概　　述

什么是战略信息战

将来会出现这样的可能性：敌人会利用信息革命的工具和技术给国家关键战略资产（例如，电信、运输和金融等国家基础设施的各关键部门）带来风险（敌人谋求使这些资产大规模瘫痪或严重瘫痪，但不谋求摧毁它们）。这种潜在危险构成本报告所述的战略信息战环境的主要方面。

地区性敌人和实力相当的竞争者，也许会发现战略信息战工具和手段在向美国、美国的盟国以及其利益提出挑战中很有用。在近期，战略信息战武器在地区性敌人所采用的“不对称”战略中会发挥最大的效用（见图 – 1）。这类敌人会通过实施更间接的攻击（或发出更间接的威胁），包括综合运用核生化武器、十分先进的常规武器和战略信息战等手段，来设法避免对美国在常规战场方面的优势直接提出挑战。

战略信息战工具和手段对美国的安全提出了两方面的挑

战：

1．对美国国家经济安全的威胁国家基础设施的关键目标可能有遭受严重瘫痪的危险，对一个或多个基础设施成功地实施攻击，会在战略上产生重大后果，包括公众对这些基础设施提供服务失去信心。

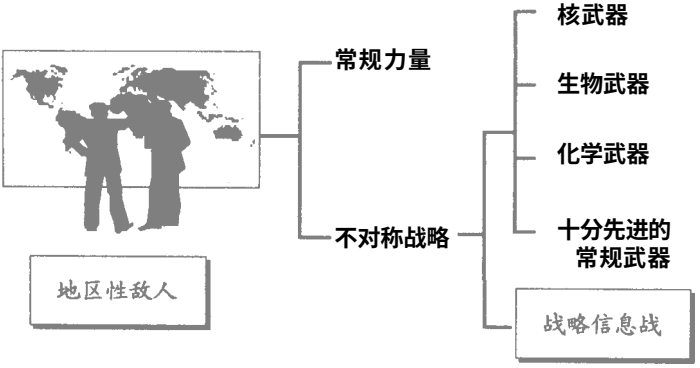


图 -1 美国未来的地区性敌人可能寻求的不对称战略

2．对美国国家军事战略的威胁存在以下这种可能性：地区性敌人会运用战略信息战威胁或攻击来遏制或中断美国在爆发地区性危机时实施兵力投送计划。关注的目标有美国境内的基础设施和在盟国国内的类似目标，这些基础设施对海外兵力部署来说至关重要。遭到这种攻击的某个关键的盟国或某个联盟的成员国会拒绝参加某个联盟，或者更糟糕的是会在战争中期退出某个联盟。

在战略战的历史上，很难找到不显示出重要的信息成

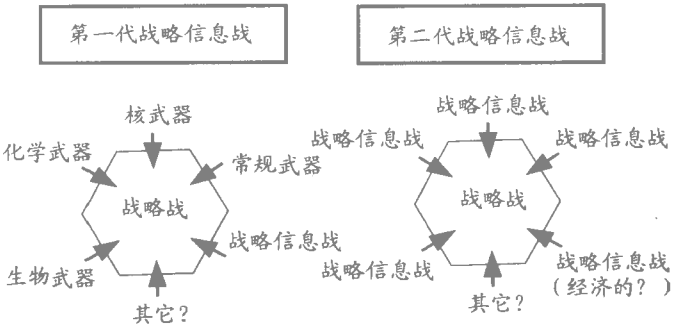
分、而又称得上“战略性”的战争。例如，孙子推崇的创造性地运用信息来避免战争并达到战略目标。还值得指出，人们无疑能够列举一系列的历史事件来说明，技术上的根本性变革会对战略战的信息成分带来根本性变革。

然而信息革命对战略战的潜在影响也许是史无前例的。在过去，战略信息战在战略战中也许主要起从属作用——早先利用常规陆军和海军产生战略性影响，后来则通过飞机、火箭或核武器产生战略性影响。然而，在出现信息革命之后，战略信息战在这类战争中也许会发挥大得多的作用。再者，随着时间的推移，信息革命对于国家关键性基础设施和其它战略资产的脆弱性的潜在影响会导致一类新的战略战，这类战略战基于完全不同的时限、以信息为中心，而且与诸如图 S－1 所示的战略战的其它潜在方面也不同。

因而可以用以下用语来提炼战略信息战的概念（见图 －2）：

1．第一代战略信息战战略信息战是未来战略战的数个组成成分之一，其广义的概念是由很多战略战手段协调地组合而成的（如图 －1 所示）。

2．第二代战略信息战战略信息战是一种独立的、崭新的战略战，这种战争是信息革命的产物，它有别于一般意义上或至少最近被看作属于战略战的那些战争，这种战争很可能在新凸现的战略战领域（例如，经济领域）并在很长的时间段（例如，历时数年，而不是历时数日、数周或数月）组织实施。



图－2　战略信息战的两个概念

对人们已确认的大国（例如美国）来说，作者们趋于认为第一代战略信息战是最初显现战略战更可能具备的形式。然而人们对这种提法有争议。例如，美国也许会发现不久的将来自身所处的形势是：美国决定在危机中经常利用其现有的信息技术优势和第二代战略信息战，否则这种危机会导致部署部队并几乎肯定会造成大量伤亡。

对那些也许尚不拥有任何其它有效的信息战手段的欠发达国家来说，第二代信息战也许具有更直接的吸引力。事实上，在出现第一代信息战之后，紧接着较少的国家也许会使用第二代信息战，或者受到第二代信息战的攻击。

拟定新决策框架的必要性

根据本项目对这项研究的描述：“本项目的目标是为了

迎接战略信息战的挑战而拟定国防部共同的战略与政策框架。”然而什么是战略与政策的决策框架呢？决策框架很可能是一系列相对简单的步骤或某个过程，这个过程代表战略、政策及有关问题，而所有这一切都需要以一种合理的体系结构，并以某种有利于这些问题的决策的方式，沿着某种合理的途径，在某个特定的态势中加以考虑。

当某个特定的问题领域出现以下情况时，就需要（或被认为可能是紧迫地需要）制定战略与政策决策的新框架：（1）似乎需要采取某种行动（或者也许马上需要采取某种行动）；（2）没有现成的决策框架可用来制定某项可实施的行动方案。

在某些情况下，旧的决策框架也许已被检验是否适用于该问题领域，可能会发现这种框架并不适用。事实上，把该问题领域，只看作是一个发展得很快的旧问题领域而不是新问题领域的人，也许已成功地运用这样一种旧框架。不尝试使用旧决策框架就很难及时地、直截了当地说明制定一种新框架的必要性。

一系列不断发展的框架

执行上述任务的历史表明，人们最初寻求一个简单、暂时稳定的框架来为战略信息战确定的功能服务。然而，不久就得出下述结论：在这个发展阶段以一个框架为这项功能服务这个概念不切实际。确切地说，能应对新的战略战组成成

分的正确结构——确实是名副其实的战略成分，而并非仅仅是另一种“战略战的替身”——必定是动态的，并可以在国际安全和信息技术环境两方面应对正在发生的变化。正确的结构必须是：(1) 一系列不断发展的框架，这些框架确认并接受将战略和政策决策过程加以汇集和执行的“断续性平衡理论”的种种现实；(2) 一个过程，这个过程认可并支持这种结构的动态和迅速发展的特点（尤其在其早期阶段）。

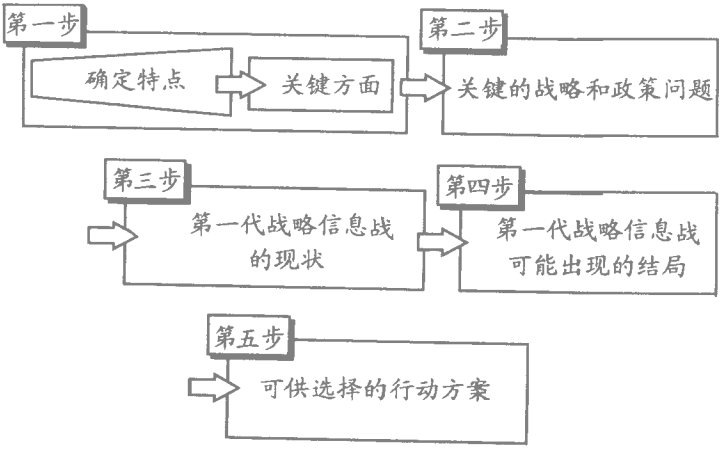
框架的最初制定

将战略信息战决策框架问题概念化的主要目标是：最初拟定的框架，可以针对自身所处环境出现的变化不断演化。这种框架需要具有不断演化的潜力，而不是推动作出决策的一种暂时的权宜之计，此后并没有多大的效用。

因为在战略信息战方面还拿不出初步的框架，最初形式的框架，会使那些对信息革命的未来感兴趣并与在这方面利益攸关的部门以及媒介感兴趣。因而可以将某个有关的第一代战略信息战的设计过程——构成这一框架的过程划分为以下若干个不同的步骤（见图 -3）。

1. 战略信息战环境的关键方面。要了解未来第一代战略信息战“环境”或“作战空间”的一些关键方面，就要了解原则上会受到近期战略和政策方面有效决策影响（也许在某个有利的方面）的那种环境的一些关键方面。一是在似是而非的第一代战略信息战环境的范围内，要鉴别第一代战略

信息战的一些主要的确定特点；二是也许会将有些特点列入经得起上述变化检验的关键方面，但对这些特点要作选择；要从这两个方面达到这一目标。



图－3 第一代战略信息战战略和政策决策框架的设计步骤

2．关键的战略和政策问题。要识别与第一代战略信息战问题关系密切的战略和政策的关键问题（以及诸如组织问题和其它问题），就要识别近期决策可能影响前面所确定的战略信息战的一些关键方面。

3．第一代战略信息战的现状。从进攻性和防御性的战略信息战能力方面，对第一代战略信息战的现状作出评估。

4．第一代战略信息战可能出现的“结局”。根据上述第一代战略信息战的范围和局面，精心设计（可行而又可能合

乎需要）第一代战略信息战的可供选择的“结局”，并用第一代战略信息战的上述的关键方面来表述。

5. 可供选择的行动方案。针对每项可能出现的“结局”，列出战略信息战战略与政策的一些关键问题，并提出实现其中的一个或多个结局的行动方案。

对任何这样的框架进行试验和鉴定，必须权衡新出现的不测事件。然而应当承认，也许只有在有关的信息技术和国际安全环境稳定下来时，才能对任何框架的切实可实行性心中有数。下面详细介绍图 -3 所示的 5 个步骤。

战略信息战环境的关键方面

如上所述，应当鉴别战略信息战环境的一些明显特点，并探索深思熟虑的战略和政策在对我们有利的某个方向上，对其中的哪些特点可能产生影响，这样就可以得到战略信息战环境的一些关键方面。因此，这些方面（见表 -1）构成了战略信息战环境中的一些基本要素，而这些要素会影响与战略信息战有关的可达到的目标，而且还会影响一些国家（和其它可能的“参与者”）有意采取的行动和战略信息战环境本身状况的变化之间的关系。

关键的战略问题和政策问题

战略信息战提出了涉及现有决策过程的一系列十分广泛

和复杂的问题和挑战。因此，我国和各国着手处理这些问题，适当地分清轻重缓急显然是合适的。因此，可以从以下三类内容来大致表述这项研究所确认的战略和政策的一些关键问题的特点。

表－1 战略信息战环境的确定特点、后果和关键方面

确定特点	后　果	关键方面
进入该领域的成本低	战略信息战作战空间的参与者很多	进攻战略信息战的参与者的数量
搞不到关于威胁的战略情报	也许搞不清楚潜在敌人的身份和能力	进攻战略信息战的参与者的数量
战术预警难度大	也许不知道攻击正在进行	战术预警能力
难以作出攻击评估	也许不知道实施者或目标	攻击评估能力，包括实施者的身份
难以作出破坏评估	也许不知道攻击的全部影响	破坏评估能力
传统边界模糊	也许不知道实施攻击之前、实施期间和实施之后，谁承担各种责任	不详
武器效应不确定	攻击方和防御方双方也许难以预料武器效应	武器效应的不确定性
基础设施脆弱性不确定，但令人怀疑	美国本土也许并非是庇护所易受损害的伙伴会使保持持续的联盟更困难	战略信息战的脆弱性程度

迎刃而解的问题。一旦能确认或确定合适的过程，我国（有时国际上）就可以轻而易举地解决这些问题。这类问题（可以举出种种方案的实例）是：

职责与职权的主体　哪个部门应当承担主要职责，是政府部门还是工业部门？如果是政府部门，政府部门的哪个实

体应当承担主要职责？如果是工业部门，那么在美国全国对战略信息战威胁作出反应的关键基础设施中，哪个环节应当承担主要职责？

——负责国家安全的联邦政府领导层；

——负责执法的政府领导层；

——负责国家安全的各国政府的联合领导层；

——负责执法的各国政府联合领导层；

——得到政府支持的各国工业领导层。

战术预警、攻击评估和应急反应　美国和世界各国，包括这些国家的政府及其工业界应当怎样组织起来，以发展种种能力和程序来了解战略信息战的威胁，并作出反应？

——政府牵头的面向安全的模式（称作国家基础设施状况模式）；

——政府牵头的面向执法的模式（称作反恐怖主义模式）；

——疾病控制与防治中心模式；

——工业界牵头模式。

脆弱性评估　政府和工业界合作应当采用什么手段和机制来进行美国关键国家基础设施的脆弱性评估？

——政府牵头的（例如，包括国防部牵头的）美国脆弱性评估；

——包括美国和其它主要国家（例如，七国集团① 与 1 或战略信息战的潜在的势均力敌的竞争者）在内的政府部门和私营部门的共同努力；

① 七国集团系西方最大的七个工业国的统称，这七国是美国、加拿大法国、德国、英国、意大利和日本。这些国家每年召开国家元首一级的会议。

——世界各国的政府部门和私营部门之间的合作关系，（例如疾病控制与预防中心和世界卫生组织）；

——工业界牵头并得到政府协助的评估。

战略信息战运用的政策声明　在战略信息战的运用及其与其它战略性军事和经济手段关系方面，美国政府应当推出怎样的政策性声明？

——主要是对任何战略信息战攻击以牙还牙地作出报复；

——主要是运用非战略信息战对这类攻击作出报复；

——运用经济手段，很可能还包括面向经济的战略信息战对这类攻击作出报复；

——关于美国怎样对付这类攻击还十分不明确。

当前面临的棘手问题

这些问题都是涉及首次勾画与战略信息战有关的长期国家目标和战略，既紧迫而又有争议。例如，这些问题包括：

研究与发展投资战略　为了实现以下四方面的目标，美国应当谋求怎样的投资战略呢？这四方面的目标是：（1）监督、攻击者识别和攻击者“追踪”方法；（2）攻击评估方法；（3）防御与重建方法；（4）破坏评估方法。

——政府牵头的面向安全的模式（称作国家基础设施状况模式）；

——战略信息战方面不进行重要的国际合作；

——侧重防御技术的有限国际合作（例如，七国集团模式）；

——通过多国在安全方面达成的现有协议来组织广泛的国际合作（例如，北约模式）；

——自愿参加的广泛的国际合作。

国际信息共享与合作　在战略信息战领域，应当运用哪些原则来指导国际合作，尤其是与盟国和联盟伙伴的合作？是否存在能与扩展性威慑相比的一种战略信息战？是否存在能与扩展性防御相比的一种战略信息战？

——面向国家安全的网络保护目标；

——与盟国协调开展防御性研究开发工作；

——世界各国禁止开展进攻性战略信息战的研究开发工作；

——私营部门或市场驱动的重点。

推迟解决的问题

例如，由于技术上的不定性而尚不具备解决条件的问题，或者更糟糕的是，有些问题如果草率地处理很可能导致“糟糕的”战略或政策决策而难以解决。这一类的问题包括：

政府内部和政府之间在政治敏感的隐私问题上的合作　必需将这个主题列入关于战略信息战的任何讨论，但是对于怎样依据一些特定的战略与政策来保护隐私权则需要作出更详细的说明。

最低限关键信息基础设施　需要作进一步的分析和概念设计，以确定最低限关键信息基础设施概念（系向重要的政府和社会用户团体提供最低限通信手段和服务的系统）在技术和成本上是否完全可行。

加密政策在美国和国际社会拟定　与加密有关的长期目标和战略时，必须将很多问题方面“拿到桌面上讨论”，而战略信息战只是其中的一个问题方面。

处理上述每个领域都要十分小心。而其中每个问题都与制定战略信息战政策等重大问题的各个方面有着千丝万缕的联系。处理战略信息战薄弱环节的行动方案需要在不同因素之间进行折中，这个概念对电脑空间环境空前不确定性来说至关重要。下一节将探讨防御性信息战和进攻性信息战问题，这些问题对战略信息战行动方案和政策的实施具有重大意义。

第一代战略信息战的现状

从美国和其它国家（或其它当事方）在进攻性与防御性战略信息战方面的绝对能力和相对能力来看，很难对第一代战略信息战的现状作出宏观评估，即使在机密层次上作出这种评估也很难。鉴于信息革命当前的动态特征和作为潜在政治－军事手段的战略信息战的初期特点，不管这种评估是秘密做出，还是公开做出，在目前做出，还是在可以预见的将来做出，都需要谨慎。

在美国看来，战略信息战评估的主要问题是：

敌对的战略信息战　强国的现有范围以及这些国家运用战略信息战攻击，能对美国利益造成严重损害的程度；

与其它国家（敌国、中立国或友好国家）的进攻性战略信息战的现有能力相比，美国的进攻性战略信息战的现有能力范围——这种现有能力是指在预防性的、先发制人的或报复性的战略信息战行动中的公开的能力或隐蔽的能力。

为了处理好这个问题，必须对进攻性与防御性战略信息战能力进行评估。

作为世界上率先开发和利用信息系统的国家，美国最有潜力成为进攻性战略信息战的“超级大国”。与那些才开始考虑战略信息战手段，在未来冲突中也许会有意义的国家相比，任何低估美国战略信息战潜力的做法都是可笑的。但是，美国的战略信息战潜力迄今已开发到什么程度？如果美国下定决心，抓紧发展进攻性战略信息战能力，那么开发速度能有多快呢？

作为进攻方，美国目前的信息作战经验虽然尚不成熟，但在美国的军事战略与军事学说中占有一席之地。美国拥有健全和成功的进攻性指挥与控制战、电子战和其他信息战的能力（例如，在波斯湾战争中大规模采用指挥与控制战，并压制敌方的防空力量所证实的那样，特种作战司令部是心理战大师，而且各军种开发并操作了电子战系统），但是在本报告的意义上，几乎不能将这些能力称作“战略性的”。将进攻性的第一代战略信息战界定为具有让一个国家的“中枢神经系统”（国家的关键基础设施网络）承担风险的潜力，与在常规战争中作为保障性任务的“信息作战”相比，这是一种敏感得多的任务。针对军事领导、通信和雷达目标与针对为医院提供电力的公共设施完全是两码事。

由于我们的朋友与盟友的敏感性，以及可能的敌人，从日益公开强调美国的进攻性战略信息战倡议中捞到政治和军事上的资本，因而在很大程度上避免披露关于这方面能力的更明确的信息。尽管美国拥有一定的战略信息战进攻能力，但是它的全部潜力在政治上和军事上都是敏感的。

美国，由于其在世界上政治、经济和技术等方面的地位，在运用进攻性战略信息战能力，以增强自身的现有武器库方面优于主要竞争者。因此，它也自然地成为战略信息战

的打击目标。美国在信息技术的开发和应用方面居世界领先地位，而且美国的社会与经济综合体严重依赖于信息系统。美国在地理位置上有利于防御，当前又拥有世界上最强大的常规军事能力。如果说在最近的将来，敌方在军事上打败或挫败美国，那么很可能归因于其竭力避免军事上发生直接对抗，而成功地采用了非对称战略。

从逻辑上说，要了解战略信息战防御的含意，第一步就是要考虑在遭到种种可以想象的广泛威胁与作战情景的战略信息战攻击的情况下，美国可能会暴露哪些潜在的脆弱性。可惜（或幸好），我们几乎十分缺乏赖以作出这种评估的“真实”经历。现在有很多自然事件（如风暴与地震）、人为差错（在软件与控制方面）以及蓄意破坏（例如迷恋网络的黑客与罪犯）都表明在各种国家基础设施中，许多事情会出错，有时候范围还相当广泛。然而，过去所有的一切就其影响来说都称不上“战略性”，而其意图也似乎看不出任何战略性。

缺乏防御性战略信息战的有关经验的一个显而易见的问题，则涉及到因果关系：因为某些未被发现的攻击还没有成功地实施，或者因为根本就没有作出这种尝试，就意味我们已经逃过了战略信息战的攻击了吗？

尽管将来在信息基础设施脆弱性方面，存在着大量的不稳定性，一系列倾向表明现在越来越多地依靠不那么安全的联网概念，尤其是，广泛采用开放式网络标准与技术则意味着：以电脑为基础的产业及其应用，也许变得更容易受到单点故障的伤害。随着电子商务的增长，基于全球信息基础设施的未来电子支付系统（称作电脑支付）的广泛出现，以及提供关键服务（如远程医疗与政府通信）的计划都是战略信

息战攻击的潜在目标。

因此，防御性战略信息战的评估，包括对信息基础设施的脆弱性、威胁的潜在可能性和脆弱性带来的后果作出评估。然而，这些评估也有其自身的问题。现有的信息基础设施系统是复杂的、动态的、灵活的和相互依存的。这些系统可以是公共的，也可以是私有的，可以是军用的，也可以是商用的。由于遭到破坏会带来潜在风险和成本问题，有些系统（如银行采用的那些系统）已经过设计而“得到加固”。其他一些系统则处在一个温和的环境下，而其功能则与威胁无关（如成本、可达性和互通性）。

标准的风险评估方法（故障树分析法、模拟法和红队法）的可适用性与未来分析潜力是不确定的，这是因为信息系统非常复杂，而且威胁可以非常残忍。信息安全的责任是分散承担的，已发现的系统特定弱点非常敏感，并出于正当理由而受到严格控制。

然而，尚未发现的危险将仍然是最大的敌人，这就表明必须始终保持警惕性，已知的问题一旦发现就可以妥善处理（如果处理问题的成本“合理”的话）。如果将已知的问题隐藏起来而得不到妥善处理，就要密切注意威胁，制订应急计划，但是，要想测量出附带危险带来的直接潜在损失（如人员生命、维修成本与替换成本、设备停机时的机会成本）就不可能了。

上述告诫有望降低对可得到的精度的期望，有鉴于此，在上述的关键方面对第一代战略信息战的现状的初步评估是：

1. 进攻性战略信息战实施方的数量：不详（可能在 0

到若干个之间)。

2. 战术预警(攻击是否正在进行?)与攻击评估(如果攻击正在进行,哪一方发起、攻击规模有多大以及攻击的打击目标是什么?):问题在于不能确定攻击者的身份以及报警信息的潜在价值和适时性。一切都是未知的,但是在第一代战略信息战中攻击者的不确定性可能很小,因为信息战仅仅是冲突的一部分(如果攻击者特意部署,不确定性也可能会增大)。

3. 毁伤评估(毁伤的大小和范围):重大的毁伤是不言而喻的;最关键的毁伤评估问题涉及进一步毁伤的潜在可能性和影响。

4. 武器效能的不确定性:很大。

5. 战略信息战的脆弱程度:不详(当然有许多值得担忧和关注之处)。

尽管我们还吃不准,就进攻性与防御性战略信息战能力而言,当前的形势究竟怎样,但是,有识之士可分为是以下两种人:(1)一种人认为,信息基础设施以往的失误表明:有一些潜在的弱点有可能被拥有重大的战略性优势的未来的敌人所利用;(2)另一部分人则将以往的经验看作是明确的证据表明:无论信息基础设施有什么弱点,这些弱点被利用的效果相对不会严重,这些系统以达尔文的“优胜劣汰”的模式逐步发展,那种发展模式将继续确保适当的防御机制不受损害,也就是说,从来不会出现诸如战略信息战等事件。要紧的是,要明确在当前(和未来)存在诸多不定因素的情况下,我们应当怎样处置?相比之下,在这两种立场之间确定正确的看法就没有那么重要。