补天系列丛书

The General Theory of Information Security

安全通论

刷新网络空间安全观

杨义先　钮心忻 ◎ 著

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

The General Theory of Information Security

安全通论

网络空间安全观

[redacted]

补天系列丛书

安全通论

刷新网络空间安全观

杨义先　钮心忻 ◎ 著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书构建了一套网络空间安全的统一基础理论体系，在理工科范围内（不含心理学、社会学、经济学、管理学等），几乎没有任何限制（如设备、环境和人员等）的前提下，揭示了黑客攻防和安全演化的若干基本规律。这些规律可以适用于网络空间安全的各主要分支。特别是本书介绍了系统安全经络的普遍存在性、黑客的离散随机变量本质、红客维护安全熵的目标核心、在各种情况下（单挑、一对多、多对一、多对多等）红客与黑客对抗的可达极限、安全攻防的宏观和中观动态行为数学特征、红客与黑客的直接与间接对抗的演化规律、网络空间安全的生态发展量化规律等。读者不要被书中大量的数学公式吓倒，如果忽略书中的具体数学证明（即假定证明的正确性），那么安全界的所有人员都能读懂此书，并从中受益。

图书在版编目（CIP）数据

安全通论：刷新网络空间安全观/杨义先，钮心忻著. —北京：电子工业出版社，2018.1
（补天系列丛书）
ISBN 978-7-121-33412-2

Ⅰ. ①安… Ⅱ. ①杨… ②钮… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 328862 号

策划编辑：李树林
责任编辑：李树林
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：720×1000　1/16　印张：24.5　字数：412 千字
版　　次：2018 年 1 月第 1 版
印　　次：2018 年 4 月第 2 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254463；lisl@phei.com.cn。

前 言

开天辟地生易经，合纵连横信息论；安全世界诸侯乱，谁成一统谁成神。

所谓“安全通论”，顾名思义，就是在一定的范围内建立统一的安全基础理论。此书的范围，指理工科范围，即不含心理学、社会学、经济学、管理学等领域。此书的安全含义，就是指信息安全或网络空间安全。

你肯定会怀疑，这样的理论存在吗？答案当然是存在，不但存在，而且已经存在了数千年；不但存在了数千年，而且还在不断具体化，不断突破新领域，不断涌现新版本。不信你看，早在人类还没有文字的时候，伏羲就用几根小棍子摆出了八卦图，这可以说是人类历史的第一部，也是涉及面最广的一部“安全通论”了。后来，约在3200年前，周文王（公元前1152年—公元前1056年）又对伏羲的“安全通论”进行了“改版”，写成了64卦的《易经》，于是完成了指导宇宙万事万物的

“安全通论”。再后来，又过了约1000年，孔子对《易经》进行了精心注解，并将其作为群经之首。如果将“吉”看作安全，将“凶”看作不安全的话，那么《易经》这部“安全通论”的“核心定理”便可以总结为“吉中有凶，凶中含吉；凶极吉来，吉极有凶”。对该“核心定理”，周文王虽未给出精确的数学证明，但是数千年来的事实已多次反复证明了其正确性！它甚至已经演化成了辩证法的精髓：物极必反！特别需要指出的是，《易经》还是中华文化之源。可见，安全通论对我们是多么的重要！

在医学领域，第一部“安全通论”叫《黄帝内经》，大约成书于先秦至西汉年间（公元前21世纪至公元8年）。虽然该书作者不详，但它的“核心定理”却是很明确的，即阴阳五行说——“水生木，木生火，火生土，土生金，金生水”或“水克火，火克金，金克木，木克土，土克水”。当然，也可以形象地总结为“通则不痛，痛则不通”，只不过此处将“不生病”看作安全，将“生病”看作不安全而已。

在军事领域，第一部“安全通论”叫《孙子兵法》，它成书于2500多年前。如果将“胜”看作安全，将“败”看作不安全，那么孙武的“安全通论”本身就已非常精练，区区6000余字含有13篇基本法则：始计篇、作战篇、谋攻篇、军形篇、兵势篇、虚实篇、军争篇、九变篇、行军篇、地形篇、九地篇、火攻篇、用间篇。当然，现在孙武“安全通论”的应用已经不仅仅限于军事领域了，甚至成为当代商家的必读经典，因为商场如战场嘛。

古人在不同领域，从不同层次和深度创立了各种版本的“安全通论”，推动着人类文明不断向前发展。其实，即使到了近代和现代，人类也还在继续着这方面的探索。

约250年前，经济学鼻祖亚当·斯密也撰写了一部非常著名、一直畅销至今的“安全通论”，简称《国富论》。在激烈的自由市场竞争中，如果将“竞争成功”看作安全，而将“竞争失败”看作不安全，那么亚当·斯密的“安全通论”便可形象地概括为一句话：看不见的手。更详细地说，就是“人人都试图

用其资本来使其生产品获得最大价值。一般来说，他并不企图增进公共福利，也不清楚增进的公共福利有多少，他所追求的仅仅是个人安乐和个人利益，但当他这样做的时候，就会有一双看不见的手，引导他去达到另一个目标，而这个目标绝不是他所追求的东西。由于追逐他个人的利益，却经常促进了社会利益，其效果比他真正想促进社会效益时所得到的效果为大”。亚当·斯密“安全通论”中的各种改进和充实层出不穷，甚至已经发展成多门学科，如数量经济学、经济数学、一般均衡理论等。

约150年前，达尔文创立的“进化论”其实就是生物界的“安全通论”。如果将生物种群的“灭绝”看作不安全，“生存”看作安全，那么达尔文“安全通论”的“核心定理”便可以总结为“物竞天择，适者生存”或“自然选择是生物进化的动力”。当然，达尔文“安全通论”的影响力已经不仅仅限于生物界了，甚至跨越了自然科学和社会科学，极大地改变了人类的世界观。

前面介绍的所有“安全通论”案例，大多出自人文或社科领域。但是，别误会，其实“安全通论”在自然科学界也比比皆是。

完全由抽象数学公式写成的“安全通论”，名叫“博弈论”，它由计算机之父冯·诺依曼等科学家于1944年最终创立，它已成为现代数学的一个新分支，也是运筹学的重要内容。如果将斗争（或竞争）中的“获胜”当作安全，“失败”当作不安全（当然，这里的“安全”或“不安全”不再有明显的界限，而是由具体的数字量化描述，行话叫“收益函数”或“权重”），那么冯·诺依曼“安全通论”就主要研究公式化的激励结构间的相互作用，研究具有斗争（或竞争）现象的数学理论和方法，研究对抗游戏中个体的预测行为和实际行为及其优化策略等。该理论的核心定理便是著名的“纳什均衡定理”。如今，冯·诺依曼“安全通论”已被生物学家用来理解和预测进化论的某些结果；被经济学家用作标准分析工具之一，并在金融学、证券学等领域扮演着重要角色；被社会科学家用于处理国际关系、政治学、军事战略等学科的重要问题。

在现代通信中，如果将“1比特信息被无误差地传输到收信端，比如1传

成1或0传成0”看作安全，而将“信息被传错，即1传成0或0传成1”看作不安全，那么此种情形下的“安全通论”便是众所周知的“信息论”，它于1948年由天才科学家克劳德·艾尔伍德·香农创立。该理论的核心只有两个定理，其一是“信道编码定理”，其二是“信源编码定理”。如今，香农“安全通论”已经成为IT领域的“指路明灯”，其重要性怎么描述也不过分。如果没有它，人类可能就无法进入所谓的信息时代、数字时代或网络时代。

如果将系统（准确地说是系统中的信息）的“失控”看作不安全，将“受控”看作安全，那么与之相应的“安全通论”便是如雷贯耳的“控制论”（其实应该叫“赛博学”），它由诺伯特·维纳等于1948年创立。虽然维纳版的“安全通论”没有明确的“核心定理”，但是它却再一次彻底刷新了人类的世界观，揭示了系统的信息变换和控制过程。虽然一般系统具有物质、能量和信息三要素，但是维纳却只把物质和能量看作系统工作的必要前提，并不追究系统到底由什么物质构造或能量如何转换等，而是着眼于信息方面，研究系统行为方式的一般规律，特别是动态系统在变化的环境中如何保持平衡或稳定状态，即“受控”中有“失控”、“失控”中含“受控”的《易经》思想。与其他只研究特定物态系统，只揭示某一领域具体规律的专门科学相比较，维纳版“安全通论”是一门带有普遍性的横断科学，其思想和方法已渗透到了几乎所有自然科学和社会科学领域。

其实，在不同领域，为了不同目的，人们还创立了多种其他版本的“安全通论”，包括但不限于：1968年贝塔朗菲等创立的“一般系统论”，1969年普里戈金等创立的“耗散结构理论”；20世纪70年代哈肯等创立的“协同学理论”，艾肯等创立的“超循环理论”，塞曼等创立的“突变论”；此外，还有诸如“混沌理论”“分形理论”等都可以在某种程度上纳入“安全通论”的范畴。

与上面创立不同版本“安全通论”的所有伟人相比，本书作者可能比较渺小。但是，“位卑未敢忘忧国”，毕竟在赛博时代，在人们一刻也不能离开的网络空间中，以黑客为代表的破坏者们已经把全世界的用户搞得焦头烂额，以至于全球安全专家（红客）随时都在忙于“救火”：黑客造病毒，红客就得杀病毒；黑客破密码，红客就得忙着加密；黑客非法进入系统，红客就得研制防火墙；

黑客兵来，红客就得将挡；黑客水来，红客就得土掩。总之，网络空间安全已经被分裂成至少十余个“几乎互不搭界”的分支，网络安全专家也被逼成了“高级工匠”，以至于谁也没精力考虑网络空间安全是否存在统一的基础理论，以及如何建立这样的统一基础理论等核心问题。作者不才，甘愿冒此风险，第一个吃螃蟹，来认真探索构建“网络空间安全基础理论”或“信息安全基础理论”的课题。

因此，本书所指的“安全通论”，实际上是“信息安全通论”或“网络空间安全通论”。但是，一方面为了使书名简洁，另一方面也由于书中的许多思路和方法来自于其他学科的“安全通论”，而且许多结果也能推广到其他学科的“安全通论”，所以采用了“安全通论”作为书名。

虽然本书篇幅已经不小（数百页之多），但我们仍然觉得“安全通论”没有最终完成，因为理想的“安全通论”应该是：

（1）要么像香农的《信息论》那样，仅仅由 1 篇文章和少数几个（2 个）定理搞定。

（2）要么像冯·诺依曼的《博弈论》那样，虽然篇幅巨大（1000 多页），但核心定理只有一个（纳什均衡定理）。

那为什么在“安全通论”没有最终成熟之前，我们就决定出版此书呢？原因有四：

（1）到目前为止，本书的某些结果已经足以刷新过去的许多安全观念，有利于网络空间安全的攻防双方改进各自的思路和方法。这也是本书为什么要增加一个副标题“刷新网络空间安全观”的原因。

（2）从纯学术角度看，本书的内容已经画出了一个完整的闭环。虽然这个闭环还不是很完美（主要是不够精练），但却已能自圆其说，一个网络空间安全基础理论体系已经清晰可见。第 1 章，从理、工、哲、经、管等角度，论述了安全的本质，特别再次剖析了信息安全，为后续各章指明了方向。第 2 章，利用数

学方法，从“我”的角度，在锁定时间和对象的情况下，将主观问题客观化，抽象地描述了安全本质和逻辑结构，即安全经络图。第3章，揭示了网络空间安全的第一主角（黑客）的本质及其最佳攻击战略、战术和生态演变规律。第4章，揭示了另一主角（红客）的量化实质（安全熵的维护者），用图灵机给出了安全问题的主观和客观描述，并给出了红客是否最佳的判别标准。网络空间安全的核心是“对抗”，接下来的第5~13章，是本书的主体，在第1~4章的基础上，对网络空间中的安全对抗进行了全面而系统的量化论述，包括各种攻防的可达极限、最佳攻防策略算法、宏观态势、中观态势、对抗的演化规律，以及由红客、黑客和用户三者形成的安全生态演变规律。特别地，发现了“信息论”和“博弈论”的异常密切联系，实现了“三论”融合，还顺便给出了困扰人们数十年的所谓“多用户信息论的信息容量极限计算”的博弈论解。另外，还对维纳提出的“对话问题”首次给出了数学模型和博弈论解答。第14~16章，分别就三种特殊的安全攻防进行了单独研究，其实相应的研究方法也可以扩展到其他安全领域。

（3）单凭作者自身的能力（甚至是全球安全界的努力，因为他们根本无暇“抬头看路”，只顾“埋头拉车”，正努力成为“合格的网络建筑师”），几乎不可能将如此厚厚一本专著浓缩成一篇短文，甚至一个定理（当然，这并不意味着我们将放弃这方面的努力）。与其自己关门苦想，还不如公开所有秘密，吸引全球特殊兴趣者共同奋斗，为网络空间创建“安全通论”。毕竟，像香农、维纳或冯·诺依曼这样的英雄人物，全世界几百年才可能出几位，而且即便这些天才，也是在前人成果的基础上才最终成功的。我们甘愿做无名的铺路石，为“安全通论”的最终成熟做出应有的奉献。

（4）还有一个不用回避的原因（虽然不那么高尚），那就是本书的副产品——科普书籍《安全简史》，刚一出版就引起了轰动，热销程度完全出人意料。因此，我们便想趁机推出《安全通论》，希望某位现在还是安全外行的潜在的“香农”（如博弈论专家、经济学家、系统论专家、数学家，甚至某位中学生等）能够偶然读到此书，并最终奇迹般地完成“安全通论”。

此外，世界观对方法论的影响在本书中也表现得淋漓尽致。因此，即使你

不关心网络空间安全，本书也许仍然对你的科研工作有所启发。比如：全书其实通篇都充满了“控制论”思想，虽然并没有在定理上体现出来（因为“控制论”本身就没有定理）；第3章、第5~7章压根儿就是“信息论”的巧妙应用；第2章和第4章完全可以看成“系统论”的一部分；第7~9章显然来自“博弈论”；第10章及以后各章无处不见“耗散结构理论”“协同学理论”和“突变论”的影子。总之，本书完成后，我们才发现，“安全通论”几乎等价于“控制论”的一种具体应用！这虽然确实出乎我们的意料，但这真的是自然形成的，并非作者刻意为之，更不是想拉“控制论”的大旗作虎皮。其实在国内，现在“控制论”都快被大家遗忘了。

本书是作者“闭关”五年，潜心研究的结果，但是由于作者能力有限，书中难免有不足之处，诚心欢迎大家批评指正，真心希望“安全通论”健康成长！

作者　杨义先　钮心忻

2017年10月19日于花溪

目 录

第1章
信息安全再认识

如今，一提起信息安全保障，业界同行马上想到的便是所谓的“信息安全六性”，即真实性、保密性、完整性、可用性、不可抵赖性、可控制性，而且全球信息安全专家都正将主要精力聚焦于如何实现该“六性”。必须承认，专家们没错，而且在当前情况下，这可能还是唯一正确的选择。但是，坦率地说，这只是低层次的工程思维！实际上，如果“网络空间安全学科”永远都被这“六性”牵着鼻子走的话，那么今天的“六性”明天可能就会扩展成“七性”，再后来便是“八性”“九性”等。相应地，解决这些“性”的方法也会越来越多，越来越专，越来越散。于是，网络空间安全学科将被撕成越来越细的“碎片”，以至于最终大家都迷失方向，像无头苍蝇一样乱撞，不断消耗着全社会的人力、物力和财力，导致攻防双方共输的局面。因此，若想建立网络空间安全学科的“统一基础理论”，就必须站在更高的角度重新来认识信息安全。

早在两千多年前，老祖宗的《黄帝内经》就指出“上医治未病，中医治欲病，下医治已病”。可是，直到如今，全世界的信息安全专家都只想到“治已病”，偶尔也有几人在考虑“治欲病”，但几乎没人考虑“治未病”！本书想在“治未病”方面做一点尝试，希望对后来者有用。为了表述方便，本书交替使用“信息安全”“网络安全”或“网络空间安全”等词汇，虽然它们略有区别，但是从建立统一安全基础理论角度来看，就没必要再做细分了。