国家安全

统筹处理内外安全

□ 皮明勇

突出“统”，注重整体性、网络化和前瞻性地统筹内外安全

国家安全已经成为一个超复杂大动态的巨系统，割裂地、片面地、零散地、局部地观察和处理问题明显不合时宜。统筹内部安全和外部安全，首先要强化系统思维，注重整体运筹，发挥统制作用。

注重整体性。贝塔朗菲认为，“一般系统论，就是对‘整体’和‘整体性’的探索”。工业时代的思维受分解法、还原论的主宰，还原论好比是切割联系的“伐木锯”，使“全局性的东西”变成了一堆模块、要素、单元的集合，变成了各个部门、各个领域、各个层次的单视角全局，导致经常出现局部合理全局不合理、局部高效整体低能的情形。突出整体性，就是要超越工业时代分解法、“还原论”和专业化的割裂，回归国家安全的整体本真，构建统一的强有力的国家安全领导体系，加强对内外安全大局的统揽，着力增强国家安全的综合效能效益。在今天的情况下，就是要充分发挥国家安全委员会的作用，以《国家安全战略纲要》为统揽，以《国家安全法》为依据，坚决突破内外相隔的狭隘，坚决跳出部门利益的束缚，坚决打破条块分割的掣肘。

注重网络化。信息时代国家安全回归整体性，但这种整体性已远不同于前工业时代，而是网络化的整体性，是网络支撑的有机体系，关键节点强则整体强，重要节点安则整体安，控制中心节点就是控制整体。美国“新美国安全中心”提出，应以“网络化”视角重新审视当前国际体系，国家正日益成为网络中的联结点，应当抢占各种网络的“中心节点”，利用网络的力量为国家安全服务。以总体国家安全观为指导统筹处理内外安全，在全球安全体系中要注重发挥联合国、上合组织和战略支点国家等的作用，注重处理与大国的关系；在经济上，运用网络化及网络节点理念布局和推动“一带一路”建设，化解经济风险，增大安全系数；在内外体系联通上，优先考虑节点的构建和节点间的联通，使形成网络化布局，产生网络化整体效应。

注重前瞻性。系统性在时间轴上表现为前后的有序连贯，需要有足够的前瞻远虑。按照罗素的观点，文明“最基本的特征就是远虑”。但另一方面，正如杜黑指出的，“未来之于现在较过去为近”，思想的进步总比物质的进步慢，保持足够的前瞻和远虑并非易事。统筹内外安全，要善于进行前瞻性谋划，捕捉和营造未来的机遇，敢于对未来进行战略性投入，收获未来的战略性回报，而不是局限于眼前的即时性回报。这种跨内外两界安全的前瞻性谋划和未来性投入，是很难由资本和市场主导的，必然属于国家行为，必须由国家担纲主责，以此带动市场作为。

突出“人”，坚持以民为本、以人为本统筹内外安全

人是万物的尺度。国家安全归根结底是“人”的安全，现代社会的发展特别是信息时代的到来增大了人的社会作用，也增加了人在社会安全中的互动性。习主席强调，必须坚持以人民安全为宗旨，坚持以民为本、以人为本，坚持国家安全一切为了人民、一切依靠人民，真正夯实国家安全基础。这就是说，维护国家安全，统筹内外安全，既要见“事”更要见“人”，人心稳则全局稳，人心顺则上下顺，人心通则内外通。也就是说，要高度重视“人”的因素，把人民所思、人民所图、人民所趋、人民所恶作为评估内外威胁、推动内外发展、维护内外安全的政策和价值取向的基本依据。

在内外发展大体系中促进民生、稳定民心。当前及未来一个时期，我国面临的主要风险和挑战在内不在外，尽管外部压力增大，但只要我自身不发生大的问题，对手是难以撼动我、击垮我的。维护国内安全，最紧要的是政治安全，关键是解决人心安稳、民心向背问题。得民心者得天下，人民的支持，老百姓的认同，是我党不断巩固执政基础的关键所在。在国内各种深层次矛盾凸显的情况下，加快推进“四个全面”战略布局，维持国家整体良好发展态势，不断提高民生水平，是安人心稳大局的重要选择。而谋发展促民生，既要立足国内，将国家的资源重点投向应对国内的矛盾问题，又要有宽阔的全球视野，把本国民生发展放在国际民生发展的大格局中一体统筹推进。特别是充分发挥“一带一路”的战略平台和纽带作用，把促民生作为根本目的，把促进内外两个民生发展作为基本的政策指向，通过自身的发展带动地区的共同发展，利用地区的发展为自己创造更大的发展空间，实现内外普遍繁荣，形成以发展促安全、以民生稳民心的良性互动。

在内外信息大互动中掌控舆情、引导民意。当前激烈的意识形态领域斗争，其实质是一场争夺人心的战争。进入新媒体、自媒体时代，网络成为意识形态较量的主阵地，网络把国内舆论与国外舆论紧密联结起来，统筹内外安全很重要的一个方面，就是在网络信息内外大互动中打赢常态化的舆情争夺战。习主席指出，没有网络安全就没有国家安全。争夺网络舆情，要坚决维护信息领域的主权权益，坚决反对网络信息领域的双重标准；充分运用互联网思维，牢固树立内外一体的理念，疏堵控结合，特别是在自主设置话题、主动引领舆情方面下更大的功夫。从网上抓住人心，在内外信息大互动中凝聚人心，是21世纪基于网络的战胜之道。

突出“度”，按照积极进取、知止行远的理念统筹内外安全

统筹内外安全，实质上是协调内外两个大局，在以国内安全为根基和重点的条件下，需要着眼有效服务和保障国内安全，科学确立对外安全的核心理念。中国古代的兵家很讲究“度”，《尉缭子》说“无过在于度数”。统筹内外安全的战略艺术，一个具体要求就是把握好“度”。要坚持有为与有节相统一，顺势造势，有力有度，既积极进取又“知止行远”。

感悟“知止行远”的古训。中华民族正在经历伟大复兴，进取是我们民族现时代的主旋律。德国诗人歌德说：“一切优良的努力则都是从内面向外面的世界进取。” 我们的进取，既是内在性的，又是由内向外的。我们在进取的道路上面临严峻的内外双重安全考验，需要伟大的战略智慧。《老子》讲：“知止不殆，可以长久”。知止，强调的是有限而不是无限，是相对而不是绝对，是“有容”而不是排斥，是利己与利人、安己与安人的统一，是软硬实力手段运用的平衡，是自制与法治的结合。特别是要将自身安全厚植在地区共同安全的土壤中，使中国的发展强大带给地区的是福祉，防止陷入地区性安全困境，转而引发内部的不安全。也就是说，在我们勇猛前行的道路上，当我们推着经济和安全两个轮子走向世界时，要把握好节和度，知道力量使用的边界在哪里，注意保持自我克制，努力规避风险，确保达到最终目标。

探索有效斗争模式。统筹内外安全问题，在确立正确的战略指导原则的基础上，注重战略与策略相结合，积极探索一些重要领域的灵活机动、可行管用斗争模式。比如，在应对周边国家对我领土主权和海洋权益挑衅和侵害时，坚持后发制人、对等反制、强力维权，既充分占据道义法理高地，又不使对手占到便宜，还不致使事态失控升级，做到对内能顺应爱国民意，对外能打消对手贪欲和图谋，取得维权维稳的双重战略效应，赢得对内对外的双重安全效果。



在天安门地区及长安街沿线举行“全要素”阅兵预演

新概念新法则

“互联网+”的新规则

□ 陈庆修

追根求源，互联网本身就是技术工具或传输通道，就像水、电一样的基础设施。“互联网+”是与其他行业有机融合、协同增效，是大数据指导下的经营管理的科学化和柔性化，也是将“蛋糕”做得更好更大的过程。就其所激发的信息资源的巨大能量来说，这种“+”是化学反应，而非简单的物理对接。

“互联网+”以提升实体经济创新活力和市场竞争力为目标，其共性是“用户为王、互联为魂、数据为源”，主要特征如下。

“互联网+”的特征

跨界融合性。“+”是业务上的开放和跨界，是产业上的调整和重塑，也是发展要素的重组和优化。只有商品、人及其交易行为整合到互联网上，才能形成“活的数据”，进而在产业上下游、协作主体之间以最低的成本流动和挖掘。从产业链看，“+”通过对生产、分配、交换、消费流程再造，提升企业管理和客户体验，利用互联网平台的长尾效应，在满足个性化需求的同时创造出规模经济效益；从宏观上看，通过“+”的催化作用，降低市场交易和组织成本，为产业智能化提供支撑，增强经济发展新的动力。

创新驱动性。“+”的关键是创新，不仅仅是技术上的也是思维、理念、模式上的创新。正是由于“+”的创新驱动作用，使互联网由经济运行中的“轮胎”变为“发动机”，体现出一种新的能力。“互联网+”是方式的转变和文明的变革，是推动万众创新大众创业的利器。以网络为载体的知识社会创新2.0模式，以互联网思维来求变革，在为用户创造价值的同时成就自身价值，全面降低创新创造创业成本，是具有信息时代特征的创新升级版。

连接开放性。“+”依托信息技术手段打破行业垄断，连接一切可连接的人或物，把以往孤立的资源连接起来，破除有形和无形的条条框框，让开放的生态把以往制约创新创造创业的消极因素化解掉。“互联网+”的连接开放性，让研发由市场驱动，更好地把脉人的体验、重视人的创造、尊重人的作用，真正体现以人为本。

“互联网+”走向未来的希望

转型升级新支点。乘着“互联网+”的顺风，转向信息化、网络化、专业化，促进产业升级，成为现代企业的必然抉择。为此，企业的业务结构要调整和优化，使之呈现金字塔型，底层是基本业务，中层是增值业务，高层是定制业务，以实现其价值创造呈倒金字塔的理想结构：底层价值很小，中层价值较好，高层价值最大。如果企业仅定位于基本业务，创造价值就有限，唯有向增值业务和定制业务倾斜，向服务领域升级，方可创造全新的更大价值。

成败关键看品质。不论是日臻成熟的网络购物、在线支付，还是方兴未艾的微商，互联网提供的主要是渠道，影响的重点是营销模式。经营产品或服务是企业最重要的基础，无论以“互联网+”为代表的主流经济模式怎样发展，先进技术和过硬品质是永恒追求，为用户提供满意的产品或服务才是最终目的。“互联网+”要求企业专注于产品主业，发扬工匠精神，精耕细作，精益求精，将产品或服务做到极致；反之，不围绕公司主业而去追求简单的“互联网+”，没有好产品或服务作保障，再先进的理念也是空中楼阁。

信用安全保长效。“互联网+”持续健康发展，需要加强安全规范，强化风险监测，完善市场监管和社会管理，保障网络和信息安全，保护公平竞争。除了技术因素外，建立互联网征信体系是其中防范风险的重要途径。要从信用档案系统着手，配合征信体系建立大数据分析系统，实现信息资源共享；要加大对失信的惩罚力度，完善以市场为基础的信用激励约束机制。

发展着力点。互联网既是“+”的前提，也是关系国计民生的重要基础设施，要做好顶层设计，制定“互联网+”发展长远战略，大力推进新一代信息基础设施建设，搭建高效开放安全的“互联网+”共享平台；在技术、标准、政策等多个方面实现互联网与传统行业的有效对接，形成与其相适应的技术--经济范式，促进互联网与传统产业融合创新；清理阻碍“互联网+”发展的政策法规，形成融合市场的监管合力，营造良好的发展环境；发挥政策的激励和导向作用，鼓励国家创新平台向企业特别是中小企业开放。

总之，“互联网+”是互联网技术的极大发展和广泛应用，是一场经济社会发展的深刻变革。它具有超常的转化和带动作用，蕴藏着促进经济转型提质增效的巨大潜力。各行各业应抓住“互联网+”的难得机遇，结合自身实际，更新观念，在推动所在行业深度融合的基础上，创造新的发展生态，进而使其效率和效益有一个大的提升。

战例启示录

美国“震网”行动及其警示

——网络空间作战进入实战化

□ 孙　强　王诗敏

2006年，伊朗重启核计划，在纳坦兹核工厂安装大批离心机，生产浓缩铀，为进一步制造核武器准备原料。以色列对此反映强烈，声称要像1981年空袭伊拉克核反应堆那样，对伊朗核工厂进行一次外科手术式打击。当时，美国处于两难境地：一方面，美方无法接受伊朗拥核的事实；另一方面，又要极力安抚以色列这个小兄弟，劝其尽量不要单方面采取军事行动，力避局面失控。

当时，美国军方适时提出了“运用网络武器阻滞伊朗铀浓缩进程”的建议。时任美国总统布什认为值得一试，因此批准启动了由美国国家安全局、中央情报局和以色列军方共同参与，代号为“奥运会”的绝密项目。2009年1月，新任美国总统奥巴马批准继续实施该项目，并明确指示，相关行动应在可控状态下进行，避免“级联效应”伤及自身；同时行动必须隐秘进行，以免因行动暴露引发不必要的国际争端。

美方经过一段时间的情报侦察发现，伊朗方面高度重视核设施的安全工作。为了防止遭到网络攻击，伊方在建设之初，即将其核设施内部计算机与互联网实施了严格的物理隔离，因此，使用传统网络攻击方式很难对伊核设备进行有效破坏。美军迅即调整策略，提出了将病毒植入伊方相对独立的内部网络，采取实施离线攻击方式达成作战目的的设想，并明确了两项重点工作：一是尽快找到将病毒植入伊朗核设施网络的渠道；二是研发新型病毒—“震网”，使其具有进入伊核网络后“自主控制”“离线攻击”的能力。

但是，直到2009年8月，美方仍未展开对伊朗核设施的有效网络攻击。眼看伊朗核计划不断取得进展，以色列方面最终沉不住气，决心独自展开行动。以方派出大量情报人员，专门针对开发工业控制软件的高技术公司展开情报搜集，逐步摸清了伊朗核工业控制软件的开发过程。以方获悉，伊朗凭借与马来西亚同是伊斯兰国家、风俗习惯相通并保有良好经贸关系的有利条件，将核工业控制软件的开发权交给了一家具有综合集成能力的马来西亚软件公司。该软件公司又将具体的软件研发工作外包给了一家印度软件公司，由印度软件公司具体编写全部或部分代码。在掌握情况的基础上，以色列决心抛开美国，在马来西亚另建指挥控制中心，直接组织实施对伊核设施的网络攻击。通过实施受控的、相对大范围内的病毒传播，以色列最后确定了伊朗核工业控制软件的开发者，并向其释放了攻击负载。马来西亚软件公司在不知情的情况下，将印度软件公司开发的、夹带“震网”病毒的离心机控制软件交给了伊朗。2010年6月，该软件在运行几周后，“震网”病毒爆发。

“震网”病毒极具毒性和破坏力，其代码编制非常精密，是世界上第一款专门定向攻击现实世界基础能源设施的“蠕虫”病毒。该病毒采取了多种先进技术，具有极强的隐身性和控制力。只要电脑操作员将被病毒感染的U盘插入USB接口，这种病毒就会在神不知鬼不觉的情况下，侵入工业专用电脑系统，并取得一些设备的控制权。同时，“震网”病毒还具有“瞒天过海”的功能：一方面，病毒会控制并破坏伊朗核设施的离心机设备，使其运行失控、高温自毁；另一方面，病毒还不断向主控机房监控系统回传“设备正常运转”的假指令，让操作人员误认为设备一切运行正常。当伊朗核设备管理部门发现问题时，已有近1000余台离心机因过热出现了永久性物理损坏，伊方不得不暂停浓缩铀进程。

由于病毒攻击行为十分隐秘，破坏发生的起初，伊朗方面并未引起重视，仅仅认为核工厂离心机出现的一系列问题，是由设备的“技术故障”造成的。直到2010年6月，国际互联网上出现“震网”病毒的相关情况介绍后，才引起伊朗方面的警觉。但伊朗方面为保持强硬形象，始终不肯承认遭到病毒袭击。与此同时，美国和以色列也保持了高度沉默。于是出现了“受害方”不肯承认，“作案方”没人认领的怪象。

直到2012年美国《纽约时报》才爆出“震网”行动的谜底。2013年7月，德国《明镜周刊》也曝料，美国“棱镜门”泄密者爱德华·斯诺登透露，美国国家安全局与以色列一起创造了袭击伊朗核计划的“震网”病毒，这才进一步证实和曝光了有关“震网”行动的作战经过。

“震网”行动，是历史上首次在没有爆发武装冲突、没有造成人员伤亡的情况下，通过虚拟空间对现实世界实施攻击破坏，并直接达成战略目的的军事行动。它标志着网络空间作战正式进入实战化时代，在人类战争史上写下了新的时代篇章。同时，“震网”行动也给我们维护国家安全，带来了一些重要警示。

首先，随着网络空间的发展，国家边疆由有形拓展到无形，网络边疆已成为主权国家的“新边疆”。国家间的一些对抗行动已经在网络空间展开，面对网络空间的无声厮杀和严峻形势，我们必须积极应对网络空间的安全威胁，树立网络空间“新边疆”的思想观念，守卫网络边疆，巩固网络国防，围绕维护网络空间安全和网络空间控制权，加强网络空间军事斗争准备，将网络边疆提高到与有形边疆同等重要的地位，并将网络国防作为国防建设的新质成分和重要内容统筹考虑。

其次，抢占技术制高点是获取网络空间安全的必由之路。网络空间安全控制权的取得，需要软件、硬件实力的综合支撑。虽然当下我国信息化建设、军队信息化建设加速推进、成效明显，但应清醒地看到，我国现有信息化设施中许多软件操作系统、硬件设备及外接配套设备都源于进口，缺少自主知识产权，容易受制于人、受控于人。需要高度警惕少数别有用心的国家，凭借其信息技术的高端优势，在芯片、软件等技术产品上“预留后门”，安装程序“定时炸弹”，妄图控制我方系统、瘫痪我方网络。这种网络技术上的相对劣势，平时可能仅仅对经济带来影响，但在某个时候则可能对国家安全带来严重打击。因此，必须立足国情，以强烈的紧迫意识加快创新驱动，实施军地联合公关，加大计算机访问控制、可信计算等信息安全建设力度，切实解决受制于人的问题，从源头上和基础上建强网络空间防护的“金钟罩”“铁布衫”。

第三，网络空间作战隐蔽性强、潜伏期长，必须时刻保持高度的网络安全防范意识。“间谍就在身边”“敌人就在眼前”，这些话用来形容网络空间领域极为准确。网络攻击行动往往采取“施放病毒、战略预置，瞅准时机、一战制敌”的方式组织实施。“震网”行动警示我们，所谓“物理隔离”的网络并非绝对安全，现实中各类监控设备显示“一切正常”的网管系统也并非绝对可靠。需要警惕的是，当前我国各类交通、能源、金融、电力、化工等基础设施网络以及军事信息系统网络中，是否也潜伏着各类病毒？也许不是没有，而是没被发现；也许不是没有被发现，而是病毒没有到达需要爆发的时候。因此，必须时刻保持高度的网络安全意识，在建网、用网、管网、治网等各个方面加强管控监督，细化制定明确的制度规范和操作细则，建立健全全寿命、全过程的网络安全管理机制。

第四，必须着眼新型作战领域特点规律，不断创新克敌制胜的新战法。“震网”行动以“不出一兵一卒、不费一枪一弹”的网络作战行动，顺利达成了以往只有实施军事行动才能实现的战略目的。“震网”病毒缓慢运动的轨迹、秘密控制机器的能力，以及其已实施攻击破坏但攻击方始终没有现身的作战方式，直接颠覆了传统作战观念，必将永远改变国际安全和外交策略，颠覆并开创军事网络防务革命新时代。我军必须着眼网络空间作战的新特点、新规律，深入探索破坏敌作战体系结构、削弱敌整体作战能力的方法路子，不断创新打击敌网络关键节点、切断其主要数据链路的破网断链新型网络战法，切实掌握控网络空间作战的主导权和控制权。