

GPS威胁基础知识

卫星导航信号正面临日渐增多的威胁，那么这些威胁会对您的关键系统造成怎样的影响，以及您应当如何应对？

执行综述

来自太空的卫星导航信号强度非常弱，很容易受到阻挡以及越来越多威胁的损坏或破坏，包括太阳活动、人为干扰、恶意GPS信号伪造，以及定位和计时信息的人为操纵。

今天，各个行业对GNSS信号和数据的依赖程度越来越高，因此理解并减轻这些威胁就成为制造商、系统和应用供应商，以及终端用户的一项至关重要的风险管理活动。

本白皮书将帮助人们理解影响GNSS依赖系统的风险因素，并确保采取适当的措施来减轻此类风险。您将在其中了解到：

- GNSS所面临不同威胁的简介，以及它们的演化趋势
- 评价您系统对GNSS威胁易感性的一些指导
- 减轻GNSS服务中断、错误和/或关键系统所受网络攻击风险的最有效技术概览
- 思博伦GNSS威胁评估和减轻服务的简介

GPS还是GNSS？

全球定位系统（GPS）曾经是世界上惟一运行的全球导航卫星系统。今天，已经有了多个专门为军事和民用用途提供时间和位置信号的卫星系统。它们包括俄罗斯的GLONASS、中国的北斗和欧洲的Galileo，还有一些区域性的系统。这些系统被统称为全球导航卫星系统（GNSS）。除非需要特指某个特定的系统，我们将在本白皮书中都使用该术语。

GPS威胁基础知识

引言：我们对GNSS的依赖与日俱增

几乎在人们毫无察觉的情况下，全球导航卫星系统（GNSS）已经开始在我们的日常生活和我们的世界产生巨大的影响。

目前，众多设备和系统都依赖来自GPS和其它卫星系统的数据，而这些系统提供的服务正是我们所依赖的。

例如：

在世界上的各个集装箱港口中，自动化的吊车通常要在GNSS引导下吊装正确的集装箱，并将其移动到正确的地方。

在海运行业中，船舶使用GNSS实现导航并将其作为自动识别系统（AIS）的基础，该系统能够在全世界范围内跟踪船只的运动和位置。

在3G移动网络中，GNSS信号提供的精确时间被用于实现呼叫信号在IP上的成功交接，并且用于传输实时数据。而在4G网络中，它们还被用于确保不间断的流视频。

农民在对其作物进行种植、浇灌和施肥时也会依赖基于GNSS的自动化系统。

商业航空行业会使用GNSS来实现遥远机场的辅助着陆，而下一代的空中运输管理系统则会利用来自GNSS的精确时间来实施4D轨迹管理。

政府机构会以各种方式使用GNSS来执行诸如监视渔业活动、指导紧急服务，以及跟踪被盗车辆等任务。

在欧洲、俄罗斯和美国，一些型号的轿车和卡车已在越来越多地使用GNSS实现事故时的自动化紧急服务。

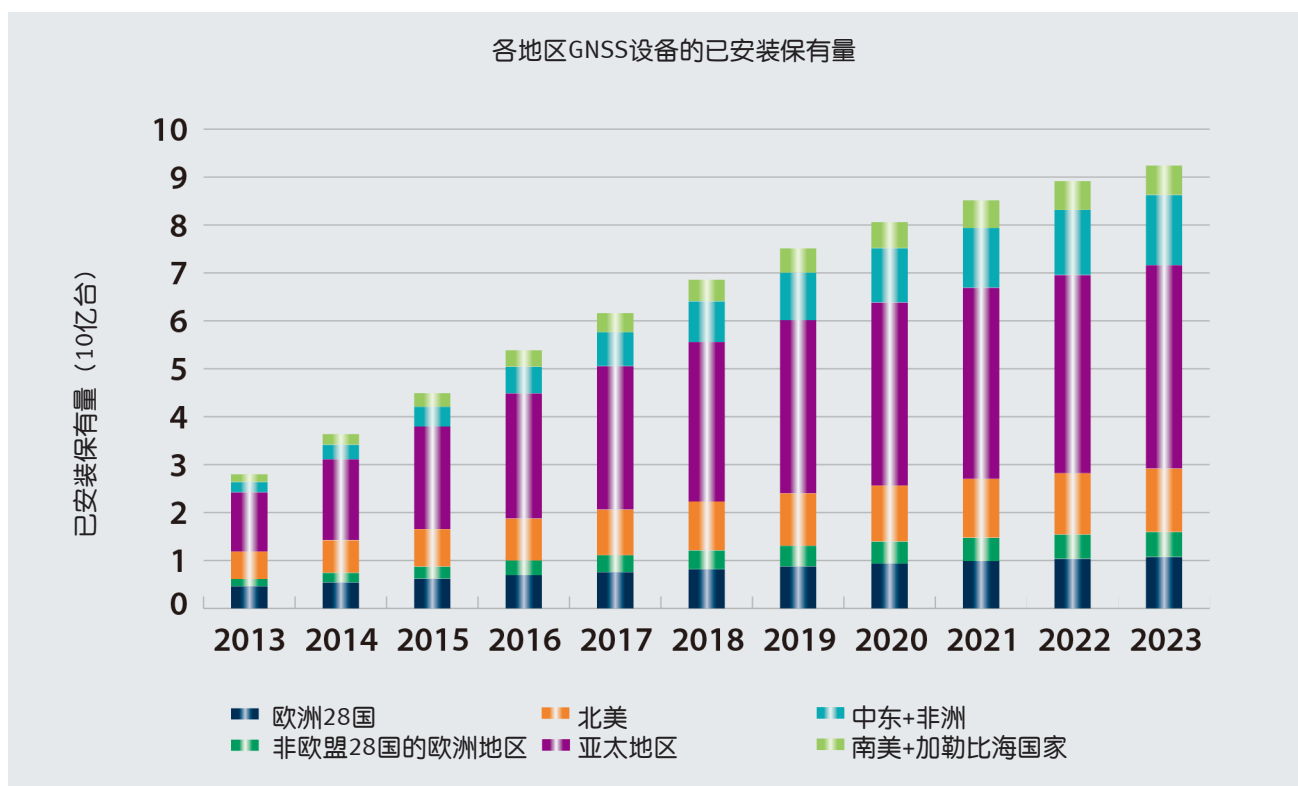
银行和金融机构则在依靠GNSS提供的精确交易时戳。

在物流和运输行业中，GNSS被用于车队管理/遥测应用，并且成为供应链中准时管理中的重要因素。

在建造和建筑行业中，GNSS被用于传送和引导自主式或高度自动化的建筑机械。

这份清单还在不断加长，因为GNSS已经渗透到我们这个世界中的每一个角落。欧洲的GNSS机构（GSA）估计，2014年时全世界在用的GNSS设备数量已达到36亿台。而根据预测，到2019年时，这一数字将会翻倍并达到70亿台，而我们将在越来越多的汽车、移动设备、网络和控制系统中发现无所不在的GNSS功能。¹

¹ 欧洲全球导航卫星系统机构，GNSS市场报告第4期，2015年3月



资料来源：GSA GNSS市场报告，2015年4_0期，2015年3月

GPS威胁基础知识

GNSS信号很容易受到日益繁多的各种威胁的

对于每天都要使用这些系统的人们来说，GNSS存在的意义就是指导他们和他们的机器在正确的时间、正确的地点，做正确的事情。

但对于负责确保这些系统正常运行的人而言，这并不是一项手到擒来的简单工作。来自太空的卫星导航信号强度非常弱，很容易受到阻挡以及越来越多威胁的损坏或破坏，包括太阳活动、人为干扰、恶意GPS信号伪造，以及定位和计时信息的人为操纵。

今天，各个行业对GNSS信号和数据的依赖程度越来越高，因此理解并减轻这些威胁就成为制造商、系统和应用供应商，以及终端用户的一项至关重要的风险管理活动。

本白皮书的目的是让人们了解：影响GNSS信赖系统的各种威胁，以及应对的办法。

本白皮书将帮助人们理解影响GNSS依赖系统的风险因素，并确保采取适当的措施来减轻此类风险。您将在其中了解到：

- GNSS所面临不同威胁的简介，以及它们的演化趋势
- 评价您系统对GNSS威胁易感性的一些指导
- 减轻GNSS服务中断、错误和/或关键系统所受网络攻击风险的最有效技术概览
- 思博伦GNSS威胁评估和减轻服务的简介

思博伦：30年积淀的GNSS威胁消减专业能力

思博伦与各类商业、政府和军事机构开展了30年的合作，帮助它们了解GPS和其它卫星导航系统所面临的威胁，并且通过使用专业的测试和测量技术来应对这些威胁。

如果您对自己的GNSS依赖产品或系统所具备的弹性心存疑虑，

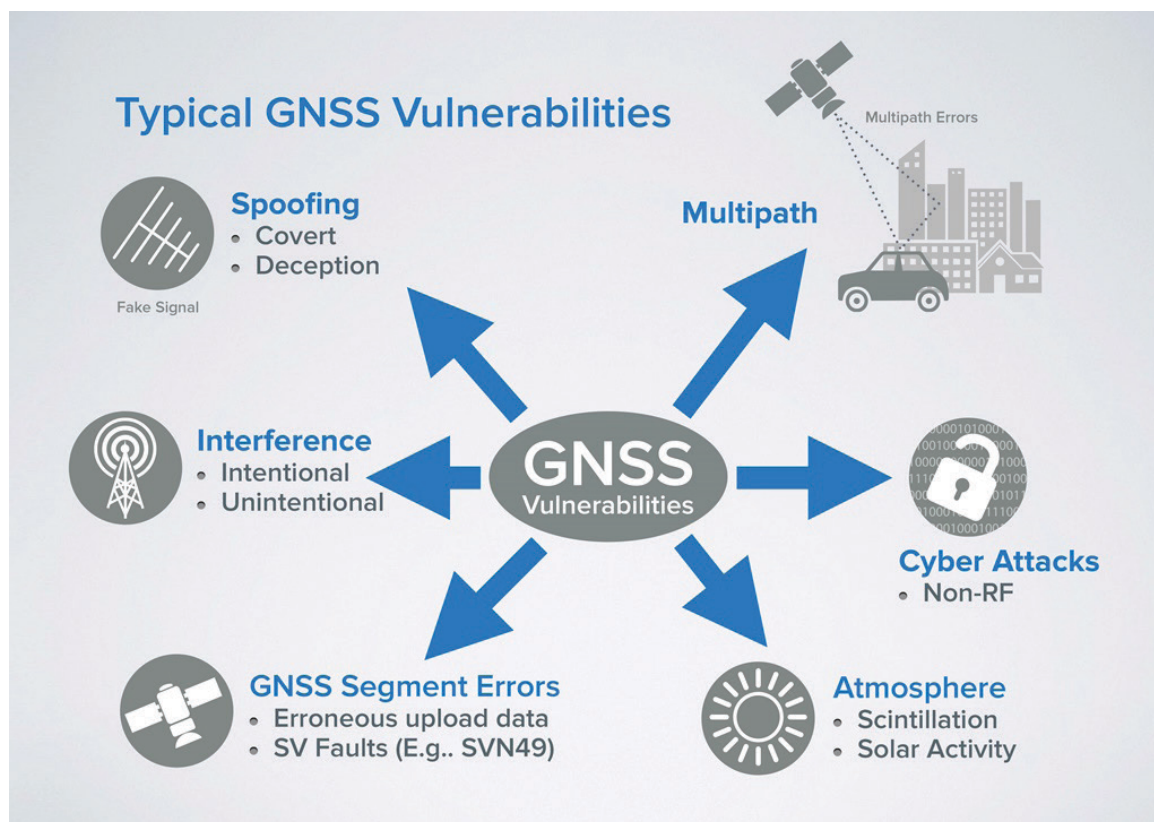
欢迎联系我们：www.spirent.com/ContactSpirent。

GNSS依赖系统所面临的威胁

商用设备所用的GNSS信号强度极弱，其功率并不比40瓦的灯泡高多少。而且，与军事用途的信号不同的是，这些信号是免费提供的，因此通常不受加密的保护。

这两项因素意味着民用卫星信号相对较容易受到阻挡、干扰、操纵和篡改，包括有意为之和无意所为。

有多种类型的威胁可能会干扰GNSS接收机接收和处理GNSS信号的能力，进而导致读数不准确，甚至完全没有读数。



GPS威胁基础知识

理解威胁的不同类型，以及它们的发生原理，对于执行精确的风险评估至关重要。

从广义上来说，这些威胁可以分为下列几个类型：

威胁来源	威胁类型	描述	盛行程度	对用户的影响
太阳风暴	自然	太阳耀斑和其它太阳活动造成的干扰将太空中的卫星信号“完全淹没”。	在太阳活动密集时会出现在全球广泛的地理区域。	信号丢失和测距错误都会对位置或计时信息的精度产生影响。
闪烁	自然	卫星信号在太空中被不规则的电离层活动折射或衍射。	闪烁的效应在低纬度和高纬度地区最为明显。	对接收机造成的影响可能包括不精确的位置信息等。
阻挡	自然	可视范围内卫星数量不足，因而无法提供精确的位置 — 由于建筑物阻挡天线的天空视野。	主要发生在室内、地下、建筑密集区域、森林地区、山谷或深沟内。	信号丢失和测距错误都会对位置信息的精度产生影响。
多径	自然	来自一颗或多颗卫星的信号被附近的建筑物反射，导致其到达接收机的路径破碎化。	通常发生在被高达玻璃建筑物包围的“都市峡谷”中。	距离错误会影响位置信息的精度。
安装不良	人为	设备天线的安装位置可能无法获得干净的天空视野或来自卫星的干净信号，或者是天线与接收机的匹配不当，可能导致看似干扰源的RF泄漏。	可能是由于产品设计不佳，或因为固定天线受到新建高大建筑物的阻挡。	天线几何形状不够好可能导致接收机无法解析其位置，而这种不精确会对位置和计时信息产生不良影响。安装不良引发的泄漏可能导致信号完全丢失。
干扰	人为	本地生成的RF干扰被用于“淹没”卫星的信号。	干扰主要（但不绝对）是由安装在公司车辆中的“个人隐私设备”造成的，其目的是避免被追踪。个人隐私设备的非法使用正在大幅增加。	信号丢失（如果干扰机阻碍了所有的卫星信号）或距离错误可能对位置或计时信息的精度产生影响（如果接收机位于干扰机作用距离的边缘）。
欺骗	人为	虚假卫星信号被广播至受害设备，欺骗它相信自己身处其它的地点，或在不同的时间点上。	欺骗曾经是极难实施的，但最近的演示表明，利用开源软件和低成本器件可以很容易地制造出GNSS欺骗机。	错误的位置和时间读数，可能会对自动和自主设备，以及依赖精确GPS计时的设备产生严重的影响。
黑客攻击	人为	对设备软件层的操纵可改变其对卫星信号数据的解读。	目前的移动电话和平板电脑等个人设备有很多遭受过此类攻击。越狱后的操作系统和用户安装的不规范应用会使GPS接收机的信息被其它应用中手动编辑的信息替代。有证据表明，海运行业中也受到严重的AIS数据操纵威胁。	错误的位置和时间读数，可能对自动化和自主设备，以及依赖精确GPS计时的设备产生严重的影响。
RF干涉	人为	来自附近RF发射机（在设备内或设备外）的噪音阻挡了卫星信号。	在强RF噪音区域（例如邻近蜂窝发射塔）或GNSS接收机与其它设备之间屏蔽不当的设备内部很容易出现。	信号丢失（如果发射机阻挡了所有的卫星信号）或距离错误，位置读数的精度受到影响（如果接收机位于发射机作用范围的边缘）。
用户错误	人为	用户过分依赖所见的GNSS数据，忽视了其它系统提供的证据，或自己看到的事实。	当用户太过依赖导航系统提供的信息时，常常会出现此类情景。	可能在多种场景下可能导致不佳的决策（例如卡车驶入太窄的车道，船只进入危险物体附近等）。

了解您的关键系统面临的风险

鉴于上文中所述的威胁数量日益繁多也越发盛行，GNSS依赖系统和相关应用的制造商需要认识到其产品、客户和终端用户可能受到的影响。

因此，执行彻底的评估，并全面掌握以下的因素至关重要：

- 精确GNSS位置和/或计时信息对系统整体功能的重要性。
- 用户依赖精确、准确和GNSS信号数据的程度。
- 系统受一种或多种已查明GNSS威胁的可能性。
- 了解系统在遭受相关威胁时最可能呈现出的行为，以及这种行为对终端用户应用的影响。
- 如果一种或多种威胁损害了系统的正常功能，业务、客户、终端用户和其它各方会面临哪些风险。

风险的剖面取决于应用，并且会在不同的机构、不同设备中呈现出差别巨大的影响。例如：

如果**集装箱港口**的自动化吊车长时间无法接收GNSS信号，港口及其客户可能遭受财务方面的损失。

如果**变电站**由GPS调节的时钟遭受时间信号“欺骗”，它可能会干扰电力在电网中的分配。

如果**跑步爱好者**无法从健身跟踪器获得准确的距离和时间计算，他们可能会叛离到其它的品牌，并且/或者在社交媒体上对产品提出投诉。

重点就是理解当前的具体风险，并且深入了解这些威胁的演化和发展趋势，并着眼于预防和消减未来的威胁。

例如，恶意干扰和欺骗都在快速演化，而黑客也能够越来越容易获得低成本的设备，使他们能够为了个人获利、恶作剧或其它邪恶的目的而对GNSS信号施加干扰。

GPS威胁基础知识

GNSS威胁消减技术概览

当您已经全面掌握了系统、产品和客户所面临的风险，您就要确保采取适当的风险消减措施来抗衡这些威胁。

依据设备、系统和风险剖面的不同，有许多威胁消减选项可供选择。它们包括但不限于：

多媒体接收机：面对能够接收多个频率信号的GNSS接收机，无论是干扰，还是欺骗都会变得困难得多。

多星群GNSS接收机：如果接收机能够处理来自多个卫星星群的信号（例如GPS、GLONASS、北斗），则接收机在面临阻挡、干扰和欺骗时抵抗所有类型干扰的能力就会更强。

经过改进的天线：有许多先进的天线设计可以抵消干扰和欺骗的影响，而且这些天线在尺寸和价格方面已经形成了完整的系列。天线是卫星导航系统中一个至关重要的组件，而且在这方面相对少量的投资可以使性能大为改观。

先进的军事用户会通常依赖的是多组件天线，即使用波束塑型技术来修改天线的辐射模式，实现最大的GNSS信号强度，并且降低干扰的效应，但这种类型的天线目前尚不供应民用市场。

位置、导航和计时数据的替代或备份来源：在这方面可以探索的选项有很多，包括航迹推算传感器、基于WiFi/蜂窝的定位、辅助GPS和特定行业的地基备份/增强系统（例如航海用途的英国eLoran、WAAS或用于航空的EGNOS）。

将收到的信号与地基参考源进行对比可查明任何可能存在的异常。参考数据技术包括差分GPS和实时动态（RTK）等。

在接收机中使用接收机自主完整性监测（RAIM）技术也可以查明和抵制可疑的信号或干扰。

在接收机中使用富于创新的数字信号处理技术能够以智能方式监测各项信号参数，并且排除干扰信号。

先进多径消减技术能够使欺骗者更加难以使用虚假信号来成功控制接收机。

使用加密GNSS信号（如果得到授权的话）：加密信号在美国只提供给军方使用，即GPS精确定位服务（PPS），而提供给欧洲关键基础设施使用的是Galileo公共规范服务（PRS）。

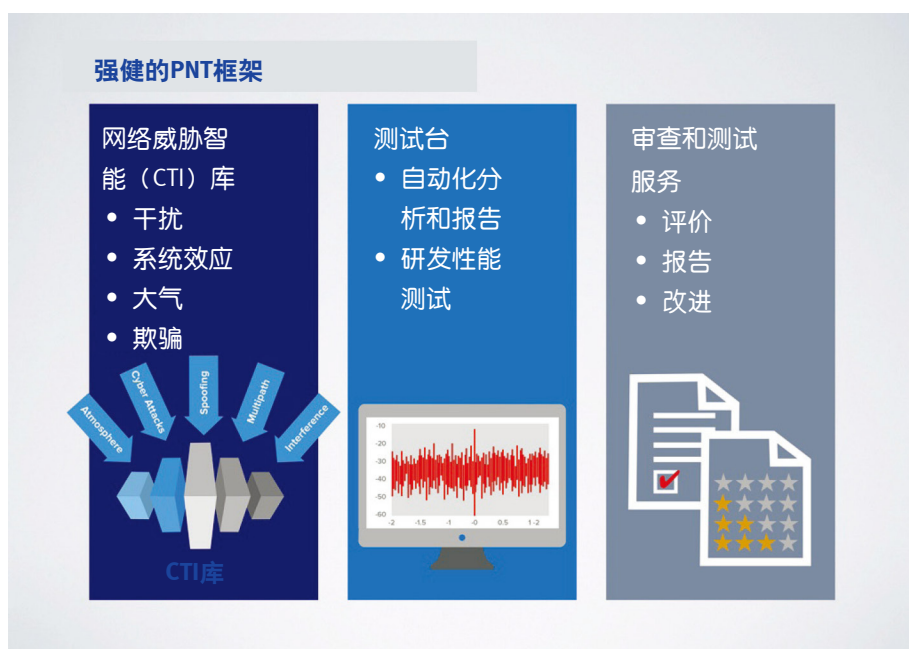
无论您采用的是哪种消减技术，最重要的是紧跟定位及计时系统威胁的发展步伐，验证您选择的技术是否能够在新的威胁出现时加以应对，或者根据威胁的变化及时更新。

协助实现GNSS威胁的识别、风险评估和风险消减

对于许多机构而言，了解和对抗GNSS依赖系统所面对的威胁将成为一个全新且陌生的学科。这项重任将落在已经在那些面对快速深化的信息安全威胁时不堪重负的CIO和CISO肩上。这项责任也可能落在对GNSS信号处理并不熟悉的风险管理部门头上。

因此，思博伦开发出一系列的产品和服务，目的就是帮助各类机构评估和对抗GNSS依赖系统所面临的威胁。凭借我们30年来与各国政府、军队、航天局和商业机构合作识别和对抗各类威胁的经验，我们将为您提供如下服务：

强健的PNT框架



系统审查：以全面、专业的方式，对您的GNSS依赖接收机、产品和系统执行面对本白皮书所述不同威胁类型时的易感性和弹性做出评价 — 我们将根据发现的情况提供完整的报告和行动建议。

GNSS威胁数据库：您可以访问GNSS依赖系统所面临现有和新型威胁的数据库，且该数据库会不断更新。该威胁数据库包含众多可下载的测试案例，可用于测试您的接收机、设备和系统在面临当今全世界各地真实观察到的威胁时的反应。

GNSS威胁测试平台：思博伦提供各类市场领先的测试设备，使您能够模拟多种威胁并了解系统的反应。我们的产品包括GNSS信号模拟器、干扰和欺骗模拟器、干扰探测器、RF记录与回放设备，以及各类测试案例和测试脚本。如欲了解更多信息，敬请访问www.spirent.com/positioning。

GNSS威胁测试培训：我们可以培训您的风险管理、质量保障和测试团队，让他们知道如何使用上面提到过的数据库和测试设备。

外包GNSS威胁测试服务：我们可以按完全外包GNSS威胁测试能力的方式向您提供上述服务的任意组合，而且可以根据您的要求加以定制。

如果您对这些服务有任何疑问，或者希望了解进一步的信息，请随时与我们联系。

关于思博伦通信公司

思博伦通信公司正在为众多高技术设备制造商和服务商提供众多软件解决方案，用于简化和加快设备及系统测试进程。开发者和测试人员可以创建并共享自动化的测试，对来自多个设备、流量生成器和应用的结果加以控制和分析，同时还可利用通过/未通过标准进行，将每一项测试详尽记录在案。利用思博伦的解决方案，企业可以在迈向自动化的同时加快质量保障（QA）周期，缩短入市时间，并且提高已发布产品的质量。通信、航空航天及国防、消费电子、汽车、工业和医疗设备等行业都从思博伦的产品中受益匪浅。

结论

随着全世界越来越依赖导航卫星信号来引导各类系统和机械，这些信号遭受的任何威胁都可能相应地带来更大的风险。

与此同时，由于我们对GNSS信号的依赖与日俱增，这也使之成为对黑客极具吸引力的目标，并且绞尽脑汁不遗余力地开发干扰和攻击GNSS信号的新方法。

对于生产GNSS依赖设备或系统的任何制造商而言，这意味着它们急需跟上新出现威胁的步伐，并确保采取有针对性的风险消减措施。

在GNSS威胁的识别、测试和消减任何方面，思博伦都能为您提供有益的建议。

欢迎现在就[联系我们](#)，与我们讨论您的需求和关切，并且进一步了解我们如何为您提供帮助。

联系我们

网址：www.hoyateq.com

电话：010-82897220

传真：010-82897320

北京市海淀区上地信息路11号彩虹大厦北楼东407室

HOYATEQ
北京浩宇巡天科技有限公司