ARTICLE IN PRESS

Engineering xxx (2018) xxx–xxx

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 xxxx

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.

© 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/).

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/).

Please cite this article in press as: Yang X-N et al. Research on the Construction of a Novel Cyberspace Security Ecosystem. Eng (2018), https://doi.org/10.1016/j.eng.2018.01.003

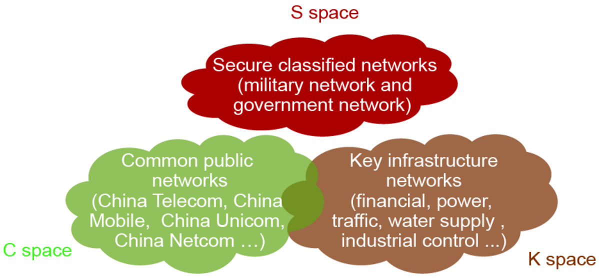
S space
Secure classified networks (military network and government network)
Common public networks (China Telecom, China Mobile, China Unicom, China Netcom …)
Key infrastructure networks (financial, power, traffic, water supply , industrial control …)
C space
K space

Fig. 1. Three subspaces within cyberspace.

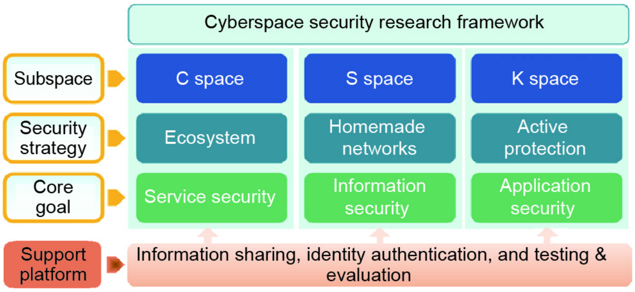

Fig. 2. Cyberspace security research framework.

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

Please cite this article in press as: Yang X-N et al. Research on the Construction of a Novel Cyberspace Security Ecosystem. Eng (2018), https://doi.org/10.1016/j.eng.2018.01.003

Download English Version:

https://daneshyari.com/en/article/6893342

Download Persian Version:

https://daneshyari.com/article/6893342

Daneshyari.com