The Study on the Test Mode of Cyber Countermeasure

Luan Yang[1,a], Dengwei Chen[1], Linying Geng[1]

[1] LEETC, Luoyang, Henan Province 471003, China ,

[a]Email: 410295894@qq.com

Keywords: Cyber space, Cyber countermeasure equipment, Range test, Test mode

Abstract. Cyber space has important position as traditional combat field like land, ocean, air and space as a new field. The paper research the classification of cyber countermeasure equipment range test based on the analysis of cyber countermeasure equipment and its technical architecture. Put forward a new test mode that is "multi range joint, Simulation and real combining, trial development, equivalent shrinkage ratio". Purpose is to support the cyber countermeasure equipment test technique.

Introduction

Cyber space will have a great impact on combat mode, combat form in the future information war[1] The dominance of cyber space is one of the most important facts of war's termination. In order to enhance the cyber operation power, we must research and develop the cyber weapons, meanwhile the range test of cyber countermeasure equipment should be carry out. The cyber weapons' targets include various information systems, networks and electronic components inside, their operation scope crown all the procedure of information's generation, processing, transmission, storage and use [2][3]. Due to the new characteristic of cyber countermeasure equipment, traditional test method is not suitable for the cyber weapons, a more scientific and normative test mode is desired to satisfy the range test of cyber countermeasure equipment.

This paper research the classification of cyber countermeasure equipment range test based on the analysis of cyber countermeasure equipment and its technical architecture. Then a new test mode is proposed based on "multi range joint, Simulation and real combining, trial development, equivalent shrinkage ratio" to support the cyber countermeasure equipment test technique.

Cyber countermeasure equipment and its technical architecture

Cyberspace operation is all the tactic operations aiming at the cybernation of cyberspace. It has the characteristic of Net electric space battle space that surrounds compete for control of the electricity network launched a variety of technical and tactical actions , complex hierarchies with battlefield combat power distribution , unrestricted operations , covert warfare , features a wide range of operational objectives [4] [5] .In the course of combat, weapons and equipment as a function of the overall system, receive information from the target and the environment, and ultimately exert influence on operational objectives. According to this information during operations processes, cyber countermeasure equipment system include:

A. Sensor equipment: including intelligence gathering, target reconnaissance, surveillance and battle damage assessment and other types of systems. Mainly focus on developing technology such as cyber signals joint detecting, cooperative reconnaissance.

B. Command and control equipment: this type of equipment can be considered as the decision-making centers of weaponry systems, auxiliary generator operation control command. Mainly focus on the development of information fusion, target information integrated processing technology.

C. Operation equipment: the implementation of such equipment includes fire attack, interfere and other support operations focus on the development of information technology, networking weapons platform.

D. Communication equipment: the components of such equipment will be connected weaponry system as a whole, and focus on developing the integration of air-space communications, the implementation of dynamic network communication technology.

Cyber countermeasure is a sophisticated high-tech combat activity with knowledge-intensive. Its technology related to cyber space reconnaissance and counter-reconnaissance technology, network attacks and counter- attacks electric space technology. Key technology system of cyber ountermeasure is shown in Figure1

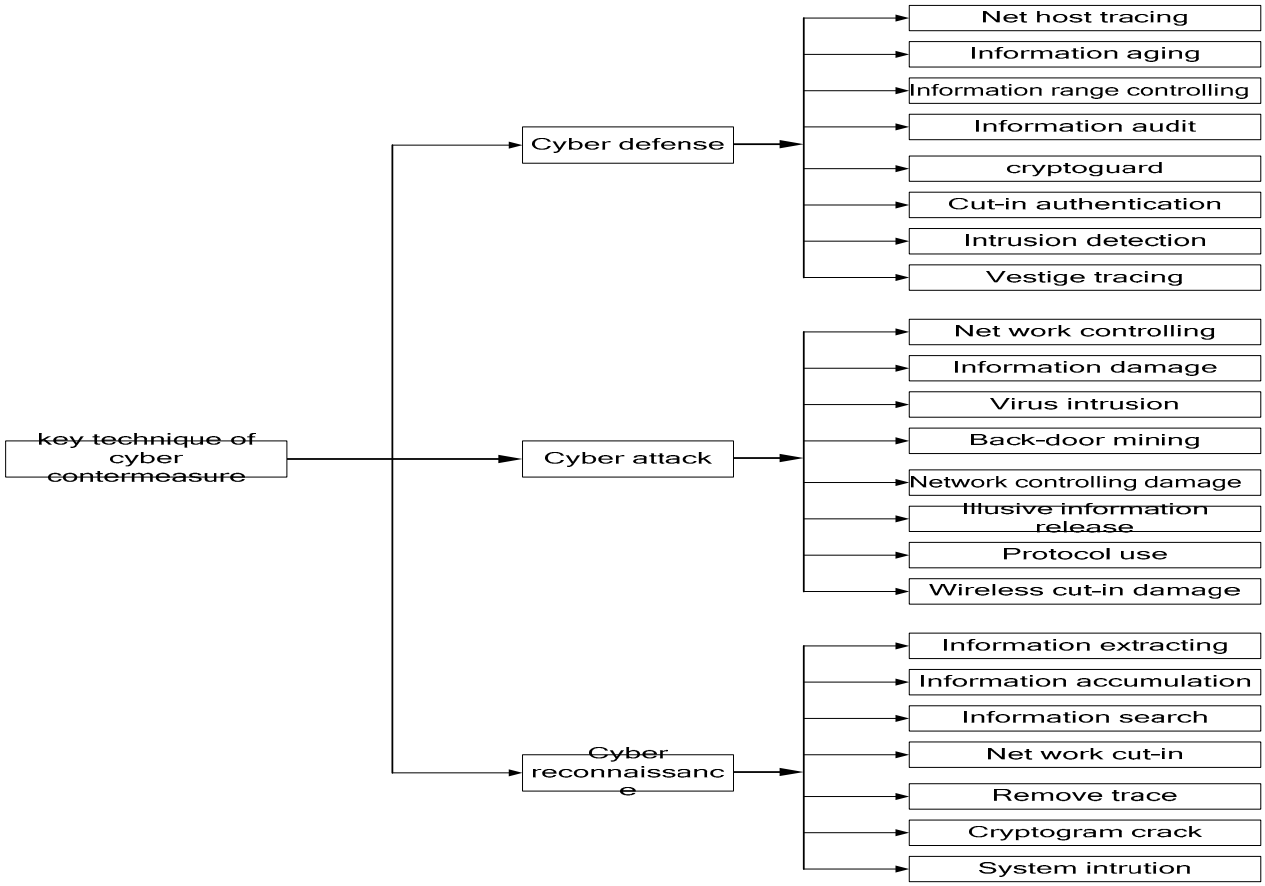

Figure 1. Key technology system of cyber countermeasure

The classification of cyber countermeasure equipment range test

The range test task of cyber countermeasure can be classified according to the type of combat equipment and testing methods for classification.

A. Classification with the process of information flow. The range test tasks can be taken into four categories by the process of information flow: sensor equipment test, command and control equipment test, communications equipment test and operation equipment test.

B. Classification with the function of equipment. Generally, cyber countermeasure equipment includes detection, attack equipment and defense equipment. Taking into account the cyber defense equipment mostly be integrated into network information system, most electricity network defense equipment in the, the range test task of cyber countermeasure can be taken three four categories: cyber detection equipment test, cyber attacks equipment test, and defenses tests of information network system.

C. Classification with the test methods. Cyber range test tasks can be divided into simulation equipment test, real equipment test and logical range test with the test methods.

The characteristics of cyber countermeasure equipment

Cyber countermeasure equipment range test has the following characteristics:

A. Open and connective

The test of cyber countermeasure equipment requires systematic, network-based target environment. Cyber space covering wide network content, involving areas of many, and the cyber test range should fully integrate and exploit the advantages of military and civilian resources, and construct joint distributed test range environment.

B. Combination of virtual and actual objects

The test results with actual equipment are objective and credible. However, due to limitations of actual equipment types and quantities of resources, geography, funding and safety, it is often difficult to form a complex battlefield for testing. The entities devices of cyber infrastructure, the size and the topology of the target network, the network behavior information such as operating mode, flow distribution, routing should be simulated for cyber countermeasure equipment range test. It requires not only software simulation technology, but also need to use physical simulation tools, combined with the actual situation, to achieve a high fidelity simulation of all kinds of cyber features.

C. Integration of test and training

Both the equipment test and military training can be realized the cyber range. After completion of the cyber equipment test, its operational performance can be examined in the cyber range, which can be used to guide further equipment test. After equipped to the troops, cyber forces can carry out training in the cyber range, and the training results can be further examine equipment. Equipment testing, performance testing and military training form a closed loop, forming the integration of test and training of cyber countermeasure equipment.

D. Equivalent subscale

When neither the actual equipment test nor the simulation test meets the cyber countermeasure test, small-scale tests can be executed on the basis of equivalent effectiveness to test the performance of cyber weapons.

The Range Test Mode of Cyber Countermeasure Equipment

According to the characteristics of cyber countermeasure equipment test, the cyber test mode can be divided into multiple range joint test mode, combined simulation and real test mode, integration of test and training mode, one mode of trial and equivalent reduction ratio test mode, equivalent subscale test mode.

A. Multi-range joint test mode

Compare with single range test mode, multi- range joint test with large-scale, widely distributed, abundant resources and other characteristics, it is able to take full advantage of each range real, virtual, construct resource. In a multi-range joint test, the joint command center manages the test resources throughout the trial, and use the information networks to share the resources and information in real-time.

Variety of distribution military information systems are described and packaged in a unified service. These services are separated physically, but can be called back by each other through a loosely coupled way. According to the require of military applications, these services can be dynamically integrated to a cyber countermeasure test command and control system.

B. Combined test mode with simulation and real equipment

Combined test mode with simulation and real equipment can take the full advantage of simulation test mode, such as reliable, repeatable, economic and less restriction by weather and space [6], while ensuring the testing process can be managed [7]. This test mode can better solve the lack of real equipment under the real equipment test mode. In this mode , simulation and test equipment are mutually beneficial to provide support , supplement and perfect , that is the real test equipment is the base of model testing and o provide correct and accurate validate of the models ; simulation tests can

be developed reasonable mounting pilot program to provide support ; another combat simulation to simulate different set of experiments want real equipment on the basis of tests, or simulations of complex cyber space environment with a larger scale . The simulation model and real mannerisms binding assay is a semi -physical simulation model, also known as " hardware in the loop " simulation (Hardware-in-loop Simulation), is a real-time simulation , the actual physical device can access real-time testing.

C. Integrated test mode of test and training

Integrated test mode of test and training integrate the test mission and training mission organically, including the equipment testing, performance testing, and the whole process of military training. Since the fast updating of the cyber equipment technology (time-sensitive), the qualities of the equipment operators play a major influence on equipment performance, human behavior affects the dynamic changes of the operational environment, the cyber range test to evaluate the effectiveness of the cognitive domain and multi -level integrated assessment, cyber range test should be integrated with cyber range training and form a closed-loop "human in the loop " with equipment test, performance test and military training to generate the capacity of rapid equipment test, comprehensive evaluation combat effectiveness , assessment of cyber combat troops.

D. Equivalent subscale test mode

It is unrealistic to build a large-scale target network with a large number of real equipment. According to the method of equal proportions, we can reduce the number of test equipment to improve the efficiency of testing. Then the operational capability of equipment can be calculated with the equivalent principle. But the equivalent subscale test mode requires certain constraints.

Conclusion

Multiple-range test is the main pattern of the cyber range test. Combined test mode with simulation and real equipment is a safety, controllable, repeatable, credible test mode and has an important role in cyber range testing. Integrated test mode of test and training can help to evaluation the operational performance of cyber equipment and improve the cyber troop’s fighting strength, is a potential test mode. Equivalent subscale test mode can solve the large-scale cyber test under certain constraints, is a good supplement to cyber countermeasure test theory.

References

[1] Department of Defense, the US International Strategy for Cyberspace, 2006

[2] Air Force Cyber Command Strategic Vision.2008.02

[3] Zhang ChunLei. Air Force Cyber Command Strategic Version[J].Communication Electronic War, 2009(1):4-10

[4] Zhao Jie,Zhao Xianbao,Wang Shizhong. Research on Cyberspace and Cyberspaee Operation[J]. Journal of CAEIT,2011(3):327

[5] Chen yongkang.The Research on American Cyberspace Operation.The 6th computer countermearsre Conference, 2012:10-15

[6] Huang Kedi.Simulation and Model Technique.Chang Sha: National Defense Science and Technology Press,2010

[7] Zhang huan.Electronic Equipment Test.Beijing: National Defense Industry Press,2005