网络如何工作：

计算机互相连接构成计算机网络，该链接可以是有线连接方式例如拨号连接、光纤，也可以通过无线连接，例如wifi、数据网络等。

主要通过 “包”的传递进行通信和交互，将数据等其它信息经过一层层协议的包裹进行发送，最终在目的地进行拆分组装。

网络安全的未来

网络威胁发展趋势：

1  网络攻击与物理攻击结合；

2人工智能恶意软件放大攻击者的能力（因为它是基于AI的，所以这种新型恶意软件将能够从其环境中学习，分析应用程序和系统以实时发现和利用新的漏洞。在这种情况下，很难区分哪些是安全的，能够免受未经授权的访问影响，而哪些是不安全的。即使以前被认为受到良好保护的信息也有可能会受到损害）

3针对联网车辆及家居的攻击数量剧增（如果这些电器受到攻击者操纵，同切被切换为“全功率”（full power）模式，将会产生意想不到的功率需求，最终造成电力过载并导致地区电网不能正常运行。随着电网宕机或严重退化，组织的能力将被削弱并难以发挥作用。）

4网络安全人员成泄露组织机密（内部威胁一直很重要，稍一出错就可能使整个组织陷入危险境地。漏洞悬赏和道德披露计划的建立，加上网络犯罪或黑客对于机密信息的需求，都促使漏洞信息的价值不断攀升。）

应对措施：

1加强《网络安全法》的完善与实施，国与国直接进行合作保护网络空间的安全；

2 培养网络安全的专业人才，提高法律和到的修养。

3加强身份认证技术：随着越来越多用户访问远程或者云端资源和越来越多的物联网设备，身份已经成为当前最主要的攻击对象。

4采用安全的协议，例如Https全面替代Http。

5对于入侵检测、漏洞挖掘和修补等领域，加强与人工智能领域的合作，只有借助机器自动化秒级的响应速度才能控制网络安全威胁。