

A study on the Information Superiority of Network Centric Warfare for Future battlefield

Hyun Seok Yoon¹, Dong Hwi Lee¹, Gangtaek Lee², Kuinam J. Kim^{1*}

¹Dept. of Information Security Kyonggi University,
71 Chungjung-Ro, Seodaemun-Gu Seoul, Korea
mostyhs@paran.com, dhclub@naver.com

²Air Force Command
Bunam-Ri, Namsun-Myun Kyeryong-City Chungnam, Korea
bdlgt@daum.net

* Corresponding Author: harap123@daum.net

Abstract

Information superiority plays very important role for winning the war. Recent Warfield have been shown rapid and precise because of new technology. Technologies such as VoIP, wireless LAN, WiBro, RFID and Bio recognition appear as new technologies for giving and receiving information effectively in our current world, it is believed to take superior position of information to address weaknesses in information transferring and protection for each system and then apply them future battlefield information system.

In this study, reviewing future battlefields system that US army goes after and those of Korean army will suggest how to accomplish information superiority for army in future battlefields.

1. Introduction

Information pre-dominance in the future war has already been shown in war between USA and Iraq. Information pre-dominance plays very important role for winning the war. According to report for Congress of USA[1][2], it was reported that although army of Iraq executed initial war adopting GPS jamming technique from Russia, the source of jamming electronic wave was directly attacked by USA fighters, thus more operation with Jamming was impossible. Like the case mentioned above, the military operation takes superiority depending on which side first identifies the location of enemy and attack them, and how accuracy the appeared Information is.

Not just with the case of war between USA and Iraq, also in FTA negotiation between USA and Korea as well, USA approaches the negotiation with the alternative plan while our country does with already

known strategy. That is clearly different with our country.

It goes without saying that if everyone recognizes importance of information, and army for every country implemented wired/wireless communication systems and operations them, those are very important. The aspect of future war is determined for winning and losing depending on whom first takes information superiority. And here, in order to take superior position for information, it depends on how they protect and identify incoming information.

Technologies such as VoIP, wireless LAN, WiBro, RFID and Bio recognition appear as new technologies for giving and receiving information effectively in our current world[3][4], but in order to protect information in future battlefields, it is believed to take superior position of information to address weaknesses in information transferring and protection for each system and then apply them future battlefield information system. This paper, reviewing future battlefields system that US army goes after and those of Korean army, will suggest how to accomplish information superiority for army in future battlefields.

2. Related Works

2.1. Why information superiority is necessary in future battlefields

Transition from platform-centric battlefield environment to network-centric battlefield environment is emerging as a reality in front of us not just a future.

Figure 1, as a system in a way that if sensor and human identifies target, it is reported through information flow system, and then weapons of soldiers

incapacitate or destroy enemy by decision and command by a command officer, may affect command and control very much depending on reporting situation by soldiers and recognition capability of sensor[5].

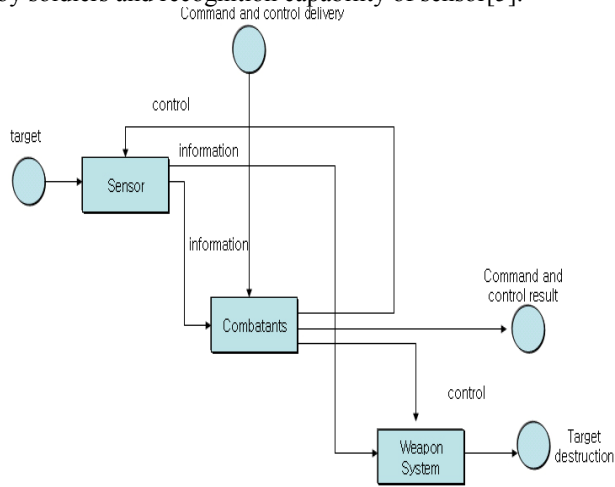


Figure 1. Platform-centric information exchange [6]

Sensor network environment in recent Iraq war shows that it collected information from satellites and sensors and with suitable decision and weapons, paralyzed attacking capabilities of enemy. And only if it has to not only be equipped with detection system(sensors) and attacking system(Shooter) but also guarantee network connectivity for operation elements, integrated each other and interfaced and guarantee perfect information protection in future network war system, it can be regarded as network centric war which can afford right role of battlefields[7].

The concept of strategy for weapon system, as a course for converting available resources of army to combat power like [Figure 2], is effectively capable of combat execution only if it is operated being equipped with supporting elements related to major equipment together. Major systems out of available resources is primary element forming combat power as a major target for acquisition management, but DOTMLPF(Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities) elements are also imperative as well for forming combat power. When these are integrated, combat power can be effectively created. Even when these kinds of major equipment attack enemies by receiving attack commands, the fact that information flow and distorted information may damage our army has already taken important role for network centric war



Figure 2. The concept of military power

Information operation is activities that information security and information system of our force to accomplish pre-dominance over battlefields through information superiority, or it is military or military related actions in war and peace in order to have influence on information or information system of relative or potential enemies. Therefore information warfare is defined as real activities of information operation which is executed to accomplish certain goals or expedite them against specific enemy.

In other words, Information operation is applied to all levels of war for it against certain enemy.

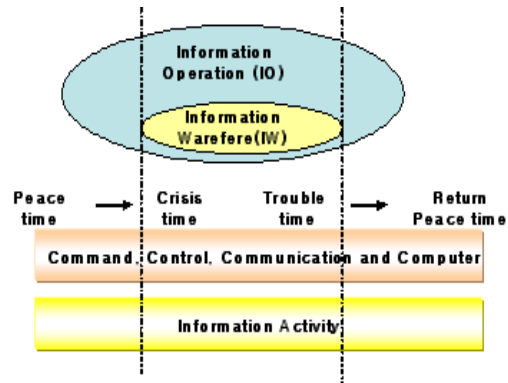


Figure 3. Terms of information operations and relations between activities for information operation support

Figure 3 is inclusive concept for information warfare, and it is targeted for activities of whole military and non-military information and information system. And information operation is a concept for accomplish pre-dominance over information in military operation, its activities is areas for military information and information system [8].

Information protection technologies that can be used in commercial purpose from military information protection are encryption (designing algorithm, recovery/management of encryption key) and authentication technologies(bio information-based authentication, software-based authentication, etc) system/network protection technologies(virtual private network, access control for network and etc), counter technologies against hacking and virus, evaluation technology for modeling simulation

standardization(model for training scenario, system penetration test and etc).

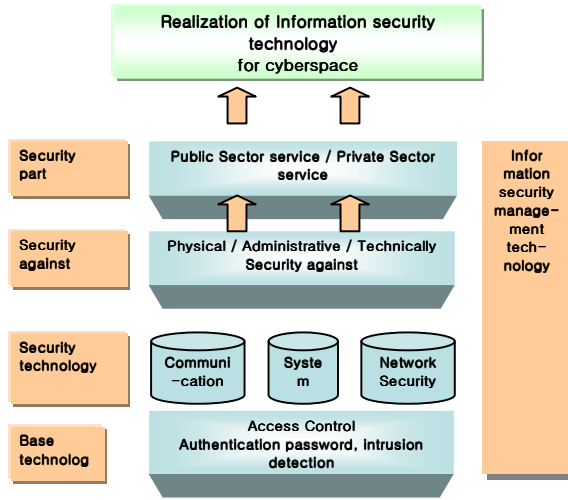


Figure 4. The conception for information security

By applying these kinds of information protection technology, counter system can be planned for several penetration accidents. But there are many cases which access more and more advanced networks with malicious intend and hamper information distribution system or information flow. it is absolutely necessary to react to malicious groups with penetration through information protection, and army can take superior position for information in aspect of future war through information protection for information network which is operated by army[9].

2.2. Trend for current information warfare

US army has prepared for attack by potential enemies (Cuba, Iran, China, North Korea and terrorists) who are able to construct network environment at low-cost, and hacking groups such as Titan Rain in China, Moonlight Maze in Russia really accessed internet network of Department of Defense and related companies and hacked and has resulted in distorted information. You can indirectly experience critical aspect of cyber hacking and information as to how national information protection affects society through a movie, Diehard 4 in which Bruce Willis played a lead actor.

Symptoms of attack in information warfare are things such as retarded computer by malicious virus and code, paralyzed elaborated weapon system. And as there usually exist cases not only in attack of physical space but also in inducing wrong decision by incapacitated body and concealing attack of enemies, they have been

strictly preparing for those kinds of attacks in terms of organization and methodology.

The trend for US army is following. The structure of US joint command for cyber war consists of several joint functional commands. They have been executing military operation constructing USSTRATCOM (United State Strategic Command) so that it can effectively integrate attack not affected by space limitation, information/surveillance/recognition, network war and unified missile defense and mass destruction weapon. Joint functional structural command integrates current operation and proposes direction for the operation.

And also US government gave US air force a new mission in order to actively react to cyber space which can be regarded a 3-dimensional space, which is the role of cyber command that can prepare for malicious attack in space and cyber space. Cyber command is preparing for counter plan against weapon system of electronic war which has not been mentioned yet, and its role is to protect electronic spectrum (X-ray, infrared, microwave, and etc) and its organization has the headquarter in 8TH Air Force under US air force and is preparing for operation of cyber space[10].

The role of battlefield operation execution in physical and cyber space is believed to protect our army information and then play a key role for information superiority. As shown in following table, US organization and businesses on information warfare is proceeding with its concrete goal so that they can pre-occupy information superiority in future war. They are doing the business taking into account change and trends for information warfare, and Department of Defense, army and government office in USA is leading policy for technologies which are imperative in future war [11].

Table 1. Organization and businesses for information warfare in USA[12]

DOD/Army/US office	Business and Plan
IAO of DARPA (Information Awareness Office)	IAO is responsible for information-related technology by accomplishing over all information recognition necessary for preemptive strike, national security warning and decision making
DARPA of TTO (Tactical Technology Office)	Duty for development of command and control system which can survive even against attack of information warfare

ATO of DARPA (Advanced Technology Office)	Research how to protect network service and system from malicious program with built-in virus and other attack methods
SPAWAR(Space War and Naval Warfare Systems Command)	Plays a role for collecting, controlling, processing and analyzing complicated information and then delivering it to national leaders and it controls communication system and information and electronic war businesses including C4ISR
USN NSWC (Naval air warfare centre)	It is an organization supporting overall technological service for sea electronic war system, and plays a role for technological service, military demand and overhaul maintenance.
USAF IWC (information warfare Centre)	It acquired core information infrastructure equipment supporting aerospace information operation, recognition of warfare space and superiority of information spectrum
US ARMY	It leads new directional system under the concept of new compound system for the purpose of laying information warfare and network-centric force in real war in US ARMY VISION 2000

80% of infrastructures used by US ARMY are commercial facilities. For composing its system except for particular infra, satellite, communication system and other infra for commercial purpose are being used. It uses not only satellite system of army but also constructs information flow through proper joint between commercial and military purpose by various route and tries to protect these infrastructures. And in case of China who is preparing for satellite attack system, China is believed to be antagonized against those systems.

US government is always in its emergency preparation composing CERT team consulting with system engineering department of Carnegie Mellon University in order to protect these infra systems, CERT team of US Army and counter team of Carnegie Mellon University by their partnership provide warning against malicious code or cyber crime, and also provide recovery procedure or guidelines after being attacked. Human resource training and information flow

depending on the shared role of civil organization and military are believed to be a lesson for our army.

As electronic warfare/counter war against electronic war is absolutely necessary to acquire information or expedite information flow, electromagnetic interference phenomenon (EMI : Electromagnetic Interference) for electromagnetic bullets is already verified through the operation Starfish Prime, and high power microwave weapon(HPM : High Power Microwave) is under development to defense missile/aircraft of enemies.

In fact, weapon systems of each advanced country transit to a way that can effectively paralyze information flow as information flow in battlefield environment is being affected by network and more and more dependent on network, researches on forming electromagnetic other than nuclear weapon are prominent [13].

3. Advancing trend for information superiority in future warfare system

3.1. Organization

Republic of Korea Army (ROKA) is executing IT implementation with a priority for military IT for the preparation of future warfare. But kinds of IT implementation have various problems and are exposed to others. In order to pre-occupy information superiority in warfare, structural reform for organizational system or physical or non-physical space is necessary, and system development taking into account interoperability is required.

Human and material resource for defense has its limitation. In order to pre-occupy information superiority, conventional platform-centric warfare needs to be advanced by connecting with network system, and military unit with platform-centric tank and fighter need to be adjusted. For timely and proper decision on situation as a basic principle for operation and tactics and for effectively guaranteeing mobility, taking advantage of sensor network system is urgent. In order to effectively enhance capability of collecting, exchanging, standardizing and sharing information, and network system need to be advanced in a way that more effectively and timely collects and exchange information and makes a decision and then attack enemies.

But as destructing effect doesn't directly appear, the priority is lowered thus reformation of organization and importance of network system is not regarded as important factors well. That is real problems.

Organizational reformation which can share vertical/horizontal state that is applied for and has operability for sensor network in which all information in upper/lower/left/right direction in platform-centric information warfare can be seen and shared at the same time and military operation can be carried out under those environment is necessary, and it is most urgent to have system in which information and decision can be timely supported. Human network construction such as committee for industry-academy-research circle is necessary so that army can take advantage of specialists who have expertise for both commercial and military purpose, and constructing network hub is needed in a way that human resource structure is reformed for long-term working.

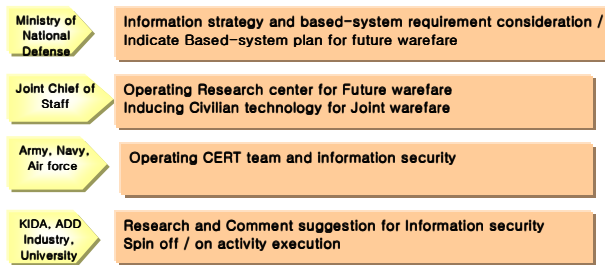


Figure 5. Mission and role for each organization (plan)

3.2. Infrastructure

There are problems coming from bottom up-typed development and acquisition without taking into account interoperability. C4I system with joint environment goes after integrating each development of each army. In order for C4I system to have interoperability between systems, reusable and common usage for its software, unified common operating environment and standardization across whole C4I system are necessary. But in ROKA, those environments are not fulfilled sufficiently.

US Department of Defense calls integrated and unified systems across whole armies' top level architecture, and they are evaluated as critical success factor and arranged and applied. Evolution method is being applied to forecast future technology advancement and apply them. Korean army is also required to accomplish system integration when it develops and applies C4I system so that interoperability can be taken into account by adopting evolution methodology to apply technological changing trends and not hampering information flow.

Information warfare system should be implemented by evolution methodology taking into account technological advancement trend for itself.

Information warfare should be directed for its advancement trend by adopting methodology such as warfare experiment for elaborated inspection about DOTMLPF, and it should also extend the opportunities to take advantage of common commercial technologies between civil and military side. By manufacturing prototype products such as network and information protection technologies used in information warfare with open system approach, inflow of commercial technologies into army was accelerated; further investment for research on military-related technologies by civil side can be expedited through extending commercial technology.

Verification of principles and organization not only evaluate effectiveness of future new principle and organization through warfare experiment which can check technological advancement trend in future warfare, but also allow for verification of alternatives improving current principle and organization which appear in military training areas as well. And it is possible to experiment principles and organization in various aspect against future threats. If there are organization and tools which can infer and experiment information warfare in a way that Carnegie Mellon University in USA finds weakness of RED and BLUE network and advance it, it is possible to pre-occupy information superiority in more information warfare and suggest important role for information protection which is basis for pre-occupying information superiority.

Human networking through industry-academy-research circle is most urgent to apply technological advancement to military, it is necessary to spin-off military technologies through organized industry-academy-research circle and to spin-on technologies of civil business and then advance information flow needed in military operation.

And also by giving opportunity for technological training to existing organization for enhancing expertise, looking for becoming elite troops through technology accumulation, domestic technology advancement should be achieved through finding demand for training in information warfare so that military operation based on network is possible. Taking into account technology advancement as following, systems for information superiority is believed to be created for advancement.

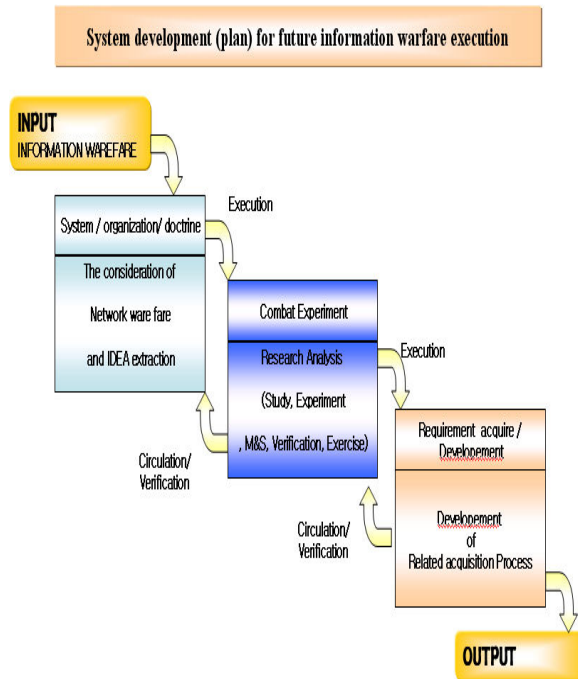


Figure 6. System development (plan) for future information warfare execution

3.3. Implementation System

In order to share unified information exchanging by relational organization in upper, lower, left and right side, interoperability is necessary and at the same time, it is impossible to enable effective information flow without detailed preparation against attack by enemy. Therefore, in order to pre-occupy information superiority in future warfare, protection from attacking system such as cyber attack against weakness of C4I and E-bomb, which can upheaval whole information warfare system, should be carried out. For implementation system, conventional warfare is network-centric war, but future war become network-centric warfare binding platform. Enemy who starts network-centric war continuously changes war strategy, and at the same time it can increase changing speed. As the result, winning the war by hampering strategy of platform-centric side is possible. Like this case, in order to accomplish information superiority, following factors should be taken into account.



Figure 7. Improvement (plan) for implementation system

Firstly, in order to maintain strategy/strategic communication against several kinds of attack including missile and aircraft attack, all level of C4I system should be equipped with field warfare typed communication lines and information protection plan. In order to pre-occupy information superiority and win the war in information warfare, development and maintain for most advanced communication technologies in both high speed lines with huge capacity for field war and high capacity of mobile radio with single channel is necessary.

Secondly, Organizations with goal of information superiority should improve huge capacity of high speed communication line at very first. Enemy sets goal for first targeting our communication infrastructure. Therefore, information communication based on network for military operation should be equipped with penetration detection and protection plan like IDS/IPS against several kinds of attacks such as physical and cyber attack

Thirdly, organization for constructing and operating network should include enough substantiality to be equal to human resource and equipment of field communication unit. The more a military unit focuses on effective grouping and mobile operation, the more important communication capability becomes, therefore communication unit will take high position in terms of human resource, equipment and cost. As high speed communication line with large capacity should consist of wired line up to user terminal, although it is for field war, its moving is retarded. User in front-line can't use it, and users in headquarter of each command can't user it either.

Therefore, hand carrying mobile radio with its maximum capacity in aspect of communication capacity and speed is necessary. Like internet mail exchange is conveniently being used by mobile phone in civil societies, whether IT implementation is successful or not depends on how much carrying vehicle attached radio can give and take information

data. If basis for information flow consists of fixed or movable types, plan for information protection and wrong information should be carefully implemented.

Fourthly, demand for improving weapon system in information warfare is continuously increasing. Need for computer, sensor network (communication network from sensor), power supply and operational organizations are continuously extending. But although change for system is being tried, organization for operating and maintain systems is almost not changed as mentioned above. As trouble and malfunction for equipments has been overlooked constructing crops-level tactics C4I, much of trouble shooting cost in operation is expected, there is no A/S by civil side in warfare, and affording support for whole network related equipments per person has limitation. For this reason, maintenance jobs for communication of each maintenance support unit should additionally include human resource and equipment-related maintenance system, maintenance for encryption equipment should be operated and maintained by improving existing system.

3.4. Training system

Budget and human resource for improving defense power is limited. This reformation in which war power is based on information network and communication is thought to be revolutionary since Japan started to improve its modern army, it entails extreme pains across all areas including military units and industries. In order to be successful in implementing defense IT, whole defense divisions first need to enhance needs and effectiveness for IT implementation at a level that sustain those pain.

Firstly, Specialized training system is not just to improve elements of existing information & communication course and give importance of NCW training which is a moving in future information warfare, but also to solve the problems in Korean army in advance in order to extend importance of infrastructure for future warfare and extend common sense sharing what demands are needed for future warfare.

Secondly, Like USA researches on information warfare environment in Carnegie Mellon University and suggest problems and improving plan and then apply it to defense divisions, in order to evolutionally apply change like network-centric warfare, ROKA, by establishing think tank with academic researcher, should react to information warfare which is rapidly being changed.

Thirdly, Future warfare-related research center is kept under additional center joint command research center, regular training systems are installed in each army's school, research on future technological advancement for warfare and training are required.

Table 2. Research on future warfare

Sectors	Research center on future war	Infantry School	Information School	Communication School	Others
Duty for each military curriculum	Technological research in each area for future warfare, opportunity for converting recognition	Strategy/tactics for future warfare	information warfare, strategy, tactics, encryption-related technology	Sensor network system, information protection technology	Finding future demand for duties for preparation of future warfare in every military curriculum

By extending recognition for information warfare and executing research on information warfare, it should make environment which plays desk role for spin On/Off of commercial technologies. [Figure 8] suggests documents about information warfare constructing training center in regular training course for each school and proposes concept of network-centric warfare and direction for executing future warfare, and the center is expected to test, analyze and make a decision on possibility for applying technologies from civil side to military purpose and then suggest opinions.



Figure 8. Mission and usage for information warfare center and post graduate school

4. Conclusion

Network-centric warfare has its ultimate goal which collects information by sensors and makes it possible for command officer and soldier in battlefield to share same information and carry out war.

Trends of this kind are like ubiquitous society which civil side is looking after. In order to pre-occupy information superiority by connection with commercial technologies, the importance for network-centric and

cyber warfare and need, effectiveness for IT implementation should be recognized.

Although importance for information superiority is recognized, as it doesn't appear in terms of its reality and availability for budget and effects, the importance for information warfare superiority was overlooked many times. Research on how many times more military power by IT implementation will be by number, whether combat operation is first confirmed and suggested after acquiring combat operation or not and whether organization and sequence is first presented through command activities after collecting document for information should continuously discussed. Information superiority in future warfare is different from platform-centric warfare.

Unless we can forecast trend for change and connect it to technological advancement, we are not expected to continuously look after peace for Northeastern Asia due to old-aged legacy. If we refer to moving of China, Japan and Russia, everyone is expected to know which direction we should follow to pre-occupy superiority in information warfare. Not only is important information and weapon system for electronic war, but also raising military power such as DOTMLPF so as to operate weapon system and military unit should be advanced together with system. Therefore, information superiority in future warfare should be accomplished.

5. References

- [1] Caly Wilson, Information Operations, Electronic Warfare, and Cyberwar , Order Code RL 31787, 2007
- [2] Caly Wilson , NCO(Network centric operation), Order code 32411, 2007
- [3] Kwon yong soo, NCW and Warfare management system, KNDU, 2001
- [4] Lee eun gon, RFID Diffusion Prosperity, KISDI, 2004
- [5] Ronald O Rourke, Navy Network warfare Concept, Order Code RS20557, 2005
- [6] Kwon yong soo, NCW and Warfare management system, KNDU, 2001
- [7] Ahn Tae nam "Modern war and information Technology" citation of presented material by Seoul University, Headquarter for Army
- [8] HA Sang-young "Research on effect on change aspect of War by advancement in information military power", Korea National Defense University, 2006
- [9] Christopher J. Alberts, Audrey J. Dorofee ,OCTAVESM Method Implementation, Canegi University, 2001
- [10] Caly Wilson, Information Operations, Electronic Warfare, and Cyberwar , Order Code RL 31787, 2007
- [11] KIM Jae-chang, CHOI Jong-sup, LEE Sung-nam, SEO Hyung-jun and etc "IT-centric country, Digital centric army for NCW implementation KIDA.
- [12] Caly Wilson, Information Operations, Electronic Warfare, and Cyberwar , Order Code RL 31787, 2007
- [13] Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issue, CRS Report for Congress, March 20, 2007.