

隨著信息技術的發展，網絡空間已成為無聲、無形的新型戰場，且對有形戰場產生至關重要的影響。除了植入木馬、病毒、拒絕服務攻擊等常見網絡攻擊手段，近年來，一種特殊的網絡攻擊樣式——“舒特”網絡攻擊，成為各國軍事研究的熱點之一。

“舒特”網絡攻擊首次披露于2001年美國國防部呈交國會的《網絡中心戰》報告中。其效能真正令世界為之震驚，則始于一場戰爭。2007年9月6日，以色列空軍10余架F-15和F-16戰機突入敘利亞領空，對預定目標實施了精確轟炸。隨後，該批戰機毫發無損地安全撤離。敘利亞軍隊建有龐大的防空體系，其部署的“道爾-M1”防空導彈系統，更是具有垂直發射和同時攻擊兩個目標的強大功能，且抗干擾和識別能力突出。如此防備到位的敘軍卻對以色列戰機的進入和撤出絲毫沒有察覺，其主要原因便是以軍使用了美國提供的“舒特”機載網絡攻擊系統，成功侵入敘軍防空網，使其防空體系處于失效狀態。

“舒特”系統是美軍高度機密的機載網絡攻擊核心技術，其名字來源于美軍“紅旗”演習的創立者理查德•穆迪•舒特上校，目的是使美空軍具備讓敵防空預警系統喪失作用的能力。在實際運用中，“舒特”系統通過敵方雷達、微波中繼站和網絡處理節點侵入敵防空網絡系統，注入欺騙信息和處理算法，實時監視敵方防空預警雷達的探測結果，或在此基礎上以系統管理員身份接管敵方網絡，實現對傳感器的控制。

美軍“舒特”攻擊系統發展很快，至今已有五代產品，並在兩年一度的“聯合遠征部隊試驗”中進行了技術能力演示。典型的“舒特”系統一般由電子偵察機、專用電子戰飛機和戰斗機組成，其攻擊流程如下︰一是對目標實施電子偵察。使用電子偵察飛機在敵防空區外進行信號和信息偵察，及時掌握敵防空體系的無線電聯絡內容，對偵收到的各類信號參數進行分析，然後將有關信息傳遞給地面指控中心。二是根據作戰目的選擇攻擊方式。第一種方式是將目標信息傳遞給電子干擾飛機後，由其對預定目標實施電子干擾；第二種方式是將目標信息傳遞給戰斗機，由其對預定目標實施反輻射攻擊或精確火力打擊；第三種方式是將目標信息傳遞給專用電子戰飛機，由其對預定目標實施網絡戰攻擊。三是實施“舒特”網絡攻擊。當地面指控中心決定以專用電子戰飛機對預定目標實施網絡攻擊時，首先由電子偵察飛機對敵方輻射源進行高精度定位，然後由專用電子戰飛機向敵方雷達或通信系統發射電子脈沖信號，向敵人脆弱的處理節點植入定制的信號，包括專業算法和惡意程序，滲入敵方防空雷達網絡，窺測敵方雷達屏幕信息，實施干擾和欺騙，或冒充敵方網絡管理員身份接管系統，操縱雷達天線轉向使其無法發現來襲目標。

“舒特”系統的強大實戰效能，對我軍打贏未來信息化戰爭帶來許多啟示︰一是增強網絡安全意識，牢固樹立官兵面對信息網絡攻擊的緊迫感；二是注重網絡安全技術人員的培養，嚴密防範網絡安全隱患，強化網絡安全防護；三是加大網絡攻防技術研發，做好電磁信息防泄漏工作，以應對“舒特”網絡攻擊帶來的威脅。