看美国如何加强网络战机构建设

魏岳江

互联网是当前最富有潜力的信息通信技术，它在给人类造福的同时，也给人类带来了沉重的灾难，特别是网络运用于军事领域，这一特征尤为明显，信息窃密与反窃密、入侵与反入侵、渗透与反渗透的斗争将以全新方式，在更广泛的空间和领域里展开。在这一时代背景下，网络战就上升到战争范畴，具有了战略意义。

组建网络指挥机构

目前，网络战争的概念正在全世界兴起。2000年以来，几乎世界上每天都发生网络黑客攻击事件，造成了极大的经济损失和秩序混乱。在美国，有57%的政府机构网络系统遭到过黑客的入侵，一半以上的企业在网上丢失过重要信息，有的损失甚至在百万美元以上。因此，美国安全局率先成立网络中心机构，建立了40多个网络机构，其中有20多个高层次的计算机战争机构。美国国家安全委员会成立了两个关键机构——国家保密政策委员会和信息系统安全保密委员会，前者负责制定军事安全保密政策和数字化战场设计方案，后者专门负责军事信息高速公路和数字化战场上秘密信息和敏感信息的安全保密管理。美国国防部成立了联合参谋部指挥与控制中心、联合参谋部信息战局、信息系统安全中心、国家保密局信息战处、国防大学信息资源管理学院等机构。

实施网络情报战

实施网络情报战，最关键的就是窃取和破解对方的密码，通过网络直接或间接地进入敌方的计算机系统。美国情报官员把对计算机系统的攻击，从中窃取情报，分成三大类：单个黑客、跨国组织和国家支持的活动。为了提高网络情报战能力，美空军的情报局成立了第92信息战入侵队。该入侵队不仅进行计算机战，获取其他国家的政治、经济、军事情报，还利用信息战其他种种工具，如电子作战装置，来破坏部队的行动。为了保护整个空军内部的计算机网络的安全，防止情报泄密，空军正在研究一些工具来进行监控，保证因特网联接以及比较可靠和秘密的内部网络的完好性。为了监视因特网联接系统，空军成立了计算机应急小组。这是美国航天司令部下属的计算机网络保护特别行动小组的一部分。计算机应急小组的主要任务是确保网络正常运转。该小组的中心长期保持10到25名工作人员，但是在两个小时内就能额外增派人员帮助修复网络。该小组还对空军的系统进行攻击，以检测网络管理人员的警惕性。

组建联合特别小组

目前，美国国防部成立的保护计算机网络联合特别小组已开始行使其使命。该小组与各联合司令部、各军种以及国防部其他机构协同工作，负责保护国防部计算机网络和系统免受入侵和攻击。美国前国防部长科恩指出，特别小组将按照联合条令的规定进行必要的行动授权。联合特别小组将成为国防部制定保护计算机网络和系统联合计划的核心机构，它将监控突发事件和针对国防部系统的潜在威胁。同时，它将通过国家基础设施保护中心与其他联邦机构建立通信链路，以便通过信息基础设施共享行动信息。当发现攻击时，该小组将负责指导整个国防部内的保护行动，以阻止对系统的破坏并恢复网络功能。