The Information Security to the Analysis of Battlefield Intelligence

Jing Wen [1, 2], Jin Shi [1] , Hongfeng Li[1*] and Yongcong Shao[3]

[1] New Star Research Institute of Applied Technology, Hefei, China
[2] Institute of Chemical Defense , Beijing, China
[3]Institute of Basic Medicine Science, Beijing, China
ellywen2008@163.com

Abstract - The information security means a lot to battlefield intelligence. The combat power can also be enhanced through improving the information security of battlefield intelligence. Battlefield intelligence analysis requires a lot of techniques such as advanced sensors and information collection technology, seamless battlefield information dissemination and transmission technology, information security technology, and the multi-function digital communication terminal technology. The battlefield intelligence security can be promoted by the safety information transmission, information filtering and information verification. The information security risk evaluation and the active defense can also be used in the analysis of battlefield intelligence.

Index terms - information security; battlefield intelligence; military

1. Introduction

The analysis of battlefield intelligence attaches great importance to the win-or-loss of the war under the new battle conditions. The battle forms have changed from the traditional one to a new one – without smoke of gunpowder. The direction of information security is to acquire the information superiority. With the help of computer system in collecting, processing and disseminating military intelligence, a commander could make a sound decision more easily [1].

Due to multi-dimensional battlespace and changeable operation plan, battlefield intelligence has been dramatically increased. The big amount of information makes the analysis processes complex and thorny. It is urgent to establish a functional intelligence system to analyze and process the battlefield information. It is also necessary to provide the real-time location and movement index of the object in the battlefield to produce precise situation maps.

The cognition of the battlefield information mainly includes the risk estimate of the intelligence, the assessment of the intelligence distortion degree and the effective protection of the intelligence. This cognition is the core technique to establish the information security of the battlefield intelligence. Through improving the information security of the battlefield intelligence, we can also enhance the combat power.

The overall combat power could be improved by strengthening information security in the battlefield intelligence analysis, changing the transferring mode of the information and by realizing information sharing. To be more detailed, the process of making decision and implementing the decision could be shortened; the information assessment and transmission could be improved; the battlefield information could be more intuitive, accurate and practical; the command and control function could be optimized; the combat power, maneuver and joint collaboration of the troops could be improved; the response speed of the weapon platform could be improved.

2. Information Security

The information security means protecting information from loss. The information is safe only in the situation that the information loss is under control. The information security is an important part of information countermeasures. In intelligence countermeasures, both sides are not only to destroy each other's information system, but also to prevent their own from destruction. In order to ensure information security, both sides use code technique to keep the confidentiality, integrity and availability of the data. Information should be protected form disclosure, disruption, modification, deletion, distortion or destruction.

The key point of information security is to ensure the safety of information transfer from a source to a sink [2]. This mainly relies on the security of the information, including the intelligence system, investigation and surveillance system, the information transfer and exchange system, the computer system and the command and control system. All these systems work together to constitute a complete information system including the detector and the decision maker, thus ensures the awareness of the battlespace and acquires superiority in the information environment. The security of the information process should prevent the electromagnetic leakage from the transmitting terminal, and the leakage during the process of storing, exchanging, transmitting and analyzing information should be also avoided. As far as the security of the information equipment is concerned, physical destruction, electromagnetic attack should be prevented. In addition, information equipment should be protected from high power microwave, sonic wave and infrared signal.

3. The Battlefield Intelligence Analysis

Battlefield intelligence analysis includes the enemy situation, self situation and the battlefield situation [3]. Intelligence analysis includes object selection and sorting, object inspection and object analysis. Due to large number of

combat forces and multi-dimensional battlespace, the ability of transferring, integrating, analyzing and disseminating information needs to be improved. According to the availability, information can be divided into three categories: real information, false information and shortage information. Different kinds of information can result in real intelligence, false intelligence and false judgment of intelligence. The relationship between these intelligences is interchangeable. Real information during certain period of time may be false when time passes. It also may be shortage information when the transfer of it is delayed. Battlefield intelligence analysis includes the protection of the real information, the ability of recognizing false information and restoring shortage information.

A lot of techniques are required in battlefield intelligence analysis. The first one is the advanced sensors and information collection technology. The first step to the digital war is the sensor technology. In the future the sensor must be required to provide the real-time image of the battlefield and the full automatic related data. This field includes the automatic target recognition, multiple sensor fusion, sensors/CPU/communications integration, intelligence sensor, and so on.

The intelligent information analysis and comprehensive technology are also needed in battlefield intelligence analysis. With the help of various sensors and other methods, a large number of battlefield information has been collected. Then the data should be analyzed, filtered and synthesized. Through analysis, correct information, instead of false or shortage information, should be transferred to the commander. This field includes target environment and background system modeling, environment reasoning, database/model base established and decision support system, and so on.

Seamless battlefield information dissemination and transmission technology are employed to use and share information. In order to disseminate the real-time information correctly, communication system should be established according to the characteristics of the digital battlefield. This communication system is the core of the digital battlefield; it needs seamlessness and dynamic connection of all the communication systems. Besides, it can provide services for information analysis. This field includes the battlefield command and control system, data distribution system and positioning system, internet and information carrier landing and information systems to the interconnection of each operation interflow.

Battlefield intelligence analysis needs complete information security and information system security technology. It is the digital information to fulfill the efficiency of the digital battlefield, but at the same time the information is under the great risk to destroy. Under normal circumstances, digitized information can immensely improve the overall efficiency in military force. However, all kinds of information systems will be the primary targets if there is lack of necessary information system safety management and technical assurance measures. Along with the development of modern, digital technology and computer technology, the control and anti-control of information will be intensifying in the future battlefield. Without information security, the information may have a negative impact on the military force. The main items in this field include digital battlefield information security strategy & technology system, information security mechanism and service implementation & management, battlefield information system vulnerability testing/evaluation/reinforcement, battlefield of comprehensive management information system (including the safety management as the information, invulnerability, the system exchange management), and so on.

The multi-function digital communication terminal technology will rapidly change the battlefield intelligence situation. It includes multi-functional digital radio, low power consumption information terminal and monitor, the war high resolution color flat-panel display, tactical and multimedia communication security terminal. These equipments will help the commanders and soldiers quickly grasp the spirit of the battlefield intelligence and conduct a reasonable and effective action.

4. Strengthening the battlefield information security

Due to the complexity and diversity of battlefield intelligence, the different information should be treated differently. Time and location is changing, and the real and effective information will also be changing. But the false information will be valuable to some degree when the interference factors are removed. The shortage information will also be used to provide certain information such as when and where the information is damaged. Therefore, scarcity of the information is also a kind of information. All of the information needs to be identified, classified and analyzed. Making full use of all kinds of information is of great importance to acquire information superiority and ensure information security.

Battlefield intelligence security is promoted through the following three aspects: information transmission, information filtering and information verification. To make information transmission safe, it is necessary to avoid the hidden danger in the information transmission, to insert the tactics against detective or to steal, modify content, destroy the illicit close set and integrity of the data. The commonly used method is to use code techniques. Information security can be guaranteed by using code techniques,

Information filtering refers to finding the information needed from the source intelligence and deleting the useless information. This technique can provide more efficient service to the user by improving the quality of information index. To ensure information security, the safe information filters need to filter the non-requested or illegal information from the dynamic source, and prevent the spread of the harmful information. The main methods of the information filter include name filter, grade filter and keywords filter. In the positive information service mode, the detection, prevention of the harmful information is very important to the information

security of the battlefield intelligence. Nowadays the multi-filter model combined with fuzzy theory, artificial neuron-network, mathematical calculations make filter of battlefield information more effective.

The information verification includes two aspects: one is the effectiveness verification, and the other is the security risk evaluation. Effectiveness verification should be taken to deal with the information from different resources, while the real time inspection is necessary to handle information related with threat, invasion and assault. In addition to the sharing of the battlefield intelligence, real time inspection and the repeat verification of the information is necessary.

The information security risk evaluation can be used to ensure the battlefield intelligence safety [4]. The safety measure can be adopted only after we evaluate the risk factors of the information security. There are several risk evaluation models: risk concept model, evaluation process model, risk analysis model and risk evaluation model [5]. The commander can make a decision according to the related battlefield intelligence.

When the information security system is attacked, the rectifying ability is needed. Through adjustment, the information security system could re-evaluate the risk quality and degree, provide the formal attack report, make and reset the priority of the recovery series of information sources. The warning message should be sent to the control system immediately. Part of the information system should be isolated and under control. The key information sources should be redesigned and the activity of the whole information security system should be recovered.

Apart from the passive protection in the collection, analysis of the intelligence and the active defense should also be taken. These techniques mainly include the detection of security loophole and the supervision of the information security [6]. The security loophole detection technique means to scan the weaken points of the information system with the know attach methods in order to detect the security loophole, to give the loophole report, and suggest the supervisor to avoid these attack by upgrading the software or cutting down the related service. The supervision technique mainly use the sign of the invasion (failure root records, abnormal network byes) to detect the illegal invasion from here and there, respond to it immediately, such as cutting down the illegal network, sounding the alarm, and so on.

5. References

[1] C. Hu, "A discussion on conception and methodology of information security," *Science & Technology Review*, no. 3, pp. 19-23, March 2004.

[2] Y. Shang and C. Hu, "Dominant battlespace awareness&Knowledge: The approach to cyberspace situation awareness," *Science & Technology Review*, pp. 37-38, July 2004.

[3] Y. Chen and Y. Gong, "Information war and information security," *Data communications*, no. 3, pp. 34-36, September 2000.

[4] Y. Liu and W. Gu, "Survey of information security risk assessment research," *Journal of Qingdao university*, vol. A23, no. 2, pp. 38-42, January 2008.

[5] M. Yang, S. Li and H. Tang, "Summary on models of assessment of security risk", *Journal of Henan Institute of Education(Nature Science Edition)*, vol. A19, no. 4, pp. 7-8, December 2010.

[6] H. Yao and X. Gu, "Network information security technique," vol.19, no. A5, pp. 515-516, May 2001.