文章编号: 2096-1618(2017)04-0353-06
稿件来源:科学网
网　　址:http://blog.sciencenet.cn/blog-453322-1049099.html
发表时间:2017-04-15

安全通论(20)

——安全攻防的经济演化规律

杨义先,　钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:借助进化论思想,以经济目标为量化手段,利用协同学中的现成结果,本文建立了网络空间安全攻防的演化模型,并给出了具体的安全演化行为公式,及其解析解的稳定性分析。根据本文的结果,针对具体的信息系统,如果能对相关参数值进行估计的话(在沙盘演练的场景下,这些参数肯定是能够获得的),那么,该系统的安全对抗演化轨迹将清晰可见,这对网络攻防的全面量化理解,显然是很有帮助的。另外,即使是不知道实际系统的相关演化参数,我们也可以事先针对尽可能多的参数,绘制出相应的攻防演化轨迹曲线图,以备实战中参照使用。

doi:10.16836/j.cnki.jcuit.2017.04.002

0　引言

由于达尔文等生物学家们的杰出贡献,如今,以“物竞天择,适者生存”等为代表的进化论口头禅,早已家喻户晓;即,由于生物间存在着生存斗争,适应者生存下来,不适者则被淘汰,这就是自然选择。而且,生物们正是通过遗传、变异和自然选择,从低级到高级,从简单到复杂,种类由少到多地进化着、发展着。更进一步地,科学家们还把进化论的思想和原理,推广到其它学术领域,并获得了不少成果,比如,形成了演化金融学、演化证券学、演化经济学等多个新兴交叉学科。纵观这些进化(或演化),它们都有一个共同特点,即,生物之间、产品之间、证券之间等,都存在着充分的竞争。而正是这些竞争,才推动了相关的演化或进化。

反省网络空间安全,其中也存在激烈的竞争(即,红客和黑客之间的对抗;这种对抗的激烈程度,一点也不亚于生物斗争),因此,很容易想到:网络安全对抗过程,其实也是一个演化(进化)过程。但是,如果仅仅到此为止,那就没什么稀奇了,因为甚至连半文盲都能作此联想,而且,进化(或演化)一词,在许多场合,早已被用滥了。

达尔文虽然断言了动物们的演化过程,但是,从数学上看,它们到底是怎么演化的呢?至今谁都不知道,因为,生物们的斗争,实在太复杂了:有的靠利齿取胜,有的用速度躲灾;有的上九天揽月,有的下五洋捉鳖;反正,各有各的招,各要各的刀。并且,生物之间的生存斗争,很难量化,即使是想转化为经济价值,也是几乎不可能的。

不过,与自然界的生物斗争等相比,网络空间安全对抗,在其进化(演化)的量化分析方面,有两大优势:

其一,斗争的形式,相对更简单,只有“攻”和“守”两招,当然每一“招”中,其手段也是千差万别(《安全通论》的最终目标,就是希望将这些“千差万别”合而为一)。而且参与斗争的人员可以很多(比如,全球70亿人都可以同时扮演着攻方(黑客)和守方(红客)的角色),而且,还可以彼此乱斗,形成海量的利益集团。

其二,也是最重要的优势是,网络空间中的攻防斗争,无能表面上的目的如何,也无论某个阶段的目的如何,其最终目的都可以用一个字来归纳,那就是“钱”!这就为本文的量化研究,奠定了坚实的基础。(注:这是从统计角度给出的结论,也许有极个别的例外,但是,绝大部分攻防都是“能够用钱摆平的”!)

如果投入 X 块钱用于攻击(称为黑客投资),虽然针对不同的攻击手段、不同的攻击者、不同的攻击对象,攻方所能够获得的经济效益(行话叫“黑产收入”)是不相同的;但是,从统计角度来看,经过一段时间的振荡后,黑产收入一定会逼近某个数值。因为,你可以将不同的攻击手段当作“商品”,经过一段时间的“竞价”后,该商品的价格(即,黑产收入的逼近值),在亚当斯密的那只看不见的手的作用下,就一定是稳定的。换句话说,投资者可以用 X 块钱,去“购买”最值的攻击。

同理,如果投入 Y 块钱用于防守(称为红客投资),虽然针对不同的防守措施、不同的防守者、不同的防守对象,防守方所能够获得的经济效益也是不相同的,而且,还是很难知道的(若只单独观察某个固定

的信息系统,甚至连信息系统的拥有者,都不知道安全防护措施到底创造了多少经济效益;实际上,从经济上看,当前全世界的安全防护都是在“跟着感觉走”);但是,从统计角度来看,经过一段时间的振荡后,该“很难知道的经济效益”也一定会逼近某个数值。因为,你可以将防守措施当作“商品”,经过一段时间的“竞价”后,该商品的价格(即,安全保障效益的逼近值),在亚当斯密的那只看不见的手的作用下,也一定是稳定的。换句话说,投资者可以用 Y 块钱,去“购买”最值的防守。

当然,必须承认,无论是黑客投资 X,还是红客投资 Y,其最终逼近值的确定,都是非常困难的问题,但是,从理论上说,它们确实也是存在的。我们不打算探讨逼近值的求解问题,下面直接用黑客投入 X 和红客投入 Y 的值,来量化攻守各方的能力。这样做的合理性,也可以直观地理解为:投入越多,回报越大嘛。

必须明确强调的是,1 块钱的红客投资所构建的防守体系,并不能抵挡 1 块钱的黑客投资所产生的攻击力;反之亦然。但是,从统计角度来看,经过一段时间的振荡后,“1 块钱的红客投资”与“1 块钱的黑客投资”之间,一定有一个比较稳定的当量比值 k,这个比值还会根据不同的网络系统、不同的攻防场景和不同的时间,而发生变化。在下面的分析中,我们假定这个比值为 1,这样做仅仅是为了简化分析而已。本文中,我们还做了许多类似的假定,毕竟过多的细节会喧宾夺主;当然,这也意味着,本文还需许多后续改进,所以,欢迎所有读者积极投入《安全通论》的研究之中。

1 网络攻防斗争的演化模型与轨迹

对给定的某个信息系统 A(比如,全世界的网络组成的网络空间,或其某个子系统等),假定共有 N 个人对该系统的攻防有兴趣(这里的“人”可能是自然人,也可能是团体等)。在时刻 t,记第 i 个人用于攻击的投资为 $E_i(t)$,用于防守的投资为 $R_i(t)$,因此,用于攻防的整体投资为 $I_i(t)=E_i(t)+R_i(t)$。这里,攻击目标和防守目标,都是系统 A 的某些子系统;当然,不同的人,所攻击和防守的目标是不相同的。也许有的人是纯黑客,只攻不守,即,$E_i(t)=0$;也许有的人是纯红客,只守不攻,即,$R_i(t)=0$。再假定,每个人用于攻防的投资总额是不变的,即,$I_i(t)$ 的总预算额不变,攻击投资 $E_i(t)$ 越多,防守投资 $R_i(t)$ 就越少。更明确地说,必要时,$E_i(t)$ 和 $R_i(t)$ 还可理解为:此人分别用于攻击和防守的投资比例。(注意:攻防开销只是网络用户的部分开销,毕竟除了攻防之外,人们还有更多、更重要的事情要做,所以,攻防之外的经费都不在本文的考虑之列)

将所有人的攻击投资之和记为 $E(t)$,防守投资之和记为 $R(t)$,于是,用于攻防的总投资额就为 $I(t)=E(t)+R(t)$。

在众多的各类攻防手段中,攻防投资的比例终将稳定在一个固定的值上,即,攻击投资平均值 $E_0(t)$ 和防守投资平均值 $R_0(t)$。当然,由于每个人的目标不同,而且外界情况也千变万化,所以,攻防投资之间的比例一定会随着时间的变化而变化,本文就是力图找出这种比例的变化规律,从而把握整体安全趋势,展现攻防对抗的轨迹。

由于 $E(t)$ 和 $R(t)$ 都围绕其平均值 $E_0(t)$ 和 $R_0(t)$ 而涨落,其涨落的幅度记为 $B(t)$,它可正可负,记 $E(t)=E_0(t)+B(t)$,于是,$R(t)=R_0(t)-B(t)$,这里 $B(t)$ 的变化范围满足不等式 $-E_0(t)<B(t)<R_0(t)$。将攻击投资与防守投资的差额在总投资中的比例定义为“攻防结构指数”$Z(t)$,即:

$$Z(t)=[E(t)-R(t)]/[E(t)+R(t)]=[E(t)-R(t)]/I(t) \tag{1}$$

将攻防结构指数 $Z(t)$ 分成其“平均值部分 $Z_0(t)$”和“涨落部分 $z(t)$”之和,即:

$$Z(t)=Z_0(t)+z(t) \tag{2}$$

其中 $Z_0(t)=[E_0(t)-R_0(t)]/I(t)$ 和 $z(t)=2B(t)/I(t)$ 将是我们的研究重点,它们将揭示整体的安全演化规律。

设在 t 时刻攻击投资的人数为 $N_E(t)$,防守投资的人数为 $N_R(t)$,于是称 $\{N_E(t),N_R(t)\}$ 为此刻的攻防者投资结构。由于每个人既可以为攻击投资,也可以为防守投资,所以,$N_E(t)+N_R(t)\leqslant 2N$。

再假定不存在纯黑客或纯红客(在现实中确实也是这样,一方面,黑客他总得投资防守自身的子系统吧,所以,纯黑客不存在;另一方面,哪一个人不想去占一点别人的便宜呢,所以,纯红客不存在),所以,$N_E(t)+N_R(t)=2N$。

由于在 t 时刻,攻防投资总额为 $I(t)$,所以,针对某个具体人来说,攻防的投资平均值就为 $i(t)=I(t)/(2N)$,再将其细分为攻击投资平均值 $e_0(t)=E_0(t)/(2N)$ 和防守投资值 $r_0(t)=R_0(t)/(2N)$,即:

$$i(t)=I(t)/(2N)=e_0(t)+r_0(t) \tag{3}$$

如果某人的攻防投资分别为平均值 $e_0(t)$ 和 $r_0(t)$,那么,就称此人为“中立者”。

如果某人的攻击投资 $e_E(t)$ 大于攻击平均数 $e_0(t)$(当然,其防守投资 $r_E(t)$ 就小于防守平均值 $r_0(t)$。注意,这里其实暗含了“投资比例”的概念,以避免某人

的绝对投资额特大或特小的情况),即,$i(t)=e_E(t)+r_E(t)$,其中 $e_E(t)=e_0(t)+b$ 且 $r_E(t)=r_0(t)-b$,此处 $b>0$。那么,此人就称为攻击型人员;

如果某人的防守投资 $r_R(t)$ 大于防守平均数 $r_0(t)$(当然,其攻击投资 $e_R(t)$ 就小于攻击平均数 $e_0(t)$。注意,这里也暗含了"投资比例"的概念,以避免某人的绝对投资额特大或特小的情况),即,$i(t)=e_R(t)+r_R(t)$,其中 $e_R(t)=e_0(t)-b$ 且 $r_R(t)=r_0(t)+b$,此处 $b>0$。那么,此人就称为防守型人员。

由于我们已经假定了:

$$N_E(t)+N_R(t)=2N \tag{4}$$

因此,攻防投资者结构 $\{N_E(t),N_R(t)\}$ 便可简化为一个变量 $N(t)$,它定义为:

$$N(t)=[N_E(t)-N_R(t)]/2 \tag{5}$$

故,攻击型人员增加一个(当然,防守型人员就要减少一个)的演化过程,就可标记为:$\{N_E(t),N_R(t)\}\to\{N_E(t)+1,N_R(t)-1\}$,也可以简化为 $N(t)\to N(t)+1$;攻击型人员减少一个(当然,防守型人员就要增加一个)的演化过程,就可标记为:$\{N_E(t),N_R(t)\}\to\{N_E(t)-1,N_R(t)+1\}$,也可以简化为 $N(t)\to N(t)-1$。

为了方便连续化处理,将攻防投资结构用下面的"攻防者结构指数"来表示:

$$x(t)=N(t)/N,\quad -1\leqslant x(t)\leqslant 1 \tag{6}$$

它其实就是攻击型人数与防守型人数之差的整体平均。在深入研究之前,我们先回答公式(1)中的攻防结构指数 $Z(t)$,和公式(6)中的攻防者结构指数 $x(t)$之间的关系。

定理 1:攻防结构指数 $Z(t)$ 和攻防者结构指数 $x(t)$之间的关系,满足如下公式:

$$z(t)=4Nbx(t)/I(t) \tag{7}$$

证明:由于 $Z(t)=[E(t)-R(t)]/[E(t)+R(t)]$,并且 $E(t)=e_EN_E+e_RN_R=N_E(e_0+b)+N_R(e_0-b)$

和 $R(t)=r_EN_E+r_RN_R=N_E(r_0-b)+N_R(r_0+b)$,将它们代入 $Z(t)$ 的定义,见公式(1),便有:

$$Z(t)=(E_0(t)-R_0(t))/I(t)+4Nb/I(t)=Z_0(t)+4Nbx(t)/I(t)$$

所以 $z(t)=4Nbx(t)/I(t)$。证毕。

注意到攻防的总投资是不变的,即,$I(t)$ 为常数,所以,根据定理 1,攻防演化规律既可以用攻防结构指数 $Z(t)$ 来描述,也可以用攻防者结构指数 $x(t)$ 来描述,还可以等价地用攻防投资者结构 $\{N_E(t),N_R(t),t\}$ 来描述,为简捷计,我们采用攻防投资者结构来展开后续分析。

虽然每个人的攻防资金总额是固定的,但是,分别用于攻或防的资金比例分配却是随机的(至少外人是不知道的,甚至,经常是当事人自己也不一定清楚其分配理由),故只能研究 t 时刻具有攻防投资者结构 $\{N_E(t),N_R(t),t\}$ 的概率分布 $P(N_E(t),N_R(t),t)$,记它为 $P(n,t)$。该概率分布当然满足如下归一化条件,即:

$$\sum_{n=-N}^{N}P(n,t)=1 \tag{8}$$

如果在单位时间内,某个防守型人员转变成了攻击型人员,将此事件发生的概率记为 $P_{E\leftarrow R}[N_E,N_R]$,或更简捷地记为 $P\uparrow(n)$;相反,如果在单位时间内,某个攻击型人员转变成了防守型人员,将此事件发生的概率记为 $P_{R\leftarrow E}[N_E,N_R]$,或更简捷地记为 $P\downarrow(n)$。

由于事件 $\{N_E,N_R\}\to\{N_E+1,N_R-1\}$(即,攻击型人员增加一个,当然防守型人员就减少一个)发生的概率等于单个防守型人员转变成攻击型人员的概率 $P\uparrow(n)$乘以可转移的防守型人员数目,即,该概率为:

$$W\uparrow(n)=N_RP\uparrow(n)=(N-n)P\uparrow(n) \tag{9}$$

同理,由于事件 $\{N_E,N_R\}\to\{N_E-1,N_R+1\}$(即,攻击型人员减少一个,当然防守型人员就增加一个)发生的概率等于:

$$W\downarrow(n)=N_EP\downarrow(n)=(N+n)P\downarrow(n) \tag{10}$$

于是,攻防的演化规律可以由概率 $P(n,t)$ 随时间变化的情况来刻画,即有如下微分方程:

$$dP(n,t)/dt=[W\uparrow(n-1)P(n-1,t)+W\downarrow(n+1)P(n+1,t)]-[W\uparrow(n)P(n,t)+W\downarrow(n)P(n,t)] \tag{11}$$

分别考察此式中的各个分项,将它们展开便知:

$$W\uparrow(n-1)P(n-1,t)=W\uparrow(n)P(n,t)-(\Delta n)\partial[W\uparrow(n)P(n,t)]/(\partial n)+[(\Delta n)^2/2]\{\partial^2[W\uparrow(n)P(n,t)]/\partial n^2\} \tag{12}$$

(注:由于所用编辑器的限制,此文用 ∂ 来代表偏微分符号)同样有:

$$W\downarrow(n+1)P(n+1,t)=W\uparrow(n)P(n,t)+(\Delta n)\partial[W\downarrow(n)P(n,t)]/(\partial n)+[(\Delta n)^2/2]\{\partial^2[W\downarrow(n)P(n,t)]/(\partial n^2)\} \tag{13}$$

将展开后的分项公式(12)和(13),代回原来的公式(11),便有:

$$dP(n,t)/dt=-\partial[(W\uparrow(n)-W\downarrow(n))P(n,t)]/(\partial n)+\{\partial^2[(W\uparrow(n)+W\downarrow(n))P(n,t)]\}/(2\partial n^2) \tag{14}$$

记 $x=n/N$,则可记 $W\uparrow(n)=N\omega\uparrow(x)$ 和 $W\downarrow(n)=N\omega\downarrow(x)$,将它们代入公式(14),便有:

$$dP(x,t)/dt=-(1/N)\{\partial[N(\omega\uparrow(x)-\omega\downarrow(x))P(x,t)]\}/(\partial x)+(1/2)(1/N^2)\{\partial^2[N(\omega\uparrow(x)+\omega\downarrow(x))P(x,t)]\}/(\partial x^2)=-\partial[(\omega\uparrow(x)-\omega\downarrow(x))P(x,t)]/(\partial x)+(1/2)\varepsilon\{\partial^2[(\omega\uparrow(x)+\omega\downarrow(x))P(x,t)]\}/(\partial x^2)$$

将此式简记为:

$$dP(x,t)/dt=-\partial[K(x)P(x,t)]/(\partial x)+(\varepsilon/2)\partial^2[Q$$

$(x)P(x,t)]/(\delta x^2)$ (15)

其中,$K(x)=\omega\uparrow(x)-\omega\downarrow(x)$ 和 $Q(x)=\omega\uparrow(x)+\omega\downarrow(x)$,以及 $\varepsilon=1/N$。用 x 乘以公式(15)的左右两边,并对 x 积分(积分的上下限分别为+1 和-1),于是,得到均值方程如下:

$$d<x>/dt=<K(x)>-(\varepsilon/2)[Q(x)P(x,t)]\Big|_{x=-1}^{x=1} \quad (16)$$

在公式(16)中,忽略边界贡献,因为,在边界 $x=1$ 或 $x=-1$ 处,所得的概率值 $P(x,t)$ 都很小,所以,便可得到:

$$d<x>/dt=<K(x)> \quad (17)$$

若 $P(x,t)$ 只有一个峰值,那么,可将 $K(x)$ 在<x>附近展开为泰勒级数:

$$K(x)=K(<x>)+K'(<x>)(x-<x>)+(1/2)K''(<x>)(x-<x>)^2+\cdots\cdots$$

只取该式的第一项,则公式(17)变为 $d<x>/dt=K(<x>)$,如果假设平均径迹就是实际径迹,那么,该式又可重写为:

$$dx/dt=K(x(t)) \quad (18)$$

结合攻防投资结构的具体模型,可写出函数 $K(x(t))=\omega\uparrow(x)-\omega\downarrow(x)$。又由于 $\omega\uparrow(x)$ 和 $\omega\downarrow(x)$ 可以写为:

$$\omega\uparrow(x)=v(1-x)exp(\delta+kx) \text{ 和 } \omega\downarrow(x)=v(1+x)exp[-(\delta+kx)] \quad (19)$$

其中,δ 表示相关人员对攻击或防守的偏好,称为“互变因子”。当 δ 为正时,表示此人喜欢攻击;当 δ 为负时,表示此人喜欢防守。当然,这种偏好也会随着时间的变化而变化。

公式(19)中的 k 值,表示某人追随别人,在攻击型和防守型之间转换的速度(即,此人是否喜欢赶时髦,随大流)。当 k 值较大时,若 $x>0$(即,多数人为攻击型),则促进了大家向攻击型人员转变;若 $x<0$(即,多数人为防守型),则不利于大家向攻击型人员转变。所以:

$$K(x,\delta,k)=2v[sh(\delta+kx)-xch(\delta+kx)] \quad (20)$$

$$V=[2v/K^2][kxsh(\delta+kx)-(1+k)ch(\delta+kx)] \quad (21)$$

于是,公式(17)变为:

$$dx/dt=2v[sh(\delta+kx)-xch(\delta+kx)] \quad (22)$$

这便是攻防斗争的演化方程,它显示了网络空间安全对抗中,攻击型人员与防守型人员之间相差值的变化情况。归纳上述论述,便有如下结论。

定理 2:在网络空间安全对抗中,在 t 时刻,攻击型人数与防守型人数之差的平均值(即,除以总人数 $2N$)$x(t)$ 的演化规律,由微分方程 $dx/dt=2v[sh(\delta+kx)-xch(\delta+kx)]$ 来描述。

该定理给出了一个很明晰的安全对抗演化轨迹。当然,针对实际的网络系统,我们很难确定其中的参数 v,δ 和 k 等,但是,在某些特殊情况下(比如,沙盘演练),经过充分的统计和测试,还是可以在一定误差范围之内,给出这些参数的估计值,从而可以明确地把握攻防对抗的演化轨迹。即使是在无法确定这些参数的情况下,定理 2 的价值也仍然存在,比如,可以罗列尽可能多的各类参数组合,事先绘制出各种情况下,攻防对抗的演化轨迹图,那么,对把握实战过程中的趋势情况也是有帮助的。定理 2 还有其它潜在的应用价值,此处就不赘述了。

由于公式(22)中的 δ 更形象,它代表了相关人员在攻击型和防守型之间的来回“跳槽”情况,所以,我们对 δ 进行单独的深入分析。由于这种转变率也是随时间而变化的,所以,我们将它记为 $\delta(t)$,并给出 $\delta(t)$ 的演化规律。

我们有理由(“反馈+微调”机制,或“阻尼”现象)假定,当攻击型和防守型人员一样多(即,$x=0$)时,$\delta(t)$ 将最终朝着没有任何偏好的方向变化,即,当时间 t 趋于无穷大时,$\delta(t)\to 0$。同时,当 $x<0$,即,防守型人员更多时,$\delta(t)$ 应趋向于朝攻击型转变,即,当时间 t 趋于无穷大时,$\delta(t)\to\delta_0$;反之,$x>0$ 时,即,攻击型人员更多时,就该向防守型转变,即,当时间 t 趋于无穷大时,$\delta(t)\to-\delta_0$。据此,可写出 $\delta(t)$ 的方程:

$$d\delta(t)/dt=\mu[\delta_0-\delta(t)]exp[-\beta x(t)]-\mu[\delta_0+\delta(t)]exp[\beta x(t)] \quad (23)$$

其中 $\mu>0$,$\beta>0$,$\delta_0>0$。于是,公式(23)又可变为

$$d\delta(t)/dt=L(x,\delta,k) \quad (24)$$

其中,$L(x,\delta,k)=-2\mu\{\delta_0 sh[\beta x(t)]+[\delta(t)-\delta_1]ch[\beta x(t)]\}$,这里的 δ_0 称为战略决策幅度,它其实就是攻、防互变的因子,它的大小是可变的,变化范围限于 δ 的允许值;β 是趋向反转的速度因子,它反映了 δ 随 x 变化的速度的快慢;μ 是攻防的灵活性参数,描述了相关人员在攻击和防守之间变换的灵活程度;δ_1 表示整体人员对防守型的偏好程度。

综上,我们有如下定理。

定理 3:在网络空间安全对抗中,在 t 时刻,在攻击型和防守型人员之间来回“跳槽”情况 $\delta(t)$,可由如下微分方程来描述:

$$d\delta(t)/dt=-2\mu\{\delta_0 sh[\beta x(t)]+[\delta(t)-\delta_1]ch[\beta x(t)]\}$$

其中各参数的定义如前面所述,此处不再重复了。同样,关于此定理的理解和应用,也与定理 2 类似,此处略去。

到此,由定理 2 和定理 3(或由公式(22)和(24)构成的耦合方程),就决定了攻防投资者结构的演化

规律,也就是网络空间安全对抗中,红客和黑客力量对比的演化规律。只要能够通过实测等手段,确定了这些公式中的相关参数值,那么,安全对抗的演化过程就被清楚地用量化方法刻画出来了。

2　攻防斗争演化的稳定性分析

在一般情况下,网络空间安全攻防斗争演化方程(即,公式(22)和公式(24))是不能求出精确解的,只能进行数值计算。下面在 $\delta_1=0$ 的假定下(即,整体人员对防守型的偏好程度为 0),证明对任何 k 值,都存在定态解,并对该解进行线性稳定性分析。

根据公式(22)和(24),定态方程为:

$$2v[sh(\delta+kx)-xch(\delta+kx)]=0 \tag{25}$$

和

$$-2\mu\{\delta_0 sh[\beta x]+[\delta-\delta_1]ch[\beta x]\}=0 \tag{26}$$

令 $\delta_1=0$,则公式(26)变为

$$-2\mu\{\delta_0 sh[\beta x]+\delta ch[\beta x]\}=0 \tag{27}$$

由公式(27)可见,对任意 k 值,$(x_0,\delta_0)=(0,0)$ 满足公式(25)和公式(27)。为了看清该定态解的线性稳定性,我们先将定态方程中的有关函数展开如下:

$$Sh(\delta+kx)=(\delta+kx)+[1/(3!)](\delta+kx)^3+[1/(5!)](\delta+kx)^5+\cdots\cdots \tag{28}$$

$$ch(\delta+kx)=1+[1/(2!)](\delta+kx)^2+[1/(4!)](\delta+kx)^4+\cdots\cdots \tag{29}$$

$$sh(\beta x)=\beta x+[1/(3!)](\beta x)^3+\cdots\cdots \tag{30}$$

$$ch(\beta x)=1+[1/(2!)](\beta x)^2+\cdots\cdots \tag{31}$$

若使零解 x_0、δ_0 受一小扰动 $x(t)\to x_0+a(t)$,$\delta(t)\to\delta_0+b(t)$,由公式(28)、(29)、(30)和(31),以及公式(25)和公式(27),得到线性化的零解扰动方程为:

$$da/dt=2v[b+ka-a]=2v(k-1)a+2vb \tag{32}$$

$$db/dt=-2\mu[\delta_0\beta a+b]=-2\mu\delta_0\beta a-2\mu b \tag{33}$$

将公式(32)和公式(33)写成矩阵形式,便是 $dQ/dt=LQ$,其中 $Q=(a,b)^T$ 是 2 维列向量;$L=[L_{ij}]$ 是 2×2 阶方阵,并且 $L_{11}=2v(k-1)$,$L_{12}=2v$,$L_{21}=-2\mu\delta_0\beta$,$L_{22}=-2\mu$。所以,它的本征方程就是 $LQ=\lambda Q$,其本征值为:

$$\lambda=[v(k-1)-\mu]+\{[\mu+v(k-1)]^2-4\mu v\delta_0\beta\}^{1/2}$$

和

$$\lambda=[v(k-1)-\mu]-\{[\mu+v(k-1)]^2-4\mu v\delta_0\beta\}^{1/2}$$

于是,关于网络安全对抗的攻防斗争演化的稳定性,就有如下定理 4。

定理 4:按照上述的术语和定义,我们有如下结论:当 $\mu+v(k-1)<(4\mu v\delta_0\beta)^{1/2}$ 且 $k=k_c=1+\mu/v=1+r$(其中 $r=\mu/v$)时,定态 $(c,0)$ 失稳,将分岔出极限环,即,产生稳定的时间周期解。也就是说,当 $k<1+r$ 且 $\mu+v(k-1)<(4\mu v\delta_0\beta)^{1/2}$ 时,$(0,0)$ 解是稳定的焦点;当 $k>1+r$ 且 $\mu+v(k-1)<(4\mu v\delta_0\beta)^{1/2}$ 时,$(0,0)$ 解是不稳定的焦点,此时,即使 k 还不是很大时,就可能出现极限环。

3　结束语

现在回顾一下本文的几个基本要素:

要素 1,用达尔文进化论(演化)的眼光去看待网络空间安全对抗,其实并不意外。因为,随着进化论的普及,当我们回过头去,重新看待世界上所发生所有事物时,都不难"事后诸葛亮"般地发现:原来这个世界,根本上就是进化(演化)的世界,而且,进化的核心原理就是"反馈+微调"!虽然关于进化论还有争论,但那是生物学家们的事,与本研究无关。虽然进化和演化其实是有区别的,但是,这种差别在我们眼里可以忽略不计,因为,我们只关心量化的动态变化规律。所以,在我们眼里生物在进化,潮汐在进化,山水大气也在进化;星球在演化,社会在进化,网络空间更是在进化。其实,网络的硬件、软件、应用程序等的兴衰存亡,无不依赖于进化。只可惜,嘴上说说"进化"很容易,但是,要搞清楚"到底是如何进化的"就难了,要想量化就难上加难了。幸好本文发现的"网络空间安全对抗的进化规律"是量化的。

要素 2,用经济学的眼光去看待网络空间安全对抗,也不意外了。因为,在《安全通论》的前面几章(比如文献[18]和[19]等),我们已经这样做过了。当然,这种直白的"向钱看"观点(即,安全攻防的最终目标是追求经济利益),会使个别道德感特强的黑客和红客很不服气,因为,他们都坚称:"自己追求的是正义事业,与钱无关"。我不想对此做任何辩解,但是,幸好安全攻防能够转化为经济指标,否则就无法进行量化研究了。能够有如此幸事的领域并不多(比如,随便就可举一个无法量化研究的例子:请问互联网将如何进化,其进化的量化轨迹是什么?)否则,进化论的许多应用就不会被认为是"滥用"了。

要素 3,用统计学的眼光去看待网络空间安全对抗,还是不意外。其实,网络空间的本名,叫"赛博空间"。而赛博学(过去被误译为《控制论》,见文献[22])的核心世界观之一就认为"赛博世界是不确定的,它会受到周围环境中若干偶然、随机因素的影响";赛博学的核心方法论之一就是"统计理论",因此,用统计指标去凝练网络空间安全对抗的相关概念的做法,既合理也自然。不过,客观地说,在当今全球的信息安全界,也许大家过于忙着应对各种紧急事件,对统计的威力还认识不够,总喜欢纠结于具体的攻防手段,而对整体的宏观规律重视不够,所以,常常是"只见树木,难见森林;甚至是只见树叶,未见树枝"。

希望《安全通论》能够适当改善此种状况。

要素4,用协同学方法去建立和分析本文中的模型,仍然不意外。其实,熟悉协同学的读者,也许会发现:本文的模型和数学推导基本上只是“小儿科”,最多可算做“一道普通的练习作业题”而已。实际上,对只有两种“力量”推动的协同系统,其协同规律基本上都可以照此办理(见文献[21])。不过,遗憾的是,在网络安全领域,人们还来不及重视《协同学》、《系统论》、《控制论》、《突变理论》、《耗散结构理论》等动力学理论,甚至只拿它们当作某种新的哲学观而已,没有深入研究它们与网络空间安全的紧密联系。换句话说,本文“没有生产矿泉水”,而只是当了“大自然的搬运工”。

总之,如果单独考察以上四个要素,个个都平淡无奇。

本文唯一出人意料的是:所有这四个平淡的要素,刚好都能在分析网络空间安全对抗的演化规律中排上用场,而且还“严丝合缝”!这就像将一堆普通珍珠,串成了精美的项链一样;或者像是用普通的食材,烹调出了一份可口的四川回锅肉。

客官,请慢用!

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,钮心忻,安全通论(19):网络安全经济学(2):安全熵论[EB/OL]. http://blog. sciencenet. cn/blog-453322-1042638. html,2017-03-30.

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

[21] 吴大进等著,协同学原理和应用[M]. 武汉:华中理工大学出版社出版,1990.

[22] 杨义先,正本清源话“赛博”[EB/OL]. http://blog. sciencenet. cn/blog-453322-994330. html,2016-08-03.