拟态防御原理

今天，人类社会正以前所未有的速度迈入数字经济时代，数字革命推动的信息网络技术全面渗透到人类社会的每一个角落，活生生地创造出一个万物互联、爆炸式扩张的网络空间，一个关联真实世界与虚拟世界的数子空间正深刻改变着人类认识自然与改造自然的能力。然而不幸的是，网络空间的安全问题正日益成为信息时代或数字经济时代最为严峻的挑战之一。正是人类本性之贪婪和科技发展的阶段性特点，使得人类所创造的虚拟世界不可能成为超越现实社会的圣洁之地。不择手段地窥探个人隐私与窃取他人敏感信息，肆意践踏人类社会的共同行为准则和网络空间安全秩序，谋取不正当利益或非法控制权，已经成为当今世界发展的“阿喀琉斯之踵”。

网络空间安全问题尽管多种多样，攻击者的手段和目标也日新月异，对人类生活与生产活动造成的威胁之广泛和深远更是前所未有，但其基本技术原因则可以简单的归结为以下五个方面。一是，人类现有的科技能力尚无法彻底避免信息系统软硬件设计缺陷可能导致的漏洞问题。二是，经济全球化生态环境衍生出的信息系统软硬件后门问题相当时期内不能指望从根本上杜绝。三是，从一般意义上说，现阶段的科学理论和技术方法尚不能有效地彻查软硬件系统中的漏洞后门等“暗功能”。四是，上述原因致使软硬件产品从源头设计、生产维护和使用管理等环节就缺乏有效的安全质量控制手段，造成技术产品的漏洞后门问题随着数字经济或社会信息化的加速而严重污染整个网络世界并使之陷

入万劫不复的境地。五是，相对补救性质的防御代价而言，网络攻击的技术门槛之低，似乎任何具备网络知识或对目标系统软硬件漏洞具有发现和利用能力的个人或组织，都可以成为肆意践踏网络空间道德或行为准则的“黑客”。

如此悬殊的攻防不对称代价和如此之大的利益诱惑，很难相信网络空间技术先行者们或市场垄断企业，不会处心积虑地利用全球化形成的国家间分工、产业内部分工乃至产品构件分工机会，施以“隐匿漏洞、预留后门、植入病毒木马”等战略性控制手段，谋求在市场直接产品利润之外，通过掌控用户数据资源和敏感信息获取不当或不法利益。作为一种可以影响个人、企业、地区、国家甚至全球社会的超级威胁或恐怖力量，网络空间漏洞后门等暗功能事实上已成为战略性资源，不仅会被众多不法个体或有组织的犯罪团伙或恐怖势力觊觎和利用，而且毫无疑问的会成为利益攸关方政府谋求“制网权”、“网络反制权” 或“制信息权”等战力建设与运用目标。事实上，网络空间的战争早已常态化，各方势力博弈无所不用其极。但是，目前的态势仍然是“易攻难守”。

现行的主被动防御理论与方法大多以威胁的精确感知为基本前提，遵循“威胁感知，认知决策，问题移除”的边界防御理论和技术模式。实际上，当前基于智能手机和终端的移动办公、电子商务等成为主流应用模式的情况下，无论是目标对象还是附加型的防护设施，不论是基于 Intranet 的区域防护还是基于“Zero Trust Architecture”的全面身份认证措施，由于两者自身都无法彻底排除或杜绝漏洞后门之类的负面影响，因而对于

“已知的未知”安全风险或者“未知的未知”安全威胁，不仅边界防御在理论和技术层面已经过时，就是其他的工程化手段也无法进行效果可量化的设防。更为严峻的是，迄今为止，既未找到任何不依赖于攻击特征或行为信息的威胁感知新思路，也未找到技术上有效与经济上可承受且能普适化运用的防御新方法。以美国人提出的“移动目标防御（Moving Target Defense ,MTD)”为代表的各种动态防御技术，在干扰或瓦解基于目标对象漏洞之攻击链可靠性方面确能取得不错的功效。但在应对潜藏于目标系统内部的暗功能或基于软硬件后门等的未知攻击方面仍未解决机理无效的问题，即使运用加密认证类的底线防御手段和机制，也无法彻底避免被宿主对象内部漏洞后门等暗功能“旁路、短路或反向加密”的风险，2017 年发现的基于 Windows 漏洞的勒索病毒 WannaCry 就是反向加密的典型案例。事实上，基于边界防御的理论和定性描述的技术体系，在支持“云-网-端”新型使用模式或者零信任安全框架部署方面正面临更加严峻的挑战。

生物免疫学的研究成果告诉我们，生物的特异性抗体只有受到抗原的多次刺激后才能形成，当同种抗原再度入侵机体时方能实施特异性清除。这与网络空间现有防御模式极其相似，我们不妨将其类比为“点防御”。同时，我们也注意到，脊椎动物所处环境中，时时刻刻存在形态、功能、作用各异，数量繁多的其他生物，也包括科学上已知的有害生物抗原。但健康生物体内并未发生显性的特异性免疫活动，绝大部分的入侵抗原应当是被与生俱来的非特异性选择机制清除或杀灭的，生物学家将这种通过先天遗传机制获得的神奇能力，命名为非特异性免疫。我们不妨将

其类比为“面防御”。生物学的发现还揭示，特异性免疫总是以非特异性免疫为基础的，后者触发或激活前者，而前者的抗体只有通过后天效应才能获得，且生物个体间存在质和量上的差异，迄今未发现关于特异性免疫的任何遗传学证据。至此，我们知道脊椎动物因为具有点面结合、相互关联的双重免疫机制，才获得了抵御已知或未知抗原入侵的能力。令人沮丧的是，人类在网络空间始终未创造出这种“具有通杀性质的非特异性免疫机制”，总是以点防御的办法去竭力应对面威胁任务。理性的预料和严酷的现实表明，“堵不胜堵、防不胜防、漏洞百出”是必然结局，战略上不可能摆脱被动应付的局面。

造成这种尴尬局面的核心问题是，科技界至今未搞清楚非特异性免疫是如何做到精准 “敌我识别”的。按常理推论，连机体特异性免疫形成的有效信息都不能携带的生物遗传基因，不可能拥有未来所有可能入侵的细菌、病毒、衣原体等抗原特征信息。就如同网络空间基于已发现的漏洞后门或病毒木马等行为特征形成的各种漏洞或攻击信息库那样，今天的库信息中不可能包括明天可能发现的漏洞后门或病毒木马等特征信息，更无法囊括未来什么形式的攻击特征信息。我们这样提出问题的目的不是企图弄明白“造物主如何使脊椎生物具有对未知入侵抗原实施与生俱来的非特异性选择清除能力”（作者猜想，也许受生物免疫细胞“处理能力”的限制，很可能采用了一种粗粒度的“指纹比对”方法，以自体基因的核心片段作为比对依据，凡是比对不一致的入侵抗原将被杀灭。作为不得不付出的代价，粗粒度比对一定存在小概率的“漏警、虚警和误警”问题。否则，脊髓生物就不会

患病或滋生癌症了，特异性免疫也就没有存在理由了。当然，比对参照系自身的可信性与可靠性，既是比对机制有效性的前提条件也是不可避免的风险所在），而是想知道在网络空间是否也存在类似的敌我识别机制，以及能有效抑制包括已知的未知风险或未知的未知威胁在内的广义不确定扰动之控制构造，并能获得不依赖（但能自然融合）任何附加式防御技术有效性的内生安全效应。运用这样的机制、构造和效应可以将基于漏洞后门或病毒木马等攻击事件归一化为传统的可靠性问题，借助成熟的鲁棒控制与可靠性理论和方法，使得信息系统或控制装置能同时获得管控软硬件故障和人为攻击影响的稳定鲁棒性与品质鲁棒性。即需要从理论和方法层面找到统一处理可靠性与可信性问题的解决途径。

首先，要把网络空间存在的 4 个基本安全问题作为一般性约束条件。因为基本安全问题既不会随系统的宿主或附加或寄生等组织形态而改变，也不会随系统服务功能的不同而变化。于是不难得出四个重要推论：凡是采用共享资源构造和层次化垂直处理机制的目标系统，安全措施存在被旁路的可能；附加式防御不能完全阻断目标对象中的后门功能；基于攻击者先验知识和行为特征信息的防护措施，无法实时防御针对未知漏洞后门等的不确定威胁；利用目标对象内生安全缺陷实施的攻击，一旦达成“内外协同”态势，任何防御都将同时面对“防外”和“防内”的挑战。

其次，要克服的挑战是如何感知未知的未知威胁，也就是说在不依赖攻击者先验知识或攻击行为特征信息的情况下，怎样才能实现低虚警、漏警、误警率的敌我识别功能。其实，哲学意义

上本来就没有绝对的已知或毫无悬念的确定性，“未知”或“不确定性”总是相对的或有界的，与认知空间和感知手段强相关。诸如，“人人都有这样或那样的缺点，但独立完成同样任务时，在同一个地点、同时犯完全一样的错误属于小概率事件”的公知（作者将其称为“相对正确”公理，业界也有共识机制的提法），就对“未知或不确定”的相对性认知关系给出了具有启迪意义的诠释。相对正确公理的一种等价逻辑表达——异构冗余构造和多模共识机制，能够在功能等价条件下，将单一空间下的未知问题场景转换为功能等价多维异构冗余空间共识机制下的可感知场景，将不确定性问题变换为可用概率表达的可靠性问题，将基于个体的不确定行为认知转移到关于群体（或元素集合）行为层面的相对性判识上来，进而将多数人的认知或共识结果作为相对正确的置信准则（这也是人类社会民主制度的基石）。需要强调的是，凡是相对性判识就一定存在如同量子叠加态的“薛定谔猫”效应，正确与错误总是同时存在，只是概率不同而已。相对正确公理在可靠性工程领域的成功应用，就是上个世纪七十年代首先在飞行控制器领域提出的非相似余度构造（DRS）。基于该构造的目标系统在一定的前提条件下，即使其软硬构件存在分布形式各异的随机性失效，或者存在未知设计缺陷导致的统计意义上的不确定失效，都可以被多模表决机制变换为能用概率表达的可靠性事件，从而使我们不仅能通过提高或改善构件质量的方式提高系统可靠性，也能通过构造技术的创新来显著地增强系统的可靠性与可信性。对于利用软硬件系统漏洞后门的不确定（或缺乏先验知识的人为攻击）威胁而言，非相似余度构造也具有与敌我识别

作用相同或相似的功效。尽管不确定威胁的攻击效果对于异构冗余个体而言往往不是概率问题，但是这些攻击事件在群体层面的反映，常常取决于攻击者能否协调一致的实现多模输出矢量时空维度上的共识表达，而这恰恰属于典型的概率问题。不过，在小尺度空间上，一定时间内，基于非相似余度构造的目标对象，虽然能够抑制包括未知的人为攻击在内的广义不确定扰动，且具有可设计标定、验证度量的品质鲁棒性。但是，其构造的静态性、相似性和确定性等基因缺陷，决定了自身漏洞后门等仍然具有相当程度的可利用性，“试错式”或“排除法”或“共模协同”等攻击手段，常常会破坏目标对象的稳定鲁棒性。

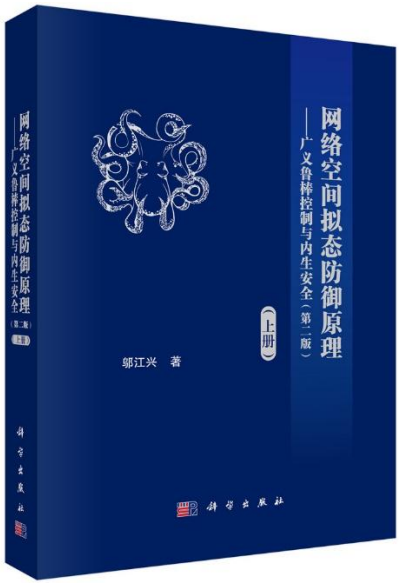
其次，如果从鲁棒控制的观点视之，网络空间绝大多数安全事件也可以认为是由针对目标对象漏洞后门等攻击引起的广义不确定扰动。换言之，由于人类目前尚不具备管控或抑制软硬件产品暗功能的能力，所以原本属于设计或制造过程中的安全质量问题，因为存在“无法突破的技术瓶颈”，就“万般无奈地溢出”成为网络空间最主要的安全污染。由此，生产厂家不承诺软硬件产品安全质量，或者不对产品安全质量引起的后果承担任何法律责任的行为，似乎都可以心安理得的归结为“世界性难题”所致。经济技术全球化时代，恢复产品质量神圣承诺和商品经济基本秩序，从源头治理被恶性污染的网络空间生态环境，需要创造出一套能够有效管控包括“试错式攻击扰动”在内的鲁棒控制构造，以及由生物拟态伪装策略驱动的反馈控制机制产生的不确定性效应，能为目标对象设计模型提供应对广义不确定摄动影响的稳定鲁棒性和品质鲁棒性。

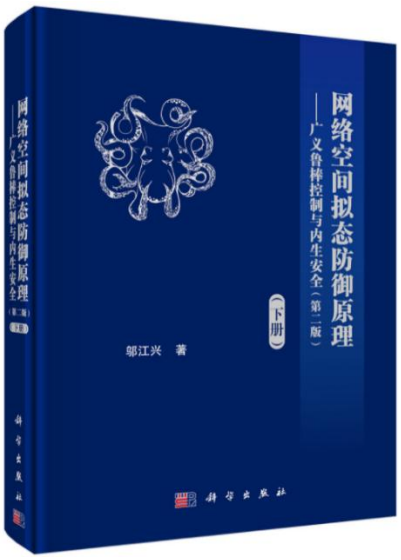
再者，即使我们不能指望广义鲁棒控制构造和拟态伪装机制产生的内生安全效应能够解决网络空间所有的安全问题，甚至都不敢奢望能彻底解决具体目标对象的全部安全问题。但是，我们仍然期望创新的广义鲁棒构造能够从机理上自然的融合或接纳现有或未来的信息与安全技术的进步。无论是导入静态防御、动态防御或是主动防御还是被动防御的技术元素，都应当能使目标对象的防御能力获得指数量级的增长，以达成信息系统“服务提供、可信防御、鲁棒控制”一体化实现的经济技术目标。

为了便于清晰理解网络空间拟态防御原理脉络，作者将理论要点归纳为“8122”即，围绕一个前提：网络空间未知漏洞后门等引发的不确定威胁；基于一个公理：相对正确公理，可以有条件的感知不确定威胁；发现一个机制：只要具有“初始信息熵不减”的自适应机制就能稳定防御不确定威胁；发明一种构造：具有广义鲁棒控制性能的动态异构冗余构造 DHR；导入一种机制：拟态伪装机制；形成一种效应：测不准效应；获得一类功能：内生安全功能；归一化处理二类问题：使得传统可靠性和非传统网络安全问题的一体化处理成为可能；产生一种非线性防御增益：导入任何一种安全技术均可指数量级的提升构造内的防御效果。

最后，需要从理论和应用的结合上完成体系架构设计、共性技术开发、原理验证到应用试点、行业示范全过程的工程实践。

“网络空间拟态防御”就是上述思想不断迭代发展与实践层面不懈探索的结果。


网络空间拟态防御原理
——广义鲁棒控制与内生安全（第二版）
上册
邬江兴 著
科学出版社


网络空间拟态防御原理
——广义鲁棒控制与内生安全（第二版）
下册
邬江兴 著
科学出版社