前面我们提到，赛博空间（Cyberspace）已经取代了电磁空间的表述，而成为新的作战空间。为了更好理解“舒特”系统，我们有必要对加深对赛博空间及赛博作战的认识。

**第五空间的博弈**

赛博空间是可以通过电子技术和电磁能量调制来访问于开发利用的电磁域空间，并借助此空间以实现更广泛和的通信和控制能力。赛博空间包含了电磁频谱、电子系统和网络化基础设施。电磁频谱包括涵盖所用通信和雷达使用的频率；电子系统包括计算机系统、片上微系统和嵌入式系统等；网络化基础设施包括因特网、无线通信网、电力网、专用网、战场指挥控制网等。伴随着赛博空间的出现，赛博作战（Cyberspace）也运时而生（简称赛博战）。赛博战包括赛博空间进攻性作战和赛博空间防御性作战。赛博空间的进攻性作战包括：拒止、削弱、中断、摧毁或欺骗敌人，其主要目的是保证自己赛博空间内自如行动的同时，拒止敌人自如地在赛博空间内行动。



在以往，电磁空间被称为第五空间，如今 赛博空间（Cyberspace）已经取代了电磁空间的表述，而成为新的作战空间

美军将电子系统攻击、电磁系统封锁与攻击、网络攻击、基础设施攻击作为赛博进攻性作战的主要内容。从上述的定义可知，赛博战既包括了传统的电子战，也包括了现代的计算机网络战，具有广阔的外延，是一种广义的信息战。上文我们把“舒特”系统归为赛博战武器，是因为“舒特”系统在攻击时是以电磁波为载体侵入敌方的网络系统。随着科技的发展，战场上网络的种类也不断增多，作用在不断增强，现代军队对其的依赖程度也在增加，如：雷达防空网、地域通信网、指挥控制网等，这些网络都是以计算机网络为基础延伸发展而出的战场网络。战场网络是赛博空间的组成部分之一，战场上的网络空间不是一个开放式的网络空间，无法直接接入，但是，军事作战网络包括了大量的开放式传感器、无线接口和链路。以开放式传感器为例，工作中的雷达（不包括无源雷达）、无线电通信系统等都是开放式传感器，其工作时都要发射电磁波。电磁波很容易被敌方相应的接收机接受，从而暴露传感器的方位及工作体制等信息。通过电子战技术以电磁波形式从天线口面或其他节点进入敌赛博空间是最为可行的途径。

笔者认为，“舒特”网络攻击系统不仅仅是美国空军空中网络攻击的网络攻击武器，美空军还以“舒特”系统和先进数据链的发展为机遇对美空军甚至海军航空兵的情报、监视与侦查平台（RC-135系列“联合铆钉”、EP-3等电子侦察机）和进攻性信息战平台（EC-130H等以软杀伤为主要目的电子干扰机）及进攻性打击平台（空军的F-16CJ、海军的EA-6B、EA-18等具备DEAD能力的电子战飞机）进行横向一体化整合，以适应赛博战的出现。这种横向一体化整合也是一个不断扩展的过程，未来即将服役MALD空射诱饵、电磁脉冲武器、海军下一代干扰机（NJG）等都将被整合在一起。横向一体化整合后的空中赛博空间进攻性作战体系为美军谋取在赛博战中的绝对优势地位提供了物质基础，在不远的将来，美海空军赛博作战将以电子战为基础，以“舒特”网络攻击系统、电子软杀伤（携带干扰吊舱、MALD空射诱饵的战术飞机）、电子硬摧毁（电子脉冲炸弹、反辐射导弹等硬摧毁弹药）等手段全空域、多维度打击敌防空指挥及通信体系。



 美空军以“舒特”系统发展为机遇对情报、侦察平台和进攻性信息战平台和进攻性打击平台进行横向一体化整合，以适应赛博战的出现

美空军以“舒特”系统的发展为机遇对情报、监视与侦查平台和进攻性信息战平台及进攻性打击平台的横向一体化整合将给其作战对手的防空系统和通信系统带来新的挑战。美军的作战对手的防空系统和通信系统不仅要面对美军不断增强的传统电子战能力，还要面对“舒特”系统通过远程无线电入侵，秘密进入防空系统或通信系统的网络攻击，尤其是后者其带来的危害更为严重。美国把中国当作军事上的主要假想敌是众所周知的事情，关注和研究“舒特”系统的发展与作战运用，重视“舒特”系统对中国防空指挥和通信系统造成的威胁，探寻应对其攻击的策略和措施应是当前解放军重点研究的课题。

**被动防护**

虽然美军透露 “舒特”系统的细节信息非常少，但还是可以根据有限的信息和JEFX演习中配置粗略分析其特点并探讨应对其攻击的措施。首先，发挥“舒特”系统的作战威力必须依赖强大的信息获取和共享能力；其次，在攻击过程中依赖数据链进行相互数据传输；最后在攻击手段上依赖大功率辐射信号实施远程无线电入侵。

在被动防护方面， “舒特”系统在作战之前首先依赖RC-135U/V/W“联合铆钉”电子侦察机对敌进行电子侦察（ES），截获敌电子通信、雷达等电磁信号，对侦搜到的各种电磁信号进行分析、识别、处理，从而获取战术情报，了解战场态势。这一工作主要由网络中心协同瞄准系统（NCCT）完成。该系统由L-3公司研制，NCCT的设计目标时能够在数秒钟之内收集并融合来自不同平台的ISR数据，并进行识别和定位敌方辐射源。其定位原理可能是在飞行中利用IP协议通过多个平台数据，采用三角测量法，协同完成对辐射源的定位。根据“舒特”系统的攻击原理和作战流程，应对“舒特”系统攻击首先要注重重点防控网络设施的电磁屏蔽，减少不必要的电磁辐射，保护频谱资源，防止作战使用电磁频谱的泄露，做到常备分离、平战分离。



 目前，美军已经完成了对RC-135系列电子侦察机的改造，改造后的RC-135飞机装备了NCCT系统

除了保护频谱资源外，还可以在重要防空设施附近部署诱饵设备发射假频率、假信号迷惑敌方电子侦察平台。从以往的北京雷达博览会展出的重要设施防御系统可知，中国的预警雷达等重要设施都配备了综合防御系统，防御系统包括GPS诱饵、雷达抗辐射导弹告警设备、诱饵、烟幕干扰设备等。针对“舒特”系统的出现，研制相应的诱饵，用于发射假频率和假信号，保护重要的防空设施。“舒特”系统主要通过发射大功率辐射信号实现对目标网络的入侵，因此采用技术手段对防空雷达和通信系统进行升级（根据现有的文献，“舒特”系统对网络的攻击，是通过对防空设施的无线通信系统的“无线入侵”进行攻击的，无线通信包括了微波通信、超短波通信、卫星通信等），拒绝异常信息，减少被攻击的可能性。

目前，“舒特”系统所攻击的目标主要是固定或机动的地面防空系统，对于移动速度较快的预警机，其可能无法进行有效的攻击，因此，装备足够数量的预警机不但有助于利用预警机飞行高度和速度的优势，提供较佳的预警与搜索效果，提高空防能力，还有助于完善空防预警系统，提高对抗“舒特”系统的能力。中国现在不但研制成功并装备了空警-2000、空警-200预警机，目前还研制成功了基于运-8三类平台，采用相控阵雷达的空警-3000预警机，这为未来装备足够数量的先进预警机奠定了基础。



 “舒特”系统对于移动速度较快的预警机，其可能无法进行有效的攻击

由于“舒特”系统的主要攻击目标是防空系统和通信系统的计算机网络，因此，加强网络防御也是对抗其攻击的措施之一。网络防御是指使用所有防御手段保护计算机网络，使其免遭扰乱或摧毁。网络防御手段包括：评估威胁的情报、对迫近攻击的指示和警告、减小攻击的影响和恢复受攻击的网络等。加强网络防御既要在硬件上下功夫，使用具有自主知识产权的计算机硬件及采用安全性更高的光纤通信，还需要在软件下功夫，分析现有防空系统的计算机网络的漏洞，使用新的杀毒软件、防火墙等措施，提高网络防御能力。为了保持重要防空网络遭到“舒特”系统袭击后的正常运行，应对重要防空网络进行备份，备份系统应和原系统有所区别，一旦发现系统遭到“舒特”系统的遥侵、遥控，应果断切换备份系统。

**主动出击**

进攻是最好的防御，在探寻应对“舒特”系统攻击的策略和措施中也应坚持这一思想。应对新出现的“舒特”系统，首先要装备适合本国作战体系，性能相近的国产版“舒特”系统，将美军对中国的防空挑战转移到美国。此外，根据国产版“舒特”系统技术和性能特性，为未来研制新型防空武器和现有防空武器升级提供相应的经验，提高防空武器对抗“舒特”系统的能力。此外，在平时演练和演习时，可以使用国产版“舒特”系统和防空武器进行对抗性演练，以在技术和战术层面上提高防空部队应对“舒特”系统攻击的能力。



 在平时演练和演习时，可以使用国产版“舒特”系统和防空武器进行对抗性演练，以在技术和战术层面上提高防空部队应对“舒特”系统攻击的能力

目前，作战飞机若要具备“舒特”网络攻击能力必须携带一种名为“长矛”的吊舱（Spear），这种吊舱装备了功率强大的专用辐射源阵列，用于发射大功率电磁波，渗透到敌方网络。我们知道，无源雷达采用无源工作体制，自身不对外辐射电磁波，敌方无法通过有效的电子侦察来发现它，隐蔽性好。通过被动接受合作或非合作信号，对目标进行探测和跟踪，其是对抗电子战飞机和隐身飞机有力武器。由于“舒特”系统在攻击时需要向攻击目标发射大功率电磁波，无源雷达就可以通过技术手段探测和跟踪装备“舒特”系统的飞机，因此，可以通过扩大无源雷达的覆盖面提早发现“舒特”系统的网络攻击。结合地面有源雷达、预警机等预警平台，及时发现装备“舒特”系统的飞机，利用战斗机或远程防空导弹击落装备“舒特”系统的飞机，从源头上抗击“舒特”系统的网络攻击。

中国曾在上世纪90年代发展出了无源雷达。科索沃战争中，捷克“维拉”无源雷达成功监视美国F-117隐身飞机的活动并协助击落了其中一架。“维拉”无源雷达在战争中的出色表现引起了中国的极大关注，战争结束后，中国就研制出了可以实战部署YLC-20的无源雷达。后来，中国又得到了捷克“维拉”E无源雷达的设计和技术资料，对YLC-20无源雷达进行了改进，据悉，YLC-20无源雷达的定位和跟踪目标的性能指标远高于“维拉”E无源雷达。YLC-20无源雷达研制成功之后，中国后来又发展出了DWL002、REWY-1等无源雷达并开始对外出售。以DWL002无源雷达为例，该雷达信号适应能力强，工作频带宽（1.0-18吉赫兹）、机动性好等优点，其作用距离可达500公里，通过多站式部署和结合日益成熟的北斗卫星定位系统，可高精度定位辐射源。中国在无源雷达方面的强大技术实力有助于提高解放军抗击“舒特”系统攻击的能力。



 由于“舒特”系统在攻击时需要向攻击目标发射大功率电磁波，无源雷达就可以通过技术手段探测和跟踪装备“舒特”系统的飞机

使用陆基机动式电子战系统对抗“舒特”系统也是值得关注的对抗措施。据俄罗斯媒体在今年6月24日报道，俄罗斯军队近期接受了4套“克拉苏哈”陆基机动式电子战系统。该系统由俄罗斯无线电电子技术康采恩集团公司旗下的“梯度”科研所研制。其可以对所有雷达的基本频率和其他无线电辐射源实施强烈电子干扰，有针对性地压制敌方电子通信设备、指挥系统和情报侦察设备，抗击敌方电子干扰。前面我们提过，“舒特”系统在攻击时需要专用辐射源阵列发射大功率电磁波，类似“克拉苏哈”的电子战系统可以通过发射大功率电磁波压制和干扰“舒特”系统。因此，在研究对抗“舒特”系统措施的过程中，还应研究使用软杀伤对抗“舒特”系统。



 陆基机动式电子战系统对抗“舒特”系统也是值得关注的对抗措施，图为俄罗斯“汽车场”机动式电子战系统