DOI 10.15302/J-SSCAE-2016.06.016

网络空间安全应急与应对

于全[1]，杨丽凤[2]，高贵军[2]，寇子明[2]，翟立东[3]

（1. 中国电子设备系统工程公司研究所，北京 100141；2. 太原理工大学，太原 030024；
3. 中国科学院计算技术研究所，北京 100080）

摘要：从我国网络空间安全的现状及面临的问题出发，指出网络空间安全应从应急转变为应对，并从网络空间安全监测、网络空间安全总体保障能力及网络空间安全人才队伍建设三个方面提出了相应的转变策略。

关键词：网络空间安全；网络安全应急；网络安全应对；转变策略

中图分类号：TP393　　**文献标识码：**A

Emergency and Response for Cyberspace Security

Yu Quan[1], Yang Lifeng[2], Gao Guijun[2], Kou Ziming[2], Zhai Lidong[3]

(1. Institute of China Electronic Equipment System Engineering Corporation, Beijing 100141, China; 2. Taiyuan University of Technology, Taiyuan 030024, China; 3. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: Based on the current situation and main problems with cyberspace security in China, this paper proposes that cyberspace security should shift its focus from emergency to response. Some transformation strategies are proposed, including three aspects: network security-monitoring capacity, network security guarantee capacity, and talents construction capacity.

Key words: cyberspace security; emergency for cyberspace security; response for cyberspace security; transformation strategy

一、前言

近年来，我国在网络空间的影响力逐步扩大。据 2016 年 1 月中国互联网络信息中心（CNNIC）发布的第 38 次《中国互联网络发展状况统计报告》统计：截至 2016 年 6 月，我国网民规模达 7.1 亿，普及率达到 51.7 %，超过全球平均水平 3.1 %，超过亚洲平均水平 8.1 %[1]；中国“.cn”域名总数为 1 636 万，超过德国国家顶级域名“.de”，成为全球注册保有量第一的国家和地区顶级域名。同时，移动互联网塑造了全新的社会生活形态，“互联网 +”行动计划不断助力企业发展，互联网对于整体社会的影响已进入到新的阶段。

我国网络空间安全依旧面临非常严峻的威胁与考验，一方面网络空间安全国际形势复杂，欧美等发达国家竞相加强网络空间部署，不断增加全球网

收稿日期：2016-10-08；**修回日期：**2016-10-18

作者简介：于全，中国工程院，院士，中国电子设备系统工程公司研究所，研究员，博士生导师，主要研究领域包括软件定义无线电、移动 Ad hoc 网络、认知无线电网络、下一代无线通信网络、空间信息网络等；E-mail: yuquan61@qq.com

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)

本刊网址：www.enginsci.cn

络空间军备竞赛的风险，跨境网络攻击和网络犯罪愈演愈烈，全球性大规模的网络冲突风险加剧；另一方面，我国在网络攻防、网络空间安全产业、网络空间安全法律法规及网络空间安全人才队伍建设等方面虽然取得了不少进展，但是我国网络空间安全的总体保障能力仍然亟待提升，我国网络空间安全方面的法制、体制、机制及相关措施亟须完善[2]。

中华人民共和国国家主席习近平明确指出：没有网络安全就没有国家安全，没有信息化就没有现代化[3]。网络安全已经成为国家安全观总体框架中至关重要的一部分。因此确保我国网络空间安全、科学应对网络安全事件意义重大。

网络空间安全应急和应对是在网络安全事件的刺激下产生的两种反应。应急一般是根据相关的应急预案或者应急主体处理类似事件的经验，对已发生的网络安全事件采取的无计划的、被动的活动，属于亡羊补牢；应对则是针对已发生的或可能发生的网络安全事件采取的有计划的、主动的、科学理性的、积极的活动，属于未雨绸缪、运筹帷幄。

我们已经充分认识到，确保我国网络空间安全，不能仅仅依赖事发后的被动应急，而必须要做到科学积极应对。努力实现从应急到应对的转变需要一个过程。

二、提升网络空间安全监测能力，保障从应急到应对的转变

网络安全事件发展的三个阶段为事前、事中和事后。应急是事后恢复处置，而应对则是事前或事中的防范与紧急控制。“凡事预则立，不预则废”，从应急到应对，如果能够在事前做好防控和预警，就能够有效地应对网络安全事件。为此，在日常工作中，不仅要做到防微杜渐，更要做到见微知著。能够及时发现这个微小的不安全因素，从网络空间安全的角度讲，利用各种先进的技术和手段加强网络空间安全的监测能力是非常重要和有效的。

（一）网络监测覆盖的范围应更广泛、更完备

网络空间安全保护的对象是什么？这是网络监测首先应该明确的问题。方滨兴院士明确指出了网络空间安全的边界：网络空间安全涉及在网络空间中的电磁设备、电子信息系统、运行数据、系统应用中所存在的安全问题，既要防止、保护、处置包括互联网、电信网、广电网、物联网、工控网、在线社交网络、计算系统、通信系统、控制系统在内的各种信息通信技术系统及其所承载的数据不受损害，也要防止对这些信息通信技术系统的滥用所引发的政治安全、经济安全、文化安全、社会安全与国防安全事件。针对上述风险，需要采取法律、管理、技术、自律等综合手段来应付，确保机密性、可用性、可控性、可鉴别性得到保障[4]。

（二）网络监测覆盖的业务应更扩大

随着网络空间的扩展，在各个领域都爆发了很多的安全事件，如在移动 APP 领域，业务的多样化导致安全问题层出不穷。网络监测不能只局限于监测传统业务，而应该把业务从表态形式、抽象形式去扩大和升级，才能更准确地分析什么是应该监测的对象。

（三）网络监测覆盖的粒度应更精细

应该进行全流量监测。一般的网络监测只针对重点流量进行，忽略了许多异常事件。因此不仅需要进行全流量监测，还要对带外数据进行要素提炼，进行关键环节的重点监测，这样才能够使得覆盖的信息量越来越多。当信息量越来越多时，就能够用大数据进行深度学习，从而得到有意义的客观的印象，进而指导网络空间安全监测的重要环节。

（四）网络监测覆盖的环节应更主次分明

从网络结构上看，需要进行网络监测的环节一般最外端是网民，中间是互联网数据中心（IDC）等，最内边是骨干网。这些环节中哪些是可以合并的，哪些是必须要留意的环节，这些环节的权重是怎样的，所有这些在进行监测时都应该要定义清晰。通常骨干网上防护能力最强，向外延伸到末端的各环节其防护能力是多维的，不能采取统一标准，应该主次分明以利于监测。

三、提升网络空间安全总体保障能力，实现从应急到应对的转变

诸多因素制约着我国网络空间安全总体保障能力的提升，如我国相关网络空间安全法制、机制及体制等相对欧美等发达国家还比较落后，网络空间

安全优秀人才匮乏，网络空间安全攻防能力不足，国内网络安全产业的基础相对薄弱。要实现从应急到应对的转变，需要从根本上改变目前的网络空间安全态势。

（一）加强网络空间安全应急联动性

大规模的应急联动是改进网络安全事件应急响应、提升网络空间安全保障能力最有效的措施。然而我国的网络安全应急体系缺乏统一的顶层领导，其应急管理因网络性质内容等不同而分属不同的部门。而各级应急组织又有地域限制，这与 Internet 的地理无关性直接矛盾。在被动应急网络安全事件时，各应急主体因行政规划等原因缺乏有效的合作。因此必须尽快进行网络空间安全管理顶层设计：成立由中央直接领导的网络安全应急响应中心，建立不同部门和不同网络之间应急响应的联动机制；整合分散在不同业务部门的网络安全应急管理职能，形成地理上分散、组织上统一的网络安全应急联动系统，以提升应急效率 [5]。另外，为了进一步加强应急联动性，应该尽快建立快捷的网络安全应急情报与资源共享机制，使网络安全风险形势研判能力得到提高，为网络安全应急提供充足的预警、决策及反应时间，实现从应急向应对的转变。

（二）明确网络空间安全应急职责

长期以来，“九龙治水”的问题一直困扰着我国的网络空间安全管理。各自为政、责权不一、职能交叉等严重影响了网络安全事件的应急响应。因此以法律形式明确网络安全应急职责，是提升我国网络安全总体保障能力的重要内容。在法律框架中，网络内容管理和技术管理的法律界限需要明确，还要明确各网络安全管理部门在应急状态下的责权及地位，明确网络安全的执法部门，完善各部门的协同配合机制等 [6]。

（三）深化网络空间安全事件的国际合作

在当前互联网治理全球化的新形势下，尤其是“棱镜门”事件以来，世界各国都在积极争取网络的主导权。深化网络安全事件的国际合作，站在立法的角度声明我国的“网络主权”，扩大我国在网络空间的国际话语权，对提升我国网络空间安全整体保障能力十分重要。首先，需要以“尊重网络主权，维护网络安全”为前提，推动建立“多边、民主、透明”的国际互联网治理体系，在网络空间国际规则制定、打击跨境网络犯罪、跨境数据流动等领域深化国际合作。其次，需要利用国际电信联盟等各种国际组织加强国际网络安全的协商与对话，扩大我国网络空间的国际影响力与话语权。再次，鼓励和引导我国的企业、学术及研究机构积极参与网络安全国际交流与研究，从理论上完善全球网络空间的新秩序。

（四）健全网络安全应急标准体系

我国的网络与信息安全事件可依据《信息安全技术信息安全事件分类分级指南》（GB/Z 20986—2007）划分为 4 个级别 [7]，但是由于现有的分级危害程度和影响范围比较宽泛，很难及时转化为具体的、可量化的经济运转和社会稳定等可评估性指标，导致无法及时预警或定级网络安全事件，影响应对工作的有效开展。因此建立包括网络安全应急管理标准、技术标准、业务标准等在内的网络安全应急标准体系框架，健全网络安全应急标准体系，尤其是网络应急监测、预警、处置等标准和预案体系，都具有至关重要的意义。

四、加强网络空间安全人才队伍建设，加快从应急到应对的转变

从人才方面看，应急因为没有充分的事前预警与准备，网络安全事件已发生，为了尽快消除事件产生的影响，对事件处置人员各方面的要求都比较高；而应对因为事前准备充分，响应方案完善，兵来将挡、水来土掩，事发时对人的依赖性最低。随着网络安全形势复杂性的增加，我国网络安全人才队伍建设的短板也日益显现，如网络安全人才供需不平衡，供远远小于需，尤其缺乏高层次的领军人才；由于激励机制不合理造成人才流失，甚至成为黑客或网络犯罪分子等。因此应对网络安全事件，应该以人为本，加快网络安全人才队伍的培养。

（一）制定网络空间安全人才系统规划

加快网络安全人才培养工作的顶层设计，制定以人为本的人才系统规划，培养和造就结构优化、布局合理、素质优良的人才队伍，对于保障我国网

络空间安全人才的延续性及核心技术的自主创新意义重大。2015 年 6 月，我国正式将“网络空间安全”列为一级学科 [8]，在明确人才培养的总体部署、制定人才培养计划、调整结构计划、优化资源配置等方面迈出了重要的一步。

（二）健全网络空间安全人才培养机制

网络空间安全人才培养以普通高等教育为主，辅以职业高等教育、社会培训等。由于行业知识更新快，面临的问题复杂度高，还需要解决网络空间安全从业人员的继续教育问题。健全网络空间安全人才培养机制，高校、研究院所、企业等可以尝试通过市场化方式，开放攻防平台、国家级网络靶场等，加大网络空间安全专业人才和复合型人才培养力度。另外需要建立相关的人才考核和激励机制，充分调动培养者与被培养者的积极性和主动性。

（三）推进网络空间安全领域领军人才培养

习近平主席指出：要不拘一格降人才，解放思想，慧眼识才，爱才惜才。对待特殊人才要有特殊政策，不要求全责备，不要论资排辈，不要都用一把尺子衡量 [9]。因此，应该在网络空间安全领域实行特殊人才的专项资金、建立领军人才的特殊考核和薪酬制度、设立重大研究计划、有重点地培养青年学科带头人等，引进和培育一批网络空间安全的领军人才。另外还可以在具有相对优势的科研单位建设若干不同安全方向的重点创新团队 , 形成一批高层次人才的培养示范基地。

五、结语

绝对的安全是不存在的，互联网的基本属性是协作与共享，丧失了这个基本属性的安全也是没有意义的。因此，要加强网络空间安全战略研究，提升网络安全监测能力，提升网络安全总体保障能力，加快网络安全人才队伍建设，实现网络空间安全从被动应急型向主动应对型、从传统经验型向现代高科技型的战略转变，对我国从网络大国转向网络强国，全面提升国家安全能力具有十分重要的意义。

参考文献

[1] 中国互联网络信息中心. 第38次中国互联网络发展状况统计报告 [EB/OL]. (2016-08-03)[2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm.
China Internet Network Information Center. The 38th statistical report on internet development in China [EB/OL]. (2016-08-03) [2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm.

[2] 国家计算机网络应急技术处理协调中心. 2015年我国互联网网络安全态势综述[EB/OL]. (2016-04-22) [2016-10-08]. http://www.cert.org.cn/publish/main/12/2016/20160422085056915532001/20160422085056915532001_.html.
National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). 2015 China internet network security situation summary [R/OL]. (2016-04-22) [2016-10-08]. http://www.cert.org.cn/publish/main/12/2016/20160422085056915532001/20160422085056915532001_.html.

[3] 中国共产党新闻. 习近平的网络观: 没有网络安全就没有国家安全[EB/OL]. (2014-11-20) [2016-10-08]. http://cpc.people.com.cn/xuexi/n/2014/1120/c385475-26061137.html.
News of the Communist Party of China. Xi Jinping’s view of the network: No network security, No national security [EB/OL]. (2014-11-20) [2016-10-08]. http://cpc.people.com.cn/xuexi/n/2014/1120/c385475-26061137.html.

[4] 方滨兴：网络空间安全包括四个层面的安全[EB/OL]. (2015-12-16) [2016-10-08]. http://tech.qq.com/a/20151216/051549.htm.
Fang B X. Cyberspace security includes four levels of security [EB/OL]. (2015-12-16) [2016-10-08]. http://tech.qq.com/a/20151216/051549.htm.

[5] 冯涛, 张玉清, 高有行. 网络安全事件应急响应联动系统模型[J]. 计算机工程, 2004,30(13):101–103.
Feng T, Zhang Y Q, Gao Y X. Network security incident response linkage system model [J]. Computer Engineering, 2004,30(13):101–103.

[6] 孙佑海. 论我国网络安全面临的十大问题和立法对策[J]. 中国信息安全, 2014(10):40–43.
Sun Y H. Ten problems and legislative strategy of China’s network security [J]. China Information Security, 2014(10):40–43.

[7] 中华人民共和国国家质量监督检验检疫总局. 信息安全技术——信息安全事件分类分级指南. GB/Z 20986-2007[S]. 北京: 标准出版社, 2007.
General Administration of Quality Supervision, Inspection and Quarantine of the People’s Republic of China, Standardization Administration of the People’s Republic of China. Information security technology—Guidelines for the category and classification of information security incidents. GB/Z 20986-2007[S]. Beijing: Chinese Standards, 2007.

[8] 教育部国务院学位委员会. 教育部关于增设网络空间安全一级学科的通知. 学位[2015]11号[Z]. 北京, 2015.
The Academic Degrees Committee of the State Council, The Ministry of Education. Notice on setting up the first level discipline of cyber space security. Degree [2015] No.11 [Z]. Beijing, 2015.

[9] 新华通讯社. 习近平总书记在网络安全和信息化工作座谈会上的讲话[EB/OL]. (2016-04-25) [2016-10-08]. http://www.cac.gov.cn/2016-04/25/c_1118731366.htm.
Xinhua News Agency. The speech of Xi Jinping on the network security and information work conference [EB/OL]. (2016-04-25) [2016-10-08]. http://www.cac.gov.cn/2016-04/25/c_1118731366.htm.