文章编号: 2096-1618(2017)04-0347-06
稿件来源:科学网
网　　址:http://blog.sciencenet.cn/blog-453322-1042638.html
发表时间:2017-03-30

安全通论(19)

——网络安全经济学(2):安全熵论

杨义先,　钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:借助充分竞争的市场经济类比,本文从中观角度,描述了网络空间安全对抗的运动规律和演化过程。结果发现,若只考察"行为举止",那么,市场经济与网络安全简直就是活脱脱的一对双胞胎:熟知的许多市场经济现象,在网络对抗中几乎都能找到相应的影子,反之亦然。过去,安全专家都只关注网络对抗的"局部微观画像"(比如,加密、病毒、木马、入侵等核心安全技术),这在节奏相对较慢的"人与人对抗"环境中,确实可以说是唯一重要的事情。但是,随着机器黑客的即将登场,"机器对机器攻防"的节奏,将以指数级速度增加,因此,从中观和宏观角度去了解网络战场,就显得十分重要了;否则,若"只见树木,不见森林",就一定会失去网络对抗的主动权。类似的情况,在半个多世纪前就已出现过:若无数据通信,就不需要《信息论》,因为,早期的电报和电话等,根本就没有带宽和速度的需求压力。幸好,结合文献[18]的结果,至此,网络安全对抗的"中观画像"和"宏观画像"都已绘制出来了。

doi:10.16836/j.cnki.jcuit.2017.04.001

0　引言

网络安全对抗很实!因为,当你中招后,你的真金白银可能瞬间化为乌有,你的电脑可能立马死机,你的汽车可能失控,甚至你的心脏起搏器也可能乱跳…;总之,你遭受打击所感觉到的真实程度,一点也不亚于当头棒喝。

网络安全对抗很虚!因为,在网络这个典型的虚拟空间中,安全对抗不但没有硝烟,甚至根本看不到敌人在哪;也很难知道你是被谁击中的,以及是如何被击中的;你对"邻居"的安全处境更是一无所知,甚至不知道他到底是敌还是友等等。

那么,我们对抽象的网络战争,就真的只能"两眼一抹黑"吗?!

当然不是,其实,顶级红客(安全专家),可通过精准分析,描述出网络对抗的局部微观战况,这便是常规网络安全技术所实现的主要目标;而在文献[18]中,我们借用经济学的一般均衡理论,给出了网络对抗的宏观画像,即,存在一只看不见的手,它能抚平对抗的各方,让大家都满意地休战,因为大家都已最大限度地达到了自己的预期目标,若再不休战,自己将受损;本文将借助耗散结构理论,给出网络对抗的中观战况画像。

从中观角度看,网络空间安全的最佳类比,也许仍然是充分竞争的市场经济:一个网络(子)系统,可类比于一种商品;相互对抗的红客和黑客,可类比于市场中的供应方和需求方;攻防双方的各种手段,可类比于市场中抬价与压价的各种花招;网络(子)系统的不安全熵,可类比于商品的价格。经济中有一只看不见的手,能通过调节商品价格,使供需各方都很满意,从而市场趋于稳定;类似地,网络(子)系统中,也有一只看不见的手,能使相应的不安全熵,稳定在某个量值,从而抚平攻防各方,使网络战场趋于平静。同样的商品,在不同的地域(时间),可能稳定于不同的价格;类似地,同样的网络子系统,处于不同的环境(时间段)时,也可能稳定于不同的不安全熵状态。一种商品(比如,汽油)的价格波动,可能引起另一种商品(比如,汽车)的价格波动;类似地,一个子系统的不安全熵的变化,可能引起另一个子系统的不安全熵的变化。供货量(需求量)的增加,将会打破平衡,引起商品价格的下降(上升);类似地,红客(黑客)水平的提高,将会打破平衡,引起不安全熵的下降(上升)……。总之,充分竞争的市场经济,与网络空间安全对抗,几乎遵从同样的变化规律。理解了相对直观的市场经济状态,就隐约看见了抽象的网络空间安全对抗。

当然,经济学与网络安全的类比,绝不是机械的照搬,甚至,从"一般均衡理论"这个研究经济学的利器角度看,供求双方价格最优化的边界条件,就完全不适用于红客与黑客的对抗,从而导致价格理论几乎无法应用于网络安全研究。

不过幸好,耗散结构理论可同时应用于研究充分竞争的市场经济和网络空间安全对抗。本文借鉴文献[20]的思路和手法,绘出了网络空间安全对抗的"中

观画像”,并且,再一次表明:市场经济与网络安全实在是“长得太像了”,若只看画像的话,它们简直就是一对双胞胎。

1 网络空间对抗的耗散行为

早在文献[1]中,我们就指出:网络安全是负熵,或不安全是熵;而且,还遵从热力学第二定律,即,若无额外的安全加固措施,那么,系统(子系统)的不安全熵就会自动增大。在文献[9]中,我们更进一步地指出:红客维护网络安全的唯一目标,就是控制不安全熵的增大。当然,在[1]和[9]中,我们其实都暗含了假设:相应的网络系统是“封闭系统”,即,与外界不进行物质和信息的交流,与外界无明显联系,环境仅仅为系统提供了一个边界,不管外部环境有什么变化,封闭系统仍表现为其内部稳定的均衡特性。

而本文考虑的网络(子)系统不再封闭,而是“开放系统”,即,在系统边界上与环境有信息、物质和能量的交流。在环境发生变化时,网络(子)系统通过与环境的交互,以及本身的调节作用,达到某一稳定状态,从而实现自调整或自适应。

一个远离平衡态的开放网络(子)系统(以下均简称为“系统”),通过红客和黑客的攻防对抗,不断与外界交换物质、能量和信息,从周围环境中引入负熵(红客的功劳)和正熵(黑客的后果),来改变不安全熵的取值。由于内部各子系统之间的非线性相互作用,通过涨落,便可能使各个子系统合作行动,从而形成某种时间、空间和功能稳定的耗散结构,使不安全熵稳定在一定的量值附近。更具体地说,系统的不安全熵的改变 dS 由三部分组成:其一,是系统内部本身的不可逆过程(比如,非人为的设备老化、自然故障等)所引起的不安全熵增 d_iS;其二,是黑客攻击系统所造成的不安全熵增 d_eS;其三,是红客保障系统安全所引起的不安全熵减 d_gS。并且,这三股熵流合成后就有 $dS=d_iS+d_eS+d_gS$,其中前两项 d_iS(自然熵流)和 d_eS(黑客熵流)均为非负,而第三项 d_gS(红客熵流)为负值。如果红客的安全保障能力足够强,使得 $|d_gS|>d_iS+d_eS$,那么,dS 就为负,即,系统因为红客的负熵流(d_gS),抵消了黑客和自然退化所引起的熵增,从而,系统整体的不安全熵就会减少,安全度就不断提高,最后稳定在一种较平衡的不安全熵总值更低的新状态,即,形成了耗散结构。

系统偏离平衡态的程度,可由三股流(自然熵流、红客熵流、黑客熵流)的“力量”强弱来表征。系统处于平衡状态时,三股“熵流”与产生熵流的“力量”综合皆为零;当系统处于非平衡态的线性区(称为“近平衡区”)时,如果“力量”和“熵流”为非线性关系,即“力量”较强时,系统就会远离平衡状态,处于非平衡、非线性区。非平衡过程的“不安全熵流”,不仅取决于该过程的推动“力量”,而且,还受到其它非平衡过程的影响;换句话说,不同的非平衡过程之间,存在着某种耦合。用 F 表示系统的不安全熵流,$\{x_i\}$ 表示系统中影响不安全熵流的各种“力量”,它们其实就是影响系统安全的各种因素(比如,红客的安全保障能力、黑客的攻击能力和系统的自然退化力等,当然,这些“能力”其实也可以分为多个组成部分),则 F 是 $\{x_i\}$ 的函数,即,$F=F(x_1,x_2,\cdots)=F(\{x_i\})$。以平衡状态作为参考,将函数 F 展开成泰勒级数,便有

$$F(\{x_i\})=F(\{x_i,0\})+\sum_i[dF/dx_i]_o x_i+(1/2)\{\sum_{m,n}[d^2F/(dx_m dx_n)]_o\}x_m x_n+\cdots\cdots$$

系统远离平衡状态时,该泰勒级数中将保留非线性的高次项,影响系统安全的“力量”与“不安全熵流”是非线性关系。如果红客的安全保障能力足够强,则不安全熵就会不断减少,最后稳定在一种不安全熵较小的较平衡状态,由此可知,系统远离平衡时,不仅影响系统不安全熵流的力量较强,而且,由于非线性的耦合作用,影响系统安全的各种因素,都会彼此作用,最终产生协同,形成新的平衡状态。而且,在该稳定状态系统中,众多子系统的不安全熵流相互弥补和抵消,保证了整体系统的宏观状态显现稳定性,而这种稳定性需要不断耗散物质、能量或信息来维持。

如果你觉得上述描绘太过定性,下面就来做些定量的描述。其实这些描述不仅仅限于网络安全对抗,而且,对经济状态[20]甚至一般的耗散系统都有效。

设非平衡系统中,各子系统的不安全熵流分别是 $q_1,q_2,\cdots,q_k,\cdots\cdots$,它们都是时间 t 和各自面临的不安全因素 $r_{k1},r_{k2},\cdots$ 的函数。所以,整体系统可以描述为状态矢量 $q=(q_1,q_2,\cdots,q_k,\cdots)=\{q_k:k=1,2,\cdots\}=\{q_k(r_{ki},t):k,i=1,2,\cdots\}$。

由于存在着不安全熵流的耗散,对于稳定的非平衡定态网络系统而言,在其内部某一确定的子系统和某一确定的时间内,红客输入的熵减,必须等于在同一子系统和同一时间内,由黑客和自然退化原因耗散掉的熵增。如果红客、黑客和自然等三方力量输入的不安全熵出现了“堆积”(无论是正堆积,还是负堆积),那么,当前的定态便会失稳。只有在无“堆积”的情况下,系统才能维持其定态的稳定,这便是网络空间安全对抗中的“不安全熵守恒定律”。

设在定态条件下,第 i 个子系统的不安全熵为 M_c(因为,对任何系统来说,安全只是相对的,不安全才是绝对的,所以,M_c 不会为 0,而是正值),外界在单位时间内向该子系统输入的不安全熵为 M_a(它其实是黑客的增熵,减去红客的负熵),与此同时,该子系统向外界耗散出的不安全熵为 M_b,则该子系统定态稳定的

条件就是:$M_a=M_b$或者,等价地 $M_a/M_c=M_b/M_c$;此处 $M_D=M_a/M_c$称为耗散参量,$M_T=M_b/M_c$称为输入参量,它们都是无量纲的参量。于是,在未达非平衡相变临界点时,系统是定态稳定的必要条件是 $M_T=M_D$。

M_D 当然是熵流 q 的函数,比如,表示为非线性泛函数 $M_D=f(q_1,q_2,\cdots,q_n)$,它与网络系统中的各种不安全因素(无论来自黑客、红客还是自然力量)都有关。假定,在整个非平衡过程中,M_T的变化是连续平滑的。由于耗散能力有限,当系统趋于平衡相变临界点时,便有 $M_T\neq M_D$,这时原有的耗散模式就不再守恒,因此,就在系统内形成"堆积",使原定态失稳。这种"堆积"迫使处于非稳的系统寻找新的耗散途径,以便重新稳定下来。这时相干性增强,各种涨落更加活跃,推动着系统进入一个新的耗散状态,使 $M_D=M_T$重新得以满足。新的耗散模式维持了系统新的定态稳定,即在非平衡定态背景下,系统由原来的状态,跃迁到一种新的状态上,从而完成了一次非平衡相变:不安全熵稳定在新的水平上。由此可见,当黑客、红客和自然退化力量的平衡被打破后,网络系统(或子系统)又会在新的情况下,达到新的平衡。

借用耗散结构理论的方法,不安全熵流矢量 $q=(q_1,q_2,\cdots,q_n)$的一般运动规律,可以用广义郎兹万方程描述为:

$$dq_i/dt=K_i(q)+F_i(t)\qquad(i=1,2,\cdots,n)$$

其中,$K_i(q)=K_i(q_1,q_2,\cdots,q_n)$是非线性函数,代表各种影响安全的力量导致的不安全熵流,$F_i(t)$是各种微扰引起的随机和涨落力。如果微扰足够小,即,$F_i(t)$可以省略不计,那么,上面的广义郎兹万方程,就可简化为:

$$dq_i/dt=\sum_{k=1}{}^{n}a_{ik}q_k+f_i(q)\qquad(i=1,2,\cdots,n)$$

此式中$\{f_i(q)\}$为 q 的一组非线性函数,由于此时系统的定态点是稳定的,其线性项系数矩阵的本征值具有负实部,即矩阵$[a_{ik}]$是负定的,即,总可以通过线性变换(或选取适当的新坐标),使得该矩阵对角化,这时便有方程组:

$$\begin{aligned}dq_1/dt&=-R_1q_1+g_1(q_1,q_2,\cdots,q_n)\\dq_2/dt&=-R_2q_2+g_2(q_1,q_2,\cdots,q_n)\\&\cdots\cdots\\dq_i/dt&=-R_iq_i+g_i(q_1,q_2,\cdots,q_n)\\&\cdots\cdots\\dq_n/dt&=-R_nq_n+g_n(q_1,q_2,\cdots,q_n)\end{aligned}$$

这里$\{R_i\}$为阻尼系数,它们都是正数,$\{g_i(q)\}$为 q 的另一组非线性函数。至此,网络中各子系统(网络)的不安全熵流变化是彼此关联的,网络整体上仍然显得杂乱无章;如果考虑到随机力 $F_i(t)$的作用,网络的安全状态(即,不安全熵),只能作无规律的起伏。但是,对一般的非平衡相变系统,其变量 q 中包含着序参量 u 和耗散参量 M_D。当红客和黑客等外界力量,使系统趋于临界点时,序参量的衰减阻尼系数将变为零,而其它参量的衰减阻尼系数虽不为零,但却有限;于是,u 就会出现"临界慢化",整个系统的演化,便将由 u 所主宰,其余变量(包括耗散参量 M_D)都将受到 u 的支配。

不失一般性,可记 $u=q_1$ 和 $M_D=q_a$,此处 $2\leqslant a\leqslant n$。于是,前面的方程组可重写为:

$$\begin{aligned}du/dt&=-R_1u+g_1(u,q_2,\cdots,M_D,\cdots,q_n)\\dq_2/dt&=-R_2q_2+g_2(u,q_2,\cdots,M_D,\cdots,q_n)\\&\cdots\cdots\\dM_D/dt&=-R_aM_D+g_a(u,q_2,\cdots,M_D,\cdots,q_n)\\&\cdots\cdots\\dq_n/dt&=-R_nq_n+g_n(u,q_2,\cdots,M_D,\cdots,q_n)\end{aligned}$$

当网络系统趋于不安全熵的非平衡相变临界点时,根据协同学原理,将出现极限 $R_1\to0$,并且,其它 $R_i>0(n\geqslant i\geqslant2)$且有限,即,此时除 u 是软模变量之外,其它量(包括 M_D)都是硬模变量。根据支配原理,若令其它参量都不随时间而变化,那么,略去第 1 个方程后,上述的方程组又可再简化为:

$$\begin{aligned}-R_2q_2+g_2(u,q_2,\cdots,M_D,\cdots,q_n)&=0\\&\cdots\cdots\\-R_aM_D+g_a(u,q_2,\cdots,M_D,\cdots,q_n)&=0\\&\cdots\cdots\\-R_nq_n+g_n(u,q_2,\cdots,M_D,\cdots,q_n)&=0\end{aligned}$$

求解这$(n-1)$个联立方程,可得 $q_2=h_2(u),\cdots,M_D=h_a(u),\cdots,q_n=h_n(u)$,即,硬模变量 $q_2,\cdots,M_D,\cdots,q_i,\cdots,q_n$都被序参量 u 支配。将这些解,代入序参量 u 的变化方程(即 du/dt 的那个方程),便有:

$$du/dt=-R_1u+g_1(u,q_2,\cdots,M_D,\cdots,q_n)=-R_1u+g_1[u,h_2(u),\cdots,h_a(u),\cdots,h_n(u)]=-R_1u+G(u)$$

注意到 M_D 的非线性泛函数表达式 $M_D=f(q_1,q_2,\cdots,q_n)$,于是,将上面的各 q_i 表达式代入此式,便知,在网络安全对抗系统非平衡相变临界点的无限小邻域内,成立 $M_D=f[u,h_2(u),\cdots,h_a(u),\cdots,h_n(u)]=E(u)$,此式中,$E(u)$是序参量 u 的某种非线性函数。当外界红客和黑客的控制力量相抵消时,序参量 u 与约化临界距离之间便有如下依赖关系:$u=\varepsilon^{\beta}(\varepsilon\to0,E\to0)$。其中,$\beta$ 为序度临界指数,其值与网络安全系统的临界类型有关;$\varepsilon=(R-R_c)/R$,此处的 R 和 R_c 的含义是:在一般情况下,非平衡相变的过程,可由系统控制参量(红客、黑客和自然退化的对抗)R 来控制,网络(子)系统趋于临界点的程度,可用临界距离$(R-R_c)$来表征,R_c 是控制参量 R 的临界值。

由于各类非平衡相变临界点,都有一个共同特征:在临界点,序参量由 0 开始,连续生成;或由非零开始,连续消失而生成。即,当系统趋于临界点时,有:$u\to0$,

($\varepsilon\to 0$, $E\to 0$)。可见,在非平衡相变临界点的无限小区域内,u 的量值很小,因此,公式 $M_D=f[u,h_2(u),\cdots,h_a(u),\cdots,h_n(u)]=E(u)$ 的右端,可按自变量 u,在临界点进行幂级数展开。设该幂展式中,低阶不为零项的幂指数为 ψ,则当系统趋于临界点($u\to 0$)时,函数 $E(u)$ 便可渐近地表示为:$E(u)\to Au^{\psi}$,这里 A 为原展式中,最低阶不为零项的系数,故在非平衡临界点的无限小邻域内,M_D 正比于 u^{ψ}。而 ψ 与系统的具体耗散模式和耗散内容有关,在非平衡系统中,对于不同的定态 ψ,可以取不同的值(正、负或零)。

这也意味着,当网络系统趋于不安全熵的非平衡相变临界点(即,$R_1\to 0$)时,耗散参量 $M_D(u)$ 也与 $|\varepsilon|^{\beta\psi}$ 成正比,它揭示了 M_D 与临界距离 ε 之间的依赖关系。当然,若 $\beta\psi=0$,则系统就处于平衡状态了。

综上可知,在网络安全对抗系统的非平衡相变临界点,耗散参量 M_D 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 $\varepsilon\to 0$ 时,意味着红客对网络安全的保障能力和黑客的破坏能力,成为至关重要的因素,它们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。

2 网络空间安全态势的中观描述

结合前面的推论,到目前为止,网络空间安全态势的“中观画像”其实已很清楚了。不过,在“知其然”的基础上,我们还想借助耗散结构理论,更进一步地“知其所以然”。

其实,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。对任何网络系统而言,安全只是相对的,不安全才是绝对的;而且,不安全性(安全性)是熵(负熵),它也遵守热力学第二定律,即,封闭网络在没有人为攻防力量介入的条件下,其自发演化的趋势将是:不安全熵达到最大。此时,不仅不能形成新的安全结构,就连原来的安全结构都将被破坏和瓦解。但是,当红客和黑客介入后,网络系统就会不断从外部(环境)引入物质、能量和信息的正负不安全熵流,并不断排出其代谢产物,吐故纳新。如果红客的安全保障能力足够强,那么,网络系统的不安全熵的总值将保持不变,甚至趋于减小,从而维持、形成并保持网络系统的安全状态。

(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。所谓平衡状态,就是指构成网络系统的各种安全要素在物质、能量和信息分布上的均匀、无差异状态。

(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。网络系统的非平衡态,有近平衡态和远离平衡态之分。这里的“远”和“近”,并非是物理上的距离,而是由影响不安全熵的“当前力量”来定义的,比如,力所不及处,便称为“远”,反之,则为“近”。网络系统的安全状态,既不能从不安全的平衡态产生,也不能从不安全的近平衡态产生;只有远离不安全的平衡态,才有可能使原有的不安全状态失稳,并进而产生新的安全结构。当然,这种安全结构必须要有足够的负熵流(来自于红客的安全保障措施)才可能产生、维持与发展。这种在远离不安全平衡态条件下,网络系统与外部环境相互作用而形成的新的安全结构,其实就是某种耗散结构,因为,这种安全状态只能依靠红客不断地从外部引入优质低熵的物质、能量或者信息。

(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。网络系统若要形成新的安全结构,那么,构成该系统的各种安全要素之间,既不能是各自孤立的,也不能仅仅是简单的线性联系。因为,线性关系是一系列不稳定状态的序列与集合,此时系统只能处于一种水无休止的发展变化之中,而得不到片刻安宁,其不安全熵更不可能趋于稳定;同时,由于受环境资源的限制,客观世界也不容许包括网络在内的任何系统,以线性方式无休止地向前发展。因此,只有在网络系统的各安全要素之间,存在非线性的相互联系和相互作用时,才能使它们产生复杂的相干效应和协同动作,使得红客的“建设力量”与黑客和自然退化的“破坏力量”形成暂时的均衡,从而网络系统进入某个暂时的稳定状态,进而形成并维持与该状态相对应的新的安全结构。

(5)“涨落”是安全结构形成的“种子”和动力学因素。“涨落”是指系统中某个变量或行为对平均值所发生的偏离。对于网络等任何多自由度的复杂体系,这种偏离都是不可避免的。但它对具有不同安全性的系统,其作用是不相同的。对于原本稳定的安全系统,由于该系统本身具有较大抵抗能力,涨落并不总能对它构成严重影响;而对于已达临界稳定状态的安全系统,即使较小的涨蒋也可能使它失去稳定性,从而导致系统从安全状态演化为不安全状态,就像那“压死骆驼的最后一根稻草”。其实,任何一种安全状态的出现,都可看作是另一参考系失去稳定性后的演化结果;因而系统就可以“通过涨落达到安全”。在系统的演化过程中,系统中那些不随时间而衰减,相反却增大的涨落,便成为新的安全结构的“种子”。

(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。任何网络系统都有保持其本质的规定性或稳定性的临界度。“度”,即保持自身特质并可以与他质相区别的阈值。当网络系统中的涨落运动所引起的扰动和振荡达到或超过一定的阈值,就会使原有系统的安全结构遭到破坏,为出现新的安全结构提供可能;相反,新的安全结构要想保持自身,就必须将系统的涨落控制在一定的阈值(即临界度)以内,否则,安全结构就会被新的结构所取代。

(7)可以用网络系统的不安全熵的阈值来表示“度”。当不安全熵不断增大时,系统可能会逐次出现相继的分叉,而且,每个分叉中既有确定性不安全因素,也有随机性因素。在两个分叉点之间,系统遵从确定性定律和化学动力学的某些规律,但在各分叉点附近,“涨落”却扮演着重要作用,甚至决定了系统所追随的分叉支线。

(8)网络系统通过“自组织”形成新的稳定安全结构。在平衡状态下,子系统表现得相对独立,而在远离平衡态的非线性系统中,子系统之间就会产生相干性,存在某种“长程力”作用,或有某种“通讯”联系在进行信息传递,以致每个子系统的行为都与整体状态有关。这时网络系统的一个微观随机小扰动,可能就会通过相干作用得到传递和放大,使微观的局部扰动发展成为宏观的“巨涨落”,使系统进入不稳定状态。在这种状态下,系统各要素之间就会相互协同作用,寻求着信息深层结构的内在联系。一旦某种信息之间建立了精约同构(即,两种事物深层次里具有的少而精的共性)的联系,系统就会由不稳定状态跃迁到新的稳定状态。

3　结束语

由于“类比”在本文中扮演了重要角色,因此,在结束语中,我们就来介绍一下“类比”这种科研方法。

对未知的恐惧,促使人类不断探索世界,发现新东西,刷新世界观;与已知现象的类比,则是理解新事物的有效手段,同时,类比也能够帮助人类揭示新奥秘。所以,社会的进步,就是在“类比”和“新发现”两者间的相互促进过程中完成的。更新世界观,将产生新的未知领域,将更新类比模式,从而将引导新发现。本文正是借助类比,利用大家比较熟悉的市场经济现象,来介绍抽象的网络空间安全对抗,这也许是一条捷径,因为,要想单独给网络安全对抗“画像”,实在太难。

“类比”是重要的科研方法,它首先针对“原问题”,寻找一个有效的并且一般来说相对容易(或已有答案)的“类比问题”;然后,通过解决“类比问题”,再反过来探索“原问题”的解决办法。虽然不能将类比对象的结果照搬到原问题,但是,类比往往确实很有启发性。可见,运用类比法的关键,是寻找一个合适的类比对象。比如,本文就以“市场经济”作为“网络安全”的类比对象。

其实,无论古代、近代,还是现代,类比就一直被普遍应用;而且,还随科学思维水平的提高而不断发展。其具体表现为:从简单到复杂,从静态到动态,从定性到定量的发展。

在古代,为认识某事物所具有的性质,往往采取将该事物与某个已知事物作定性类比;即,根据两者具有相类似的许多性质,从而推想它们还具有其他类似的性质。例如,我国古代科学家宋应星,为了认识声音的传播,就把击物的声音与投石击水的纹浪进行类比:既然水能以波动方式传播,那么声音也能以波动方式传播。

在近代,类比已不再局限于定性了,定量的类比、甚至是定性和定量相结合的类比,被普遍应用于科研工作之中。例如,科学家欧姆,就把电流的传导同热传导进行类比:把电流类比成热量,电压类比成温差,电导类比成热容量。于是,已知的热传导数学公式“热量=热容量 x 温差”,就被类比于电流传导中的数学公式“电流=电压 x 电导”,从而,在电功的研究中,取得了重大突破。

如今,类比方法(包括定性、定量、以及两者的结合)在自然科学研究中,已变得越来越重要了。一般说来,定性类比是定量类此的前提和条件,定量类比则是定性类比的发展和提高。甚至科学发展已与定性类比密不可分:巧妙的定性类比,往往能为科学的进一步发展指明方向;当然,后续还必须有充分的定量研究,才能达到精确的规律性认识。因此,用市场经济来类比网络安全,这只是一个开端,还必须有更深入的后续量化研究。

与科研中的归纳法和演绎法相比,类比法有时会独树一帜,发挥特有的效能。虽然,归纳、演绎和类比都是重要的推论方法,都可能从已知前提推出未知结论,而且,这些结论也都要在一定程度上受制于前提;但是,它们的结论被前提制约的程度是不同的:演绎的结论受到前提的制约最大,其次是归纳,再次才是类比;即,类比的结论受到前提的限制最小。因此,类比在科学探索(特别是初期探索)中发挥的作用最大。而网络安全对抗的中观和宏观“画像”,就处于初期探索的状态,但愿基于市场经济的类比,能够发挥有效的作用。

在科研前沿,由于探索性强、资料奇缺(当前网络安全攻防就处于这种状况),类比的运用就更加重要。例如,上世纪 60 年代,物理学家们,正是通过将抽象的“夸克”与当时已了解较深的磁极进行类比,才把夸克

理论引向了新的起点,并做出了重要预测,从而开辟了一条建立夸克基本理论的新途径。

类比还常用于解释新理论和新定义,因为,类比具有很强的提升理解力的作用。当某新理论提出时,最有效的做法是:通过类比,用熟知的理论去说明新理论和新定义。比如,在气体运动论刚被提出时,就是将气体分子与一大群粒子进行类比:假定粒子服从牛顿定律并发生碰撞而无能量损失。事实证明,该类比在气体行为理论的历史中,发挥了非常重要的作用。只有与已知理论进行类比,新理论才能得以解释,才能被更好地理解。

类比还与模拟实验密切相关。所谓模拟实验,就是在客观条件受限而不能直接考察被研究对象时,依据类比而采用的间接实验。例如,生命是如何起源的,这一直是个谜,由于生命的原始状态已无法回溯,所以,无法直接研究了。于是,科学家米勒,只好通过类比,设计了一个生命起源的模拟实验。他在密封的容器里,放入了氢、氧、碳、氮、甲烷和水等物质,然后,又模拟了风、雨、雷、电等原始大气环境。一周后,在容器里竟然发现了多种氨基酸!这为揭开生命起源的奥秘,迈进了一大步。这些成果再一次充分显示了,以类比为逻辑基础的模拟实验是多么重要。

总之,类比在科研中的作用,决不可忽视。其实,全球网民一刻也离不开的东西,也要归功于类比;因为,计算机就是类比人脑的产物,所以,它本该叫做“电脑”。

参考文献:

[1] 杨义先,钮心忻,安全通论(1)之“经络篇”[EB/OL]. http://blog. sciencenet. cn/blog-453322-944217. html,2015-12-18.

[2] 杨义先,钮心忻,安全通论(2):攻防篇之“盲对抗”[EB/OL]. http://blog. sciencenet. cn/blog-453322-947304. html,2016-01-01.

[3] 杨义先,钮心忻,安全通论(3):攻防篇之“非盲对抗”之“石头剪刀布游戏”[EB/OL]. http://blog. sciencenet. cn/blog-453322-948089. html,2016-01-04.

[4] 杨义先,钮心忻,安全通论(4):攻防篇之“非盲对抗”之“童趣游戏”[EB/OL]. http://blog. sciencenet. cn/blog-453322-949155. html,2016-01-09.

[5] 杨义先,钮心忻,安全通论(5):攻防篇之“非盲对抗”收官作及“劝酒令”[EB/OL]. http://blog. sciencenet. cn/blog-453322-950146. html,2016-01-13.

[6] 杨义先,钮心忻,安全通论(6):攻防篇之“多人盲对抗”[EB/OL]. http://blog. sciencenet. cn/blog-453322-954445. html,2016-02-04.

[7] 杨义先,钮心忻,安全通论(7):黑客篇之“战术研究”[EB/OL]. http://blog. sciencenet. cn/blog-453322-956051. html,2016-02-14.

[8] 杨义先,钮心忻,安全通论(8):黑客篇之“战略研究”[EB/OL]. http://blog. sciencenet. cn/blog-453322-958609. html,2016-02-25.

[9] 杨义先,钮心忻,安全通论(9):红客篇[EB/OL]. http://blog. sciencenet. cn/blog-453322-960372. html,2016-03-04.

[10] 杨义先,钮心忻,安全通论(10):攻防一体的输赢次数极限[EB/OL]. http://blog. sciencenet. cn/blog-453322-984644. html,2016-06-14.

[11] 杨义先,钮心忻,安全通论(11):信息论、博弈论与安全通论的融合[EB/OL]. http://blog. sciencenet. cn/blog-453322-989745. html,2016-07-11.

[12] 杨义先,钮心忻,安全通论(12):对话的数学理论[EB/OL]. http://blog. sciencenet. cn/blog-453322-993540. html,2016-07-30.

[13] 杨义先,钮心忻,安全通论(13):沙盘演练的最佳攻防对策计算[EB/OL]. http://blog. sciencenet. cn/blog-453322-1000428. html,2016-09-02.

[14] 杨义先,钮心忻,安全通论(14):病毒式恶意代码的宏观行为分析[EB/OL]. http://blog. sciencenet. cn/blog-453322-1001684. html,2016-09-08.

[15] 杨义先,钮心忻,安全通论(15):谣言动力学[EB/OL]. http://blog. sciencenet. cn/blog-453322-1003586. html,2016-09-18.

[16] 杨义先,钮心忻,安全通论(16):黑客生态学[EB/OL]. http://blog. sciencenet. cn/blog-453322-1005963. html,2016-09-30.

[17] 杨义先,钮心忻,安全通论(17):网络安全生态学[EB/OL]. http://blog. sciencenet. cn/blog-453322-1007253. html,2016-10-07.

[18] 杨义先,钮心忻,安全通论(18):网络安全经济学(1):攻防一体[EB/OL]. http://blog. sciencenet. cn/blog-453322-1040388. html,2017-03-19.

[19] 杨义先,刷新你的安全观念[EB/OL]. http://blog. sciencenet. cn/blog-453322-983276. html,2016-06-08.

[20] 蔡绍洪等著,耗散结构与非平衡相变原理及应用[M]. 贵阳:贵州科技出版社,1998.