在计算机科学中，图是由两个部件组成的一种数据结构：顶点 (vertices) 和边 (edges)。一个图 G 可以用它包含的顶点 V 和边 E 的集合来描述。尽管传统的深度学习方法被应用在提取欧氏空间数据的特征方面取得了巨大的成功，但许多实际应用场景中的数据是从非欧式空间生成的，传统的深度学习方法在处理非欧式空间数据上的表现却仍难以使人满意。很多应用场景中，图结构是十分关键的，因此产生了图神经网络。

在课程学习中，我们基本了解了图嵌入与图神经网络，简单了解了基于GCN的节点分类，在网络安全方面，图神经网络GNN除了可以用在恶意代码检测以外，还可以运用在很多其他方面。

图神经网络可以运用在社交网络安全上。目前的深度学习针对对象主要是图像、语音和文本，端对端的学习机制使得深度学习的效率有了很大的提高。在图神经网络上，扩展了深度学习对于非欧几里得数据的处理能力，而现实世界中社交网络就是一个典型的图结构。目前针对社交网络主要的安全问题在于：恶意软件、钓鱼攻击和隐私泄露等，由于图神经网络有着良好的对非规则数据提取的能力，因此除了应用在生物医疗中的分子结构以外，可以较好的解决上述的安全问题。针对钓鱼攻击，可以针对钓鱼URL，采用诸如PangeRank一类的网页排名算法，利用图神经网络对非欧几里得的数据处理能力，智能的判断一个网页的真实性；针对恶意软件，由于图神经网络针对文本有很强的分类、分析能力，也能够很好的识别出某软件是否是恶意的，目前恶意软件主要有恶意浏览器插件和第三方恶意软件等，图神经网络可以在用户安装使用这些软件前对其进行扫描识别，从而提醒用户该软件的安全性；社交网络安全中，社交的安全是重中之重，例如经常有某用户谎称是朋友的朋友来添加好友，并且进一步实现其恶意目的，由于图神经网络的高效性，可以通过图结构来快速判断假冒用户的社交网络图，以大致分析其是否在说谎，从而避免很多诈骗、隐私泄露等行为的出现。

除了在社交网络上的应用，图神经网络在识别分类上也有良好的应用场景。进而来讲，图神经网络在WEB安全上有着良好的表现。针对目前流行的WEB攻击例如SQL注入攻击、溢出攻击、XSS攻击和CSRF等，已有很多深度神经网络能够很好的对抗，其原理就是通过大量的样本来提取请求特征，从而判断是否符合上述攻击类别的典型特征。随着黑客技术手段的不断提升，攻击方式也越来越复杂，例如文件上传漏洞中可以综合运用13中不同的变异手段来构造请求消息从而实现文件上传（【NDSS 2020】FUSE: Finding File Upload Bugs via Penetration Testing）。针对这样的攻击手段，图神经网络可以依靠其良好的特征提取、分类能力，更好的识别出恶意请求，从而很大程度避免这样的攻击事件的发生。

除上述应用以外，我认为图神经网络还能在入侵检测等方面发挥作用。比如工业风控方面，当收到请求时，需要实时的判断这是真实用户还是机器流量，可以通过一个使用的数据包括设备ID、IP、用户以及其行为数据的模型来判断，在入侵检测上图神经网络也能很好的进行异常检测、特征检测等。