Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Cybersecurity—Article

构建新型网络空间安全生态体系　实现从网络大国走向网络强国

杨小牛[a,*]，王巍[a]，许小丰[a]，庞国荣[b]，张春磊[a]

[a] Science and Technology on Communication Information Security Control Laboratory, Jiaxing, Zhejiang 314033, China
[b] Science and Technology on Electro-Optical Information Security Control Laboratory, Tianjin 300300, China

ARTICLE INFO

Article history:
Received 9 February 2017
Revised 26 Mar 2017
Accepted 3 May 2017
Available online 1 Aug 2017

关键词
网络空间安全
生态体系
SMCRC 环
网络空间三分论

摘要

首先面向我国网络空间实际情况，提出网络空间“三分论”，针对公共互联网（C 空间）、党政军保密网（S 空间）和关键基础设施网（K 空间）三大网络空间的不同需求，给出了相应的安全应对策略和研究框架。然后重点针对公共互联网，探讨了基于 SMCRC 环（situation awareness，monitoring，cooperative defense，recovery，countermeasure）的网络空间安全生态体系的功能特点和内在信息交互方式，并分别对“SMCRC 环”中态势感知、持续监控、协同防御、快速恢复、溯源反制等五大环节的核心关键技术进行了讨论，以期对国家网络空间安全研究起到抛砖引玉之作用。

1. 引言

随着我国网络空间应用的不断普及以及对网络空间依赖程度的不断增加，网络空间安全性问题日益凸显，中国在网络空间内所面临的现实和潜在威胁也不断提升。网络空间安全问题已成为国家心腹大患，严重威胁到国家安全。正如习主席指出的：“没有网络安全，就没有国家安全。”

在网络空间安全领域，我国目前所面临的主要现实问题可概括为：欺诈多发攻击猖獗，网络安全形势严峻；持续监控难以实现，被动封控效果有限；产业薄弱后门敞开，供应链受控于人；防御分散响应缓慢，攻防管控各自为战；溯源反制基础薄弱，网络空间威慑无从谈起。而世界一些发达国家在网络空间安全领域形成了巨大的技术优势，并将在网络空间的这种技术优势适时转换为产业优势，通过技术出口、产品供给、市场垄断，获得种植后门和隐匿漏洞的卖方优势，进而在网络空间取得信息单向透明和行动绝对自由的战略优势[1–5]。这种情况导致在相当长时期内我国的信息化建设不得不使用“有毒带菌”的构件，并且在相当长时期内网络空间安全体系也不得不基于“有毒带菌”环境来构建。面对复杂多变的网络空间安全形势，我们必须开拓创新、敢为人先，提出切实有效的网络空间安全应对策略，有力支撑建设“战略清晰、技术先进、产业领先、攻防兼备”的网络强国战略目标的实现。

* Corresponding author.
E-mail address: jec@jec.com.cn (X.-N. Yang).

2095-8099/
英文原文: Engineering 2018, 4(1): 47–52
引用本文: Xiao-Niu Yang, Wei Wang, Xiao-Feng Xu, Guo-Rong Pang, Chun-Lei Zhang. Research on the Construction of a Novel Cyberspace Security Ecosystem. *Engineering*, https://doi.org/10.1016/j.eng.2018.01.003

2. 分而治之的网络空间安全应对策略

网络空间安全问题层次多样、错综复杂，应优先关注影响国家政权稳定、经济发展、军事安全的重大网络空间安全问题，即国家层面的网络空间安全问题。另外，不同类型网络特点不尽相同，安全诉求也不相同，因此解决的重点和思路也不尽相同，必须采取分而治之的网络空间安全应对策略。

2.1. 三大网络空间特点与安全需求分析

公共互联网（C空间）、党政军保密网（S空间）和关键基础设施网（K空间）这三类网络功能不同，各有特点。如图1所示，公共互联网是指全球连通的网络，威胁来源广泛，具有开放、互联、技术体系国际通用等特点，是网络空间攻防博弈前沿阵地。党政军保密网是指对国家主权具有重要影响的军事、政治、外交等网络，它是行使国家独立主权、维护国家安全的核心系统，承载国家重要秘密信息，是网络空间信息安全固守阵地。关键基础设施网是指对国家利益具有重要影响、对外开放的网络，与公共网络互联，并支持国家关键基础设施（电力、交通、金融、工控）运行，是网络空间防御主战场。

三类网络的特点不同，安全需求也有区别，如表1所示。公共互联网主要要求保障关键服务安全可控，维护网络空间良好生态、保障公民网络空间合法利益、提高网络安全态势感知和预警处置能力及网络安全监管能力等。党政军保密网主要要求国家秘密信息万无一失，确保政治、外交、军事行动任务的成功开展。关键基础设施网主要要求国家关键基础设施正常运行，保障关键应用可信安全，确保我国能源、交通、金融等核心应用的正常运行。

2.2. 安全应对策略

根据我国的现实情况，我们提出网络空间“三分论”的思想，即把网络空间分为公共互联网、党政军保密网、关键基础设施网共三大类。这三类网络的特点、安全需求差异明显、各有侧重，因此，应因地制宜，利用分而治之的应对策略，从易到难、彻底解决我国网络空间存在的问题。

以三大网络空间划分为基础，本文给出网络空间安全研究框架如图2所示。对于公共互联网空间，其对应的安全策略是构建网络空间安全生态体系，确保互联网服务安全[6–8]；对于党政军保密网，其对应的安全策略是构建自主安全网络，确保信息安全，严防信息泄露；对于关键基础设施网，其对应的安全策略是构建固若金汤的主动安全防护体系，确保应用安全[9,10]。同时，网络空间安全一体化战略还必须依托三大支撑平台，即全域（从互联网数据到安全威胁情报）的信息共享平台、统一的身份认证平台、综合的试验评估平台来加以实施。

综上所述，必须统筹区分公共互联网、党政军保密网络、关键基础设施网络三类网络的不同需求，有针对性地开展研究攻关。对于公共互联网，借鉴生态和免疫的思想，发展网络空间生态体系协同能力，加强网络治

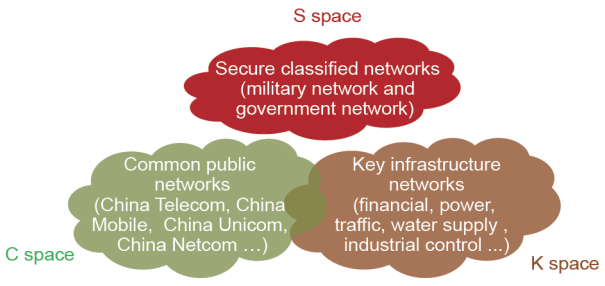

图1. 三类网络示意图。

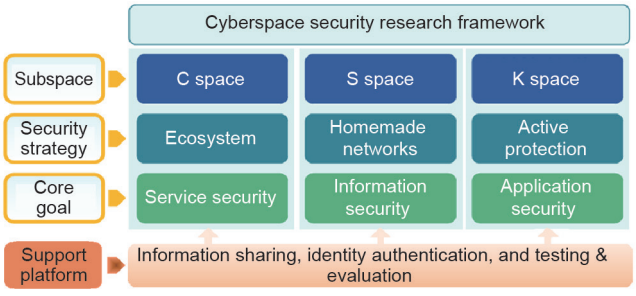

图2. 网络空间安全研究框架。

表1 三类网络不同的安全需求

Subspace	Security requirement	Effect to achieve
C space	• A healthy and orderly cyberspace security ecosystem • Critical services ensured and trusted	Illegal acts must be caught
S space	• Absolute safety for important national secrets • Secure and manageable critical information	Sensitive information remains unrevealed
K space	• Proper operation of critical infrastructure • Secure and reliable critical applications	Core services are impregnable

理、管控和防护，形成态势感知、持续监控、协同防御、快速恢复和溯源反制的联动协同处置能力。对于党政军保密网，采用本质安全的思想，通过研制新型安全网络和计算架构，实现产业链重要产品的自主、可控、安全、可信，杜绝隐患，捍卫国家核心利益，形成自主可控的安全防护能力。对于关键基础设施网，利用动态博弈的思想，实现网络主动防护体系，通过纵深、动态、弹性的网络安全防护手段，形成层层限制、抵御攻击，增加攻击代价，保障核心业务，快速状态重置的主动防护和应急恢复能力。

下面，我们主要针对公共互联网的安全需求讨论网络空间安全生态体系构建设想。

3. 网络空间安全生态体系——SMCRC 环

由于我国公共互联网空间面临多种多样的安全威胁，所以不能依靠单一的网络安全防御技术确保网络空间的安全性，而应该能够根据外界环境自我调节、协调安全能力，保证网络系统正常运行。即通过跨域协同共享建立全域监测、主动防护、快速反应、精准溯源的大协作机制，构建新型的网络空间安全生态体系应对安全威胁，将安全威胁消灭在初期状态。

在这一网络空间安全生态体系中，各种安全手段将成为内置网络属性，网络节点之间通过协同方式交换可信信息、共享安全策略，调配不同的安全手段，形成针对不同事件的安全处置能力，达成期望的网络空间安全服务，如近实时阻止网络攻击、限制攻击传播范围、最小化攻击危害程度、快速恢复网络状态等。

因此，本文提出了一种基于SMCRC（situation awareness，monitoring，cooperative defence，recovery，countermeasure）环的网络空间安全生态体系，如图3所示。该体系中，通过身份认证、信息共享、试验评估三大基础支撑平台将态势感知、持续监控、协同防御、快速恢复、溯源反制等多项网络安全功能进行有机整合，形成网络安全动态生态体系，确保网络舆情有序管控、用户隐私安全可控、网络设施可信受控、安全事件溯源能控。

3.1. 网络空间安全生态体系的功能特点

SMCRC环是个有机的整体，数据在环中流动起来，可将整网安全资源配置合而为一，形成彼此互相支撑的统一安全生态环境。在SMCRC环中，五个核心功能和三大基础支撑平台缺一不可。

（1）从环的角度来说：S（态势感知）为M（持续监控）提供感知数据支撑；M为C（协同防御）提供预警信息；C是R（快速恢复）的前提，为自动响应与快速处置提供保障；R为C提供攻击样本数据库，使其可以做到精确溯源，从而实施反制威慑；C返回来又为S（态势感

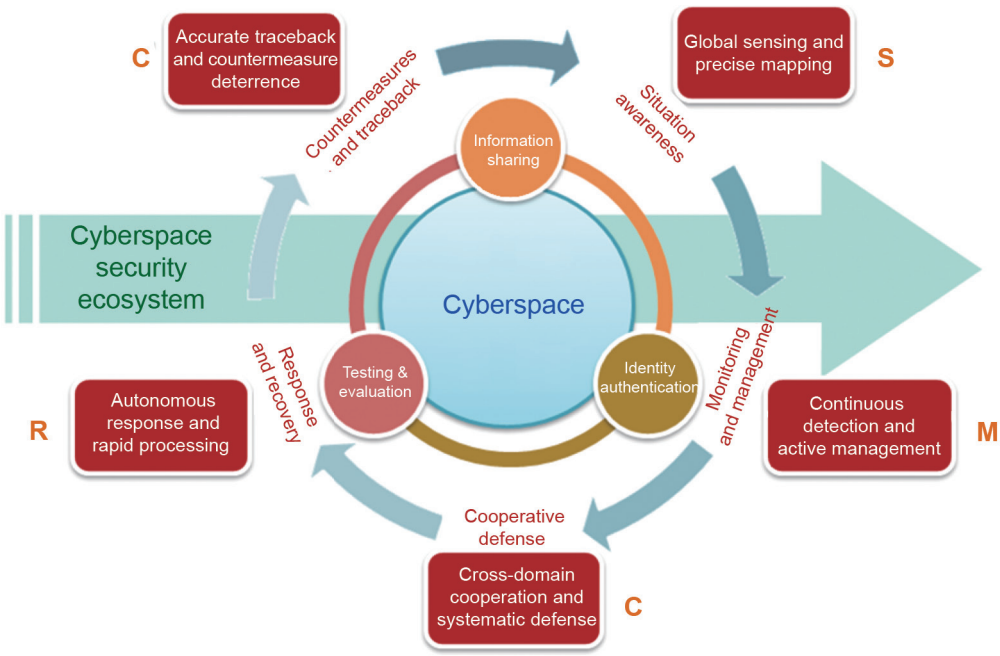

图3. 基于SMCRC环的网络空间安全生态体系。

知）提供获取网络入侵方的情报内容及反制结果信息，从而丰富全球感知与精确测绘的内涵。

（2）从平台支撑角度来说：要使环流动起来，需要建设信息共享、身份认证、试验评估三类基础平台进行支撑。三大平台可为SMCRC环系统构建提供如下支撑能力：①提供数据实时采集能力，为不同部门、领域、机构提供统一的网络数据服务和威胁情报共享服务；②确保网络各参与方身份可信，支持网络空间安全身份统一管理，提升取证、溯源、归因、防御、定向威慑能力；③提供统一的试验、测试、评估、认证环境和攻防演练等相关服务，确保网络安全技术、产品的有效性和实用性。

3.2. 安全生态体系内在信息交互

对于安全生态环境来说，各组成部分之间的相互作用是无时不在、无处不在的。因此，SMCRC环中各部分数据流没有严格的流向限制。例如，态势感知的数据可直接发送到溯源反制使用；持续监控的结果可为快速恢复提供参考。SMCRC环诸要素之间的信息交互矩阵如表2所示。

4. SMCRC 环关键技术体系

围绕公共互联网的具体安全需求，建设网络空间安全生态体系SMCRC环需要解决以下关键技术。

4.1. 态势感知——全球感知、精确测绘

针对我国网络态势掌控能力囿于国内、无法及时发现高级持续性威胁（advanced persistent threat，APT）类攻击以及网络资源测绘能力限于公网的问题，我们认为态势感知技术应从数据全域获取、网络深度探测这两方面入手，重点关注全球感知和精确测绘。

（1）在全球感知方面，研究网络多点侦测、分布式数据获取、海量数据融合分析、隧道协议深度分析、恶意行为识别、攻击数据关联与挖掘分析方法，通过多种手段获取境内外网络数据并进行融合分析，形成全球关键网络设施、系统、节点的全方位感知能力，把握全网的运行状态。

（2）在精确测绘方面，研究暗网探测分析、网络动态资源探测、网络资产关联分析、分级网络地图绘制、多粒度态势呈现等方法，多角度综合分析各种网络资产的时间、空间、网络特征，实现对网络资源、交互关系、安全事件、威胁等级等网络特征的分级、深度测绘能力，为不同领域部门提供各自需要的细粒度、多层次的网络资产蓝图。

4.2. 持续监控——持续监测、主动管控

针对我国目前无法对全网数据进行不间断的及时监测分析以及被动封堵手段难以有效管理网络空间的困境，本文认为持续监控应从网络大数据压缩存储、网络数据线速深度分析、网络行为正向引导等方面入手，着力形成持续监测、主动管控能力。

（1）在持续监测方面，研究分级式网络数据无损监测、海量网络数据分布式处理和融合分析、深度全域网络数据快速处理等方法。通过构建多级网络数据监测系统，在保护用户隐私的前提下实现对网络数据的全方位、深层次、高持续、近实时监测分析，为国家部委机关提供有效的网络治理手段。

（2）在主动管控方面，研究面向用户的网络数据实时推送、网络用户行为预测、网络群体行为引导干预、多源多语种多媒体快速舆情分类、涉恐网络信息深度关联分析、非法网络数据清洗等方法。通过构建网络行为正向引导系统，对网络上影响政权稳定、社会安定、经济发展的违法犯罪、恐怖活动、颠覆行动及时阻止处置，

表2 SMCRC环诸要素之间的信息交互矩阵

	Situation awareness	Monitoring and management	Cooperative defense	Response and recovery	Countermeasures and traceback
Situation awareness		Situation-awareness data	Threat data	Threat data	Reconnaissance data
Monitoring and management	Monitoring result		Early warning information	Damage information	Monitoring data
Cooperative defense	Defense result	Management and control time		Response time	Data support
Response and recovery	Response result	Response result	Response result		Attack sample
Countermeasures and traceback	Attribution result	Countermeasure result	Defense support	Response to threat	

引导大众形成健康有序、合法文明的网络行为习惯。

4.3. 协同防御——跨域协作、体系防御

面向国内网络职能部门协调时效慢、多种网络防御系统各自为战、无法形成体系化网络防护能力的问题，协同防御技术应从情报共享、入侵行为跨域引导阻断、安全策略协同等层面出发，实现跨域协作、体系防御。

（1）在跨域协作方面，研究网络空间协同防御任务设计、跨域网络安全策略协同、面向任务的多系统分级协作等方法。通过任务多领域协同、策略一致性协同、处置行动分级协同，实现侦察、预警、防御、反制、指挥、管理等力量在行动层面的跨域协作和融合，解决跨部门、跨领域的深度协作问题。

（2）在体系防御方面，研究一体化网络空间安全协同防护体系架构、基于网络威胁情报的协同防御、网络资源智能调度、网络动态防御、网络入侵行为引导阻断欺骗协作处置等方法。从系统体系的角度出发形成一体化网络安全架构，达到计划合理统筹、行动协调一致、合力攻坚克难的效果，极大提升对网络空间威胁识别、定位、响应和处置等行动的能力和效率。

4.4. 快速恢复——自动响应、快速处置

美国的网络空间安全战略认为：无法确保网络空间绝对安全、网络攻击不可避免，“固守城池”防御低效而且成本高昂，但是可以通过种种手段缓解网络攻击的后果，网络快速恢复能力至关重要。

针对网络被攻击后防御分散响应缓慢的现状，我国也应大力发展网络快速恢复技术，从网络事件处置行动自动化、网络可重构设计、网络系统重建、网络服务和数据恢复等方面入手，聚焦自动响应、快速处置能力。

（1）在自动响应方面，研究网络行动过程自动处理、网络事件处置标准化设计等方法。

（2）在快速处置方面，研究网络系统快速重建、网络服务重构自愈、网络数据可信恢复、基于虚拟化的网络自修复等方法。

通过可重构、模块化、虚拟化的系统、网络、服务、数据架构设计，实现自动化、标准化、快速化的网络事件响应处置，以最快速度达到阻止入侵事件、限制破坏范围、减小攻击影响、恢复关键服务等网络安全目标，保障核心网络业务的正常安全运行，从而减轻网络攻击危害，降低网络安全事件对社会、政治、经济活动影响。

4.5. 溯源反制——精确溯源、反制威慑

针对我国目前非合作网络的溯源分析能力以及反制过程智能化、自动化能力欠缺的现状，本文认为溯源反制关键技术应重点强调精确溯源与反制威慑。

（1）精确溯源：实现对敌攻击路径分析、行为特征提取、攻击方式取证能力，针对网络实体在不同层面的特点，结合生成的网络行为画像，研究自适应选择网络流量水印载体的追踪攻击溯源技术，较大可能实现对使用跳板节点主机、匿名通信系统、僵尸网络等手段隐藏真实身份的网络攻击溯源，结合黑客指纹库，进一步准确定位非合作攻击者的具体位置，为精确溯源提供技术支撑。

（2）反制威慑：实现反制手段的隐蔽化，从通信、系统、存储、进程、抗查杀、防检测等方面对反制行为进行隐匿；研究网络空间威慑机理，从原理上探索在网络空间中与重要对手实现战略平衡的可能性；在掌握目标网络漏洞分布的基础上，研究针对目标区域内具有同类漏洞的网络节点、应用系统实施批量化自动反制方法，实施大规模反制，达到对目标区域内的大量节点、应用的控制、瘫痪等效果，达到吓止和报复的威慑效果。

4.6. 支撑平台

除了上述与SMCRC环紧密耦合的技术以外，还需要开发一些共性、基础性技术，才可确保基于SMCRC环的网络空间安全生态体系的正常运行。具体技术包括：全域信息共享、统一身份认证、综合试验评估三大支撑平台技术。

（1）全域信息共享：目前我国网络空间攻、防、管、控四个体系分属不同的部门管理，相互之间缺乏有效的信息共享和交换、共同态势感知和联合分析手段。因此，需要研究新型网络安全体系架构、监测预警、协同防御、网络反制等各项技术，利用网络云平台构建一体化信息共享、统一态势感知、联合数据分析平台，从而为网络空间资源整合、控制、应用提供一体化共享平台；促进网络空间攻、防、管、控之间不同管理部门、执行系统之间的横向协作，支持国家、省、市、县等各级单位之间的纵向协作。通过信息共享技术，把各部门、各军种、各高校、各企业的能力联系起来，以支撑形成整个网络空间的安全体系，起到1+1>>2的效果。

（2）统一身份认证：在网络空间中，存在大量的身份欺骗和身份窃取现象，网络罪犯和其他攻击者可利用个人、网站、邮件系统、基础设施中的身份标识的薄

弱性，对整个网络空间进行破坏。因此，需要建立具有可信、不可抵赖标签的网络空间个人身份识别平台。网络空间身份认证需要结合个人、组织、计算和通信设备、网络、信息系统、应用和数据等各方面进行一体化可信标识，即对人的身份、机器的身份、程序的身份进行统一化综合，从而将网络空间中的数据身份与真实世界中的个人身份一一映射起来，为阻止网络欺诈、监控舆情煽动、溯源恶意攻击等网络行为提供支撑，促进取证、防御、定向威慑能力，实现国家网络空间可信身份战略。

（3）综合试验评估：随着网络空间技术的发展，传统测试与评估遇到了越来越多的挑战，被测试对象由单个系统向联合的复杂网络和信息系统演变，测试与评估难度大幅增加，对测试与评估人员、技术和设施的要求更高。为了调动国家与社会的各种资源，突破军与民、政府与企业、高校与研究所的界限，需要共同建设“联合任务环境试验平台”（国家网络空间靶场），对网络空间的各种复杂协议、软硬件信息系统中存在的漏洞、后门、脆弱性进行纵向、横向深入分析，为网络空间安全系统、产品提供统一的试验、测试环境，验证评估网络防护、检测、响应、恢复能力，为国家网络空间靶场建设提供技术支撑。

5. 结语

1935年7月英国植物生态学家坦斯利（A. G. Tansley，1871—1955）在《生态学》杂志中首次提出生态系统（ecosystem）的概念[11]，目前这一概念的外延已经扩展到了多种领域，网络空间更是一个典型的生态系统。

网络空间安全生态系统具备防御动态化、元素可认证、行为可监控、全系统态势可感知、功能可自演进、本质安全等能力。要实现这些能力，还需要很多层面的努力、很长时间的改进、很多机构的协同、很多政策的指导，非一日可就。

美国国土安全部高层也曾表示，“完美的网络生态系统也许永远都无法打造出来”。但不管怎样，人类既然打造出了网络空间，就同样背负上了将其打造成一个健康、有序、自洽生态系统的责任，这一责任无法回避，亦无法回头。

Compliance with ethics guidelines

Xiao-Niu Yang, Wei Wang, Xiao-Feng Xu, Guo-Rong Pang, and Chun-Lei Zhang declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Applegate SD. The principle of maneuver in cyber operations. In: Czosseck C, Ottis R, Ziolkowski K, editors. 2012 4th International conference on cyber conflict: proceedings; 2012 Jun 5–8; Tallinn, Estonia. Tallinn: NATO CCD COE Publications; 2012. p. 1–13.
[2] Office of the US Air Force Chief Scientist. Cyber vision 2025: United States air force cyberspace science & technology vision 2012–2015. Report. Washington, DC: US Department of the Air Force; 2012 Dec. Report No.: 2012–0439/460/715.
[3] Cyber Priorities Steering Council. Cyber S&T priority steering council research roadmap. Washington, DC: US Department of Defense; 2011 Nov.
[4] Desk N. Cyber maneuvering and morphing—Are defense networks on course to “self awareness”? [Internet]. Qadima: Defense Update; c2002–2017 [updated 2012 Jul 21; cited 2017 Jul 26]. Available from: http://defense-update.com/20120721_raytheon-to-develop-cyber-maneuver-technology-for-us-army.html.
[5] Marlborough M. Raytheon to develop cyber maneuver technology for US Army: Proactive cyber approach to improve network defense in high-threat environments [Internet]. Waltham: Raytheon Company; c2015 [updated 2012 Jul 16; cited 2017 Jul 26]. Available from: http://raytheon.mediaroom.com/index.php?s=43&item=2136.
[6] US Department of Homeland Security. Blueprint for a secure cyber future: the cybersecurity strategy for the homeland security enterprise. Washington, DC: US Department of Homeland Security; 2011 Sep.
[7] Reitinger P. Enabling distributed security in cyberspace: building a healthy and resilient cyber ecosystem with automated collective action. Washington, DC: US Department of Homeland Security; 2011.
[8] Dombroski MJ, Carley KM. NETEST: estimating a terrorist network’s structure—Graduate Student Best Paper Award, CASOS 2002 Conference. Comput Math Organ Theory 2002;8(3):235–41.
[9] Beraud P, Cruz A, Hassell S, Meadows S. Using cyber maneuver to improve network resiliency. In: Proceedings of the 2011 Military Communications Conference; 2011 Nov 7–10; Baltimore, MD, USA. Piscataway: Institute of Electrical and Electronics Engineers; 2011. p. 1121–6.
[10] Defense Advanced Research Projects Agency. Clean-slate design of resilient, adaptive, secure hosts (CRASH): Broad agency announcement [Internet]. Arlington: Defense Advanced Research Projects Agency; 2010 Jun [updated 2010 Jun 1; cited 2017 Jul 26]. Available from: https://www.fbo.gov/index-?s=opportunity&mode=form &id= 4022d960a15e87bcaf0fb70101ab53b8&tab=core&_cview=1.
[11] Tansley AG. The use and abuse of vegetational concepts and terms. Ecology 1935;16(3):284–307.