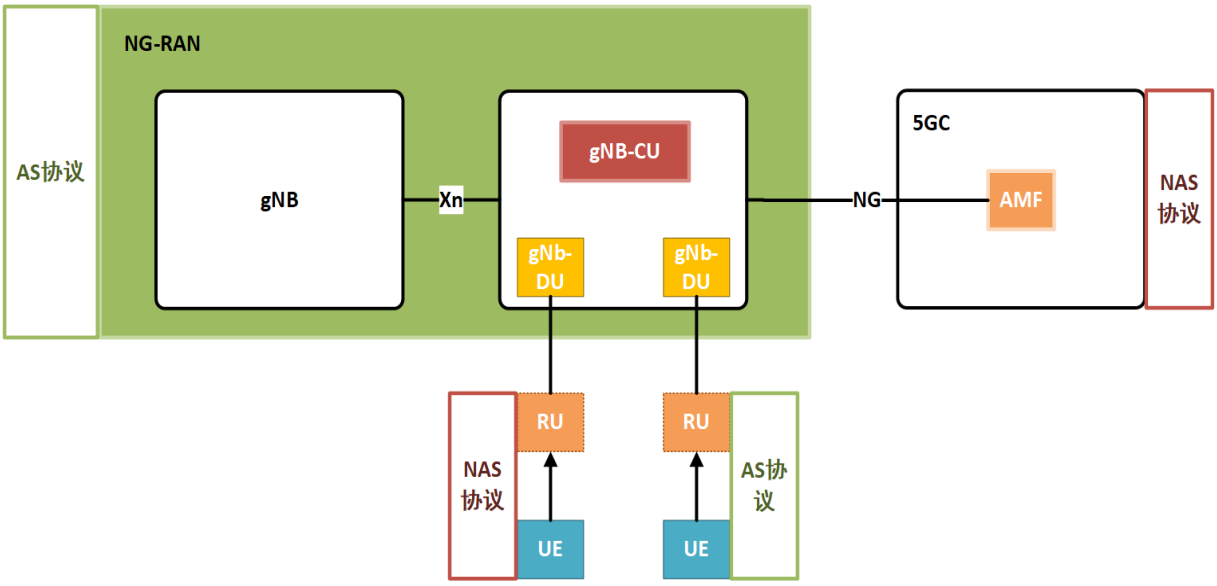
网络切片是以 NFV 为基础而实现的，在 5G 系统架构中是基础支持部分。在 3GPP 定义的 5G 系统构架中，网络切片是通过对指定功能进行模拟集成，共同形成向 UE 设备提供完整 PLMN（公共陆基移动网）功能的系统。5G 环境的切片系统十分强大，包含涵盖了整个 PLMN。网络切片允许建立特定功能的 PLMN 系统，这些定制的 PLMN 将为不同环境下的不同需求提供服务。网络切片是灵活的，其可以根据具体的应用场景，通过 MANO 调整其内部的服务功能。

2.4 网络编排管理器(MANO)



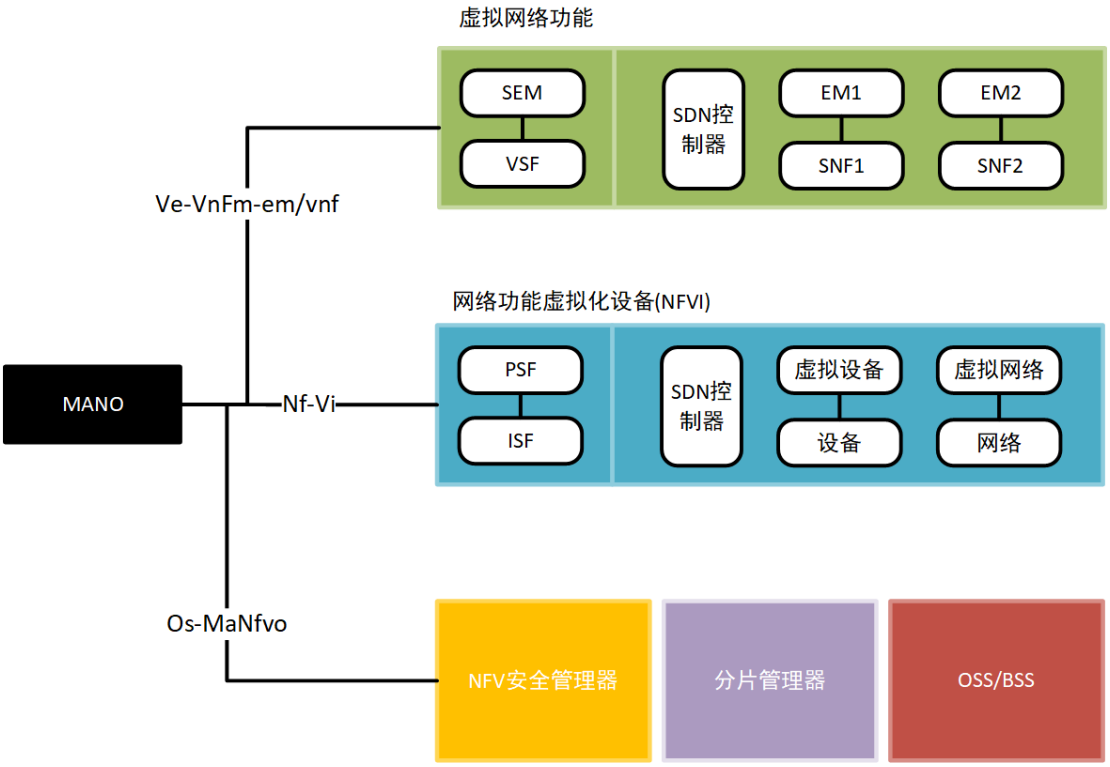
网络编排管理器是 5G 的重要组成部分之一，他负责 5G 所有重要组件的功能配置与管理，包括网络功能虚拟化（NFV）、虚拟化网络功能（VNF）、虚拟化基础设施（VIM）。通过 MANO 可以控制整个 5G 网络的基础设备，所以应该对其进行严格的权限分配，以应对未知风险。

2.5 无线电接入网络(RAN)



在 5G 环境的 NG-RAN 单元中，3GPP 将 F1 接口拆分成三个部分：集中式单元（CU）、分布式单元（DU）、以及服务数据适配协议（SDAP）。在 SDAP 体系中，无论是 CU 的数据包传输协议 PDCP，还是 DU 的空气无线电链路控制 ARLC，所有的传输都是基于 TNL/Ethernet 的 IP 传输。NG-RAN 也可以以服务的形式，在多层结构中适用。这些设计可以有效提高 5G 服务效率，降低的延迟，提高处理能力。

2.6 网络功能虚拟化(NFV)

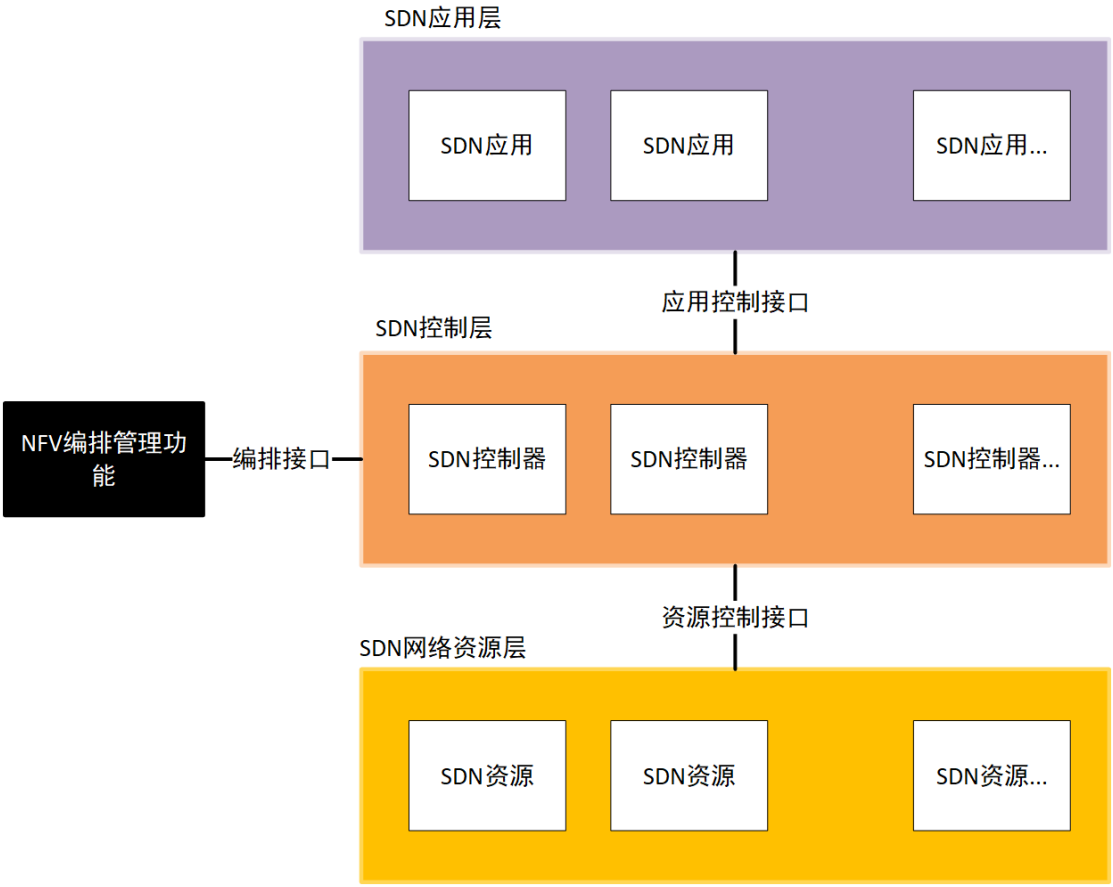


NFV 是 5G 网络最重要的基础服务之一，5G 使用标准 IT 虚拟化技术对网络功能进行虚拟化部署，降低部署门槛，提高通用性，以便更加便捷的提供新的网络服务。5G 网络环境中，网络功能虚拟化(NFV)包含了虚拟网络功能（VNF）、OSS/BSS、以及安全管理软件，他们能够通过 MANO 统一调度与其他功能产生交互，从而使各个模块紧密快速的联系在一起。NFV 具备的功能列表如下：

- 策略控制功能(PCF)
- 会话管理功能(SMF)

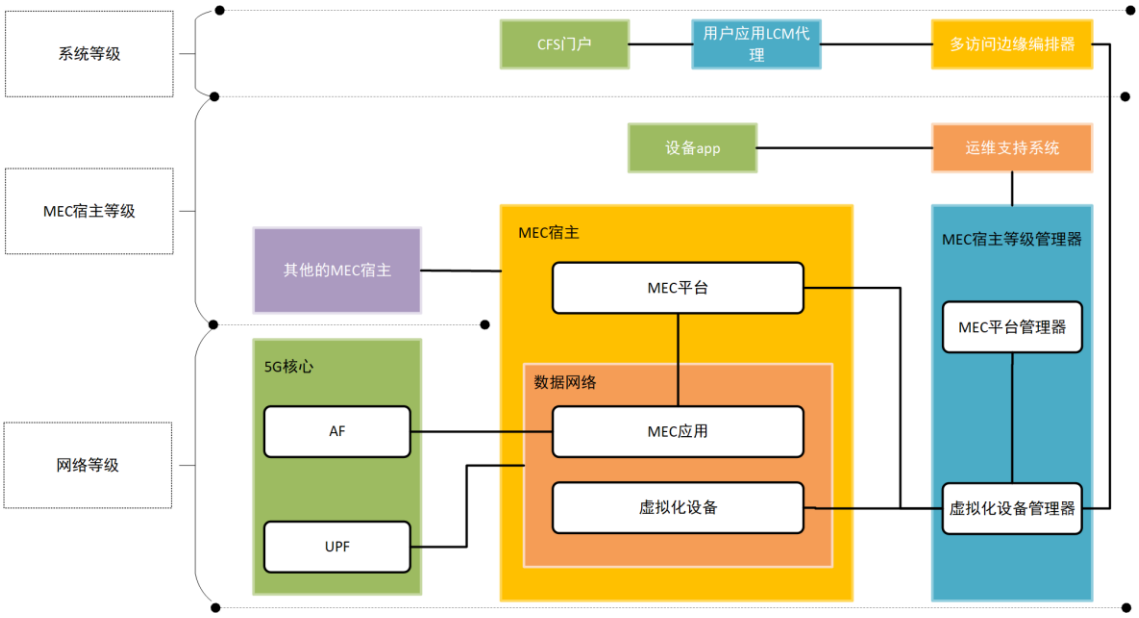
- 统一数据管理(UDM)
- 统一数据存储库(UDR)
- 用户平面功能(UPF)
- 访问和移动管理功能(AMF)
- 非结构化数据存储功能(UDSF)
- 网络曝光功能(NEF)
- 网络存储库功能(NRF)
- 网络切片选择功能(NSSF)
- 应用功能(AF)
- 5G-设备身份登记册(5G-EIR)
- 安全边缘保护代理(SEPP)
- 网络数据分析功能(NWDAF)
- 身份验证服务器功能(AUSF)

2.7 软件定义网络(SDN)



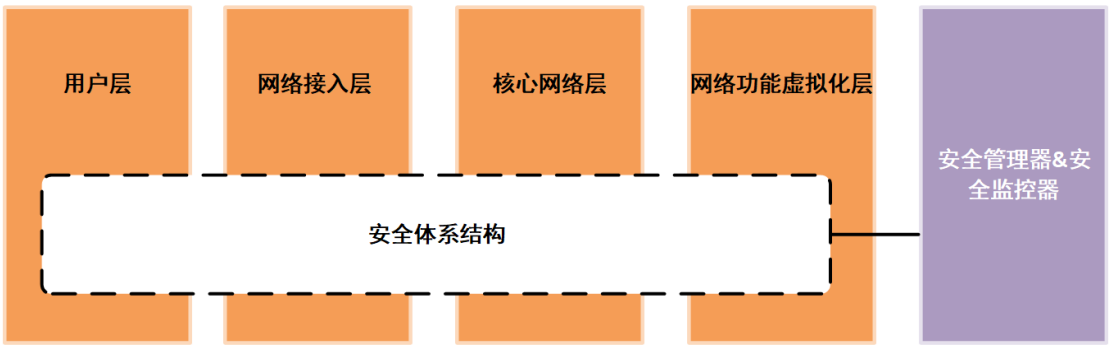
SDN 是 5G 所有的特色服务。SDN 通过解耦网络，来控制、分组、转发网络功能，从而实现对网络功能的集中控制。为了更好的优化网络服务，在 SDN 中，转发和控制是分开的。SDN 依赖于网络中控制和分组转发功能的解耦，在经典网络中，这两个功能由专用物理设备负责，在 SDN 中，这两个功能被隔离为两个功能平面：控制平面和数据平面。网络的功能分离，一方面降低了配置与更改的难度，另一方面，提供了同一的控制器，增加了普适性。

2.8 多访问边缘计算(MEC)



如无人驾驶、远程手术等应用情景，需要极高的带宽、极低的延时。为了确保这些应用可以正确运行，则需要 MEC 服务进行支持。MEC 提供了在网络边缘进行云计算的能力。MEC 通常是已授权的第三方服务，其通常位于基站的逻辑附近，可为 5G 用户提供应对不同场景的处理和存储能力。MEC 是 5G 生态系统中的创新之处，它会覆盖前几代通信设备，来增强用户体验。MEC 可将不同的应用流量，按照类别进行分类处理，如视频、定位位置、虚拟现实等。这样可根据不同的优先级，对有限的资源进行不同的安排。

2.9 安全体系结构(SA)



5G 安全构架负责保护端对端的通信，提供身份验证、安全审计、安全管理等其他安全相关的功能。5G 安全构架由多种网络功能（NF）构成，所以安全体系结构需要横跨很多的其他组件结构。安全构架需要保障 5G 构架的方方面面，如无线电接入网络（RAN）、边缘计算功能（MEC）、网络功能虚拟化（NFV）等。

三、安全威胁

针对上述的 5G 环境，阿尔法实验室总结了适用 5G 环境下的攻击技术，并对其进行技战术分类。需注意的是，多数情况下，这些攻击技术，并不专属于 5G 网络。除少数（如虚假 MEC 节点等），更多时候技术是由传统的网络安全技术发展而来的，如中间人劫持技术，早在 2003 年,Belkin 无线网络路由器进行了一次著名的非加密 MITM 攻击[4]。它会定期接管通过它路由的 HTTP 连接,劫持流量到 Belkin 产品的广告上，在 5G 时代这些诸如中间人劫持的技术还依然延续着。

3.1 初始接入

初始接入，是指攻击者初始入侵目标载体，从而在目标环境中获得立足点的战术。通常情况下，初始接入包含的主要技术方向分三类：劫持运营商设备资产、利用目标网络中风险 IT 资源、利用暴露的风险远程外部服务。除此之外攻击者还会通过具有特殊访问权限的第三方实体或者第三方用户，来接入目标网络。这些受信任第三方，可能包括供应商、维护人员、工程师、外部集成商以及参与物理设备操作的其他外部实体。

这些受信任的第三方供应商是旁路入侵的重点，在 5G 环境中，供应商维护的资产可能包括物理设备、软件、操作系统，有时他们需要根据需求人为的接触设备，这样就很容易通过维护人员感染核心设备。特别是，一些特殊权限的访问权限的 IoT 设备与通信设备，他们在整个网络中处于中间者的位置，一旦权限失守，将会造成不可预估的财产与资源的损失。

初始接入包含的技术也可以适用在一些不安全的信道传输设备，诸如无线电设备、可移动存储设备。攻击者如从感染信道传输设备开始到接入目标设备，管

理者可能是全程无感知。

初始接入	
外部远程服务	恶意使用数据中心互连(DCI)协议 恶意远程访问 利用合法的监管功能
供应链威胁	恶意修改硬件设备
恶意利用信任关系	恶意网络功能注册 利用应用程序编程接口(API)
利用面向公众的应用程序	利用配置不当的系统/网络 利用设计不良的体系结构 基于UICC格式攻击 利用不安全的用户设备
有效账号	共享资源利用
恶意利用储备的身份验证资料	用户身份验证/授权数据的恶意使用 漫游身份数据的利用

在 5G 环境中，初始接入战术包含了六大类具体技术，分别是外部远程服务、供应链威胁、恶意利用信任关系、利用面向公众的应用程序、有效账号、恶意利用存储的身份认证资料。

（1）外部远程服务

攻击者可以研究暴露在外网的远程服务，寻找服务中的默认账号、泄露账号等手段，来入侵目标。如攻击者利用默认的 VPN 账号密码，远程访问服务，便可以直接访问目标内网资源，造成危害。

恶意使用数据中心互连(DCI)协议：

这种威胁适用于虚拟化系统。因为虚拟化系统部署在数据中心内，所以应考虑数据中心的安全问题。攻击者可使用数据中心互连(DCI)协议的特定漏洞，如

使用缺乏认证和加密的密钥通过 DCI 链接创建欺骗性质的流量。相较于传统技术，新的设备使用的技术有时是更复杂的，所以很容易引起这种设计不良导致安全问题。

恶意远程访问：

这种攻击必须先存在一个恶意参与者，恶意参与者通过社工等手段，可以远程访问关键的网络组件，并控制受害机器，以执行其他类型的攻击。远程访问接口是一种常见的接口，可以方便的在远程使用接口，用以维护和使用特定程序。通过非法远程访问功能，恶意参与者可以在外网不受限制的，访问核心领域的操作系统和应用程序。通过访问内部网络中的机器，恶意参与者可以从事其他活动，如篡改配置数据和分发恶意软件。这种技术很常见，并不是 5G 专有，如 APT28 针对格鲁吉亚内政部（MIA）的攻击事件[5]，APT 先得到 MIA 邮件管理员权限，然后使用管理员的权限远程访问邮件服务发送邮件，让 MIA 设置虚假域，以达到进一步入侵。

利用合法的监管功能：

网络运营商、接入提供商、服务提供商等机构，会根据法律或执法机构要求对 5G 流量进行监管管控，以确保社会的和谐稳定。一旦监管机构被渗透，或运营商提供的监管接口不安全，攻击者便可以利用这些安全问题对网络运营商进行渗透，进行未经授权的访问，绕过审核机制，造成网络运营商无法检测的初始渗入。

（2）供应链威胁

入侵者在产品生产，或者软件开发的过程中，对供应链中的组件进行入侵渗透，使正常产品在出厂阶段就具有恶意功能。由于 5G 环境需要大量的新设备，所以要严格注意供应链安全问题。通常针对供应链的入侵，可能发生在产品发售的任何阶段，如带有恶意代码的开发环境、注入恶意代码的公有私有代码库、不安全的更新过程、受感染的可移动磁盘、风险硬件上游厂商提供的硬件、在物流

过程中的拦截、供应商伪造商品等。通常情况下，为了使恶意代码具有更多的执行机会，攻击者会把重点放在软硬件的分发、更新渠道上。

另外许多开源项目也可能成为添加恶意代码的手段。如 2018 年黑客在 Node.js 的库中注入了恶意代码[6]，该恶意代码具有窃取钱包程序中比特币的功能，当时 Node.js 每周下载近 200 万次，含有恶意代码的 Node.js 已被数百万的程序员下载。可见开源程序也会受到供应链威胁。

恶意修改硬件设备：

这种威胁发生在供应商或产品开发商在生产或销售时，供应商有意或无意的在产品中包含隐藏的硬件或软件，使恶意功能随着产品一起售卖到使用者手中。这种威胁发生在产品开发的初始阶段，或者在应用不受控制的更新和新特性的维护过程中。一个典型的案例是在 2018 年，施耐德电气在其太阳能产品 Conext ComBox 和 Conext 电池监视器附带的 USB 驱动器上发现了恶意代码。施耐德表在第三方供应商工厂的制造过程中，示恶意代码就感染了 USB 驱动器。

（3）恶意利用信任关系

是指攻击者利用受信任的第三方来进行攻击。攻击者可能会用诱骗钓鱼或技术入侵等方式接入受信任的第三方，再利用受信任的第三方做跳板对目标进行入侵。通常而言，为了提高效率，目标网络对受信任的第三方的审查会比较少，入侵将变得容易。例如在 2016 年，APT28 先入侵了美国民主党会竞选委员会（DCCC），然后以此为跳板入侵美国民主全国委员会（DNC）控制大选[7]。

通常而言目标网络会向第三方外部合作者提供更高的访问权限，以允许他们管理云环境的内部系统。在 5G 环境中，这些第三方合作者，可能是一些 IT 服务承包商、云托管安全提供商、基础设施承包商等。第三方合作者有时必须利用一些内部访问来维护目标设备，但这个维修用的专线可能与企业的核心信息位于同一网络，这样就导致了可以用第三方合作者的线路，获得内部网络系统的有效帐户，从而达到初始接入的目的。

恶意网络功能注册：

恶意网络功能注册是指内部人员或供应商，向移动网络运营商（MNO）网络中，注册未经授权或被植入恶意代码的网络功能程序，以达到初始接入的目的。在 5G 环境中，服务基础架构（SBA）存在被恶意网络功能注册攻击的风险，攻击者可通过钓鱼、诱骗等方式、将恶意代码在核心网络中注册，然后通过网络存储库功能（NRF）公开其他高风险应用接口。攻击者还可以通过注册未经授权的网络功能，访问网络中的敏感信息，以执行其他类型的攻击，例如 DoS、分发恶意软件、窃取敏感信息等。

利用应用程序编程接口(API)：

应用程序编程接口(API)对 5G 应用生态系统非常重要，因为它允许在不同的网络环境下的实体操作 5G 核心系统暴露的功能。它允许 5G 核心网络环境中的应用和服务，受控于各种互联网运营商。同时要指出，互联网运营商为了向用户提供便捷的功能，亦会向公众提供可编程的 API 接口，这些暴露给公众的 API 接口底层调用的是 5G 核心系统暴露给运营商的接口，如果权限分割管理的不当，运营商暴露给大众的风险接口很有可能威胁到核心网络。

（4）利用面向公众的应用程序

在 5G 网络中，攻击者可能会使用畸形的流量、数据、命令、文件等，向 5G 设备系统或设备中的应用程序漏洞发起攻击，从而引发不可预知的恶意行为。应用程序常见的漏洞有下载执行类漏洞、溢出类漏洞等。系统漏洞引起的可能是系统错误、故障、执行类漏洞、提权类漏洞等。

存在漏洞的应用程序通常是数据库、标准服务、网络设备管理协议应用。有或者是具有公网访问权限的何其他应用程序，例如 Web 服务器和 web 相关服务等。如果一些有风险的应用程序托管在 5G 核心系统架构上，则可能会导致基础实例受到损害。

利用配置不当的系统/网络：

一般这种攻击适用于 5G 的核心网络环境。它是针对配置不当系统或网络的，以专项研究为前提的，基于配置错误漏洞的利用攻击方式。通常这种配置不当会发生在意料之外的场景，攻击者会利用一个系统的错误配置，使其能够在网络中获得敏感资源，从而进行渗透，达到初始接入与持久性控制的战术目的。

在设备或程序开发的每一个不同阶段，都可能发生配置不当问题。如在程序的发布的过程中，debug 开关忘记关闭导致敏感信息泄露问题。在 5G 的环境中，随着核心设备的日益复杂化，可能的出现配置不当的场景也随之增多，如访问控制规则配置、编程使用的 API 配置、安全防护软件配置、网络切片配置、流量隔离配置、管理权限配置、虚拟化环境配置、边缘节点配置、编排软件配置等。

利用设计不良的体系结构：

指的是开发者在开发过程中安全意识不周全引起安全威胁，此种类型威胁适用于所有 5G 核心网络设备。这类威胁通常是无意引起的程序功能缺陷，如在设计开发过程中低估复杂程度导致的构架开发不完善，没有按照安全标准操作等等。通常此类威胁是某一个特定功能没有得到充分的实现和保护引起的，可类比于 IoT 设备比较常见的升级漏洞，在 IoT 设备升级时，风险 IoT 设备由于没有充分校验升级包，导致被植入恶意代码，设备陷落。此类安全缺陷，是开发者在设计阶段就没意识到，进行某项常规功能作业时候的安全隐患，设计出不良的升级体系结构引起的安全问题。

基于 UICC 格式攻击：

新的 UICC 格式可能会导致应用程序和系统不可预测的新漏洞，这些漏洞可能导致：逻辑类漏洞、溢出类漏洞、中间者劫持、欺诈、DDOS、水坑钓鱼等攻击。不同类型的 UICC 的组件会存在不同的问题，如 eUICC、iUICC 引起的可能是基于协议的 Dos、欺诈等攻击，而虚拟 SIM 卡则很可能由于接口的开放，而造成不可预估的逻辑类漏洞和溢出类漏洞。

利用不安全的用户设备：

随着 5G 时代带给移动端厂商的冲击，必将出现大量风险的 5G 用户设备，可能会引入新的漏洞，包括低成本不安全的物联网设备、山寨 5G 手机、低成本低安全保障的 AI 设备等。这些漏洞可能会对用户数据的机密性和完整性做出挑战。

（5）有效账号

指攻击者盗取和利用现有帐户凭据，达到初始接入、持久性、特权升级或防御逃避的目的。被盗取的用户凭证，通常会被用来访问内部网络上共享的各种资料。如果被盗取凭证的权限过高，甚至可能被用来对目标暴露的远程外部服务进行入侵。被盗取的凭证也可以用来做本地提权，或者授予对受限制网络的访问权。如在 2014 年，Duqu2.0 利用 CVE-2014-6324，将非特权域用户升到域管理员帐户，从而进行横向移动，实现进一步渗透[8]。

通常而言，攻击者不会将盗取的有效账号编写在恶意程序内，因为一旦这些黑客工具被截获，关键账户的凭据被盗就会被发现，所以为了隐蔽起见，被盗取的有效账户凭据会与恶意程序配合，但分开使用。

共享资源利用：

这种威胁涉通常是指在共享资源中发现与凭证相关的数据，从而猜到或得到用户凭证，进行渗透入侵，修改或访问未经授权的 5G 设备关键数据。端到端的密钥可能被窃取或从集中的密钥服务器泄漏，因此，端到端安全通信对于攻击者而言是相对脆弱的。被丢弃的缴费单、网络运营商（MNO）的身份认证单等，是攻击者收集账号密码信息的主要手段之一，所以应建立隐私机制，防止隐私信息泄露。

（6）恶意利用储备的身份验证资料

攻击者可以使用储备的身份验证材料，进行初始接入、绕过系统防御、提权、横向移动。这些储备的身份验证资料，包括密码哈希、Kerberos 票根、Cookies、应用或服务的访问令牌。通常，初始的身份验证过程，需要有效的身份验证信息，如用户名与密码、指纹、物理智能卡，令牌生成器等，在用户或应用程序通验证

后，系统会根据合法的登入信息生成备用身份验证数据。种备用的身份验证数据，可用来快速验证访客身份，而无需用户再次提供账号密码重新验证。

由于这些备用身份验证数据必须由使用者维护，所以必须存储在使用者设备的流量、磁盘或者内存中，因此，攻击者可以通过凭据访问包含的技术来盗取身份验证资料。通过使用被盗取的资料，攻击者可以绕过访问安全限制向系统进行身份验证，而无需知道明文密码或任何其他身份验证因素。

用户身份验证/授权数据的恶意使用：

在 5G 环境中，这种威胁会影响多个网络设备点，包括：漫游与垂直服务、移动设备、物联网设备、管理接口等。攻击者通常会尝试钓鱼、社工、账号暴力破解、盗取等手段获得已经验证的用户凭证授权数据。然后使用授权数据掩盖自己的真实身份，骗过核心系统的安全机制，达到初始接入、提权和防御规避的目的。

漫游身份数据的利用:

在漫游的相关场景中，用户通常需要从主网络获取用户身份认证标识符或者其他令牌信息，如果攻击者获得此令牌，可能会利用此令牌访问移动网络运营商（MNO），达到社工、截获验证消息、初始接入、提权等目的。如在 Positive Technologies 的报告中提到[9]，攻击者可利用攻击者可利用 IMSI（订阅者标识符）或 TEID （隧道标识符），进行欺诈信息发布、拒绝服务攻击、恶意使用未授权服务等。

3.2 持久性控制

持久性控制是指攻击者在目标环境中，建立持久性立足点的技战术，用以达到长期控制目标设备，进行进一步渗透的目的。常见的用于持久性技术有：事件触发类、使用有效凭证、使用外部远程服务等。通常而言，攻击者在初始接入之后会建立持久性控制，以达到扩大战果和长期控制的目的。如果在利用暴露在外部的服务时，使用效用户凭证，如 windows 远程桌面，则会产生服务抢占现象，

所以攻击者会选择更谨慎的使用此类技术。除此之外，修改和替换合法的应用程序代码，也是常用的手段。

持久性控制	
事件触发执行	操纵网络核心设备配置数据
有效账号	共享资源利用
外部远程服务	恶意使用数据中心互连(DCI)协议 恶意远程访问 利用合法的监管功能

在 5G 设备上，情景应与 Iot 设备相似，除使用效用户凭证与外部远程服务外，主要的持久性方法应该是修改设备固件或 flash 中的配置信息已达到持久性，属于事件触发执行类技术。由于利用有效账号与利用远程服务，在初始接入阶段已经描述，这里则不再赘述。

事件触发执行：

现代计算机系统，都拥有基于特定事件触发执行的机制，比如双击事件、订阅事件、用户登录事件、启动事件、联网事件等。攻击者可针对计算机支持的各种事件做触发，达到持久性控制、权限提升的战术目的。攻击者获得对受害者系统的访问后，可以创建或修改事件触发流程，用以在操作系统触发执行正常流程时，调用执行恶意代码。如发生在 2017 年的 Amnesia 僵尸网络事件[10]，攻击者会根据当前用户的权限，在/etc/cron.daily/中创建文件，以保证每天都会触发执行，用以维持持久性控制。

修改核心网络设备的配置数据：

一般为读取配置信息时不加校验或限制引起的安全问题。在 IoT 设备中，通常配置信息是直接存储在 flash 芯片里的，在开机过程中，一般会启动很多预置进程，开发者会把要启动的进程的参数写入 flash 的固定地址中，攻击者可以通

过修改此处的内容，影响正常的执行流程，导致的直接后果可能是意料之外的系统行为（如随进程启动）或者未经授权的访问，从而给与攻击者驻留系统的机会，进而威胁网络的机密性和完整性。

在 5G 环境下，这种威胁适用于大多数核心网络设备，如 SDN 控制器、管理和编排功能设备等。攻击者也可通过精心配置数据来发起攻击(DOS)、启动 shell 进程（如 telnetd）、下载恶意程序、启动参数溢出等。

另外，传统的技战术模板中，还存在着“修改引导或修改登录自动启动执行”技术分类，此分类与“事件触发执行”并列在持久性控制里。虽然很多技术（如“修改核心网络设备的配置数据”）可以归类为前者，但经过研究后决定，依然把其放在“事件触发执行”类别中，原因有二：引导和开机自启动在一定程度上也算是“事件触发执行”的一种，可抽象为开机事件触发；另一原因，是因为这些技术，在更多情况下不仅仅具有“修改引导或修改登录自动启动执行”的特征，更多的表现为“事件触发执行”的特征，比如在“修改核心网络设备的配置数据”这项技术中，可通过修改配置影响 link 文件的设置，当管理员或者其他使用者，启动目标文件时候，才会执行恶意代码。

3.3 防御规避

防御规避是指，攻击者为了避免入侵被发现，而对防御者进行的对抗和规避行动。为了确保系统的安全性，通常情况下系统拥有者都会建立一定的防御机制，试图发现或阻拦攻击者的入侵行为。作为攻击者则需要对这些防御机制进行对抗，使其攻击的每一个环节都不可见。防御规避所包含的技术种类繁多，常见手段有：恶意数据去特征化、抑制危险报告响应、软硬件漏洞利用。除此之外，攻击者还可以伪装或侵入到特定的设备或进程中，利用受信任的设备或进程来隐藏其恶意行为。

防御规避所包含的技术，由于存在必须不引起防御机制预警的特性，所以其手段要被动很多，比如 APT 组织图拉的多脚本链运行技术，把一个技术流程，分批次的，缓慢的分解执行。甚至有些防御规避技术不是面对防御系统，而是面对人。如利用欺诈性邮件，让管理员暂时关闭防火墙。

防御规避	
有效账号	共享资源利用
恶意使用权限管理机制	绕过网络虚拟化 恶意利用网络资源编排器
恶意利用储备的身份验证资料	用户身份验证/授权数据的恶意使用 漫游身份数据的利用

针对于 5G 环境，可使用于防御规避技术有：利用有效账号、恶意利用频谱资源、恶意使用权限管理机制、恶意利用储备的身份验证资料。其中有效账号和恶意利用储备的身份验证资料不再累述。

恶意使用权限管理机制：

攻击者可能会通过技术或社工手段提升权限，利用权限管理规则达到逃避监管的目的。大多数现代系统，都包含了权限管理，这种权限管理限制用户在计算机上的执行特权。换而言之用户必须得到较高的授权，才能做被认为具有较高风险的操作。

绕过网络虚拟化：

这种威胁建立在不安全的切片实现或不安全的切片配置上，一旦被恶意利用，可能导致机密数据泄露、绕过流量监管等后果。在切片系统中，不同的租户使用的网络，需要确保只有符合规范的流量，才能进入或离开特定的网络切片系统，而这些规范通常是由用户的需求产生的，所以根据不同的需求需要不同的安全级别来隔离数据，以防止攻击者入侵其他切片流量。如果攻击者，在核心网络级别上，对管理层的服务与应用进行漏洞利用，破坏切片规则侵入低安全管制的流量，那么很有可能做到规避安全管制逃离或入侵目标网络。

恶意利用网络资源编排器：

此种威胁是针对网络资源编排器的攻击行为，这种威胁通常是通过恶意修改

编排器中的设置，来影响网络编排器的网络行为，导致网络功能模块的分离被打破。此种威胁的影响与绕过网络虚拟化类似，不再累述。

3.4 权限提升

特权提升包含攻击者用来在目标设备或网络上,获取更高级别权限的技术。攻击者通常可以进入和探索无需权限即可访问网络,但是通常而言攻击者的目标都是被隔离或者被保护起来的，需要攻击者提升权限才能实现他们的目标。例如由 user 权限提升到 admin 权限，或者由 admin 权限提升到 system 权限等。常见方法有：系统漏洞提权、配置漏洞提权等。

权限提升所使用的技术通常与防御规避、初始接入是重合的。

权限提升	
有效账号	共享资源利用
事件触发执行	操纵网络核心设备配置数据
恶意使用权限管理机制	绕过网络虚拟化 恶意利用网络资源编排器

在 5G 环境中，提升权限的方法分为：利用有效账号、事件触发执行、恶意使用权限管理机制。这些战术下包含的技术，前文都已说明，此处不再累述。

3.5 横向移动

横向移动所包含的技术，是指攻击者在目标网络设备上移动的技术。这些技术通常被用来侵入和控制同一网络环境下的其他设备。其包含恶意盗取使用有效账户、暴力破解、漏洞利用、社会工程学等。通常横向移动战术的起始位置是内网环境与外网环境的交叉点，如在 2015 年 Maccaglia 揭露了一次 APT28 的网络攻击，在外网 APT28 利用鱼叉钓鱼成功入侵了内部人员拥有的可移动系统，然后内部人员携带带有恶意代码的系统接入到内网，APT28 以此电脑为根据点展开横

向移动，攻陷目标网络的其他设备。

攻击者使用横向移动包含的技术，在目标环境中，将恶意行为转移到下一个设备，直到将自身移动到其认为合适的位置为止。通常而言，攻击者如果想要进行横向移动，需要先遍历目标网络，收集目前网络中的设备信息，找到其下一个目标，随后找到侵入目标的方法对目标进行渗透。多数时攻击者会尝试利用默认的工具使用默认的账号密码来进行横向移动，如失败则会安装自主开发的定制的远程工具来完成“横向移动”。

横向移动	
恶意利用储备的身份验证资料	用户身份验证/授权数据的恶意使用 漫游身份数据的利用

在 5G 环境中横向移动战术包含的技术为使用备用身份验证资料，前文已经描述不再累述。

3.6 凭证窃取

凭证窃取战术，是攻击者利用社会工程学、密钥记录、转储技术，在目标设备上窃取目标的账户名和密码。使用合法的凭据可以在访问目标系统的时候提高隐秘性，配合防御规避中的日志删除技术，可以做到无感知入侵。通常窃取到的凭证会具有很高权限，可利用高权限创建更多其他账户，用以实现攻击者的战术目标。

凭证窃取	
获取已流失凭证	测通道攻击
操作系统凭证转储	内存抓取
流量嗅探	流量嗅探
中间人	地址解析协议(ARP)欺骗 MAC欺骗 虚假或流氓MEC网关 虚假的网络节点 恶意修改网络配置数据

在 5G 环境中，凭证盗取战术包含：获取已流失凭证、操作系统凭证转储、窃取已认证的凭证、暴力破解、网络嗅探、中间人攻击等。

（1）获取已流失凭证

攻击者可以利用不安全的系统，获取或推演出已经流失的凭证。这些流失凭证曾经可能被存放在系统的任何位置，包括磁盘上的文本文件、命令行的历史记录、存储库中、输出的 log 中等等。攻击者通常会使用工具直接读取这些凭证，但多数情况下这些凭证都是使用后删除，所以可以收集相关的线索推理还原出凭证，或通过技术手段恢复曾经使用的密码。如在 2018 年巴西，黑客使用 NetPass 工具来恢复 LAN、邮件、IE 浏览器、远程桌面曾经使用过的密码，以此来进行进一步入侵[11]。

侧通道攻击：

测通道攻击又称旁道攻击，与传统的凭证获取技术不同，它基于现实中的物理现象来推测密码，而非使用暴力破解或者算法中弱点破解。例如，利用 5G 设备的运算时间信息、消耗功率变化、电磁变化、声音变化，建立网络链接所需时间等，来还原推断出用户凭证或加解密过程中所需的密钥。通常整个测通道攻击过程，需要目标系统的内部信息才可以进行（半黑盒），比如加密解密使用的算

法，在对算法有一定了解的基础上，才可利用侧通道攻击拿到算法密钥。

（2）操作系统凭证转储

攻击者通常会尝试从操作系统或者从第三方软件中转储凭证，这些凭证通常是以 hash 或者明文密码存在的。当攻击者获取凭证成功后，会利用其对受限制的网络进行访问、横向移动。有时安全维护人员也会对系统的凭证进行转储，所以除了攻击者自定义的工具，攻击者也会使用一些通用凭证转储工具，如上文提到的 2018 年巴西的例子。

内存抓取：

内存抓取是指，攻击者利用内存扫描，或者在内存中进行数据结构解析，从内存中提取未经授权的敏感信息的技术手段。特别是一些面向用户的 IoT 设备，用户往往会使用远程登录或者直接接触来登录设备设备，很多情况下，设备是根据账号密码生成的 Hash 的进行校验，想要碰撞 Hash 有时并非易事，但是攻击者却可以通过内存抓取的方式，抓取内存中未来得及销毁的账号密码。

（3）流量嗅探

流量嗅探是攻击者为了探测目标信息的常用方法。攻击者会在流量中探索与目标有关的信息，被嗅探的信息会因其重要程度不同而造成不同重要程度的后果。一些信息泄露威胁程度较低，如广播通知、浏览的网页信息、DNS 解析信息等等。另一些信息则威胁程度较高，如密码 hash、Telnet 账号密码等，这些未加密的协议都可以在流量中被找到，从而造成的更严重的危害。另外流量嗅探也可以用于识别目标设备身份,如获取目标设备的系统版本号、主机名、VLAN ID 等。嗅探攻击可能发生在 5G 中的任何情景中，如在软件定义网路（SDN）中，攻击者可以针对中央控制器的未加密流量进行拦截嗅探，获取关键信息。

（4）中间人攻击

攻击者通常会尝试使用中间人攻击（MiTM）技术，将自己放在两个或多个互

联网设备之间，用以支持诸如网络嗅探、数据窃取等后续恶意行为。中间者攻击通常被用来进行流量操作，如记录、修改和阻止流量，或者将新的流量注入到通信流。通过修改流量，攻击者可以做到防御规避（阻止检测报告）、事件触发执行（修改参数）、未授权的命令执行等。

地址解析协议(ARP) 欺骗：

这种攻击也被称为 ARP 缓存欺骗。攻击者通常会发送欺骗性质的 ARP 消息，将攻击者的 MAC 地址与另一个目标主机的 IP 地址相关联（如默认网关），从而导致将该 IP 地址的任何流量发送给攻击者。ARP 协议是无状态的，不需要身份验证。因此，设备可能会错误地在其 ARP 缓存中添加或更新 IP 地址的 MAC 地址。要完成此种攻击，攻击者需使用自身的 MAC 进行 ARP 请求回复，同时要比合法的 IP 地址更快的答复 ARP 请求，之后被动的等待 ARP 数据感染目标设备的 ARP 缓存，从而使受害者相信他们正在与预期的互联网设备交互。

MAC 欺骗：

MAC 欺骗是一种在网络设备上改变 MAC 地址的技术。通常 MAC 欺地址是固化在网络接口控制器(NIC)上的，基于此，MAC 欺骗可分为两种：使用设备厂商提供的驱动修改 MAC，虽然 MAC 被要求固化在设备上，但是一些厂商仍然会提供驱动接口修改此 MAC；此外，还有一些工具可以欺骗系统，使其相信当前使用的 NIC 具有选择 MAC 的功能。本质上，MAC 欺骗的目的是伪装成另外的设备，进行下一步欺骗攻击。

虚假或流氓 MEC 网关：

在 5G 网络种，由于 MEC 边缘网关具有一定的开放性，所以用户自身的设备也可以作为边缘设备的一部分参与进来，如私有云、智能电视盒等等。从而让攻击者参与到恶意 MEC 网关部署的情景种，从而获得中间人攻击的机会。

虚假的网络节点：

攻击者把虚假基站伪装成合法的基站，一旦基站的合法性认证成功，则可以进行中间人攻击、截获凭证、修改流量、伪造信息进行社工。

恶意修改网络配置数据：

由于对关键配置数据的保护不足，可能导致不可预测的系统行为，或导致未经授权的访问，从而影响网络的机密性和完整性。在 5G 环境中，这种威胁会涉及许多核心网络功能，如 SDN 控制器、网络管理和编排器等。原则上，这种攻击可以涉及到 5G 环境中的任何组件数据，所以这项技术用途也很多（如提权、长期驻留），比较常见的有：路由表修改、Host 配置文件修改、DNS 修改等，这些攻击是中间人攻击的必要步骤，所以把此类攻击归类为中间人攻击。

3.7 发现

攻击者调查目标环境，并获得有关内部网络、系统设备、敏感知识的技术。这些技术可帮助攻击者观察环境，并帮助其决定下一步横向移动的目标。在发现和探索的过程种，攻击者通常会把可控制的设备和关心的敏感知识作为目标，并对收集来的信息进行分析，制定下一步计划。同时“发现”所包含的技术，多数情况下也可以用来进行“收集”战术，以帮助攻击者获得敏感的内部资料的目的。从工具上来讲，可以用来发现的工具，通常是使用目标设备上自带的功能接口，编写的自定义工具或脚本来完成的。

在 5G 环境种用于发现的技术为流量嗅探在前文中已经介绍，这里不再累述。

3.8 收集

攻击者在入侵成功后，会尝试收集他们的感兴趣的数据，如受保护的文档、未公开的代码文件等等。通常来说收集数据的下一步操作就是把收集的数据渗透出去，常见的收集目标包括驱动器类型、浏览器数据、音频、视频、电子邮件等。

收集	
IMSI捕获攻击	IMSI捕获攻击
审计工具的恶意利用	审计工具的恶意利用
中间人	地址解析协议(ARP)欺骗 MAC欺骗 虚假或流氓MEC网关 虚假的网络节点 恶意修改网络配置数据

（1）IMSI 捕获攻击

IMSI 捕获攻击是指，攻击者通过安全漏洞，收集 IMSI 与设备的对应关系，进而对受害者发起粗粒度定位、拒绝服务等攻击的技术手段。此威胁与蜂窝寻呼协议有关，受害者附近的攻击者可以利用蜂窝寻呼协议将受害者的身份 ID（例如 TEID、电话号码、微博 ID）与受害者的寻呼时机关联起来。这种攻击名为被称为“ToRPEDO”攻击[12]，随后攻击者可以利用 IMSI 收集受害者的粗粒度位置信息，或注入伪造的寻呼消息发起拒绝服务攻击。

（2）审计工具的恶意利用

通常移动网络运营商（MNO），会使用审计工具对信息进行综合审计，恶意攻击者可以使用社工钓鱼等手段，获得 MNO 内部人员权限，进而从审计工具中提取敏感信息。在 5G 环境中审计工具通常被 MNO 来监视网络的活动，审计工具统计的信息，可用于多种目的，如开发优化、信息安全、商业推荐等。在审计工具的数据库中，往往保留了有关网络配置及其用户的信息统计信息，这些信息可降低攻击者寻找目标制定方案的难度。

3.9 信道威胁

攻击者通过操作流经设备的信号或流量，达到拒绝服务、降级协议等恶意目

的。这类技术通常可用来影响信道资源的分配与传输，从而营造对攻击者有利网络的环境。如恶意利用无线电频段、无线电干扰等。

（1）干扰或拒绝服务

攻击者可能会干扰无线电信号（例如 Wi-Fi、蜂窝网络、GPS），以防止移动设备正常运行，从而给攻击者创造有利时机。

身份验证流量峰值：

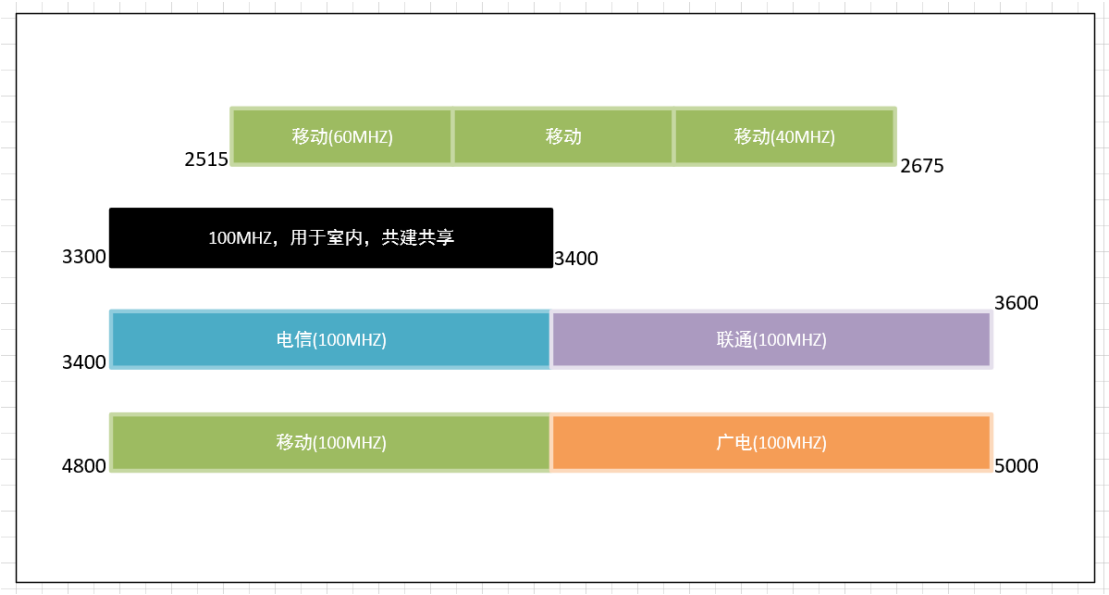
此威胁是指攻击者在短时间内，向 5G 系统发送的大量身份验证请求，造成拒绝服务的情况。恶意攻击者会让身份验证类的信号或者流量，达到 IoT 设备能响应的峰值，此时设备将遇到很多急需处理的信号和身份验证请求，导致机器性能下降，或触发限制规则，限制网络，降低用户体验。此类攻击可被视为拒绝服务的特殊情况，这种攻击可能导致已经授权设备的身份验证失败，从而导致连接丢失。

无线电干扰：

攻击者可以短暂或持续性的干扰无线电接入相关的网络服务，通常会造成无线电接入服务阻塞、或者由于噪声过多而无法响应，妨碍目标用户使用网络资源。

恶意利用频谱资源：

由于各个运营商的不同，5G 频段分配方案也不同，攻击者可以利用空闲的频段资源进行 CC 通信、信息渗漏等事件，从而达到防御规避的目的。通常而言，实际中一般不会出现空闲频段，各个频段已经被运营商所占用：



但很多时候这些频段资源是可以根据配置信息动态分配的，如果攻击者抢占一些频段资源，则可能会允许攻击者模仿合法的单位，占用特定的空闲频谱带，对正常的无线电频率造成干扰。由于缺乏空闲资源的实时客观存在着，频谱的这种非法占用还可能导致网络节点拒绝尚未得到许可的机构对频谱资源进行申请，从而将某人或阻止从核心网络中拒之门外。

3.10 影响

攻击者用技术手段破坏、危害、操控目标，致使目标操作系统、设备、数据的完整性与可用性遭受损害。影响包括可直接影响和间接影响。直接影响的技术可能会导致目标系统，任务流程意外中断、设备环境的损坏、数据的丢失等，如 DDOS 造成的设备意外重启等。间接影响的技术则相对温和，被控制或破坏的操作系统设备可能看上去是正常运行，但是实际上已经进行了更改，如入侵后破坏了安全防护程序的报警功能等。通常而言攻击者渗透的最终目的就是为了要影响设备，但也有可能是以影响设备为掩护，进行更机密的行动。

影响	
端点设备拒绝服务	洪水攻击 边缘节点过载 虚拟化主机资源滥用 云计算资源的滥用
数据处理	恶意修改网络流量

在 5G 环境下，影响包括端点拒绝服务与数据处理。

（1）端点设备拒绝服务

攻击者通过 DoS 攻击，破坏设备的功能，影响设备正常运行。如在短时间内，向目标设备进行大量设备不知如何处理的网络链接请求，使目标设备不堪重负，导致设备响应中断或响应超时。根据设备自身定义一些规则，设备可能因为响应超时、意外崩溃等原因，在 DoS 攻击下不停重启，并影响设备的正常使用。除此之攻击者也可以利用程序、服务、内核、硬件逻辑等错误，使目标程序执行攻击者的控制代码，导致设备看似正常运行，但是对外界刺激无反应，引起拒绝服务。如西门子 SIPROTEC 设备漏洞 CVE-2015-5374[13]，此漏洞利用成功后，目标设备将停止对任何命令的响应，直到手动重启为止。

洪水攻击：

在 5G 环境中，这种攻击可发生在无线电对外接口上，攻击者通过传输大量数据来产生洪水攻击，这些数据可以迅速耗尽组件资源，导致组件射频减少或完全关闭。洪水攻击也可能发生在特定的 SDN（软件定义网络）组件中，攻击者只需发送一小部分请求，SDN 控制器会将这部分请求放大，引发大量的请求响应。虽然很多现有的网络协议已经设计了针对这种攻击进行了保护，但 SDN 控制器的引入，却提供了更多洪水攻击的可能性。洪水攻击也可能来自于大量的分布式 DoS 攻击，如网络僵尸引起的 DoS 攻击事件，攻击者可以感染大量的网络设备作

为 DoS 攻击的基础，同时向同一目标进行攻击。

边缘节点过载：

在本地或在特定服务器上，对指定的边缘网络进行网络攻击，这些攻击会干扰边缘设备临近的网络区域。通常攻击者会由特定的网络应用程序或者由特定的物联网设备，向边缘节点组件发起大量请求，导致某特定边缘节点过载。

虚拟化主机资源滥用：

是指在虚拟化主机上运行的应用程序，恶意占用来自虚拟化环境的共享资源。在虚拟主机租户之间，会在环境中共享一些物理资源，攻击者可能会通过这些共享资源获取敏感信息。如，在虚拟环境中，从已经弃用或删除的资源中获得敏感信息所造成的危害，要比在物理系统中更巨大。如果在虚拟环境中共享资源被抢占或独占，那么其危害将更大，因为这将导致相同物理设备上的其他虚拟环境中的服务，在使用资源的时候发生等待释放的情景，从而导致外部请求无响应类 DoS 攻击。

云计算资源的滥用：

用户通过简单的注册，就可以在云计算服务的运营商处获得强大的云计算基础设施。攻击者可以利用强大的计算能力，在很短的时间内发动暴力破解攻击或 DoS 攻击。

（2）数据处理

攻击者可能会对数据进行插入、与修改，导致其外部结果不准确，从而隐藏自身的活动、影响决策者的决定、影响业务流程。修改的目标数据，其类型及其所产生的影响，取决于被修改的数据以及攻击者的意图。对于一个健全而复杂的系统，攻击者可能需要长期驻留在其中，反复的对数据进行修改，以达到目的。

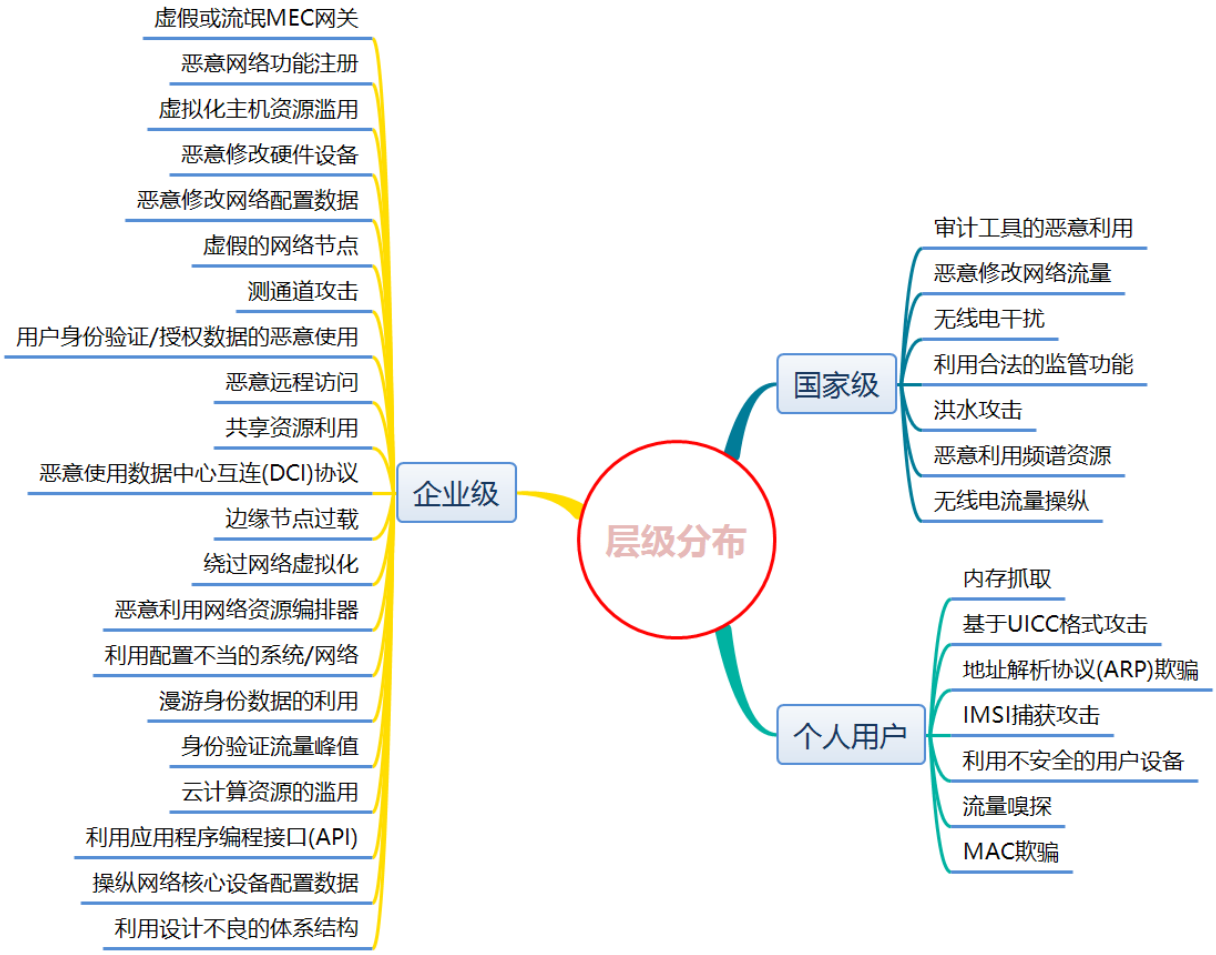
恶意修改网络流量：

恶意修改网络流量是指，修改或伪造正在传播途中的数据，或者向目标网络注入数据的技术手段。这类攻击通常是由信息校验不严格导致的攻击，攻击者通常会识别流量中的文档信息，修改相关的数据或文本，或延时转发数据。以达到影响决策者或者业务流程的目的。

四、受众目标

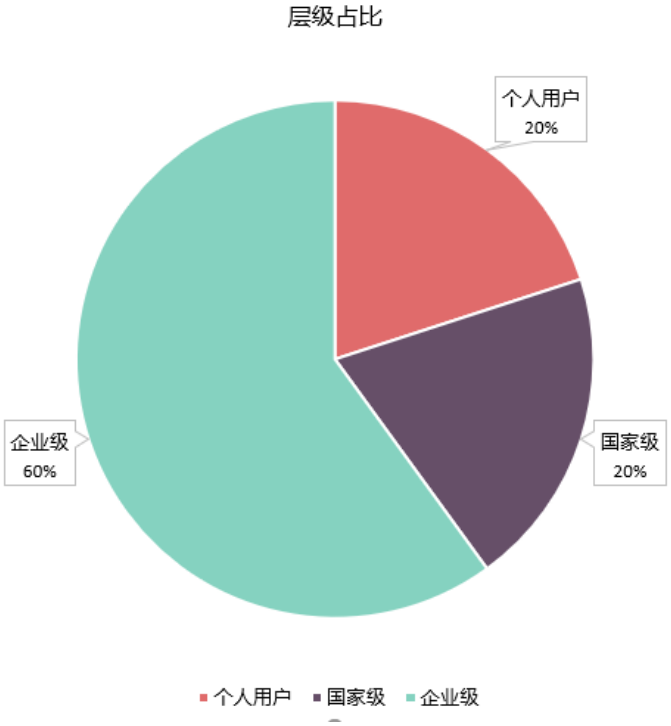
5G 环境所带来的安全威胁，其威胁目标是不同的，如 IMSI 捕获攻击，其面向的目标是个人的隐私信息，再如恶意利用频谱资源攻击，其面向的目标则为国家分配的频段资源。虽然这些威胁目标各不相同，但仍可按其所影响的受众层级进行分类。监管和研究机构可根据其分类等级不同进行不同的处理。

各级别具体分类如下：



层级分为三部分：个人用户级、企业级、国家级。这些级别的威胁程度逐渐

增加，最低为个人用户级，最高为国家级。这些层级为向下包含关系，即在国家级的威胁技术同样适用于企业级与个人用户级，其严重性是逐渐提高的。



同时从数量上来看，企业级占比是最高的，为 60%，国家级威胁占比 20%，个人用户级威胁占比 20%。可见 5G 环境下安全威胁都集中在企业级，少数分布在国家级与个人用户级别。

4.1 个人用户级

Technology_Lv2	Technology_Lv1	Tactics	Affect	Aims
内存抓取	操作系统凭证转储	凭证窃取	个人用户	核心设备
基于UICC格式攻击	利用面向公众的应用程序	初始接入	个人用户	其他
地址解析协议(ARP)欺骗	中间人	凭证窃取;收集	个人用户	信道
IMSI捕获攻击	IMSI捕获攻击	收集	个人用户	信道
利用不安全的用户设备	利用面向公众的应用程序	初始接入	个人用户	其他
流量嗅探	流量嗅探	凭证窃取;发现	个人用户	核心设备
MAC欺骗	中间人	凭证窃取;收集	个人用户	信道

个人用户级所包含的攻击手段，通常被用于攻击个人用户终端。这些攻击手段通常只关心个人的存款、个人隐私、个人的知识产出。虽然有些攻击手段同样适用于企业级甚至国家级，但是最常见的攻击目标却是普通的个人用户，如 IMSI 捕获攻击、流量嗅探这样的技术，其攻击目的则是获取个人用户的位置等隐私信息，但是如果这个目标用户恰好是某个政客，则其影响则可能更广，不过这类技

术最常见的是针对目标是普通个人用户，所以归类为个人用户级。这类威胁主要集中在个人的信息泄露和个人的隐私窃取上，尤其在用户设备这一方向，用户很轻易的就会选择不安全的 5G 设备，如山寨手机、山寨路由器等等，这些设备中往往会存在者大量漏洞和问题，严重威胁着个体用户的网络安全。

4.2 企业级

Technology_Lv2	Technology_Lv1	Tactics	Affect	Aims
虚假或流氓MEC网关	中间人	凭证窃取;收集	企业级	边缘设备
恶意网络功能注册	恶意利用信任关系	初始接入	企业级	核心设备
虚拟化主机资源滥用	端点设备拒绝服务	影响	企业级	虚拟化
恶意修改硬件设备	供应链威胁	初始接入	企业级	其他
恶意修改网络配置数据	中间人	凭证窃取;收集	企业级	信道
虚假的网络节点	中间人	凭证窃取;收集	企业级	信道
测通道攻击	获取已流失凭证	凭证窃取	企业级	核心设备
用户身份验证/授权数据的恶意使用	恶意利用储备的身份验证资料	防御规避;横向移动;初始接入	企业级	核心设备
恶意远程访问	外部远程服务	持久性控制;初始接入	企业级	核心设备
共享资源利用	有效账号	权限提升;持久性控制;初始接入;防御规避	企业级	核心设备
恶意使用数据中心互连(DCI)协议	外部远程服务	持久性控制;初始接入	企业级	虚拟化
边缘节点过载	端点设备拒绝服务	影响	企业级	边缘设备
绕过网络虚拟化	恶意使用权限管理机制	权限提升;防御规避	企业级	虚拟化
恶意利用网络资源编排器	恶意使用权限管理机制	权限提升;防御规避	企业级	核心设备
利用配置不当的系统/网络	利用面向公众的应用程序	初始接入	企业级	核心设备
漫游身份数据的利用	恶意利用储备的身份验证资料	防御规避;横向移动;初始接入	企业级	核心设备
身份验证流量峰值	干扰或拒绝服务	信道威胁	企业级	核心设备
云计算资源的滥用	端点设备拒绝服务	影响	企业级	虚拟化
利用应用程序编程接口(API)	恶意利用信任关系	初始接入	企业级	核心设备、边缘设备
操纵网络核心设备配置数据	事件触发执行	权限提升;持久性控制	企业级	核心设备
利用设计不良的体系结构	利用面向公众的应用程序	初始接入	企业级	核心设备

企业级威胁包含的攻击手段，通常被用于攻击企业或组织的服务或设备。其可以影响一个企业或组织的正常运作，或盗取一个企业的知识财产。与个人等级不同的是企业级类攻击一般是极其由针对性和目的性的，进攻发起人一般为某黑客组织，这些黑客组织受雇于竞品公司、政府机构、做空公司等。其一般渗透目标明确，渗透手段成熟。同样此级别的技术通常也可以用来在国家级设备或机构上产生攻击，但是通常而言，常见的此类技术攻击场景，都将在企业级机构中。即使这种攻击引起了国家战略资源损失，但是其直接作用面也是在企业层面的，如 2009 年震网行动，攻击者利用漏洞，攻击伊朗工业设施，导致大量工业设备无法正常工作。

企业级威胁在技战术层面上，都集中在初始接入、权限提升、凭证窃取等技战术上，这是由企业级机构的特点决定的，通常而言 5G 在企业或组织中的应用是通过服务体现的，新增加的服务必然会带来新的入侵点，如通信网络中，网络供应商通常会向大的合作公司或者组织提供编程 API 接口，这种接口一旦出现逻

辑漏洞或权限漏洞，则极容易被用作企业级的网络攻击。

4.3 国家级

Technology_Lv2	Technology_Lv1	Tactics	Affect	Aims
审计工具的恶意利用	审计工具的恶意利用	收集	国家级	核心设备
恶意修改网络流量	数据处理	影响	国家级	核心设备
无线电干扰	干扰或拒绝服务	信道威胁	国家级	信道
利用合法的监管功能	外部远程服务	持久性控制;初始接入	国家级	核心设备
洪水攻击	端点设备拒绝服务	影响	国家级	核心设备、边缘设备、信道
恶意利用频谱资源	干扰或拒绝服务	信道威胁	国家级	信道
无线电流量操纵	无线电流量操纵	信道威胁	国家级	信道

与企业级威胁不同的是，国家级威胁所包含的攻击手段，通常被用于直接攻击国家所拥有的社会和军事资源，以影响决策则产生决策。社会和军事资源一般会受到比较全面的保护，很少有直接作用其上的攻击手段。国家级攻击手段一旦攻击成功，则通常会具有较高的管理权限和地域影响力。攻击者可以通过国家级的攻击手段，影响执政机构的信息流通，影响决策者的决策，影响国家的正常运作，如 2015 年 12 月，乌克兰伊万诺·弗兰科夫斯克地区停电事件[14]，在事件中，攻击者对电话系统进行拒绝服务攻击，阻碍事故报告，延长了停电时间。

五、防御手段

通过分析归类 5G 环境下的网络安全威胁，可以从如下几个方面给出防御意见与建议：

5.1 开发阶段防御

在开发过程中，开发人员的安全意识会影响到安全威胁技术防御的各个方面。所以需要对开发人员进行网络安全意识培训，在开发初期就尽量考虑安全问题，提高开发质量。在开发阶段，首先要确保应用程序不会以明文的形式存储敏感数据或者凭证数据，在凭据验证时采用 Hash 验证，而非明文比对。可以鼓励开发人员对敏感数据进行非对称加密解密，或进行远程存储，并禁止开发人员将敏感数据打印到本地 log 日志上。

对于危险函数，要在确保其参数不被外部影响的情况下适用，如 system 函数，其参数需要不能被外界影响与修改，或者直接使用安全替代类函数如 execl 等。在进行堆栈操作时，要充分校验数据的上下限以防止崩溃溢出产生。对于屏幕抓取，安卓开发人员可以使用 FLAG_SECURE 将其敏感数据应用在敏感屏幕上，从而使捕获屏幕内容更加困难。对于已经完成的代码，可虑使用代码审计工具进行自动安全审计。对于硬件设施，推荐把芯片型号信息从丝印上移除增加破解难度。在使用第三方功能库或使用第三方硬件时，应尽量考察其历史安全性，对第三方设备或第三方库进行安全评估，严防供应链攻击。

5.2 密码防护

密码相关的防御手段，主要防御的初始接入、横向移动等战术。密码的设置规则需要满足一定的强度，推荐使用 NIST 的密码规则以保证强度[15]，其可有效防止暴力破解等技术，增加暴力破解的难度。不要在系统之间重复使用本地管理员帐户密码。确保密码的复杂性和唯一性，以使密码不会被破解或猜测。在程序安装后或部署到生产环境之后，应立即修改默认密码，如有可能，应定期更新使用 SSH 密钥的应用程序。

在密码存储的过程中，应使用高强度的 HASH 进行存储，应该避免明文存储。每一个用户的默认密码应随机生，避免使用固定默认密码。应尽量密码存储在云设施上，以避免被本地接触获取。在 web 应用的环境中，可根据当前服务的重要

性，修改凭证存储策略，如高权限账户禁止缓存 cookies 等。在内存 dump 方面，有些密码会被有意或无意的存储在正在运行的进程中，如 windows 的 lsass 进程，开发者应在驱动层对这种关键进程进行隔离，使被保护进程运行在沙箱里，或者使其他进程无法对被保护进程进行内存读写操作，以防止内存被 dump。最后，在密码生成时，密码应该与设备进行关联，当本设备的密码丢失，可以有效控制影响。

5.3 合法性校验

此种防御是指使用数字签名或其他安全手段，来验证待运行程序、待读取文件、待接收数据的合法性。此种防御主要用来对抗权限提升、防御规避、持久性控制。校验的过程中，应采用非对称加解密算法，以防止数据被篡改。

对于即将运行或即将安装的应用程序，操作系统需验证其程序签名，当不符合规则时禁止运行。对于 TSL 等通信协议，应校验证书的有效性与合法性，对于证书应设置过期期限，在算法选择上需尽量避免选择低版本的算法，以保证算法的强壮性。在系统启动过程中，从 bootloader 开始，每一步都要验证即将要启动的子系统的合法性，这样可以大大提高接触类的破解的成本，防止固件和芯片被进一步破解。在读取配置文件时，也要对配置文件或注册表中的每一个配置变量进行合法性校验，尤其在 IoT 设备中应该特别注意，很多时候攻击者为了达到长久驻留的目的，会修改 IoT 设备中的配置变量，当配置变量在程序或脚本中展开的时候，很容易造成任意执行的漏洞，达到长期驻留的目的。

5.4 特权提升防御

特权相关的防御手段，主要用于防御权限提升战术和持久性控制战术。攻击者通常是从低权限账户开始的，所以应从账户管理与账户策略入手。

在账户管理上，应从本地管理员组删除不经常使用用户，必须保证在终端上，禁止管理员权限缓存，如在 linux 中把 timestamp_timeout 设置成 0，强制要求用户每次执行 sudo 时候都输入管理员密码。分化用户组，为特定需求定制特定

权限的用户组，此用户组里的用户只能做特定的事情。禁止使用管理员权限做日常操作。在 windows 系统上 PowerShell 的使用应限制为系统管理员。system 服务单元文件的创建和修改也应该限定为管理员。管理员的凭证应该与任何其他账户不同。

同时，在文件访问方面应做好文件的读取和访问权限分离，特别是禁止制所有关键 log 日志的删除权限，以方便入侵检测。特别要注意对配置文件和注册表的权限管理，低权限用户应无权访问配置文件。在进程通信方面，应禁止和调试相关的函数的调用，并施行重要进程单独隔离的策略，防止内存抓取和注入。在公用库加载方向也需要进行权限管理，防止发生通过加载共享库提权。同时应阻止用户改变和历史记录相关的环境变量。在网络方面，应该对网络构架进行细分，不同的网络构架设置不同的权限，对敏感域应该采用网络分段管理，并隔离 SNMP 流量。

5.5 反病毒与反入侵防御

反病毒与反入侵相关防御手段适用于各个技战术环节。其可分为本地反病毒防护与网络反入侵防护。

在本地防护方面，需要管理者及时对设备固件进行更新，病毒数据库进行升级，漏洞及时用补丁修复。应按照需求进行定时定期反病毒扫描和安全漏洞扫描，安全级别较高的设备推荐以每小时为单位扫描一次。目前的网络环境是具有高对抗性的，所以理应提高安全检测级别，即开启本地反病毒引擎的 rootkit 检测功能和启发性检测功能。

在网络防护方面，需要对防火墙进行配置以限制非授权人员对关键系统和域控制器的访问。对于设备访问而言，需要限制端口访问，即仅允许必要的端口访问和流量进入和退出网络。同时也需要对流量中的数据进行检测，需要配合势态感知和公开威胁情报，识别流量中的恶意流量。在必要时防火墙需要具有断网自保护的权限。

5.6 其他类防护

在 5G 环境中，可根据目标设备的情况限制安装硬件插件。很多设备如虚拟化服务器，由于其支持硬件扩展，这也就侧面增加了接触类的初始接入手段，所以需要根据设备的使用情况，限制硬件设备的扩展性，如限制即插即用设备等。

如环境允许，开发者应该考虑远程 log 记录方法，即定时的上传 log 到远程服务器，或者直接把 log 日志打印到远程服务器的接口上。这样做的好处显而易见，除了可以防止设备被入侵后，入侵记录资料被销毁，还可以让安全维护人员远程查看 log 日志，以便及时发现问题。

在设备上，需要做受损设备检测，一旦发现意外受损或者人为破坏等情况，应做到第一时间感知。在重新写入设备启动引导程序时，需要进行设备引导锁校验，如很多手机刷固件时需要进行注册解锁，以方便提前发现设备恶意更改，提高漏洞挖掘难度，增加溯源性。

六、总结

本文对 5G 网络威胁的技术进行了战术分类与受众分类，对分类结果进行了数据统计与结果展示，并在文章的末尾对一些常见的攻击技战术的防御措施进行了讨论。本文填补了三方面空白，即 5G 环境下网络威胁的技战术分类、5G 威胁的受众层级分类、技术级别的防御意见。

在第一章，文章对 5G 的大环境进行概述，并对技战术分类情况进行统计，得出结论：5G 的攻击主要发生在初始接入阶段，其威胁的目标主要攻击都集中在 5G 核心网络层面。

第二章，介绍了一些 5G 特有的体系结构，为后面的章节做知识铺垫。

第三章，对 5G 环境下的网络攻击进行一些技战术总结，并对每一个技战术点进行介绍与讨论。这些技术一部分是 5G 环境特有的，一部分则是从传统网络安全集成过来的。技术所对应的战术是一对多的，技术固定但使用方式灵活，即是说同一技术可被用来达成多种战术目的。

第四章，对这些威胁技术的危险程度进行了评级，评级分为个人用户级、企

业级、国家级，其威胁程度逐级增加，并向下包含，即国家级的威胁对于企业级也适用。

第五章，结合技战术分类，给出防御意见。与其他不同，本文是从技术与实战的角度出发给出的防御意见。

进攻与防御是相互对抗的，攻击者往往利用一些逻辑或技术上的漏洞，对目标进行攻击，而防御者在知晓（或提前发现）漏洞的情况下进行补救。攻击者为了不被防御则往往会投入巨大精力在比较生僻的地方下功夫以求突破。然而技术上的对抗始终是道高一尺魔高一丈，在技术上可以成功的事情，按照其成功概率一定会复现成功。在技术固定的情况下，这是确定的事情。整个环节中唯一不确定的则是由人操作的环节，在某些情况下人的网络安全意识是脆弱的，即使发现了攻击者的入侵痕迹，也会因为当时个人的状况等因素，概率性的忽略掉。如在传统网络安全中，成功率最高的初始接入依然是带有社会工程学性质的钓鱼技术，其目标在人。

所以网络安全除了技术上的对抗，更多的是要提高相关人员对网络安全的意识，所以应该多对用户进行网络安全培训，告知用户什么情况可能是被入侵了，入侵的应急处理应该是如何，为了不被入侵用户平时应该在使用产品的时候注意些什么。提高用户认知，防范这因为意识不足导致的后知后觉。而在组织和国家层面，应该预备更完善的应急响应方案来处理突发事件，并应定期进行公司、学校、组织、社区规模的网络安全演习防范未然。

关于天融信阿尔法实验室

天融信阿尔法实验室成立于 2011 年，一直以来，阿尔法实验室秉承“攻防一体”的理念，汇聚众多专业技术研究人员，从事攻防技术研究，在安全领域前瞻性技术研究方向上不断前行。作为天融信的安全产品和服务支撑团队，阿尔法实验室精湛的专业技术水平、丰富的排异经验，为天融信产品的研发和升级、承担国家重大安全项目和客户服务提供强有力的技术支撑。

引用：

[1] https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-world-economic-forum.pdf

[2] https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

[3] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2885

[4] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[5] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

[6] https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

[7] https://www.justice.gov/file/1080281/download

[8] https://www.secureworks.com/research/bronze-union

[9] https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf

[10] https://unit42.paloaltonetworks.com/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/

[11] https://www.cybereason.com/blog/information-stealing-malware-targeting-brazil-full-research

[12] https://homepage.divms.uiowa.edu/~comarhaider/publications/LTE-torpedo-NDSS19.pdf

[13] https://us-cert.cisa.gov/ics/advisories/ICSA-15-202-01

https://paper.seebug.org/1047/

[14] http://aeps.alljournals.ac.cn/uploadfile/aeps/20160125/%E5%88%98%E5%BF%B5%E7%AD%89.%E7%BD%91%E7%BB%9C%E5%8D%8F%E5%90%8C%E6%94%BB%E5%87%BB%EF%BC%9A%E4%B9%8C%E5%85%8B%E5%85%B0%E5%81%9C%E7%94%B5%E4%BA%8B%E4%BB%B6%E7%9A%84%E6%8E%A8%E6%BC%94%E4%B8%8E%E5%90%AF%E7%A4%BA.pdf

[15] https://pages.nist.gov/800-63-3/sp800-63b.html