Engineering 4 (2018) 47–52

Contents lists available at ScienceDirect

Engineering

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

Research
Cybersecurity—Article

Research on the Construction of a Novel Cyberspace Security Ecosystem

Xiao-Niu Yang [a,*], Wei Wang [a], Xiao-Feng Xu [a], Guo-Rong Pang [b], Chun-Lei Zhang [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 8 December 2017
Revised 30 December 2017
Accepted 5 January 2018
Available online 26 February 2018

Keywords:
Cyberspace security ecosystem
SMCRC loop
Tripartite theory of cyberspace

ABSTRACT

Given the challenges facing the cyberspace of the nation, this paper presents the tripartite theory of cyberspace, based on the status quo of cyberspace. Corresponding strategies and a research architecture are proposed for common public networks (C space), secure classified networks (S space), and key infrastructure networks (K space), based on their individual characteristics. The features and security requirements of these networks are then discussed. Taking C space as an example, we introduce the SMCRC (which stands for “situation awareness, monitoring and management, cooperative defense, response and recovery, and countermeasures and traceback”) loop for constructing a cyberspace security ecosystem. Following a discussion on its characteristics and information exchange, our analysis focuses on the critical technologies of the SMCRC loop. To obtain more insight into national cyberspace security, special attention should be paid to global sensing and precise mapping, continuous detection and active management, cross-domain cooperation and systematic defense, autonomous response and rapid processing, and accurate traceback and countermeasure deterrence.

1. Introduction

The ever-increasing proliferation of and dependence on cyberspace in the nation makes cyberspace security a serious problem and increases both practical and potential threats. Cyberspace security threats have become a major risk to national security; as President XI Jinping stated, “There is no such thing as national security without cyberspace security.”

The nation is facing many challenges in cyberspace security, including: overwhelming online fraud, which presents a major cyberspace challenge; a lack of continuous monitoring and a limited effect from passive blockading; an inferior industrial foundation, resulting in multiple backdoors; an uncontrollable supply chain; cyber defense that is dispersed and slow; a lack of collaboration between cyber protection and cyberspace management; and limited cyber attribution and countermeasure capability, as well as little cyberspace deterrence. Meanwhile, some developed countries have gained great technological advantages in this field, which have been transformed into industrial advantages. These countries have then gained the seller’s advantage through technology exportation, product supply, and market monopoly, thereby obtaining opportunities to implant backdoors and hide vulnerabilities [1–5]. Under these circumstances, the nation must use these products, which may contain vulnerabilities or viruses, and its cyberspace security architecture must rely on this environment. Therefore, a practical and effective way of supporting the national cyberspace power goal is required, which will involve having a clear strategy, enhancing technology, and taking the lead in industries, both offensively and defensively.

2. A “divide-and-rule”-based cyberspace security strategy

Cyberspace security is a multilevel and complex problem; the national level of cyberspace security is the main focus of this paper, as it affects regime stability, economic development, and military security. In addition, different networks have different features and security requirements; therefore, a “divide-and-rule”-based cyberspace security strategy must be employed.

We therefore propose the tripartite theory for cyberspace, based on the current situation. This theory divides cyberspace into three subspaces: common public networks (C space), secure classified networks (S space), and key infrastructure networks (K space), as presented in Fig. 1. The issues of these three subspaces should be addressed differently, in accordance with their unique features and

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

https://doi.org/10.1016/j.eng.2018.01.003
2095-8099/© 2018 THE AUTHORS. Published by Elsevier LTD on behalf of Chinese Academy of Engineering and Higher Education Press Limited Company.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

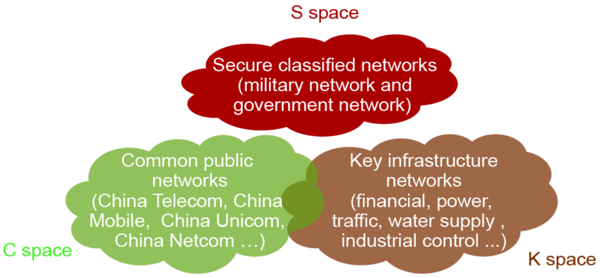
S space
Secure classified networks (military network and government network)
Common public networks (China Telecom, China Mobile, China Unicom, China Netcom …)
C space
Key infrastructure networks (financial, power, traffic, water supply , industrial control …)
K space

Fig. 1. Three subspaces within cyberspace.

security requirements, in order to solve the problems in cyberspace in a stepwise manner.

2.1. Features and security requirements of different networks

Different subspaces have their own features and security requirements:

- *C space* refers to globally connected common public networks, and features comprehensive threats, openness, interconnection, and common technology standards, making C space the front line for offensive and defensive cyberspace operations.
- *S space* refers to the military, political, and diplomatic networks, which comprise the core system through which sovereignty is exercised, national security is ensured, and critical national classified information is borne, making S space the fortress for cyberspace information security.
- *K space* refers to open networks that are of great concern to national interests. These are connected to C space and support the normal operation of national critical infrastructure (financial, power, traffic, water supply, and industrial control, etc.), making K space the main battlefield of cyberspace defense.

The different security requirements of the three subspaces are shown in Table 1.

The major requirements of C space include: keeping critical services credible; maintaining a clean cyberspace; ensuring the legitimate interests of citizens; and improving the capabilities of situation awareness, early warning, and monitoring.

The major requirements of S space include: maintaining absolute safety for important national secrets; and maintaining the normal operation of military, political, and diplomatic missions.

The major requirements of K space include: maintaining the assured operation of critical infrastructure and its applications, such as financial, power, and traffic operations; and ensuring that critical applications are secure and reliable.

Table 1
Security requirements of different subspaces.

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

2.2. Security strategy

A cyberspace security research framework based on the tripartite theory is shown in Fig. 2.

The main focus for C space is on establishing an ecosystem and ensuring service security [6–8]. For S space, the focus is on constructing domestically made networks and ensuring information security. For K space, the focus is on performing active protection and ensuring application security [9,10]. In addition, three support platforms are established to support an integrated strategy; these include an all-domain (from Internet to threat intelligence) information-sharing platform, a consolidated identity-authentication platform, and an integrated testing-and-evaluation platform.

To summarize, the different networks must be studied and their issues addressed on a respective basis.

- The major goal for C space is to develop an ecology and an immunology-inspired collaborative cyberspace security ecosystem, in order to improve network management, control, and protection, thereby shaping a collaborative system of situation awareness, continuous monitoring, cooperative defense, rapid recovery, traceback, and countermeasures.
- The major goal for S space is to establish a built-in security-based, domestically made, and controllable security-protection capability, which will be based on newly developed secure networks and computer architecture. These capabilities will ensure that critical products are domestically made, controllable, secure, credible, and immune to vulnerabilities.
- The major goal for K space is to develop game-theory-based active protection and emergency-recovery capabilities, in order to establish a defense architecture that is multilayered, in-depth, dynamic, and resilient, thus ensuring that critical applications remain secure and reliable.

The following paragraphs focus on the establishment of a cyberspace security ecosystem for C space.

3. A cyberspace security ecosystem based on the SMCRC loop

Considering the various challenges facing the public Internet, no single cyberspace defense technology can act as a "sovereign remedy." The practical solution is to self-adjust according to changes in the environment, enable collaboration, and ensure normal operation of the network. In other words, a grand collaboration mechanism needs to be established through cross-domain cooperative information sharing; this will enable collaboration among all-domain monitoring, active protection, rapid response, and precise attribution. A novel cyberspace security ecosystem can solve the abovementioned problems and catch threats early on, before they develop into major issues.

In this cyberspace security ecosystem, various security techniques become embedded network attributes, and network nodes

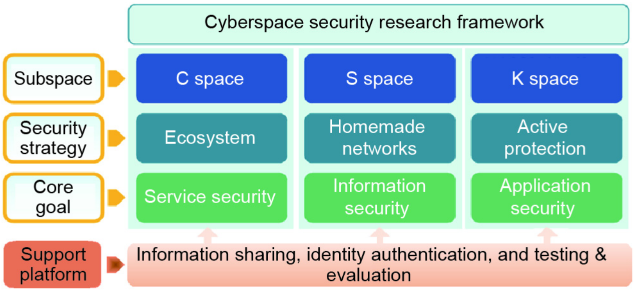

Fig. 2. Cyberspace security research framework.

exchange credible information and share security policies in a collaborative way. These techniques can combine in different ways to deal with different security events, thereby achieving the goal of cyberspace security service by, for example, denying cyberattacks, limiting the spread of cyberattacks, minimizing the effect of cyberattacks, and enabling rapid recovery of the network condition.

We propose a cyberspace security ecosystem based on the SMCRC loop, where "SMCRC" stands for "situation awareness, monitoring and management, cooperative defense, response and recovery, and countermeasures and traceback," as depicted in Fig. 3. Inside this ecosystem, through three support platforms (i.e., an information-sharing platform, an identity-authentication platform, and a testing-and-evaluation platform), various cyberspace security functions are organically integrated, producing a dynamic cyberspace security ecosystem. This ecosystem can ensure that online public opinion, user privacy, network facilities, and the attribution of security accidents remain manageable.

3.1. Features of the proposed cyberspace security ecosystem

The SMCRC loop is an organic whole, in which the data is always flowing. This loop can integrate all cyberspace security resources, thus enabling an interdependent and consolidated environment.

(1) **The SMCRC loop.** S (situation awareness) provides situation-awareness data to M (monitoring and management); M provides early warning information to C (cooperative defense); C is the precondition for R (response and recovery), supporting an automatic and rapid response; R provides the cyberattack sample database to the second C (countermeasures and traceback), enabling precise attribution and countermeasures; and the second C provides threat intelligence and countermeasure results back to S, thus enriching global awareness and precise mapping.

(2) **The support platforms.** Three support platforms can provide the SMCRC loop with the following capabilities:

- Real-time data gathering, which provides various sectors, fields, and agencies with consolidated network data services and threat intelligence-sharing services;
- Credible and consolidated identity authentication, thus enabling cyber forensics, attribution, defense, and targeted deterrence; and
- Consolidated testing-and-evaluation environments and services, thus ensuring the effectiveness and utility of cyberspace security technologies and products.

3.2. Internal information exchange inside the proposed cyberspace security ecosystem

No information-flow control is mandatory inside the SMCRC loop. The information exchange between different factors is depicted in Table 2. The transferring methods and content of information among the SMCRC components depend on their specific applications. All information must comply with certain formats and rules for automatic processing and interoperability. These mutual pieces of information can be statistical data, metadata, or original data for security-related and privacy reasons.

4. Key technologies of the SMCRC loop

Considering the specific security requirements of C space, the following key technologies must be studied in order to build a cyberspace security ecosystem.

4.1. Situation awareness: Global sensing and precise mapping

At present, the nation can only monitor its domestic network; we are unable to identify advanced persistent threat (APT) cyberattacks in a timely fashion. Our ability to map network resources is confined to the public network. Therefore, we believe that situation-awareness technologies should be studied in two ways: by collecting data from all domains and performing in-depth network detection, and by focusing on global sensing and precise mapping.

(1) **Global sensing.** Research should be done on network multidetection, distributed data collection, fusion analysis of massive

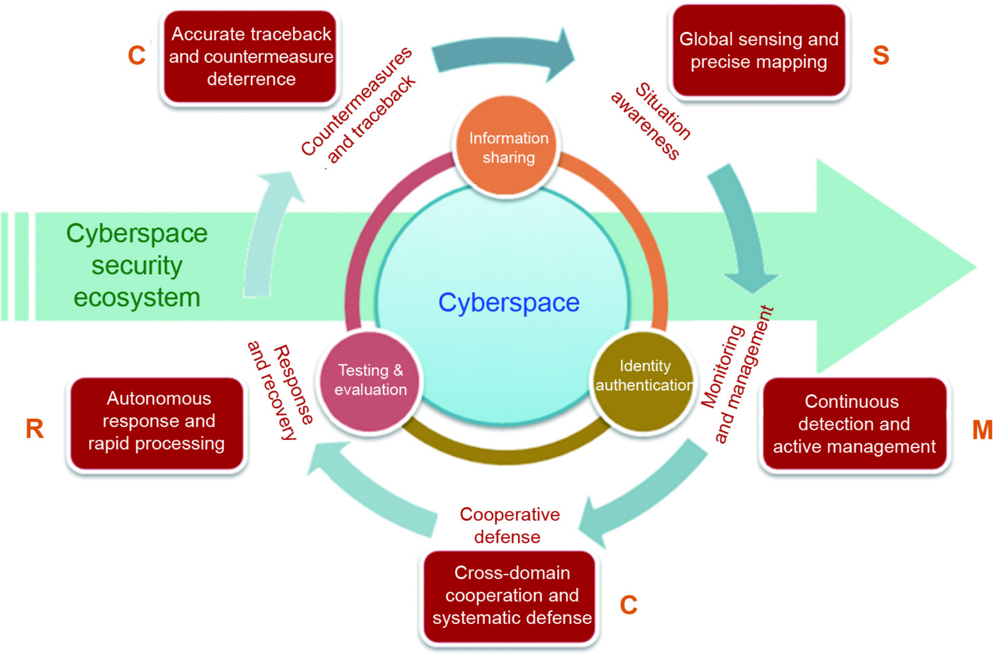
C
Accurate traceback and countermeasure deterrence
Countermeasures and traceback
Global sensing and precise mapping
S
Situation awareness
Information sharing
Cyberspace security ecosystem
Cyberspace
Monitoring and management
Continuous detection and active management
M
Identity authentication
Testing & evaluation
Response and recovery
R
Autonomous response and rapid processing
Cooperative defense
Cross-domain cooperation and systematic defense
C

Fig. 3. A cyberspace security ecosystem based on the SMCRC loop.

Table 2
The information-exchange matrix of the SMCRC loop factors.

	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	

data, tunnel protocol in-depth analysis, malicious behaviors identification, attack data correlation, and analysis methods exploitation. This can be accomplished by collecting network data from domestic and foreign sources using various means, and then executing fusion analysis so as to realize the ability to sense global key network infrastructures, systems, and nodes, and be aware of the whole network operation status.

(2) **Precise mapping**. Research should be done on the analysis of dark net detection, network dynamic resources detection, assets correlation analysis, hierarchical mapping, and multiple granularity situation visualization. Through comprehensive analysis of the time, space, and network features of various network assets, these features will be classified and mapped, including network resources, interactive relations, security accidents, and threat levels. Doing so will provide a network assets blueprint for different departments in various domains, along with the granularity and level required.

4.2. Monitoring and management: Continuous detection and active management

Because the nation is unable to continuously detect and analyze all network data, and because responsive blocking methods cannot effectively manage cyberspace, we believe that continuous monitoring should focus on network big data compression storage, network data linear speed in-depth analysis, and network-behavior positive guidance, in order to realize continuous detection and active management.

(1) **Continuous detection.** Research should be done on hierarchical network data lossless monitoring, distributed processing and fusion analysis of large volumes of data, and fast processing of the in-depth network data of all domains. By creating a hierarchical network data-monitoring system, we can achieve all-round, in-depth, persistent, and nearly real-time monitoring analysis without disrupting users' privacy, thus providing a means of effective network management for national agencies.

(2) **Active management.** Research should be done on user-oriented network data real-time push services; network crowd-behavior guidance and intervention; multisource, multilingual, and multimedia rapid public-sentiment classification; the in-depth correlation analysis of terrorism-related network information; and illegal network data cleaning. By creating a network-behavior positive-guidance system, any Internet activities that threaten political stability, social security, or economic development can be stopped or processed in a timely fashion, including crimes, terrorism, and subversive activities.

4.3. Cooperative defense: Cross-domain cooperation and systematic defense

It is undeniable that there are many flaws in the current cyber system, including inefficient cooperation between domestic functional departments, stovepipe network-defense systems, and a lack of systematic network-defense abilities. Therefore, cooperative defense technologies should focus on intelligence sharing, cross-domain guidance, blockading hacking activities, and safety-policy cooperation.

(1) **Cross-domain cooperation**. Research should be done on cyberspace defense mission design cooperation, cross-domain network-security policy cooperation, and task-oriented multi-systems. With mission multi-domain cooperation, policy-consistent cooperation, operation-level cooperation, cross-domain cooperation, and fusion of surveillance, it will be possible to realize early warning, defense, countermeasures, and operational command and management, thus solving the problems affecting interagency cross-domain in-depth cooperation.

(2) **Systematic defense**. Research should be done on integrated cyberspace security cooperative defense architecture, network threat intelligence-based cooperative defense, network resources intelligent scheduling, network dynamic defense, and guidance and blockade cooperation against network-hacking activities. The cyberspace security structure should be developed from the perspective of systematic theory in order to realize a reasonable overall arrangement and cooperative operation, thus significantly improving our ability and efficiency in the fields of cyberspace threat identification, location, response, and processing.

4.4. Response and recovery: Autonomous response and rapid processing

The US cyberspace security strategy is based on the belief that there is no way to guarantee absolute security in cyberspace and that cyberattacks are inevitable. A static fortress style of defense is inefficient and expensive. However, it is very important to minimize the consequences of cyberattacks by various means. Therefore, recovery ability is essential.

The national network defense is separated and slow to respond after cyberattacks; therefore, great effort should be made to develop rapid network-recovery technologies, and to study the autonomous processing of network events, along with reconfigurable designs, services, and data recovery. Above all, the focus should be on autonomous response and rapid processing.

(1) **Autonomous response**. Research should be done on the autonomous processing of network operation procedures, standardizing event procedures, and so forth.

(2) **Rapid processing**. Research should be done on network system rapid rebuilding, network service restructuring and self-healing, network data assured recovery, and virtualization-based network self-healing, among other relevant topics.

By designing a system, network, services, and data structure that are reconfigurable, modularized, and virtualized, network accidents can be responded to in an autonomous, standardized, and rapid manner. This makes it possible to stop intrusion, confine areas of disruption, mitigate the effect of cyberattacks, recover key services as soon as possible, and guarantee that the operation of core network services goes back to normal.

4.5. Countermeasures and traceback: Accurate traceback and countermeasure deterrence

At present, the nation is unable to attribute and analyze non-cooperative networks, and its countermeasures are insufficiently intelligent and automatic. The solution to this issue is based on accurate traceback and on countermeasure deterrence.

(1) **Accurate traceback**. It is necessary to be able to analyze an adversary's cyberattack path, extract behavior features, and obtain evidence of cyberattack modes. Based on the characteristics of a network entity on different levels, such as its network behavior and traffic watermarking, it is possible to identify the true sources of cyberattacks that use jump server hosts, anonymous communication systems, and botnets to hide themselves. By combining this information with a hacker-profile database, it is further possible to identify the specific location of non-cooperative attackers, and to provide technical support for accurate traceback.

(2) **Countermeasure deterrence**. It is necessary to study the principle of cyberspace deterrence and explore the possibility of maintaining a strategic balance with vital adversaries in cyberspace. After discovering the distribution of target network vulnerabilities, great effort should be put into studying autonomous and batch countermeasures in order to control a large number of network nodes and applications.

4.6. Support platforms

In addition to the technologies that are closely related to the SMCRC loop discussed above, it is necessary to develop some general basic technologies to ensure that the cyberspace security ecosystem based on the SMCRC loop functions smoothly. The technologies of these three support platforms include: all-domain information sharing, consolidated identity authentication, and comprehensive testing and evaluation.

(1) **All-domain information sharing.** At present, cyberspace defense, offense, administration, and control are under different domestic authorities, making it very difficult to effectively share information, form a common situation-awareness picture, or form a joint analysis. Cooperation should be boosted between the different departments that are responsible for different functions, and among the different agencies at national, provincial, and municipal levels. Leveraging information-sharing technologies can make it possible to consolidate the abilities of various departments, services, academies, and industries, thus establishing a cyberspace security architecture with an ability that is much greater than that of its individual parts.

(2) **Consolidated identity authentication.** A great deal of identity cheating and identity theft occur in cyberspace. Cyber criminals and other attackers may exploit the vulnerabilities of identity authentication in personal sites, websites, email systems, and infrastructures in order to sabotage cyberspace as a whole. Therefore, a personal identity-authentication platform in cyberspace with authentic and undeniable labeling is needed. Cyberspace identity authentication should be combined with various factors, such as personal or organizational computing and communication devices, networks, information systems, applications, and data. This will create a consolidated and authentic identity label in order to match digital IDs in cyberspace with identities in the physical world. It will be helpful for stopping network fraud, monitoring public-sentiment agitation, attributing malicious cyberattacks, and enhancing the abilities of forensic, defense, and directional deterrence.

(3) **Comprehensive testing and evaluation.** With the development of cyberspace technologies, traditional testing-and-evaluation methods are being challenged. The subjects to be tested are evolving from single systems to complex joint networks and information systems. Therefore, testing and evaluation are becoming more and more difficult, resulting in higher requirements from testing-and-evaluation staff, technologies, and facilities. To fully capitalize various resources and break the barriers between the military and civil fields, governments and industries, and academic institutions, it is necessary to create a joint testing platform—that is, a national cyberspace range. Such a platform will provide a consolidated testing-and-evaluation environment for the in-depth analysis of the flaws, backdoors, and vulnerabilities of various complex protocols, software, and hardware information systems in cyberspace. It will also be able to evaluate their ability to detect, defend, respond, and recover.

5. Conclusion

In July 1935, the British botanist Arthur George Tansley (1871–1955) [11] introduced the concept of the ecosystem for the first time, in the journal *Ecology*. This concept has been used in many domains, of which cyberspace is a classic example.

A cyberspace security ecosystem has many features including autonomous defense, certified elements, monitored behaviors, overall system situation awareness, self-evolved functions, and inherent security. To achieve these features, considerable effort must be made, which will take time, cooperation, and political guidance.

A senior official of the US Department of Homeland Security has pointed out that it is improbable to be able to achieve a perfect cyberspace ecosystem. However, now that humans have created cyberspace, we should also take responsibility to make it a healthy, orderly, and autonomous ecosystem. There is no turning back on this road.

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.