《信息对抗技术》

电子讲稿

李朝晖

南开大学 网安学院

2024

信息对抗的主要能力

信息对抗的能力包括进攻与防御两种：

- 进攻型的信息对抗是综合利用各种攻击手段，对敌方的信息和信息系统实施摧毁、瓦解、侵入、扰乱和终止信息传输的各种行动。
- 防御型的信息对抗是将政策、法规、情报、行动和技术在内的多种手段综合与协调起来，对信息与信息系统实施保护的过程；

这些能力的实现需要靠信息技术的支持才能实现。

信息对抗的防御能力

信息对抗的防御包括保护、发现与监控攻击和恢复三种能力。

- 保护能力是为了实现信息安全、作战安全和信息完整性。
  - ✓信息安全的目标是在多种复杂的安全策略下，对有意和无意的未经授权的泄漏、访问、操作和更改提供保护；
  - ✓作战安全的目标是消除由于己方能力的局限性和有关意图的信息被敌方利用而造成的脆弱性，或将其降低到可接受程度；
  - ✓信息完整性的目标是确保信息的真实性与完整性不受损害。

信息对抗的防御能力（续）

- 发现与监控攻击能力是为了能够及时发现敌方对己方信息系统与网络的攻击，并对其攻击过程实施监控，防止破坏蔓延。
- 恢复能力则是为了在己方信息系统的正常运行遭到破坏，甚至被瘫痪的情况下能够迅速恢复到正常运行状态。

信息对抗的防御能力需要以下功能实现：

1、信息抗毁功能：通过合理分布、适当重复、完整备份、恰当隐蔽等手段实现信息的抗毁功能有助于提供保护能力，确保信息、信息系统的安全与完善。

2、预警功能：用于为己方信息系统和子系统提供即将发生的信息攻击提供预警信息。

3、脆弱性评估与规划功能：提供真实评估对抗双方信息系统与信息流程。对己方系统的评估有利于风险管理和脆弱性分析；对敌方系统的评估可为攻击提供准备与基础。

信息对抗的防御能力需要以下功能实现：（续）

4、入侵检测与威胁告警功能：用其探测各类人员的入侵企图和已成功的入侵。

5、访问控制和服务的安全性功能：在确证用户身份的条件下，根据事先制定的安全策略，只允许授权的人员访问信息系统，拒绝任何非授权访问，以确保信息系统的安全。

6、服务的可用性功能：依靠支持分布式计算机通信来确保信息在需要时的可用性。

信息对抗的防御能力需要以下功能实现（续）

7、网络管理和控制功能：运用可重新配置的、抗破坏的协议和控制算法，实现自我修复并管理在不同种类平台与网络上的分布计算。

8、损害评估功能：用于确定攻击（或被攻击）的效果，既可以用于防御信息战，也可以用于进攻信息战。

9、应急响应功能：可以隔离入侵者对网络与系统的威胁与干扰，使决策者具备隔离、控制和纠错等能力，其中纠错能力还包括系统的恢复、资源的重新配置与重建等能力。

信息对抗的进攻能力

信息战的攻击包括控制、欺骗和摧毁等三种能力。其中：

- 控制能力包括阻止、破坏、削弱和利用能力，其目的是通过阻止对信息的访问与利用，以及对操作能力的破坏，或有选择地降低服务水平等进攻手段来控制对方对信息、信息系统的使用；
- 欺骗能力的目的是对对方依赖的信息、信息源进行欺骗性攻击，有选择地影响对方对信息、信息流、信息系统和计算机网络的使用或使用的可靠性；
- 摧毁能力的目的是采用信息攻击武器，破坏对方信息的收集、传输和访问与使用的能力，对对方信息、信息流、信息系统和计算机网络进行有选择性的破坏。

信息攻击武器有以下一些类型：

拒绝服务、病毒、控制对方计算机系统，或向对方数据库置入假信息进行欺骗，误导对方业务活动，如使后勤混乱、关闭电网使空中交通控制混乱等。

实现信息进攻的的7种功能：

1、破坏对方信息和信息系统的功能。

瘫痪对方信息系统，或降低对方信息系统的运行效率，或破坏对方信息的真实性。可以在进入对方信息系统前后采取行动。

2、破解对方信息系统的保护功能。

破解对方信息系统中，对硬件、信息、软件、信息系统及其支撑系统的保护机制。利用对方系统中的各种漏洞破坏对方信息系统的保护机制是有效的方法之一。

实现信息进攻的的7种功能：（续）

3、侵入对方信息系统的功能。

提供强行侵入对方信息系统、网络和信息库并注入虚假信息的能力，与此同时还要包括隐蔽入侵踪迹的能力。

4、对对方信息与信息系统的实体的软破坏与硬毁伤的功能。

软破坏包括释放病毒、拒绝服务等攻击手段；硬毁伤包括使用电磁炸弹、火力毁伤等破坏手段。

实现信息进攻的的7种功能：（续）

5、切断敌方信息传输功能。

破坏信息流入对方信息系统或其内部信息流动的任何途径，包括各种有线的或无线的信息传输手段。

6、向对方信息系统实施“间谍战”。

向对方信息系统安插己方人员，或收买对方信息系统操作人员，通过他们获取对方信息系统中的信息，或向其中注入错误信息。

7、伪装攻击源的功能。

采用“跳板”或代理等手段伪装己方的攻击源，阻止对方了解己方的攻击行动，使对方无法找到反击的目标。

填空题 3分

信息对抗的防御包括［填空1］、［填空2］和［填空3］三种能力。

信息对抗的防御包括保护、发现与监控攻击和恢复三种能力。

填空题 3分

信息战的攻击包括 [填空1] 、 [填空2] 和 [填空3] 等三种能力。

信息战的攻击包括控制、欺骗和摧毁等三种能力。


信息对抗的主要能力
end