C3安全峰会
CYBER | CLOUD | COMMUNICATION

网络威胁泛滥下的新型安全观
《安全通论》与《安全简史》剖透

杨义先 教授
北京邮电大学信息安全中心主任

《安全通论》《安全简史》作者

刷新您的安全观

- 《安全通论》
  - 定位
  - 榜样
  - 目标
  - 类比
  - 新结果
- 《安全简史》
  - 定位
  - 榜样
  - 目标
  - 内容
  - 新视角

C3安全峰会
CYBER | CLOUD | COMMUNICATION

《安全通论》剧透

关于第1本《安全通论》：用数学语言写成！

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 定位：顶天！为网络空间安全学科，建立一套统一的基础理论，改变全球安全界“盲人摸象、头痛医头，足痛治足”的现状。
- 榜样：香农《信息论》，将通信领域的各个分支，统一起来；仅用区区两个定理（信源编码定理、信道编码定理），就为现代通信竖起了“指路明灯”。
- 目的：刷新业界安全观！

关于第2本书《安全简史》：用文学语言写成！

- 定位：立地！外行不觉深，内行不觉浅。内容将涵盖信息安全的各主要分支。
- 榜样：霍金的《时间简史》，布莱森的《万物简史》，格雷克的《信息简史》。它们不但出神入化，而且还能改变读者的世界观！
- 目的：信息安全知识的全民科普（包括普通用户和安全专家）。
- 两本书综合起来的梦想：为百姓明心，为专家见性；为安全写简史，为学科开通论

《安全通论》的进展

- 年底成书，明年正式出版。
- 已经在全国包括清华大学、北京理工大学、北京交通大学、电子科技大学、西南交通大学、中山大学、西安电子科技大学、西安交通大学等若干所大学，进行了以“安全通论---刷新你的安全观”为题的学术报告44场
- 欲知相关细节，请读我（杨义先）的科学网实名博客

有关《安全通论》的几个类比1

- 如果将“吉”看作安全，将“凶”看作不安全的话，那么，《易经》便是我国的第一部“安全通论”
- 其“核心定理”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！

有关《安全通论》的几个类比2

- 在医学领域，第一部安全通论，名叫《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）。
- 其“核心定理” 即是阴阳五行说：“水生木，木生火，火生土，土生金，金生水”或更形象地总结为“通则不痛，痛则不通”。
- 只不过，此时将“不生病”看作安全，将“生病”看作不安全而已。

有关《安全通论》的几个类比3

- 在军事领域，第一部安全通论，名叫《孙子兵法》，它成书于2500多年前。
- 如果将“胜”看作安全，将“败”看作不安全的话，那么，孙武“安全通论”本身就已非常精练，只有区区六千余字。
- 当然，现在 “孙武安全通论”的应用，已不仅仅限于军事领域了，甚至成为了当代商家的必读经典，因为，商场如战场嘛

有关《安全通论》的几个类比4

- 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”，简称为《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”看作不安全的话，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。

有关《安全通论》的几个类比5

- 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”看作安全的话，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，改变了人类世界观

有关《安全通论》的几个类比6

- 完全由抽象数学公式写成的“安全通论”，名叫《博弈论》，它由冯·诺依曼等科学家，于1944年最终创立。
- 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”不再有明显的界线，而是由具体的数字量化描述）。
- 冯·诺依曼“安全通论”，就主要研究具有竞争现象的数学理论和方法等。

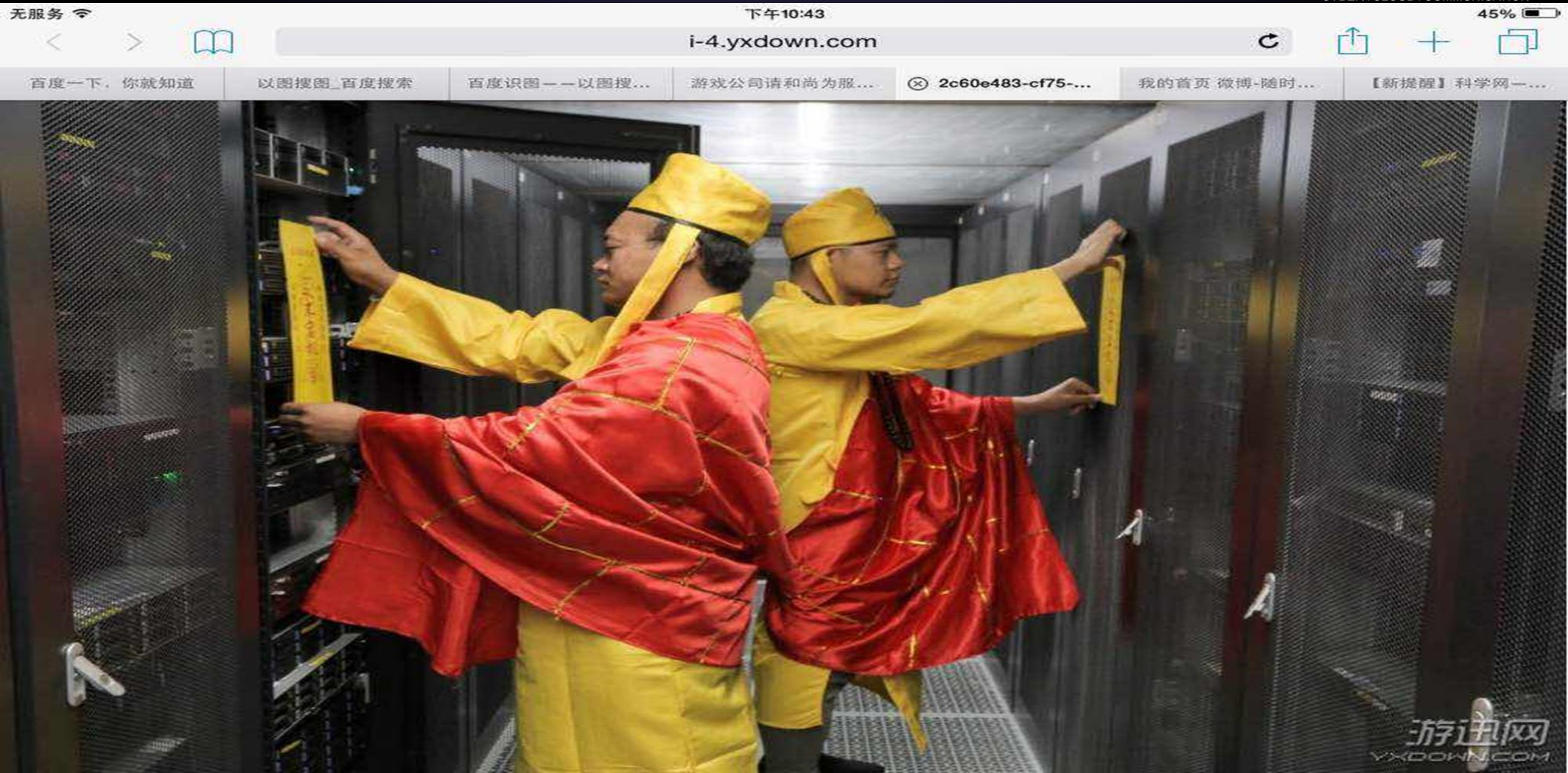
有关《安全通论》的几个类比7

- 如果将“信息比特被无误差地传输到收信端，即，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”看作不安全的话，那么，此种情形下的“安全通论”便是香农《信息论》。
- 该理论的核心只有两个定理，其一叫“信道编码定理”，其二叫“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”

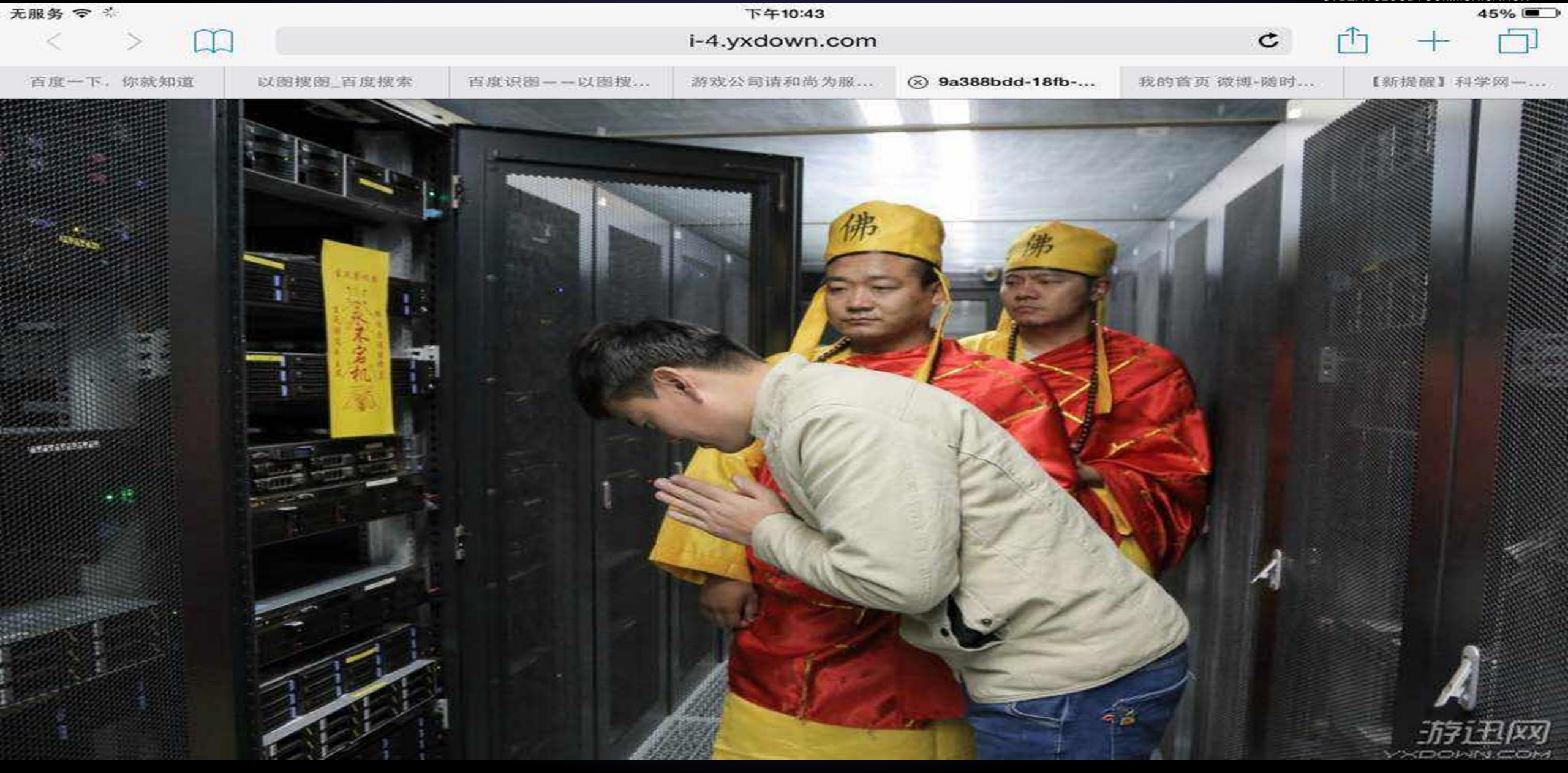
有关《安全通论》的几个类比8

- 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”看作安全的话，那么，与之相应的“安全通论”，便是如雷贯耳的《控制论》，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。”

类比9：百姓喜闻乐见的“安全通论”



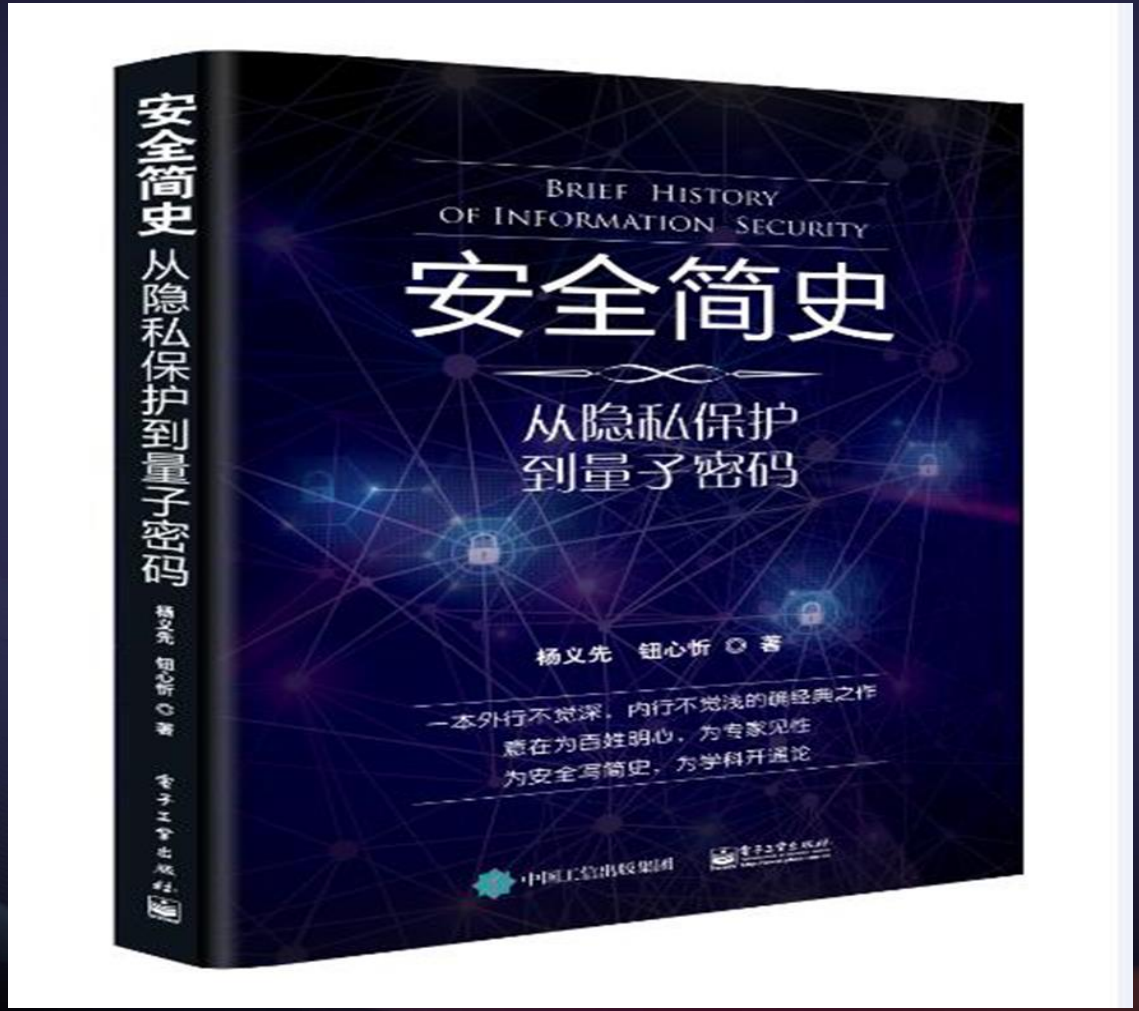
类比9：百姓喜闻乐见的“安全通论”



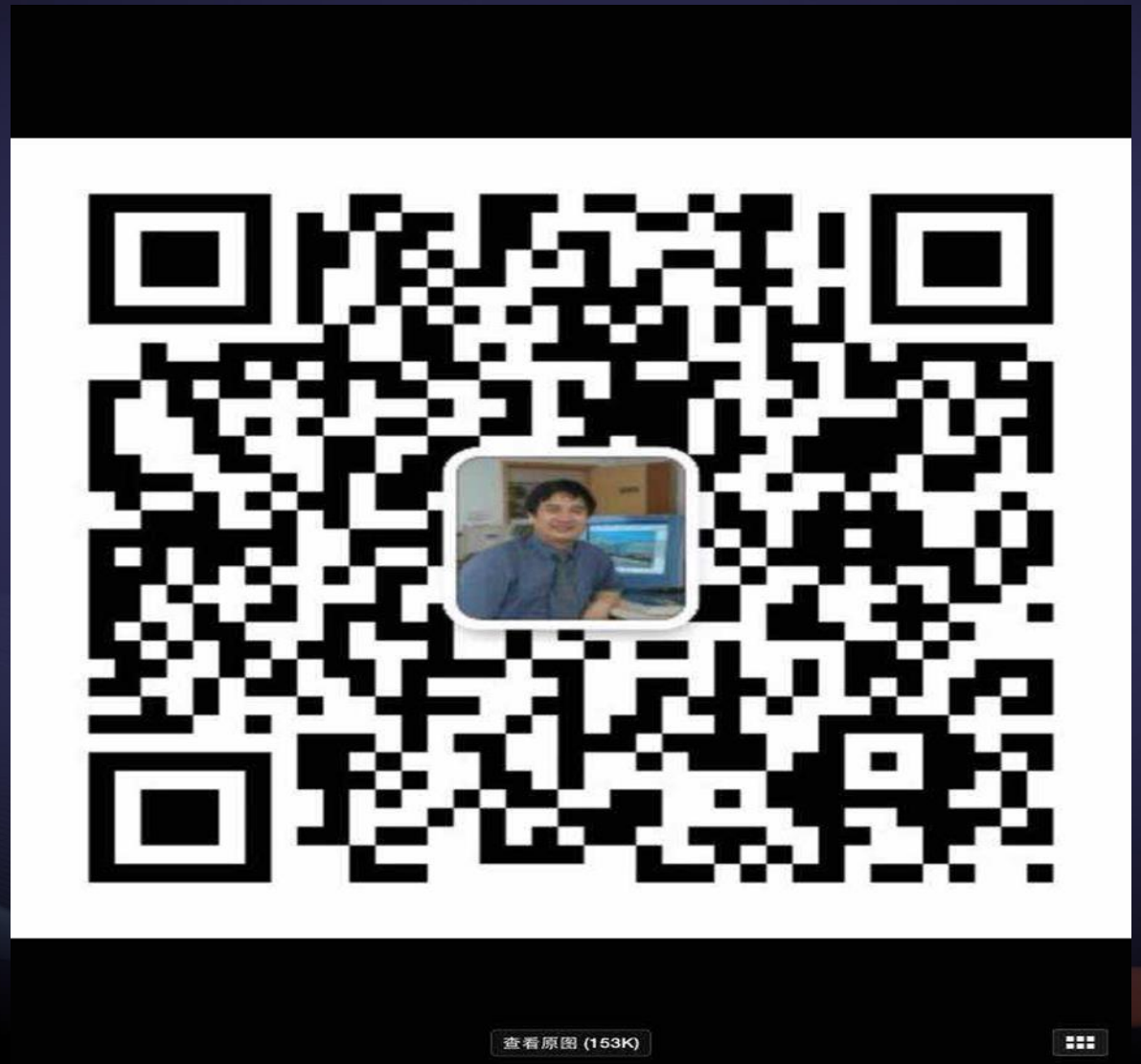
有关我的《安全通论》

- 敬请关注即将完成的网络空间《安全通论》
- 限于时间，今天只略讲《安全通论》的几个核心成果及其第1个副产品《安全简史》

《安全通论》的第一个副产品



欲及时了解《安全通论》与《安全简史》的更多剧透，
请关注专用公众号： 亦仙亦凡



《安全通论》的主要意外结论1：安全是什么？

- 安全经络图是存在的，针对任何“不安全事件”，不必直接急急忙忙地“头痛医头”，而只需要找出经络图中，与该“不安全事件”连接的最末端“穴位”，医治好该穴位就行了。
- 安全是负熵，若无“外力”干涉，任何封闭信息系统的“不安全性”将越来越大，直至最终达到“热平衡”状态，即，系统的“不安全”状态，将最终稳定成一些彼此互不相容的“不安全素事件”之并。
- 系统的安全演化过程，其实就是耗散结构的演化过程！

《安全通论》的主要意外结论1：安全是什么？

- 意外结论1的启发意义在于：
  - 一方面，过去那种“头痛医头，足痛医足”的做法必须改进为：“头痛”则要医治与“头”连接的不安全的“穴位”；
  - 另一方面，也不能盲目地“头痛医足”或“足痛医头”，而是应该科学地将所有安全威胁因素，分解成互不相容的一些“专科”，然后，再开设若干“专科医院”来集中精力“医治”相应的病症。

《安全通论》的主要意外结论2：黑客是什么？

- 黑客是离散随机变量（X）；
- 什么样的黑客（X）最厉害？答：香农信息熵最小的黑客（X），最厉害，具体地说：信息熵每小1比特的黑客，其获取黑产收入的最佳能力，将翻倍！
- 黑客的生态环境环境演化过程，等同于马尔萨斯“人口论”的演化过程！控制黑客的最好办法，是控制其生态环境！

《安全通论》的主要意外结论2：黑客是什么？

- 意外结论2的启发1：
  - 黑客数量，可以划分为五个阶段：
    - 1）开始期，也称为潜伏期，黑客数量很少，数量和密度的增长缓慢；
    - 2）加速期，随着黑客数的增加，密度也迅速增加；
    - 3）转折期，当黑客数达到饱和密度的一半（K/2）时，密度增长最快；
    - 4）减速期，当黑客数超过K/2以后，密度增长逐渐变慢；
    - 5）饱和期，黑客数量达到K值而饱和，这意味着K是稳定的。

《安全通论》的主要意外结论2：黑客是什么？

- 意外结论2的启发2：
  - 基于启发1，欲从生态学角度对付黑客，那么就该：
    - 1）消灭黑客要宜早不宜迟，即，在黑客数还没有达到最小生存量K0时就动手，效果最好；
    - 2）如果成本较大，那么，不必对黑客斩尽杀绝，只需要将其数目控制在K0之内，黑客便会自动灭亡；
    - 3）如果错过了最佳时机（即，黑客数已经超过K0），那么，黑客数将在随后的短时间内，呈现指数级的爆炸性增长，此时，不必与黑客硬拼，而应该充分运用黑客之间的竞争机制，让他们互相制约（见logistic模型）；
    - 4）控制黑客的关键是控制内亶增长率r，这又有两种思路：
      - 其一是减少出生率b；
      - 其二是增加死亡率d。

《安全通论》的主要意外结论3：红客是什么？

- 人、网、环境等组成的网络系统，可以等价于某个图灵机；系统的任何安全漏洞，都会体现在图灵机的有限映射表之中：
- 记Q(t)为由某有限个不安全因素引发的系统不安全熵，那么，当dQ(t)/dt>0时，系统的不安全性，越来越高；当 dQ(t)/dt<0时，系统变得越来越安全；当 dQ(t)/dt=0时，系统安全性保持整体稳定态势。

《安全通论》的主要意外结论3：红客是什么？

- 意外结论3的启发：
  - 红客的唯一任务是维护系统的“不安全熵”；
  - 最佳红客的标准是，他能够保护网络系统，使得各个pi=1/n都相同，此时系统的安全熵达到最大值log(n)。该结果也是很直观的，它便是安全界熟知的所谓“木桶原理”，即，如果系统没有明显的软肋，那么，其安全性最高；或者说，系统的安全性，取决于它的最薄弱处的安全强度；因为，“各个pi=1/n都相同”意味着“这个安全木桶没有短板”。

《安全通论》的主要意外结论4：攻防有极限吗？

- 无论是黑客与红客单挑对抗，还是一个黑客对付多个红客，或是多个黑客对付一个红客，或是多个黑客对付多个红客；无论是攻防分离，还是攻防一体（即，参与者同时既是黑客又是红客），……；总之，无论在什么情况下，攻防各方胜败次数都是有可达极限的！
- 具体可达极限的描述需用话多数学公式，现仅举一例：

《安全通论》的主要意外结论4：攻防有极限吗？

- 黑客与红客单挑对抗的可达极限定理：设黑客X欲攻击红客Y，那么，若黑客攻击n次，并且获得S次“真正成功”攻击，那么，一定有S≤nC。其中，C是把随机变量X作为输入，Z=(X+Y)mod2作为输出，的通信信道，称为“攻击信道”，的香农信道容量。同理，若红客经过N次防卫，获得了R次“真正成功”的守卫，那么，一定有R≤ND。其中，D是以Y为输入，Z=(X+Y)mod2为输出，的通信信道，称为“防御信道”，的香农信道容量。

《安全通论》的主要意外结论4：攻防有极限吗？

- 意外结论4的启发：
  - 随着机器人黑客的不断普及，攻防节奏将空前加快，到那时，各种极限将扮演着重要的“指路”作用；
  - 对抗场景下攻守实力判断：设C和D分别表示“攻击信道”F和“防御信道”G的“信道容量”，那么，如果C<D，那么，整体上黑客处于弱势；如果C>D，那么，整体上红客处于弱势；如果C=D，那么，红黑双方实力相当，难分伯仲。

《安全通论》的主要意外结论5：三论融合

- 信道容量与纳什均衡的融合定理：当信道固定时，若以输入和输出之间的互信息为收益函数，那么，发信方和收信方之间的标准式博弈一定存在纯战略的纳什均衡，而且，当达到纳什均衡时，他们的收益函数就刚好是收发双方之间的信道的信道容量。

《安全通论》的主要意外结论5：三论融合

- 意外结论5的启发：
  - 在信息通信领域，有一本“圣经”，叫《信息论》。在经济学领域，也有一本“圣经”，叫《博弈论》。这两本圣经，几乎同时诞生于上世纪中叶，分别由香农和冯.诺伊曼创立。但是，过去七十年来，谁也没想到，这两本“圣经”其实是同一本圣经的上下两册，它们的灵魂是完全一致的。而偶然发现这个秘密，并将这两本圣经融合起来的，便是正在努力探索中的《安全通论》！

《安全通论》的主要意外结论5：三论融合

- 意外结论5的启发（续1）：
  - 刷新通信观：甲与乙之间的通信，还可看成是黑客甲和红客乙之间的对抗，只不过是一种协同式对抗，即，攻防双方的利益是一致的！
  - 多用户信息论中“网络容量”的新思路：将N个用户之间的网络通信，看成是它们彼此间的一种对抗，其利益函数为相应的条件互信息；当该对抗达到纳什均衡时，所得的收益函数，便是多用户的“网络通信容量”
  - 过去人们的“网络通信容量”观念可能有误！

《安全通论》的主要意外结论6：维纳对话

- 维纳的辩论式问题的描述1（维纳原话）：正常的通信谈话，其主要敌手就是自然界自身的熵趋势，它所遭遇到的并非一个主动的、能够意识自己目的的敌人。而另一方面，辩论式的谈话，例如，我们在法庭上看到的法律辩论以及如此等类的东西，它所遭遇到的就是一个可怕得多的敌人，这个敌人的自觉目的就在于限制乃至破坏谈话的意义。因此，一个适用的、把语言看作博弈的理论应能区分语言的这两个变种，其一的主要目的是传送信息，另一种的主要目的是把自己的观点强加到顽固不化的反对者头人……”

《安全通论》的主要意外结论6：维纳对话

- 维纳的辩论式问题的描述2（维纳原话）：……噪声可以看作人类通信中的一个混乱因素，它是一种破坏力量，但不是有意作恶。这对科学的通信来说，是对的；对于二人之间的一般谈话来说，在很大程度上也是对的。但是，当它用在法庭上时，就完全不对了……

《安全通论》的主要意外结论6：维纳对话

- 维纳提出的挑战：协作式对话的主要破坏力量是噪声，《信息论》已经对它有完美的研究了；但是，协作式对话的成果，完全不适合于法庭上的非协作式对话！如何解决维纳的这个辩论式问题？
- 《安全通论》发现的结论：针对如下几种情况，维纳辩论式对话的信息传递可达极限都是存在的，而且就是某种博弈（我们已构造出了相应的博弈模型）在纳什均衡条件条件下的收益函数。

《安全通论》的主要意外结论6：维纳对话

- 已经被解决的辩论式对话情况：
  - 情况1：“1对1对话”，例如，单边谈判；
  - 情况2：“1对多的辩论式对话”，例如，诸葛亮舌战群儒；
  - 情况3：两派之间的辩论式对话，例如，鹰派与鸽派之间的辩论；
  - 情况4：多对多的辩论式对话，例如，头脑风暴研讨会。
- 由于涉及到过多的数学公式，具体的博弈型极限就不在此介绍了

《安全通论》的主要意外结论6：维纳对话

- 意外结论6的启发：虽然维纳提出辩论式对话问题时（约1948年），博弈论已经诞生（约1945年），但是，直到很久以后（约20年后），解决维纳问题的关键(Glicksberg定理)才被发现，但是，却没有人发现该定理与维纳问题之间的联系，直到《安全通论》偶然揭示了这种关联。因此，对话也可看成某种对抗，这也许从另一个角度，再一次揭示了“三论融合”的本源！

《安全通论》的主要意外结论 7 ：宏观看安全

- 当黑客与红客之间的对抗，达到充分激烈的程度后，一定存在“一只看不见的手”，它仅仅通过调节一个指标(“价格”)，就能够抚平对抗各方，使得攻防各方“休战”，或者说使得系统的安全状态达到动态平衡。（《安全通论》其实已经给出了这只“手”和“价格”的精确量化描述，但是，由于涉及到过多的数学公式，此处略去）

《安全通论》的主要意外结论 7 ：宏观看安全

- 意外结论7的启发：
  - 过去，人们一直咬定：安全对抗就是“水涨船高”或“鱼死网破” 等。但是，结论7表明，其实安全对抗应该更像“潮汐” ：来潮时，惊天动地；退潮后，风平浪静。或者说，安全对抗像“间隙式喷泉” ：喷时轰轰烈烈，歇时安安静静。也可以说安全对抗像“拳击摆台赛” ：轮中打斗，你死我活；轮间休息，却和平相处。总之，无论用什么现象来形容网络空间安全对抗，关键是要明白：有一只“看不见的手”能够安抚各方，最终达到共赢。因此，红客方应该调整自己的战略，使得：和平期尽可能长一些，并且为下一轮的对抗做足准备。

《安全通论》的主要意外结论8：中观看安全

- 黑客与红客之间的对抗过程，其实是一种耗散过程，在非平衡相变临界点，耗散参量会出现某种奇异特性，即，可能出现某种跃变或发散。当控制参量ε→0时，红客和黑客将导致网络的安全状态稳定在更高一层的安全状态，或跌落到更低一层的安全状态，甚至可能造成网络的彻底崩溃。（《安全通论》本来给出了具体耗散结构的微分方程组量化描述，但数学公式太多，此处略去）

《安全通论》的主要意外结论8：中观看安全

- 意外结论8的启发：网络空间安全的发展过程，是一个典型的演化过程，推动该演化的力量主要来自三方面：网络系统的自然退化、黑客的攻击、红客的安全保障措施等。演化的要点，可以概括为如下八个方面：
  - 1）网络系统及其子系统的开放性（即，攻防各方的介入）是形成新的安全状态（不安全熵稳定在新的量值）的前提和基本条件
  - 2）自然退化和攻防对抗的非平衡，是不安全熵达到新稳态的源泉
  - 3）远离平衡态是形成新的安全结构（新的不安全熵量值）的最有利条件

《安全通论》的主要意外结论8：中观看安全

- 4）“网络系统内部，攻防各方之间，存在非线性的相互作用”是新的安全结构形成并得以保持的内在根据。
- 5）“涨落”是安全结构形成的“种子”和动力学因素
- 6）“涨落达到或超过一定的阈值”是使系统形成新的安全结构或使系统原有安全结构遭到破坏的关键
- 7）可以用网络系统的不安全熵的阈值来表示“度”
- 8）网络系统通过“自组织”形成新的稳定安全结构。

《安全通论》的其它主要意外结论：

- 红客与黑客间接对抗的演化规律
- 网络安全生态学
  - “黑客+用户”生态学
  - “黑客+红客”生态学
  - “用户+红客”生态学
  - “黑客+用户+红客”生态学

《安全通论》的其它主要意外结论(续）：

- 计算机病毒的行为分析：
- 谣言的传播规律
  - 一个机构内的谣言动力学
  - 多个机构内的谣言动力学
- 民意（选票）的演化规律

C3安全峰会
CYBER | CLOUD | COMMUNICATION

《安全简史》剧透

《安全通论》与《安全简史》的关系

- 《安全通论》是用数学语言写成的《安全简史》；
- 《安全简史》是用文学语言写成的《安全通论》！
- 如果您不想陷入数学公式中，那么，建议您只阅读《安全简史》
- 如果您想吃透《安全通论》，那么，也建议您先读《安全简史》
- 下面用“诗和远方”来简介《安全简史》，当然，您若想更爽，建议您直接阅读《安全简史》

《安全简史》这样讲“大数据隐私保护”

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 小时候，还只有电脑，
- 隐私只是小小的疑虑，
- 因为，秘密在屋里头，威胁在屋外头；
- 长大后，出现了网络，
- 隐私变成萌萌的小虎，
- 因为，隐私在网这头，黑客在网那头；
- 现如今，有了大数据，
- 隐私已是倒悬的利剑，
- 因为，秘密在云里头，我也在云里头；
- 看未来，万物互联了，
- 隐私早已被牢牢控制，
- 因为，秘密虽在屋外头，我却安然藏屋里头。。

《安全简史》这样讲“区块链”

- 寻寻觅觅，深深浅浅，区区块块链链。
- 乍暖还寒难辨，真币假钱。
- 饭票钞票白条，怎敌他换代改朝！
- 雁过也，正伤心，财富一夜丢尽。
- 满地黄金堆积，支票损，狂喜竟然哭泣！
- 守着齿贝，独自怎生得意！
- 真钱更像细雨，到黄昏，点点滴滴。
- 求上帝，早促成电子货币！

《安全简史》这样讲“计算机病毒”

悄悄的我走了，
正如我悄悄的来；
我悄悄一动手，
就划走你的钱财。
你电脑的秘密，
是夕阳中的新娘；
骑上无形的木马，
疯狂奔向我心房。
软件上的蠕虫，
悠悠的在网上招摇；
在互联的世界里，
你甘心不如菜鸟！
那云端下的一潭，
不是清泉，是病毒宏；
揉碎在代码间，
正为你沉淀着噩梦。
寻梦？像一只僵尸，
向青草更青处漫溯；
满载一船喽啰，
在拒服攻击里放歌。
但你不能放歌，
悄悄躲着泪流成河；
夏虫也为你沉默，
沉默因今晚的事故！
轻轻的我走了，
正如我轻轻的来；

《安全简史》这样讲“社会工程学”

安全几时有？
把酒问青天。
不知“社会工程学”者，
吃亏定在眼前。
我欲细论详情，
又恐误用双刃剑，
反诱出人渣行骗。
揭秘弄清影，
正义留人间。

减私欲，少贪婪，补缺陷。
不应有恨，
凡事警惕长心眼。
人有好坏善恶，
月有阴晴圆缺，
此事古难全。
但愿人长久，
网上共婵娟。

《安全简史》这样讲“黑客”

- 大江东去，浪淘尽，千古黑客人物。
- 故垒西边，人道是，三国侠客剑客。
- 乱石穿空，惊涛拍岸，卷起千堆雪。
- 江山如画，一时多少豪杰。
- 遥想荆轲当年，小瞧孤家了，雄姿英发。
- 羽扇纶巾，谈笑间，刺客灰飞烟灭。
- 悟空神游，多情应笑我，早生毫发。
- 人生如梦，极客还酹（ lèi ）江月。

《安全简史》这样讲“密码”

- 老夫聊发少年狂。
- 巧加密，赛铜墙。
- 秘钥不知，穷举也白忙。
- 倾巢进攻一夫守，轻戏虎，笑看狼。
- 酒酣胸胆尚开张。
- 妙破密，又何妨。
- 持矛云中，铜墙变朽框。
- 手挽雕弓如满月，西北望，盾难挡。

《安全简史》这样讲“认证”

实连身世两茫茫， 不思量，自难忘。 千里网民， 确认身份无话讲。 纵使相逢却不识， 尘瞒面，应无双。	夜来幽梦忽还乡， 数据库，小视窗。 相顾无言， 认证信息云里藏。 料得黑客篡改处， 无月夜，也曝光。

《安全简史》这样讲“信息隐藏”

- 问世间，“藏”为何物？直教真假相虚。
- 天南地北飞黑客，老猫难斗悍鼠。
- 藏也乐，找也苦，就中更有痴儿女。
- 君应有语，渺万里层云，千山暮雪，真像向谁去？
- 横汾路，寂寞当年幻术。荒烟依旧平楚。
- 替换变换何嗟及，黑客暗啼风雨。
- 天也妒，未信与，图像视频俱无物。
- 千秋万古，为留待骚人，狂歌痛饮，欢迎读此书。

《安全简史》这样讲“防火墙”

- 少年不识墙滋味，
- 爱上层楼，爱上层楼，
- 为吐心声说墙丑。

- 而今识得墙滋味，
- 欲说还羞，欲说还羞，
- 却道天凉墙也旧。

《安全简史》这样讲“入侵检测”

- 我问佛：为何要给网络黑客披荆斩棘的宝剑？
- 佛曰：那只是昙花的一现，用来蒙蔽世俗的眼
- 没有什么剑可以抵过一颗纯净仁爱的心
- 我把它赐给每一个网民，
- 可有人让它蒙上了灰。
- 我问佛：网间为何有那么多混蛋？
- 佛曰：网络是个野蛮世界，野蛮既混蛋，
- 没有混蛋，给你再多安全也不会觉得稀罕。

续1

- 我问佛：如何让黑客的心不再充满贪婪？
- 佛曰：每一颗心生来就是贪婪而残缺的，
- 多数带着这种残缺度过一生
- 只因与能使它圆满的另一半相遇时
- 不是疏忽错过，就是已失去了拥有它的资格。
- 我问佛：如果遇到了可信赖的人，却又怕不能把握该怎么办？
- 佛曰：留人间多少爱，迎赛博千重变
- 和同道人，做随心事
- 别问是劫是缘。

续2

- 我问佛：如何才能如你般睿智？
- 佛曰：佛是过来人，人是未来佛
- 我也曾如你般天真
- 佛门中说一个人悟道有三阶段：勘破、放下、自在

《安全简史》这样讲“灾备”

- 是否 灾备已被遗忘
- 不然为何杳无音信
- 天各一方
- 是否 你已把我珍藏
- 不然为何 微笑总在装饰我的梦
- 留下绮丽的幻想
- 是否 我们有缘
- 总是遇难成祥
- 有惊无险
- 是否 我们无恙
- 岁月留给我的将是

《安全简史》这样讲“安全熵”

让我怎样感谢你，熵 当我知道你的时候 我原想收获一缕春风 你却给了我整个春天	让我怎样感谢你，信息熵 当我读懂你的时候 我原想撷取一枚红叶 你却给了我整个枫林
让我怎样感谢你，热熵 当我了解你的时候 我原想捧起一簇浪花 你却给了我整个海洋	让我怎样感谢你，安全熵 当我使用你的时候 我原想亲吻一朵雪花 你却给了我银色的世界

《安全简史》这样讲“安全管理学”

我叮咛你的
你不能遗忘
你告诉我的
我也全都珍藏
对于我们来说
安全管理是治乱法宝
——永远闪闪发光
威胁的暴发总是很短
灾后的纠错却是很长
在那网络空间
激荡起多少心动的诗行
如果你要想念我
就望一望书上那
优美的文字
有我渴望你的
目——光

《安全简史》这样讲“安全心理学”

- 也许，终究会有那一天
  - 安全心理学将辉煌
- 也许，终究会有那一天
  - 网络似铁壁赛铜墙
  - 也许，只能是这样
  - 黑客攻却不达顶峰
  - 也许，只能是这样
  - 虽惊险却掀不起浪
- 也许，我们将给予你的
    - 会是一颗
  - 饱经沧桑的心

《安全简史》这样讲“安全经济学”

给予你的
当然要期望回报
安全付出
就是为了有一天索取
并且，安全效益越高越好
如果安全是湖水

投资便是堤岸环绕
如果安全是山岭
价值便是装点安全姿容的青草
人，不一定能使自己伟大
但一定可以
使自己崇高

第16回：正本需清源，赛博话当年

- 借用歌德的情诗《我爱你 与你无关》来讲述《赛博学》中“控制”与“反馈”的爱情故事，并以此归纳并结束本回：

《安全简史》这样为赛博正本清源

它爱你，与你无关
即使控制对反馈的思念
也只属于它自己
不会带出系统
因为它只能存于循环链

它爱你，与你无关
就算它此刻站在天才身边
依然背着你的双眼
不想让你看见
就让它只隐藏在风后面

它爱你，与你无关
此乃为啥你记不起它的笑脸
却到处能感觉
它的陪伴
无论是什么时间和地点

它爱你，与你无关
《控制论》不够分明
所以我选择平反
赛博学必须正本带清源

它爱你，与你无关
面对新型方法论
你不能躲开
顺应潮流才能领先

它爱你，与你无关
真的啊
它占据时代核心
带给人类幸福
但你必须
更新世界观

《安全简史》这样讲“信息与安全”

- 第一最好不相恋，信息根本看不见。
- 第二最好不相思，比特与熵很难知。
- 第三最好不相欠，系统首要保安全。
- 第四最好不相忆，对付失控需妙计。
- 第五最好不相弃，蚁穴虽小能溃堤。

续1

- 第六最好不相亏，内外兼顾显神威。
- 第七最好不相误，泄密信息价值负。
- 第八最好不相堵，畅通反馈有帮助。
- 第九最好不相依，一劳哪能得永逸。
- 第十最好不相攻，和谐相处好轻松。
- 但曾相见便相知，安全保障最及时；
- 信息若能充分用，免教得失作相思。

《安全简史》这样讲“系统与安全”

假如你不够快乐 也不要把眉头深锁 系统论本来难懂 安全系统论就更加苦涩 打开尘封的门窗	让整体观和动态观遍及各角落 走向生命的原野 让风儿熨平前额 博大可以稀释忧愁 学科能够更加出色

《安全简史》这样讲“量子密码”

你可暂时欺瞒别人 却无法欺瞒自己 当你咬定量子密码绝对安全 失败就不再是一个谜 向上的路 总是坎坷又崎岖	要永远保持最初的浪漫 真是不容易 有人悲哀 有人欣喜 你不必跨越一座座高山 但必须跨越一个真实的自己

《安全简史》这样结束

不去想本书是否能成功
既然选择了远方
便只顾风雨兼程

不去想它能否给咱功名
既然钟情于玫瑰
就勇敢地吐露真诚

不去想出版后会不会袭来寒风冷雨
既然目标是地平线
留给世界的只能是背影

我们不去想未来是平坦或泥泞
只要热爱生命
一切，都在意料之中

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You