Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Cyberspace Security—Article

网络空间内生安全

邬江兴

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

ARTICLE INFO

Article history:
Received 14 April 2020
Revised 26 August 2020
Accepted 16 May 2021
Available online 6 August 2022

关键词
网络空间内生安全问题
不确定威胁
网络空间内生安全
相对正确公理
动态异构冗余架构

摘要

基于未知漏洞后门等产生的不确定威胁是当前网络空间最为严峻和棘手的安全问题。本文分析了系统漏洞后门等“暗功能”存在的哲学与技术层面的原因，并作为系统“内生安全问题”存在的必然性依据，指出“内生安全问题”在理论和工程层面不可能完全彻底地消除，需要“开发或利用”系统架构自身的“内源性安全功能”，使目标对象能够通过“内生的安全体制机制”来有效规避或化解内生安全问题可能引发的安全风险。文章给出了网络空间内生安全的定义和期望的体制机制及其主要技术特征，介绍了基于动态异构冗余架构的内生安全体制机制及其内生安全特性，阐述了创新的基于DHR架构的编码信道理论内涵。

1. 引言

大量的网络安全事件表明，网络空间绝大部分安全威胁都是由人为攻击这个外因，通过目标对象自身存在的漏洞后门这个“内生安全问题”[1–4]之内因的相互作用而形成的。遗憾的是，迄今为止，传统的网络安全思维模式和技术路线很少能跳出“尽力而为、问题归零”的惯性思维，挖漏洞、打补丁、封门补漏、查毒杀马乃至设蜜罐、布沙箱，层层叠叠的附加式防护措施，包括内置层次化的检测构造方式（借鉴生物学的内共生思想），在引入安全功能的同时不可避免地会引入新的内生安全隐患。怎样才能破解基于内生安全问题的不确定威胁影响，是既需要重大理论创新又需要重大技术发明才能解决的科学技术难题。

本文从“一切事物都是自在的矛盾、任何事物有利必有弊”的哲学原理出发，分析了信息系统“内生安全问题”存在的必然性，给出了网络空间内生安全问题的概念、特征，指出内生安全问题作为自在矛盾的一方，在理论和工程层面都不可能彻底消除，需要开发或利用系统元构造（算法）自身的“内源性安全效应”，或者形成“内生的安全体制机制”才能有效规避或化解由自在矛盾引发的安全风险。本文给出了期望的内生安全的体制机制定义和技术特征，并在可靠性理论与方法的启示下，通过“相对正确公理”的再发现，在香农信道编码纠错理论基础上创立了编码信道理论，发明了动态异构冗余架构（DHR），阐述了DHR架构能够归一化地处理传统可靠性问题与非传统网络安全问题的原理。

* Corresponding author.
E-mail address: ndscwjx@126.com.

英文原文：Engineering 2022, 15(8): 179–185
引用本文：Jiangxing Wu. Cyberspace Endogenous Safety and Security. *Engineering*, https://doi.org/10.1016/j.eng.2021.05.015

2. 网络空间“内生安全问题”

2.1. 内生安全问题的定义和内涵

信息世界网络空间与现实世界物理空间一样有着相同的哲学本质，如同德国哲学大师黑格尔所说的那样“一切事物都是自在（内生）的矛盾，矛盾是一切运动和生命力的根源”。矛盾的同一性是事物存在和发展的前提，且互为发展条件。矛盾的斗争性则会促进矛盾双方此消彼长，造成双方力量的发展不平衡，为对立面的转化和事物质变创造条件。以信息技术为例：大数据技术能够根据算法和数据样本发现未知的规律或特征，而蓄意污染数据样本、恶意触发算法缺陷也能使人们误入歧途；区块链技术开辟了无中心记账方式的新纪元，51%的共识机制却不能避免市场占有率大于51%的COTS级软硬件产品中的漏洞后门问题。

当代计算技术的发展使人类步入了辉煌的信息时代，但是既有的计算技术本身的安全缺陷也使得网络空间充满风险和不确定威胁。由此可见，内生安全问题与内生安全机制是同一系统构造或算法在不同应用目标、不同使用场景、不同技术条件下的不同形态表现，符合矛盾的对立统一规律。网络世界也概莫能外，一个软硬件构造或算法除本征（元）功能之外，总存在着伴生/衍生的显式副作用或隐式暗功能，如果其中的一些副作用或暗功能被某种自然或人为因素触发，影响到本征功能的正确表达，则称这类副作用和暗功能为网络空间“内生安全问题”。

内生安全问题可以进一步抽象为两类问题。一类是狭义内生安全问题，特指一个软硬件实体除了设计的本征或元功能之外，总存在包括副作用、脆弱性、自然失效等因素在内的显式或隐式表达的非期望功能；另一类是广义内生安全问题，专指在狭义内生安全问题之上，还包括蓄意让最终用户不可见的设计功能，或所有未向使用者明确声明或披露过的软硬件隐匿功能，例如刻意设计的前门、后门、陷门等“暗功能”问题。

2.2. 内生安全问题的特性

由内生安全问题的定义和内涵，可以归纳总结出内生安全问题所具有的特性[4]。

2.2.1. 存在的必然性

漏洞和后门总是时不时被人们发现，从未间断过。根据统计规律，漏洞的数量与代码数量存在一定的比例关系，随系统复杂性的增加和代码数量的增大，漏洞数量也随之增加[5]。同时，由于全球化经济的发展和产业分工的专门化、精细化，集成创新或制造成为普遍的生产组织模式，各种产品的设计链、工具链、生产链、配套链、服务链等供应链条越来越长，涉及的范围和环节越来越多，这给后门的预埋植入提供了众多机会。上述这些非主观因素引入的软硬件代码漏洞（陷门）或人为预埋进入信息系统的后门，不论从矛盾的自在性、技术发展的阶段性还是从利益博弈角度来解释，其出现都是必然的，且难以从根本上避免。

2.2.2. 呈现的偶然性

纵观整个漏洞被发现的历史，虽然时不时有漏洞被发现，但是每个漏洞在什么时候被发现，是怎么被发现的，都有其偶然性，是一个无规律的现象。从认识论关于“事物总是可以被认识的”观点出发，漏洞的存在和发现都属于必然事件，但是具体在什么时间、什么系统上和以什么样的方式呈现出来却是偶然的。这其中既有对漏洞认识的技术阶段性或时代局限性问题，也有对复杂代码完备性检查的理论方法和技术能力问题。

2.2.3. 认知的时空特性

漏洞是客观存在的，但是漏洞的发现则具有时空属性，需要随着实践认知不断积累到一定程度才能使漏洞呈现出来。今天认为安全的系统，明天未必安全；“我”认为安全的系统，在“他”眼里未必安全；在环境A里面安全的系统，放到B环境中未必安全[3]。这就是漏洞因认知而呈现的时空差异。

2.2.4. 威胁的不确定性

在经济学中，美国人富兰克·奈特区分了风险与不确定性的关系：风险是一种人们可知其概率分布的不确定性，但是人们可以根据过去推测未来的可能性；而不确定性则表示人们根本无法预知没有发生过的将来事件。不难看出，“内生安全问题”可能引发两类安全威胁，一是显著影响目标对象本征功能或元功能的可靠性、可信性和可用性，二是非法获得或侵犯他人隐私信息与数据资源。由于“内生安全问题”的性质所致，上述两类安全威胁的发生均不可预知，属于不确定性范畴中的未知威胁。

从更加一般的意义上说，由于人类技术发展和认知水平的阶段性特征导致软硬件设计脆弱性或漏洞问题不可能彻底避免也不可能穷尽或彻查，加之全球化时代，开放式产业生态环境，开源协同技术模式和“你中有我、我中有你”的产业链使得软硬件后门问题不可能完全杜绝，因此迄今为止，对基于内生安全问题的不确定性威胁之防御，除了用附加型安全技术尽力而为地阻断来自攻击表面的扰

动影响之外，几乎没有可量化设计、可验证度量的有效安全防御方法或技术手段，即使采取类似加密认证、可信计算等“底线防御”措施，也往往会因为宿主系统自身的内生安全问题而被攻击者“旁路或短路”。

3. 破解网络空间内生安全问题的思考

3.1. 变换问题场景和解题思路

基于“网络空间绝大部分安全威胁都是由人为攻击这个外因，通过目标对象自身存在的‘内生安全问题’之内因相互作用而形成的”认知，一个直观的推论就是，欲彻底解除网络空间安全威胁就必须彻底排除其内生的安全问题，因为外因只能通过内因起作用。然而，理论研究和工程实践告诉我们，内生安全问题是自在性矛盾，不可能“彻底消除”。首先，在全球化大趋势下，开放式、协作化的创新链和产业链正成为人类技术开发、现代社会生产活动的基本模式，仅凭一国之力几乎不可能做到技术链、供应链层面的彻底自主可控与安全可信；其次，软硬件设计缺陷导致的漏洞问题，目前在理论和技术上尚无有效的应对办法，试图从根本上杜绝此类问题也违背人类认知和科技发展阶段性之客观规律。这意味着无论从理论上、技术上还是经济上，都不可能完全保证网络空间构成环境无内生安全问题，即“无毒无菌”几乎是安全领域不可能实现的愿景。

基于上述分析，一个很自然的推论，就是如何变换问题场景和解题思路，在网络空间“有毒带菌”的条件下，实现有安全保障的“沙滩建楼”，缓解“已知的未知”风险和“未知的未知”威胁挑战。这需要跳出传统架构下“亡羊补牢”附加型修复式防御思维定式，使得信息装备的安全性不再过度依赖元件、器件、组件或个体形态软硬件设计、制作、运行和管理环节的自主可控程度与安全可信水平，也就是要找到赋予信息系统基础构造内源性安全功能或内生性安全机制的技术途径，在一定程度或约束条件下能够宽容软硬构件内生安全问题及其影响，使本征功能无论对随机性故障还是网络攻击都有很好的稳定鲁棒性和品质鲁棒性。

3.2. 生物免疫学的启迪

生物学的知识告诉我们，人类通过遗传特性获得的与生俱来的非特异性免疫，对绝大多数入侵病原微生物都能作出“无特异性清除”反应，属于一种“面”防御。科学研究表明，自然界的病原微生物总是在不断地变异，是什么因素保证非特异性免疫仅靠生物遗传信息，机体就能够对现实世界变化着的各种入侵病原微生物具有非特异性选择清除的功能；什么情况下、需要何种条件、通过什么样的方式才能激活特异性免疫机制；遗传信息具有相对的稳定性但在生物机体全生命周期内是否需要更新，以及何时更新，怎样更新；特异性免疫（属于“点”防御）的记忆效应如何及怎样才能影响非特异性免疫的遗传信息等。

由此产生的启迪意义，就是我们能否在软硬件装置或系统中，也设计出一种类似脊椎动物免疫机理的融合式防御能力，以便对“基于目标对象内生安全问题的未知攻击活动产生没有特异性选择的清除功能”，并能适时触发类似特异性免疫机制那样的点防御功能。由此作者以为，这种源于目标对象自身构造机理的防御功能，用内生安全的概念来定义是最恰当不过的事情了。

3.3. 网络空间内生安全

所谓内生安全是指具有内生或内源性安全功效的构造或算法及其体制机制[4]。按字面意思，内生就是靠自身因素而不是外部因素得到的内源性效应。内生安全就是利用系统的架构、算法、机制、场景等内在因素获得的安全功能或属性，如，脊椎动物的非特异性免疫和特异性免疫学习机制就是一种内生安全功能。内生安全应该具有的体制机制和技术特征如下：

3.3.1. 期望的内生安全体制

（1）内生安全体制应当基于开放的组织架构，不排除架构、模块和构件中包含任何的内生安全问题；

（2）内生安全体制应当基于一体化的融合构造，能同时提供高可靠、高可信、高可用的使用功能；

（3）内生安全体制应当能够充分发挥多样性、随机性和动态性防御要素的综合效应；

（4）内生安全体制应当同时具有异构、冗余、动态、裁决和反馈控制之构造要素；

（5）内生安全体制应当能够自然的接纳传统安全防护技术或其他技术的使用并可获得指数量级的防御增益；

（6）内生安全体制应当具有普适性应用意义。

3.3.2. 期望的内生安全机制

（1）内生安全机制与广义不确定扰动应属于人-机、机-机、机-人博弈关系；

（2）内生安全机制应当可以条件管控或抑制广义不确定扰动造成的负面影响；

（3）内生安全机制的有效性应当不依赖（但可以融合）关于攻击者的先验知识或附加、内置、内共生的其他安全措施或技术手段；

（4）内生安全机制应当能以融合方式为目标对象提供一体化的高可靠、高可信、高可用的使用性能；

（5）内生安全机制导致的广义安全性应当具有可量化设计、可验证度量的稳定鲁棒性和品质鲁棒性；

（6）内生安全机制的使用效能应当与运维管理者的技术能力和过往的经验弱相关或不相关。

3.3.3. 期望的技术特征

（1）内生安全应当是基于目标对象基础构造或算法的内源性安全功能，具有与脊椎生物非特异性和特异性免疫机制类似的“点面融合”式防御特点，与目标对象本征或元功能具有构造层面的不可分割性；

（2）内生安全功效应当不依赖攻击者先验知识和行为特征信息，对独立的攻击资源、攻击技术、攻击方法形成的“差模攻击效应”应当具有天然的抑制功效。换言之，凡是基于0-Day性质的漏洞后门、病毒木马等网络攻击，内生安全功能可使之在机理上无效；

（3）突破内生安全防御除社会工程学的手段外，只能通过时空一致性的精准协同攻击才有“共模逃逸”的可能，但首先要克服时空非一致性的“测不准效应”，然后需逾越“基于策略裁决的异构冗余目标反馈调度迭代机制”，其次必须解决共模逃逸的稳定维持问题；

（4）内生安全功能应当能够归一化地解决传统可靠性问题和基于目标对象的网络安全威胁问题；

（5）理论上，“差模逃逸”不可能发生，“共模逃逸”属于可量化设计的小概率或极小概率事件，“即使攻击成功也可能只此一次”，在内生安全环境内的攻击行动或成果都不具有稳定鲁棒性和品质鲁棒性。

4. 基于DHR架构的内生安全体制机制

4.1. 可靠性问题的启示

作者在长期的研究和探索中发现，可靠性问题与网络安全问题虽属两个领域且扰动因素不同，前者以随机性扰动为主要表现形态，而后者则完全由攻击者人为行为所致。但也存在许多相似甚至相同的理论与技术问题，相关的理论方法和体制机制应当具有“他山之石可以攻玉”的相互借鉴意义。

我们知道，可靠性领域最具挑战性的问题是如何应对系统的不确定性故障或失效。涉及两个基本问题：一是如何应对由无源或有源器件或零部件物理性错误或故障导致的不确定失效问题，二是怎样才能避免由未能发现的软硬件设计缺陷或错误导致的不确定失效问题。尽管故障或失效产生的机理和影响程度不同，但是共同的特征都是故障或失效发生的时间、部位、性质和结果等都不确定。换言之，可靠性技术同样需要克服相关领域内生安全问题导致的不确定错误、故障乃至失效。

4.2. “相对正确公理”的再发现

“相对正确公理”（也有研究者称之为共识机制）是指“人人都存在这样或那样的缺点，但极少出现独立完成同样任务时，多数人在同一个地点、同一时间、犯完全一样错误的情形”。相对正确公理在可靠性工程领域的成功应用，是20世纪70年代首先在飞行控制器领域提出的非相似余度构造[1]（dissimilar redundant structure, DRS），其抽象模型如图1所示。基于该构造的目标系统在一定的前提或约束条件下，即使其软硬构件存在分布形式各异的随机性故障，或者存在未知设计缺陷或错误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差模或共模事件，从而使我们不仅能通过提高或改善材料、构件质量的方式提高系统可靠性，也能通过系统工程技术的创新来显著增强系统的可靠性与可用性。

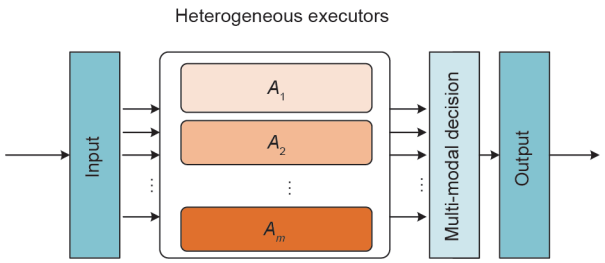

图1. DRS架构的抽象模型，其中，$A_i(i = 1, 2, \cdots, m)$表示第i个异构执行体，m表示异构执行体的数量。

就目标对象内生安全问题的不确定威胁而言，DRS构造从某种意义上说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功能等价的异构冗余个体而言往往不是概率问题，但是这种攻击事件在群体层面的反映通常会以差模形态呈现，并具有随机性质的概率属性。换言之，在给定的约束条件下，不确定的个体表现可以被相对正确公理变换为群体层面的概率问题。在小尺度空间上，基于DRS构造的目标对象，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。

4.3. 动态异构冗余架构

进一步研究不难看出，尽管基于DRS构造的目标对象能够抑制包括未知的人为攻击在内的广义不确定扰动，但DRS架构内各执行体的运行环境以及相关漏洞后门等

的可利用条件是静态确定的，且执行体的并行部署方式通常也不会改变攻击表面的可达性，因而，对DRS的攻击成功经验具有可继承性，方法具有可复现性，攻击效果具有可持续利用价值。换言之，DRS架构的静态性、确定性和相似性在非传统安全领域成为构造或算法层面的基因缺陷，其抗攻击性与可靠性不具备稳定鲁棒性。

作者研究发现，从信息熵角度观察，攻防双方实际上是围绕防御方初始信息熵的增减或维持展开的博弈。DRS构造的容侵属性之所以缺乏时间稳定性是因为随着针对性尝试攻击或试错式攻击的持续进行，构造内的初始信息熵因为没有任何的自维持机制只能作熵减少运动，直至初始信息熵低至攻击链能够可靠地发挥期望的作用，构造的本征功能或防御功效彻底丧失为止。

不难推论，如果能在DRS架构中导入初始信息熵不减（或熵平衡）机制就能使其容侵属性具有一定程度的鲁棒性。例如，添加动态、随机、多样、重构或加密认证、入侵检测、入侵预防等传统防御元素，或导入策略裁决、控制律反馈、可迭代收敛的鲁棒控制机制等，理论上应当能够改变DRS运行环境的静态性、确定性和相似性在非传统安全领域的基因缺陷。期望这种经“基因工程”再造后的控制构造和运行机制，由于具有初始信息熵不减（包括熵平衡）特性，因而无论在容侵还是容错方面都应该具有可量化设计、可验证度量的稳定鲁棒性和品质鲁棒性。

作者将这种创新的技术构造命名为“动态异构冗余架构”（Dynamic Heterogeneous Redundancy, DHR）。DHR架构抽象模型如图2所示。

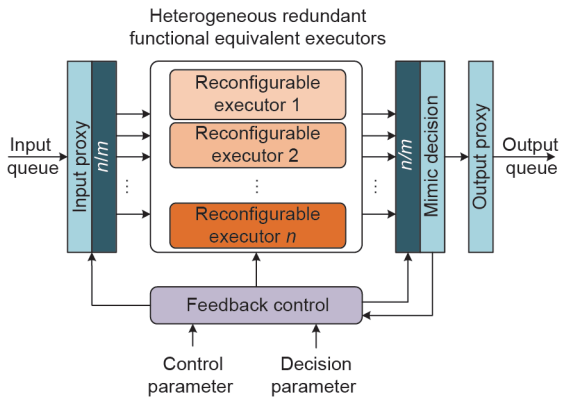

图2. DHR架构的抽象模型，其中，n表示异构执行体的数量。

DHR架构的核心思想是：依据“构造决定安全”的公知，在保证本征功能集不变条件下，导入基于多模裁决的策略调度和多维动态重构鲁棒控制机制，赋予运行环境动态可重组、软件可定义、算法可重构的功能属性，形成攻击者视角下的测不准效应，使目标运行场景在抑制广义不确定扰动方面具备可迭代收敛的动态性、随机性、多样性。

同时，严格隔离执行体之间的协同途径或尽可能地消除攻击者可资利用的同步、共享机制，最大限度地发挥基于动态异构冗余环境、非合作模式、多模裁决对蓄意利用内生安全问题的不确定威胁的规避或瓦解作用，显著提升软硬件差模故障或随机性失效的容忍度。换言之，期望通过DHR架构获得多位一体的内生安全功能，既能有效抑制基于目标对象内生安全问题的非配合或差模攻击扰动，又能保证即使出现协同攻击逃逸情况仍能够控制模型摄动范围在给定的阈值之内；不仅能显著增加攻击链的不确定性，还能充分增强包括高可靠、高可用、高可信一体化机制在内的广义鲁棒控制服务或应用性能；期望能显著弱化非相似余度苛刻的异构性设计要求，使得DHR构造能够成为具有广泛应用前景的新型使能技术。有关DHR的基本原理、典型与非典型构造、技术目标与典型功效、安全性量化分析的相关论述参见参考文献[1–4]。

4.4. DHR架构的内生安全特性

DHR从组织结构、运行模式、制度安排等方面具备内生安全体制需要的全部要素，在目标对象中运用DHR的过程就是为其建立内生安全体制的过程，具体表现在如下几个方面。

（1）DHR是完全开放的组织架构，允许架构内的软硬模块或构件中包含任何的内生安全问题，即可以在任何“有毒带菌”场景下可靠的发挥期望的作用；

（2）DHR是一体化的融合构造，能同时提供高可靠、高可信、高可用的使用功能。不仅能解决传统的功能安全问题还能管控非传统安全问题；

（3）DHR架构能够综合使用多样性、随机性和动态性之防御要素，形成内源性的测不准效应和难以窥探的“防御迷雾”；

（4）DHR架构本身是由异构、冗余、动态、裁决和反馈控制五大环节组成，能最大限度地发挥“动态、多样、随机”防御三要素的协同效应；

（5）DHR架构能够自然地接纳传统安全防护技术或其他技术的使用并可获得指数量级的防御增益；

（6）DHR架构对所有软硬件系统具有普适性应用意义。

此外，基于DHR架构、功能、相关策略等形成的协同关系造就了一种具有独特优势的内源性安全机制，具体表现在如下几个方面：

（1）DHR安全机制形成的测不准防御迷雾正是为了

管控或抑制基于目标对象内生安全问题的广义不确定扰动，属于典型的人-机博弈关系，如果导入人工智能和大数据等后台处理功能完全可以在人-机、机-机、机-人博弈中占据优势；

（2）DHR 安全机制可以条件管控或抑制针对目标对象的广义不确定扰动，但不可能完全杜绝共模逃逸现象的发生，尽管这种逃逸属于可量化控制的极小概率事件；

（3）DHR 安全机制的有效性不依赖任何先验知识或附加、内置、内共生的其他安全措施或技术手段，但可以融合使用相关技术成果指数量级地提升安全增益；

（4）DHR 安全机制能用同一技术架构以融合方式为目标对象提供一体化的高可靠、高可信、高可用的使用性能；

（5）DHR 安全机制形成的安全效应可通过可靠性验证理论中的“白盒注入”测试法检定，并具有可量化设计、可验证度量的稳定鲁棒性和品质鲁棒性；

（6）DHR 安全机制的使用效能与运维管理者的技术能力和过往的经验弱相关或不相关，具有全生命周期难以比拟的效费比优势。

需要郑重声明的是，DHR 只是网络空间内生安全体制机制的一种而不是全部。

4.5. DHR 架构编码信道模型

1949 年香农提出著名的信道编码定理[6]，奠定了现代通信特别是纠错编码的理论基础。香农第二定理（有噪信道编码定理）的目的是在无记忆信道引入随机噪声的情况下，通过在传输的消息中添加一个适当设计的冗余，然后在接收器处使用该冗余来重建原始消息，最终完成消息的正常传递。该定理虽然仅是存在性的，但对通信的指导意义十分明显，它给通信工作者指出了进行可靠通信的新方向和新途径，纠错编码正是在该定理指导下发展起来的。DHR 构造的内生安全机制也可以描述为如何在一个存在非随机噪声的可重构有记忆信道上正确地处理和传输信息的问题。作者认为，对于网络攻击所导致的信息处理和传输错误与可靠性错误与通信噪声错误等的性质类似，都可以采用纠错编码思路进行解决。但与经典香农通信传输模型中的无记忆信道假设不同，DHR 可以抽象为一种有处理能力的可重构有记忆信道。与香农假设的随机噪声不同，网络攻击具有明显的非随机性，可以抽象为非随机噪声，这里将随机通信噪声、随机物理失效、人为攻击噪声等统一称为广义不确定扰动。DHR 构造等效传输信道模型和香农传输信道模型如图 3 和图 4 所示。

如果从香农的冗余编码理论视之，DHR 结构在时空上可以展开为一组基于动态异构冗余方式的“编码结构”（coding-structure）之集合[4]，目的是为了对抗与信道噪声类似的随机或非随机的“结构扰动噪声”（structure disturbances noise, SDN）的影响。但是，香农信道编码理论的分析对象是“随机无记忆信道”，而 DHR 的异构冗余迭代防御场景则相当于“随机或非随机的有记忆信道”。因此，不能直接用香农理论及方法来量化分析 DHR 构造的安全性或广义鲁棒性，需要从信道编码理论发展出一种“编码信道”理论[4]（coding channel theory, CCT），以便能对 DHR 的“编码结构”体制机制在抑制“结构扰动噪声”方面的性能进行量化分析。而编码信道理论是否成立的关键是相关存在定理的证明，需要从理论上阐明在广义扰动条件下，针对特定离散有记忆信道，如何构造合适的

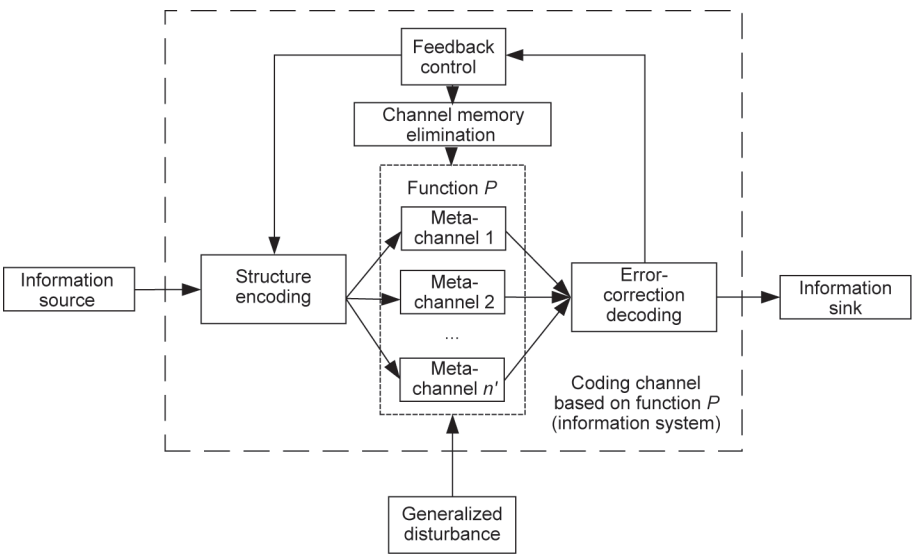

图 3. DHR 构造等价传输信道模型，其中，P 表示通道函数，n' 表示元信道的数量，n' 与图 2 中的 n 具有相似的含义。

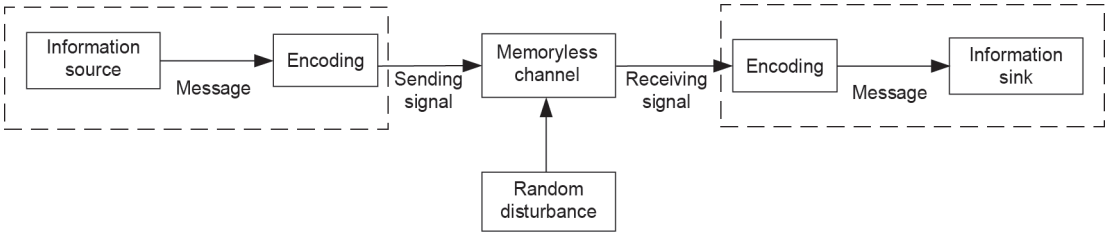

图4. 香农传输信道模型。

信道与编码来提供正确服务的问题。所谓“正确”的概念就是采用适当的编码与译码步骤，使得在具有内生安全属性的系统架构内，当存在随机或人为加性干扰时信息传递和处理的误差足够小。简而言之，编码信道理论是由内生安全构造数学模型和两个存在定理及相关定义、引理及数学证明构成，涵盖且应当涵盖香农第二定理的内容。

4.6. DHR架构编码信道数学模型

假定攻击以速率$\lambda\,(\lambda>0)$到达，以及假定存在以下三类单个执行体被攻击成功的概率$P_s(t)$与时间t的数学表达式：

$$P_s(t)=\begin{cases}p=1-\dfrac{1-e^{(t-T_s)}}{1-e^{-T_s}},t\leqslant T_s\\1,t>T_s\end{cases}\tag{1}$$

$$P_s(t)=\begin{cases}p=1-\dfrac{1-e^{(-t+T_s)}}{1-e^{T_s}},t\leqslant T_s\\1,t>T_s\end{cases}\tag{2}$$

$$P_s(t)=\begin{cases}p=\dfrac{t}{T_s},t\leqslant T_s\\1,t>T_s\end{cases}\tag{3}$$

式中，T_s表示干扰到达的时间；p表示部署差模元信道的概率，首次以概率p部署差模元信道没有任何危害。

可以证明[4]动态异构冗余与反馈记忆消除信道构造方案使得编码信道结构与元信道记忆具有不确定性，保证了系统失效的随机性。

4.7. 编码信道存在定理

将编码信道内具备同等功能和性能的子信道称为元信道，元信道的噪声随机到达（在内生安全问题中表现为未知的漏洞后门），对于任意随机噪声，信道输出出错的概率$P_e<1$。加之信道的无记忆性，对于任意时刻t的随机噪声，使信道输出出错的概率$P_e(t)<1$。因此，在随机噪声无记忆信道条件下，编码信道中n'个元信道构造满足香农第二定理：信道噪声随机且信道n'次扩展无记忆条件的约束前提[6]。

针对输入X的样本空间为$x=\{0,1\}$，输出响应Y的样本空间为$y=\{0,1\}$。

4.7.1. 编码信道存在第一定理

噪声（扰动）随机到达，若编码信息传输率$R<C$，其中，C表示离散无记忆信道的信道容量，当存在无记忆元信道n'足够大的编码信道，总可以在输入集合找到$M=2^{n'R}$个码字组成一个码集合，其中，n'表示码长，M表示异构元信道组合的总数，其与图1中的m含义相似。在一定译码规则下，可使信道输出错误概率$P(t)\leqslant\varepsilon$，其中，ε表示任意小正数。

在随机噪声无记忆信道下，编码信道噪声随机，构造的元信道均为无记忆信道。香农第二定理要求信道进行n'次无记忆扩展，各扩展信道的噪声随机，均为无记忆信道。因此，随机噪声无记忆信道下编码信道存在第一定理与香农第二定理满足条件等同[4–5]。

4.7.2. 编码信道存在第二定理

噪声（扰动）非随机到达，动态异构冗余与反馈消记忆构造后的离散有记忆编码信道的信道容量C，$\forall t>0, C(t)\in[C_s,C_0]$，其中，$C_s$表示稳态信道容量，$C_0$表示初始状态信道容量。若$t$时刻编码信息传输率$R(t)<C(t)$，则只要码长与编码元信道构造数$n'$足够大，总可以在输入集合找到$M=2^{n'R}$个码字组成一个码集合。在一定译码规则下，可使信道输出错误概率$P_e(t)\leqslant\varepsilon$，其中，$\varepsilon$表示任意小的正数。

5. 总结

基于目标对象内生安全问题的攻击理论和方法是造成当前网络空间泛在化安全威胁的最主要原因之一，虽然内生安全问题不可避免，但由此带来的安全威胁影响应当可以通过内生安全的体制机制设法规避或化解（网络空间拟态防御就是这一机理的成功应用），这不仅涉及网络空间安全防御思想与观念的转变，更关系到信息技术（IT）、信息通信技术（ICT）、信息物理系统（CPS）、工业控制系统（ICS）等领域安全理论与产品技术的跨越式发展，也为众多学科拓展了新的研究方向。

本文分析了破解网络空间内生安全问题的思路和方

法，提出了网络空间内生安全的概念和技术特征，介绍了具有内生安全特性的DHR架构的产生过程及其核心思想。作者相信网络空间内生安全必将成为新一代软硬件产品的赋能技术，这将使得从软硬件产品源头开始治理网络空间安全秩序、打造安全可信的人类网络命运共同体成为可能。

致谢

本文工作得到国家自然科学基金创新群体项目（61521003）资助。

References

[1] Wu J. [Introduction to cyberspace mimic defense]. Beijing: Science Press; 2017. Chinese.
[2] Wu J. [Principle of cyberspace mimic defense: endogenous safety−security & generalized robust control]. Beijing: Science Press; 2018. Chinese.
[3] Wu J. Cyberspace mimic defense: generalized robust control and endogenous safety–security. Berlin: Springer International Publishing; 2019.
[4] Wu J. [Endogenous safety and security in cyberspace: mimic defense and generalized robust control]. Beijing: Science Press; 2020. Chinese.
[5] Nie C, Zhao X, Chen K, Han Z. An Software vulnerability number prediction model based on micro-parameters. Comput Res Dev 2011; 48(7):1279–87. Chinese.
[6] Shannon CE, Weaver W. The mathematical theory of communication. Urbana: University of Illinois Press; 1949.