

《信息对抗技术》

电子讲稿

李朝晖

南开大学 网安学院
2024

文A



信息对抗的内涵与模型



信息对抗的内涵

在军事上，信息对抗的本质是两个或多个敌对者在信息领域内，利用先进的电子信息技术和装备，使己方获取对战场信息的感知权、控制权和使用权而展开的斗争。

由于斗争是限定在信息领域中进行的，因此信息对抗是围绕着信息的整个生命期过程（包括信息的获取、传输、储存、处理和决策、利用与废弃等阶段）而展开的。

文A

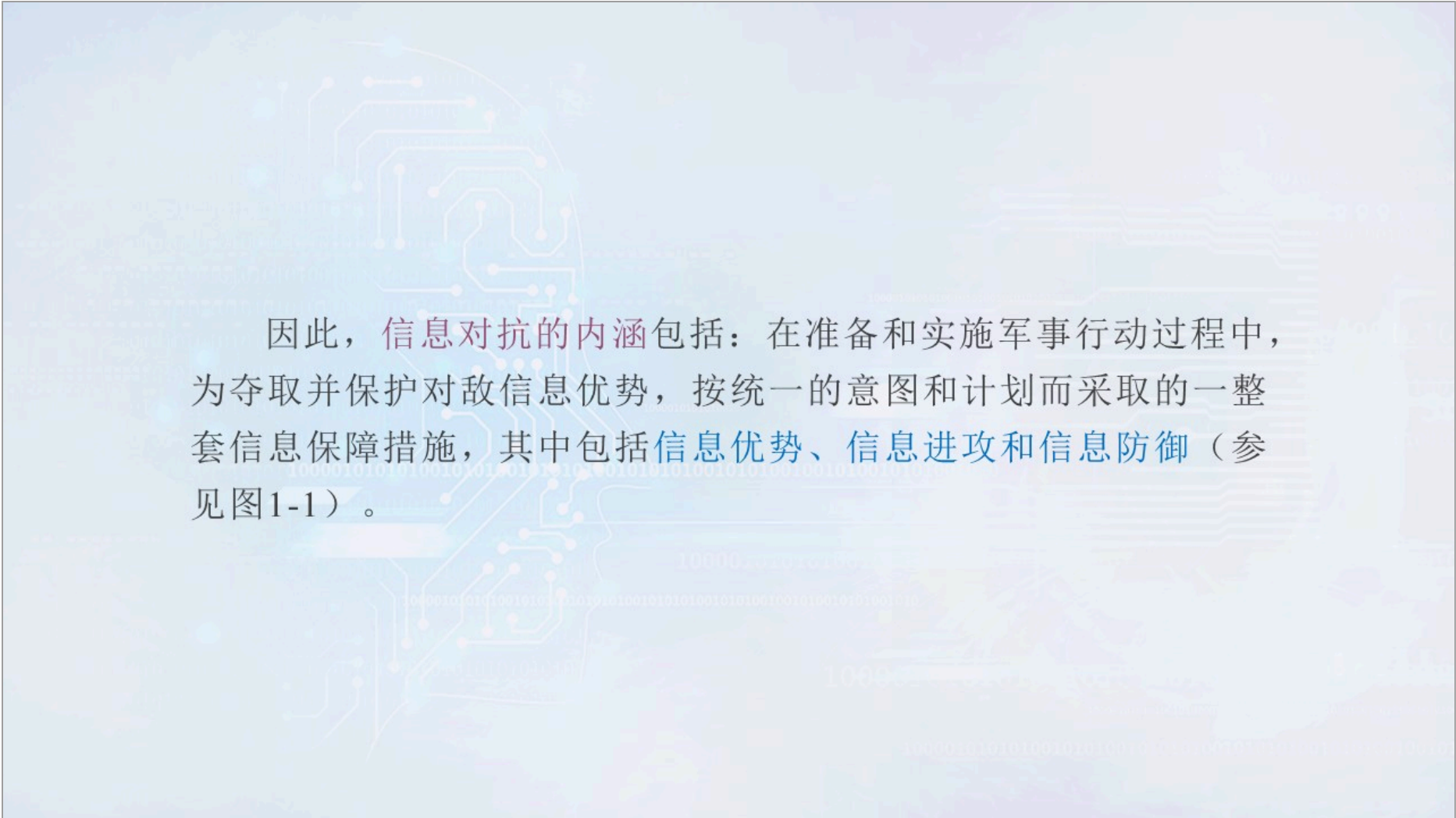
在计算机网络日益普及的今天，信息的储存、处理与利用都必须依赖于信息系统，信息的传输必须依赖于有线的或无线的网络系统，因此，信息对抗实际上是围绕着信息整个生命期过程，在保护己方的信息、信息处理、信息系统和计算机网络空间安全的同时，为破坏敌方的信息、信息处理、信息系统和计算机网络空间安全而采取的各种行动。

信息对抗的战略目的

支持信息的产生、传输、处理和储存的设施称为信息基础设施，这就是说，信息对抗是在信息基础设施中展开的。广义的信息基础设施由数据、信息、设备、电信系统和人员等要素组成，信息对抗的目标就是要获取明显的信息优势，进而获取决策优势，最终使军队获取整个战场优势。

信息对抗的战略目的是在保护己方信息系统安全的同时，通过利用、封锁及施加影响等手段，攻击对方的国家和国防信息基础设施，以夺取和保持决定性的优势。

在军事领域中，信息对抗争夺的焦点是信息的独占权、控制权和使用权，其攻击对象是敌方的军事信息系统或具有军事价值的民用信息系统，其中主要的是敌方用于获取信息的探测系统、传送信息的通信系统、指挥控制系统（包括信息服务器、决策支持与指挥系统、计算机处理平台以及操作人员）等。



因此，信息对抗的内涵包括：在准备和实施军事行动过程中，为夺取并保护对敌信息优势，按统一的意图和计划而采取的一整套信息保障措施，其中包括信息优势、信息进攻和信息防御（参见图1-1）。

文A

信息优势是指能够及时获取敌我双方准确而完整的信息，近实时生成战场态势，通过信息分发为各级指挥员提供可靠决策依据；



信息防御是在敌方对己方实施信息进攻的情况下，为确保己方信息系统的正常运转而采取的各种措施。

信息进攻是使用各种软硬件（信息的或火力的）进攻手段，破坏敌方的信息保障能力和敌方的信息系统（如指挥自动化系统C⁴ISR系统<Command, Control, Communications Computers Intelligence, Surveillance and Reconnaissance —— 指挥、控制、通信、计算机、情报、监视与侦察>）等一整套措施；涵

信息优势是指能够及时获取敌我双方准确而完整的信息，近实时生成战场态势，通过信息分发，为各级指挥员提供可靠决策依据；

信息进攻是使用各种软硬件（信息的或火力的）进攻手段，破坏敌方的信息保障能力和敌方的信息系统（如指挥自动化系统C⁴ISR系统<Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance —— 指挥、控制、通信、计算机、情报、监视与侦察>）等一整套措施；

信息防御是在敌方对己方实施信息进攻的情况下，为确保己方信息系统的正常运转而采取的各种措施。



C4ISR系统

在战场上双方的C⁴ISR系统通过电磁空间互相交连，同时各自又与自己后方的战略网连接。C⁴ISR系统是国防信息基础设施的基础部分，是双方实现各自信息保障，进行信息对抗的最主要的硬件基础与工具，这已得到各国军方的认同。因此要求C⁴ISR系统必须是具备信息攻防兼备能力的综合性军事信息系统，其作战职能包括探测预警、情报侦察、通信、指挥控制和电子战分系统。

文A



信息对抗分类

- 按层次分，信息对抗可以分为国家信息对抗、国防信息对抗、战略信息对抗和战术信息对抗；
- 按性质分可以分为进攻性信息对抗和防御性信息对抗；
- 按杀伤机理分可以分为软杀伤类的信息对抗（如计算机网络攻击、病毒战、情报战、心理战等），硬杀伤类信息对抗（如强力电磁炸弹攻击）和“软硬兼施”的信息对抗（综合利用火力打击与信息武器）；
- 按时间划分，可分为和平时期的信息对抗、危机时期的信息对抗和战争时期的信息对抗。

和平时期的信息对抗包括政治信息战、经济信息战、文化信息战、网络情报战、心理战等形式；和平时期信息战的样式基本上都可以应用于危机时期或战争时期，在平时与危机时期，信息对抗主要以获取各类情报为主，不会去破坏对方信息系统与网络的正常运行，但到了战争时期，由于双方已经处于敌对状态，对对方的网络及信息系统实施破坏战，甚至是瘫痪战可能会成为主要的信息对抗样式。

填空题 3分

按杀伤机理分可以分为 [填空1] 类的信息对抗（如计算机网络攻击、病毒战、情报战、心理战等），[填空2] 类信息对抗（如强力电磁炸弹攻击）和“[填空3]”的信息对抗（综合利用火力打击与信息武器）；

文A

信息对抗的模型

信息对抗模型抽象描述了信息防御行动、进攻行动和其他相关行动之间的相互关系，图1-2中描述了这三者之间的关系。

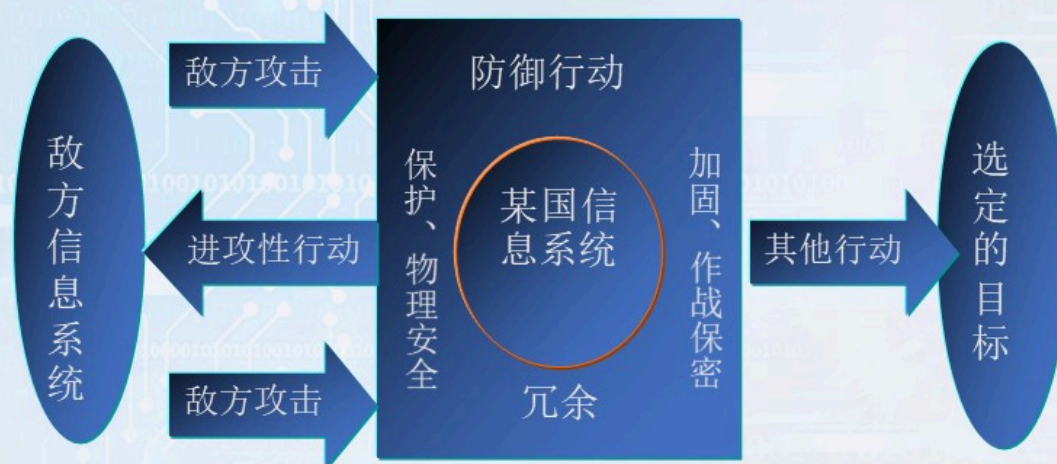


图1-2 信息对抗模型



防御性行动包括：

- ◆ **保护**是指保护自己信息系统安全的各种措施；
- ◆ **加固**是指加固信息系统，增强其抗攻击能力；
- ◆ **作战保密**是采取作战保密措施，防止敏感信息的泄露；
- ◆ **冗余**是对信息系统进行冗余设计与配置，也包括对信息进行备份；
- ◆ **物理安全**是采取一些物理措施保护硬件设施的安全，增强系统的可靠性和抗毁性。



进攻性行动包括：

- ◆ 摧毁对方信息系统或造成敌人的信息系统饱和，超出其工作能力；
- ◆ 利用对方信息系统中的资源；
- ◆ 修改、弄假对方信息系统中的信息，破坏其信息完整性；
- ◆ 用信息来震慑、恫吓（音：动贺）对手，进行心理战；
- ◆ 有意向对方提供或泄露一些假信息，增加对手误判的机会；
- ◆ 瘫痪对方的各种信息能力（如获取、传输、处理、利用等）；
- ◆ 干扰对方的传感器；
- ◆ 胁迫对方利用不完整的信息，影响他们的各种行动。



其他行动:

其他行动是指利用信息对某些目标施加影响。例如，利用救灾或人道主义救援等和平行动，改善在受灾国和世界人民心中的形象，达到军事上的影响与利益。例如，日本政府以人道主义援助为由，**派遣自卫队去伊拉克**就是属于此类行动，既可以突破自卫队的活动范围约束，获得军事上的好处，也希望改变日本旧军队在世界人民心中的恶劣印象；



其他行动（续）

在2004年年底发生的印度洋海啸大灾难中，美军派航母舰队去救援印尼灾区难民，也是为了改善美军在世界上尤其是穆斯林世界中的形象，并获得军事上的影响与利益，但此举也引起了印尼政府的担心，他们公开要求外国救灾军队离开的越早越好。

C⁴ISR

进攻型信息对抗和防御型信息对抗都需要通过双方的C⁴ISR（指挥自动化系统）进行，在战场上，双方的C⁴ISR通过无线信道交连，一方通过攻击手段影响对方系统的正常运行，甚至被瘫痪，而另一方则通过信息防御手段尽量保持自己系统的正常运行。因此，C⁴ISR系统对攻防两类信息对抗都非常重要，是信息对抗能力的不可或缺的因素与组成部分。

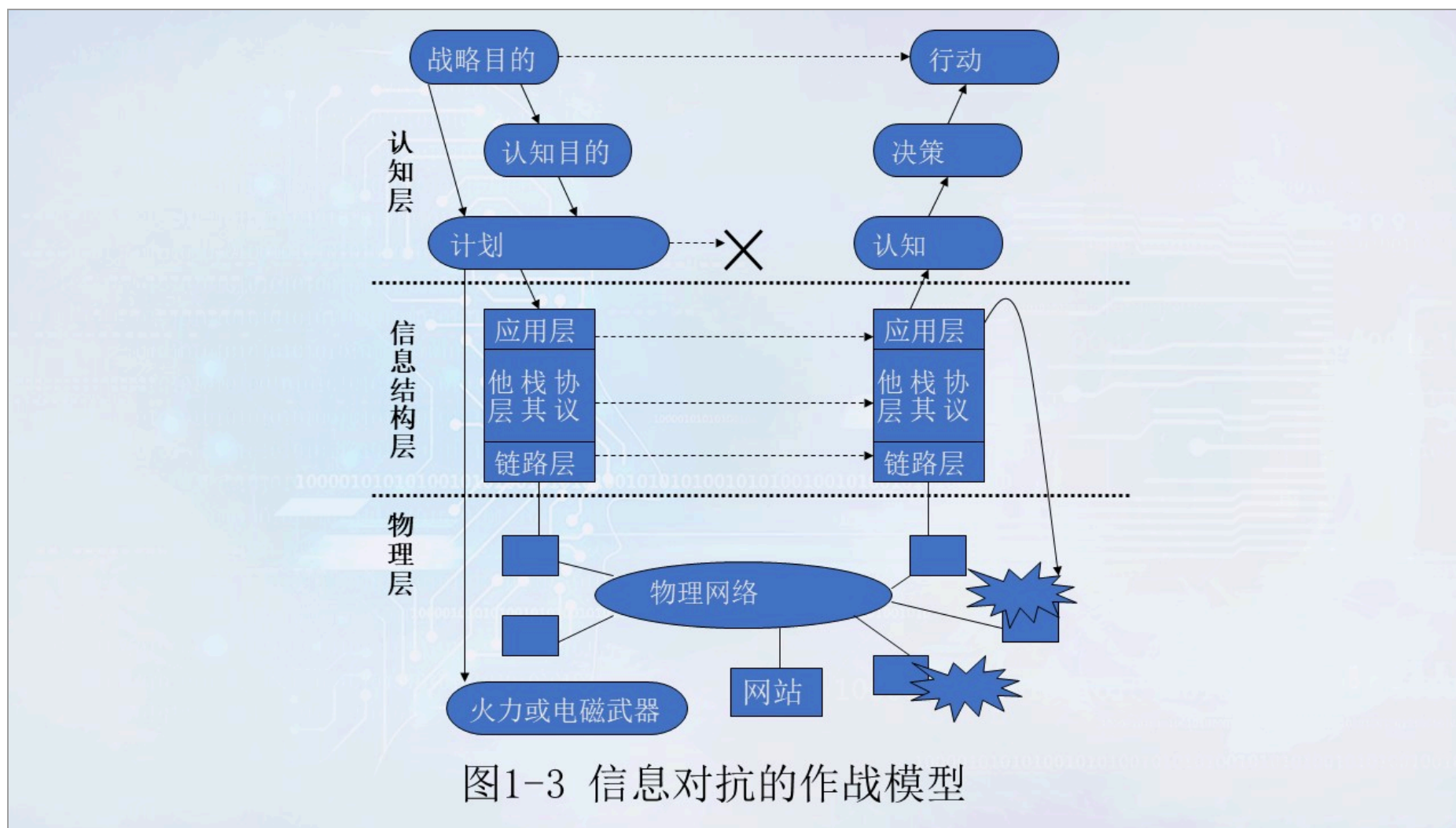
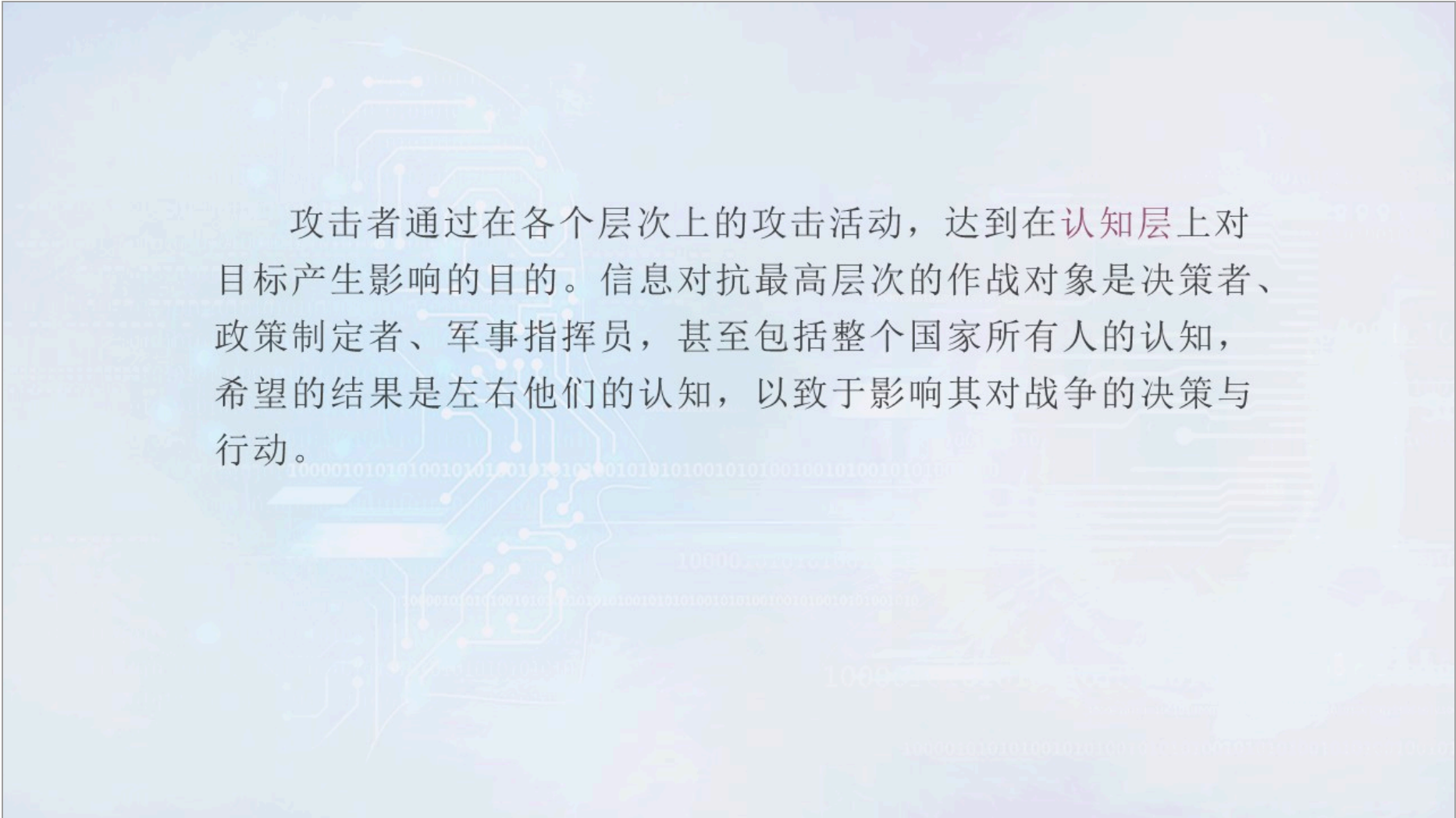


图1-3是从作战角度描述了信息对抗的作战模型。该图把信息对抗的作战过程划分为三个领域，或称为三个层次：**物理空间**、**计算机空间**和**参战者的认知空间**。该模型区分了攻击者和目标双方功能的3个层次，反映了自下而上的从对攻击者到对目标的影响。



攻击者通过在各个层次上的攻击活动，达到在认知层上对目标产生影响的目的。信息对抗最高层次的作战对象是决策者、政策制定者、军事指挥员，甚至包括整个国家所有人的认知，希望的结果是左右他们的认知，以致于影响其对战争的决策与行动。

文A



信息结构层

中间层次是信息结构层，或称为计算机空间层。该层包括信息采集与输入、传输与储存、处理与利用等抽象的信息基础结构，图中利用开放系统互连（OSI）体系结构模型（俗称7层协议栈结构）来描述信息的接收、传输、储存与利用。平常说的恶意软件和利用电脑空间进行攻击就是发生在这个层次中。



信息结构层（续）

这个层次中包括数据、信息和知识的处理过程和结构，相应的对抗可以影响到系统的功能性行为。需要注意的是，这一层次的应用层可以向上层的人发送信息和知识，影响他们的认知与心理，也可以控制底层的物理域中的目标，如计算机、通信和工业过程。因此，在这个层次中的对抗行为可以在认知层和物理层两层中发生特定的或重叠的双重效果。

文A



认知层

模型的顶层是认知层或心理层，这个层次是抽象的，主要表示对对抗目标的接受者的认知施加影响，达到最终影响作战行为的效果。这种影响可以导致优柔寡断而拖延决策，或影响其决策的正确性，形成一个有偏见或有缺陷的决策。该层次的抽象成分包括目的、计划、认知、心理、信仰和决策等方面。



物理域层

第三层也是最低层是物理域层，是由信息基础设施中的物理系统组成，它包括实现网络信息系统的计算机、物理网络、电信和辅助结构部分（如电源、设备、运行环境等）。在这个层次中，除了物理设施外，还有大批的管理人员和操作人员。实质上这个层次的作用是技术性的，它影响着整个系统的技术性能。对这个层次的攻击主要是火力打击和电磁武器毁伤。

(1.2信息对抗的内涵与模型)

end

文A