网电一体化攻击到底如何实施

电磁攻击。现代防空网必然要依赖无线电或者数据链通信联络。攻击时，RC-135在防区外作为情报核心，在利用ELINT装备搜集到对方的雷达和无线电情报数据后，便根据电磁波信号的频段、振幅，频率，相位、极化方式，到达角与数据库中已有信息作出比对，确定信号的性质。机载计算机将这些信息发送给EA-18G或者F-16CJ后，这两个单元便可以针对性的发射反辐射导弹和干扰波对其进行摧毁。舒特系统就实现了第一步——电磁战。但这种方式并不新鲜，关键是其第二种能力，网络攻击。



负责网络注入攻击的EC-130H是实施网电一体化攻击的关键节点，但它的攻击并不是单靠本机就能实现的。

网络攻击。要进入对方的数据链网络系统接管作战单元，需要对通信信号进行解码，完全弄清对方信号的加密方式，破解对方通信的密钥，从而获得访问权限，注入病毒、木马甚至成为系统管理员。这个过程其实在生活中极为常见，有些人的Wi-Fi被蹭网其实就是如此。雷达站和指挥中心之间无论多复杂，只要对外辐射电磁波进行联系，就完全可以视为一个路由器。

黑客通过字典破译、抓包破解等方式破解Wi-Fi网络，只要时间足够，无论加密方式如何，都可以被破解。这种技术同样被用在了作战系统上，但因为军用网络加密程度极高，且经常处于调频、扩频和密码变换状态，因此要实现破解，光用EC-130H这种机载计算机显然不现实。EC-130H要做到这一步，应该将探测到的信号回传到美国本部的超级计算机上利用超算进行破解才能实现“舒特”的网络切入过程。



RC-135作为“舒特”系统的核心，起到情报分析和分发、作战任务的作用。

此外，和无线Wi-Fi不同的是，对方作战系统采用操作系统和软件是未知的，而数据链天线发射接收也往往带有指向性，因此“舒特”系统作战前提是必须要有足够的间谍获取对方作战系统足够的情报，且能够在战场上对敌方通信系统的入口进行精确定位，从而发射准确的信号从无线入口注入。这在攻击对方固定式雷达站和指挥中心时往往不成问题，因为可以提前通过卫星或者人员实地测量获得，但在对方移动式通信系统时，EC-130H想在防区外准确定位目标基本不太可能做到。

从上述可以看到，舒特系统实际上是以大量的机械、人力情报工作为基础的，以ELINT分析能力为前提的，因此也并非是无懈可击，可以对其进行针对性防范。

未来网电一体战的发展趋势

现今作战网络中心、一体化联合的趋势越来越明显，网电一体作战系统在未来的作战中也必将成为主角，发展这类系统必须引起各国的高度重视，未来的网电一体化作战系统应当在“舒特”系统上有以下进展。

任意平台，任意组网能力。网电一体化作战平台应当赋予每个前沿平台更多的情报侦搜和分析、干扰能力，并不只依赖于现有平台，例如在未来美军可能采取F-35这种隐身作战平台代替EC-130H和RC-135的作用，实现抵近侦察雷达信号，传递到作战网络中任意能够对目标实施最有效打击、干扰、无线注入的平台上，各个平台之间可以快速组网建成网电一体战系统。

有源无源情报融合能力。舒特系统应当能够将有源、无源，空天电网各类情报融合到一起综合处理，实现对移动平台的精确定位，以实现实时的对移动单位的网电攻击能力。还应和国家情报系统融合在一起，在整个赛博空间实现大范围的情报整合处理。

更强大的渗透能力。面对防御网电攻击的各类手段，网电一体战系统的电子情报截获、密码破译，网络渗透的能力必然要求更加强大，要求不但能够入侵一般的系统，还可以入侵到敌方任意作战单元，对其实施操控，这既要求更快速的算法也要求更高速的计算机处理速度。