Network and Electromagnetic Spectrum Management

Takashi Amagai

It must be noted that the English version does not necessarily reflect the original Japanese text.

1. Introduction

In modern warfare, networks are considered to have a significant influence on the course of the war because data links and various other networks serve as very effective tools for sharing information and make it possible to take a host of actions, including operations, expeditiously.

In the theater of operation, in addition to the upgraded performance of platforms such as sensors and shooters, improvements have been made to communication methods, electromagnetic waves as a medium and communication lines, and tactical networks have been evolving day by day. The formation of new networks has brought about changes in tactics and operations. On the other hand, as risks to networks are becoming increasingly apparent, the defense of networks, more than their construction, is becoming a focal point, including networks such as infrastructures that take on the function of bases not directly engaged in combat.

The Ministry of Defense, including the Air Self-Defense Force (ASDF), uses a diverse array of networks as a means of command and control. In view of the situation where networks have become indispensable in order to give full play to the organizational capacity, this paper analyzes the threat to networks and look at the future direction in light of the roles of networks and their management

systems that have changed since the Gulf War.

2. Transition of Efforts Concerning Networks

In the Gulf War, the multinational force, with the United States at the core, turned in the significant military achievements by building up the networks that combined various command and reconnaissance/surveillance systems, including Airborne Warning and Control System (AWACS) and Joint Surveillance and Target Attack Radar System (JSTARS),[1] with Tomahawk missiles and other sophisticated weapons of attack. Based on these achievements, the United States sought to further enhance collaboration between systems after the Gulf War. In particular, this system of systems concept has become widespread from the "sensor-to-shooter" perspective, designed to enable real-time sharing of information from "sensors," such as AWACS, reconnaissance satellites and JSTARTS, with "shooters" that operate precision-guided weapons, thereby dramatically enhancing combat effectiveness by executing immediate attacks.

Under this trend, in 1998, Vice Admiral Arthur Karl Cebrowski, then with the Chief of Naval Operations of the U.S. Navy, proposed the Network Centric Warfare (NCW),[2] which is designed to gain an advantage in combat by creating an information advantage through the sharing of situational awareness by networks.

The Office of Force Transformation (OFT),[3] established within the Department of Defense in October 2001, described NCW as the "very core of transformation" in a brochure, titled "Implementation of NCW. In the brochure, the OFT positions NCW as the core concept of the U.S. military transformation designed to break away from attrition-based warfare and shift to joint operations, effect based operation (EBO),[4] agility of speed, and precision-oriented firepower.

The transformation is the concept first proposed in 1997 by the

National Defense Panel, an advisory committee for the Department of Defense, in its report, "Transforming Defense: National Security in the 21st Century,"[5] and considered with the aim of enhancing combat power through the utilization of science and technology. The consideration of this concept was taken over by the Bush administration that embarked on full-fledged reform of the Department of Defense and the U.S. military forces. In 2003, the Department of Defense, its report, "Transformation Planning Guidance," defined the transformation as "a process that shapes the changing nature of military competition and cooperation through new combinations of concepts, capabilities, people and organizations that exploit our nation's advantages and protect against our asymmetric vulnerabilities to sustain our strategic position, which helps maintain peace and stability in the world."[6]

The OFT has fleshed out and spread this concept of transformation, and at the same time made the term NCW generally and widely acknowledged. And in 2004, the U.S. Department of Defense, in its report, "Data Sharing in a Net-Centric Department of Defense," defined NCW as, "An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, expedited of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities[7] in the battlespace." The OFT was closed in 2006 upon the determination that it has completed its mission to drive the concept and process of transformation.

From then on, the view began to emerge that it is important to promote NCW while making sure to understand the characteristics of NCW. In 2007, for example, the Congressional Research Service (CRS) took up NCW in its report released after studying combat in

Afghanistan in 2001 and in Iraq in 2003 (hereinafter referred to as "the CRS Report"). The CRS Report cited, among others, "shortening of linkage time between sensors and shooters," "enhancement of potential capabilities of individual units," "promotion of flexible operations" and "fusion of wisdoms of front-line and rear units" as advantages of NCW. But these, not surprisingly, have all been utilized already in operations of the U.S. forces. The CRS Report, on the other hand, pointed out that the fog in battlefields, which NCW was supposed to dispel, has not been dispelled easily and that the U.S. forces rely too heavily on information and tend to underestimate its adversaries. It also raised many doubts about the NCW capabilities of the U.S. forces, such as inadequate resistance to cyberwar and electronic warfare.[8]

In December 2009, Secretary of Defense Robert M. Gates, in a contribution to the Foreign Affairs journal, "A Balanced Strategy," raised the question that the Department of Defense's strategy at the time had grown increasingly out of balance,[9] calling for a review of the U.S. defense strategy. While Gates strongly called for an appropriate balance between costs, required performance and development span, he set out a policy to support the current war by proactively taking advantage of the effectiveness of NCW recognized by the CRS Report and came out with the stance to utilize intelligence, surveillance and reconnaissance (ISR) capabilities, provide human and fiscal support for the use of drones and information process analysis, and attach importance to space assets to maintain networks and cope with cyberattacks.

The 2010 Quadrennial Defense Review (QDR), released in February 2010, cited "Deter and defeat aggression in anti –access environment," along with "Operate effectively in cyberspace," as priority items, giving instructions for enhancements of future long-range strike capabilities, C4ISR and space assets. Furthermore, the operational

concept, Air-Sea Battle (ASB),[10] released by the Department of Defense in 2013, said that its central idea is "to develop networked, integrated forces capable of attack-in-depth to disrupt, destroy and defeat adversary forces (NIA/D3)." Based on the above, it can be interpreted that NCW is being implemented with its concept being altered and deepened in accordance with the changes in the times.

3. New Networks

At present, the U.S. forces are trying to establish methods of attacks on standoff targets and organizational and efficient attacks by a variety of platforms by building new networks. The U.S. Navy has developed the Naval Integrated Fire Control-Counter Air (NIFC-CA) system, which enables attacks against targets below the horizontal line that cannot be detected by warships. By using E-2D maritime patrol and air control aircraft as a sensor or communication relaying apparatus, the NIFC-CA system transmits menacing target intelligence, such as cruising missiles, detected outside the field of search of shipborne radar to warships, which then launch missiles, etc. to destroy, or intercept, them (See Figure 1). Tests on NIFC-CA are still being conducted even after the system's introduction started in 2015, and the plan is also on the table to use the F-35 fighter jet as a sensor or communication relaying apparatus.[11]

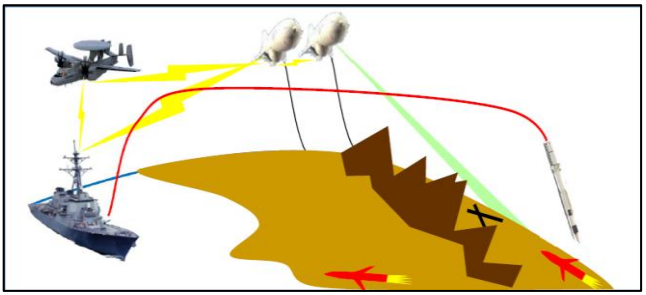

Figure 1 NIFC-CA Conceptual Drawing[12]

The building of networks is also under way for air defense and ballistic missile defense. In order to simultaneously respond to multiple threats of ballistic missiles, cruising missiles and aircraft, it is necessary to efficiently operate own assets by making prompt decisions. In order to meet these requirements, the U.S. forces are conducting research on Integrated Air Missile Defense (IAMD), which operates aircraft and missile units in coordination under the integrated command transcending the military branches. In April 2017, the U.S. forces successfully tested Integrated Battle Command System (IBCS), a part of IAMD.[13]

In addition to the development of sensors and shooters, such as NIFC-CA and IAMD as well as operation-level networks that efficiently link decision-makers, tactical-level networks and new networks are also starting to be constructed. The U.S. Air Force has developed data links between same-model fighter jets, such as Intra-Flight Data Link (IFDL) for F-22 jets and Multifunction Advanced Data Link (MADL) for F-35 jets. These data links within the formations of fighter jets can transmit and receive much larger volumes of data than conventional networks and also can enhance the situational awareness of pilots while securing strong resistance to jamming. Furthermore, since MADL has been designed on the premise of coexistence with data links the North Atlantic Treaty Organization (NATO) has been using heretofore, F-35 fighter jets are supposed to be able to assume the command of joint operations while securing the interoperability with combat aircraft of the NATO member countries.[14] On top of this, the U.S. Defense Advanced Research Projects Agency (DARPA) announced the Dynamic Network Adaptation for Mission Optimization (DyNAMO) program,[15] which is intended to link data

communication between same-model fighter jets, such as IFDL for F-22s and MADL for F-35s, to LINK-16 and other existing data links. Thus, the U.S. forces are promoting NCW in the direction of expanding its advantages, including "enhancement of potential capabilities of individual units."

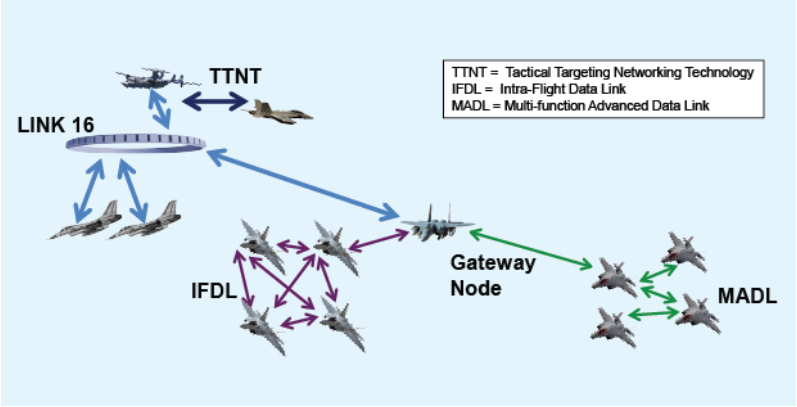

Figure 2 DyNAMO Conceptual Drawing[16]

Information in IFDL for the formation of F-22 fighters, MADL for the formation of F-35 fighters and LINK-16, including Tactical Targeting Networking Technology (TTNT), is shared via Gateway Node aircraft.

4. Threats to Networks

As NCW is based on the idea that "actions by forces in the networked conditions outstrip actions by non-networked forces,"[17] moves are becoming active to nullify the superiority of a networked adversary.

The Joint Operational Access Concept (JOAC), released by the U.S. Joint Chief of Staff in 2012, cited (1) the dramatic improvement and proliferation of weapons and other technologies; (2) the changing U.S. overseas defense posture; and (3) the emergence of space and cyberspace as increasingly important and contested domains, as three recent three trends in the operating environment, and pointed out that

the force projection by the U.S. forces is beginning to be disrupted by the enhancement of an enemy's air defense capability, cyberattack capability and electronic warfare capability. This may indicate that the superiority of NCW, which is based on the idea that "actions by forces in the networked conditions outstrip actions by non-networked forces," is beginning to diminish due to attacks to the friendly networks and the networking of potential adversaries.

4.1 Threat of Electromagnetic Pulse

In order for networks to function as designed, various equipment comprising a system needs to function properly and the communication among those equipment needs to be secured. If one of the equipment malfunctions due to a defect in the electronic circuit, this may result in the dysfunction of the entire system. Furthermore, today, as almost every equipment that constitutes the network incorporates electronic circuits, the dysfunction of the network caused by defects in electronic circuits of the equipment is not an issue just for the defense system.

For example, an accident that occurred in the Province of Quebec, Canada, on March 13, 1989, was triggered by the failure in the electric power infrastructure, causing the blackout throughout the province. The accident was traced to the failure in the equipment on the ground and power cables under the influence of the electromagnetic pulse (EMP) generated when a strong solar storm reached the earth's ionized layer. The recovery from the accident took almost an entire day, and a local newspaper then reported that the loss from the accident, even when limited to power stations alone, was estimated to amount to some ¥70 billion.[18]

Such example clearly shows that EMP poses a threat to the equipment that forms the network, including the defense system. Furthermore, EMP that causes enormous damage to electronic devices

occurs as a natural phenomenon, but the means has also been established to generate EMP artificially by calculating the targets and scope of its effects.

High altitude electromagnetic pulse (HEMP) generated by a high-altitude nuclear explosion and EMP generated by a high-power microwave generating equipment are said to have impacts on electronic circuits within a certain scope. In fact, the blackout in Quebec, Canada, is said to have been caused by the destruction of the power grid by the continuance for 92 seconds of changes in the magnetic flux density of 480nT/min on the ground.[19] In the former Soviet Union, an experiment was successfully conducted to generate the changes in the magnetic flux density of 1300nT/min for a duration of 20 seconds. It has been recorded that this experiment caused failures of ground and underground power transmission lines, telephone cables, generators for motors, and electronic devices, such as radars and wireless equipment.[20] Recognizing these effects of EMP, the U.S. forces have developed projectile weapons that attack electronic equipment along flight paths by mounting high-frequency generating tubes on warheads.

In addition to the situation described above, present-day EMP weapons are no longer the exclusive possessions of a military force or a state. The manufacturing of radio frequency (RF) weapons is said to be relatively easy as it does not necessarily require high costs or sophisticated technology. In fact, among simple magnetic equipment called transient electromagnetic devices (TEDs) that generate EMP, there reportedly are devices that can be put away in regular brief cases, though they need to come close to the targets as their valid range is limited due to low output power. In the present situation where warnings are being issued against terrorist attacks using TEDs,[21] it would be necessary to develop comprehensive measures to guard against EMP to not only secure the defense system but also prevent

social turmoil.

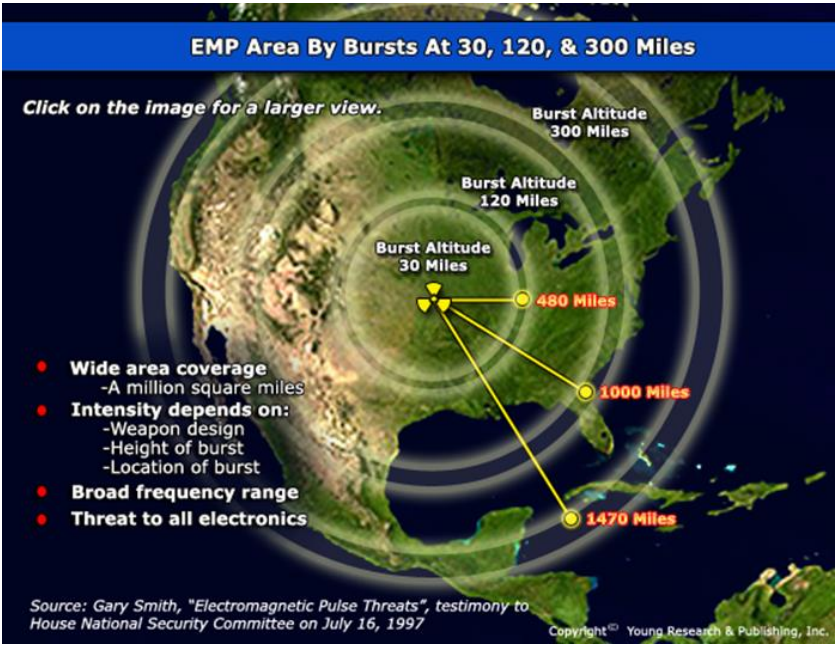

Figure 3 EMP Valid Range[22]

When an explosion occurs at an altitude of 300 miles (about 580 kilometers), the valid range of EMP covers almost the entire area of the North American continent.

4.2 Cyberattacks Using Electromagnetic Spectrum

EMP weapons can deliver a fatal blow to the network functions and thus are considered to be a threat to networks. However, no actual use of EMP weapons has been confirmed so far. In recent years, on the other hand, there have been several cases where cyberattacks using the electromagnetic spectrum (hereinafter referred to as "electromagnetic cyberattacks"), a threat to networks other than EMP, have been used to support air attacks or capture enemy weapons.

Previously, an enemy's closed network and sensors were neutralized or interrupted in electronic warfare. With the enhanced capabilities of electronic counter-countermeasures (ECCM) of sensors and networks, however, activities have actually been undertaken to penetrate the network of an adversary to neutralize or disrupt its sensors by cyberattacks. In fact, Israel's attack on a Syrian nuclear power reactor in 2007 and Iran's capture of a U.S. surveillance drone in 2012 are among the examples of such attacks, indicating the possibility of electromagnetic cyberattacks.[23]

In launching an attack on Syria's nuclear power reactor in September 2007, Israel penetrated Syria's air defense system to prevent its attack aircraft being detected. In doing so, Israel is said to have used the electromagnetic spectrum to send "false" signal information to the air defense system in an effort to mislead the Syrian air defense's surveillance.[24] Consequently, Israel's attack airplanes avoided Syria's detection and successfully attacked and destroyed a Syrian nuclear reactor without losing any aircraft.

In December 2012, Iran disrupted communication between the American reconnaissance drone RQ-170 and the control station of the U.S. forces, creating the situation where the drone had to switch to autonomous navigation. Iran is believed to have used the electromagnetic spectrum in transmitting the false positional coordinates to the unmanned reconnaissance plane, forced to autonomously navigate due to Iran's jamming, to cause the drone to falsely recognize its position, steering it to land on the location of Iran's designation.[25]

These attacks that use the electromagnetic spectrum to take advantage of the vulnerabilities of software used in remote control of drones and global positioning system (GPS) receivers are called advanced persistent threat (APT) attacks.[26] The problem of particular

concern today is the vulnerability of satellite communications. Besides drones, it was reported in 2011 in the United States in 2011 that the networks of Landsat-7 and the Terra EOS (Earth Observing System) satellite were penetrated twice each from 2007 to 2008, with access to them disrupted.[27]

These examples indicate the danger that even when the networking helps enhance ISR capabilities, expand the range of activities and make the accuracy of attacks more precise, it would become impossible to make the right decisions promptly if electromagnetic cyberattacks neutralize sensors or disrupt the communication that links the networks.

Figure 4 Video of RQ-170 Released by Iran[28]

5. Future Direction

The Joint Operational Access Concept (JOAC) seeks to exploit advantages in one or more domains out of the five domains (land, sea, air, space and cyber) to disrupt or destroy an enemy's anti-access/area denial (A2/AD) capabilities, and places a particular emphasis on the acquisition of the control of the domain of air. It also says that the domains of space and cyber are not only the areas of operations themselves but also important to provide support for the other areas of operations. In other words, in order to acquire and maintain air superiority in the initial phase of operations, it is also necessary to secure the freedom of action in space and cyberspace.

The U.S. Department of Defense classifies the cyberspace

comprising a myriad of networks and nodes into the three layers: Physical Network Layers consisting of hardware, software and infrastructure, Logical Network Layers formed by Physical Network Layers, and Cyber-Persona Layers covering accounts and mail addresses that exist in Logical Network Layers (as shown in Figure 5). As Physical Network Layers are the places of Signal Intelligence (SIGNT), including Computer Network Exploitation (CNE), the Department of Defense positions the physical domain as the gateway to military activities in cyberspace.[29]

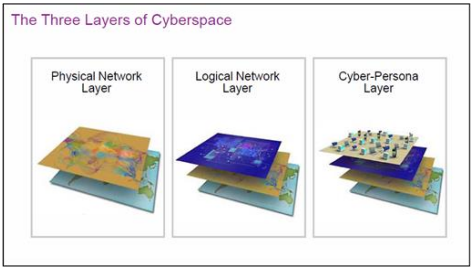

Figure 5 Three Layers in Cyberspace[30]

The cyberspace comprises the Physical Network Layers, Logical Network Layers and Cyber-Persona (virtual personality) Layers. The Physical Network Layers consist of wired networks and electronic (radio) networks.

5.1 Securing of Superiority in Space and Cyber Domains to Acquire Air Mastery

In order to acquire air mastery on the premise of the networking of an adversary, it is necessary, as mentioned above, to protect our own networks and destroy the function of an enemy's network. Thus, Operational Access Precepts of the JOAC plans a surprise attack by actions in the space and cyber domains in the initial phase of a combat in order to disrupt an enemy's A2/AD capabilities. Cited as the three

requirements for successful surprises are deception, stealth and ambiguity.

However, these actions in the space and cyber domains are conducted by the opposing forces. In other words, in order to acquire our own air mastery, it is necessary to secure the superiority in capabilities to enable surprise against an enemy's networks in the space and cyber domains and also deny an enemy's surprise.

Since the space and cyber domains undertake the role of providing support for critical position, navigation, and timing, command and control, missile warning, weather, and intelligence collection, the relative merits in these two domains have a major impact on the offense and defense in network warfare, and eventually, the acquisition of air superiority. For this reason, the success and failure of electromagnetic cyberattacks in the apace and cyber domains are considered important.

Generally speaking, satellite communication is not encrypted, and it has been pointed out that there is the risk of critical infrastructure, including electric power plants, being taken over, along with articles of daily use, such as vehicles and cell phones.[31] In other words, networks and equipment consisting of communication that use the electromagnetic spectrum can be targets of electromagnetic cyberattacks, regardless of whether they are in the public or private sectors.

In the United States, research teams of the Georgia Institute of Technology and the University of Virginia, with capital infusion by the Department of Defense, have jointly developed the System-Aware Secure Sentinel system and succeeded in the system's demonstrative tests. This means that the United States is moving closer to the establishment of a method to counter electromagnetic cyberattacks against drones.[32] In addition, DARPA is currently in the process of developing the High Assurance Cyber Military System (HACMS),

seeking to develop a system that can withstand cyberattacks by establishing technology to build a highly-reliable cyber physical system by the mathematical approach.[33] At the present stage, HACMS is designed for military-use drones. But it is being redesigned for use in the private sector, raising the likelihood of progress being made in responses to electromagnetic cyberattacks in both the military and private sectors.

In order to secure the superiority in the space and cyberspace domains, it is essential to respond to electromagnetic cyberattacks. As responses to electromagnetic cyberattacks also mean the offense and defense over network vulnerabilities, various countries are making efforts to overcome such vulnerabilities. It can be argued that Japan as well needs to overcome its vulnerabilities to such electromagnetic cyberattacks.

Figure 6 Image of Test on Anti-Hacking System[34]

An experimental unmanned air vehicle (UAV) equipped with an anti-hacking system

Figure 7 Video Image of Test on HACMS[35]

The first test conducted by mounting HACMS on a robot's operating system.

5.2 For Securing Superiority in Electromagnetic Spectrum

As stated above, the war over networks can be termed as the war in the domain of the electromagnetic spectrum. The ability and speed of detecting and neutralizing an enemy's electromagnetic spectrum activities influence the relative merits and demerits of war in the domain of the electromagnetic spectrum. The United States recognized the importance of this in 2012, and Admiral Jonathan W. Greenert, then the Chief of Naval Operations, turned his attention to the fact that activities in the space and cyber domains have a significant impact on other operational areas, and announced a research paper, in which he claimed that "activities in the domain of the electromagnetic spectrum brings a victory in combat."[36] In "Winning the Airwaves," released by the Center for Strategic and Budgetary Assessments (CSBA) in 2015, presented the recognition that as a result of the progress in the networking of the friendly and adversary forces, the U.S. forces are beginning to give away the superiority of the electromagnetic spectrum they have built up, and advanced a proposal to recapture that superiority.[37]

In view of the importance of the electromagnetic spectrum in networks, the U.S. Army established the concept of Cyberspace and Electronic Warfare Operations, and sorted and rebuilt the relationships between cyberspace actions and electronic warfare (EW) in and out of the Department of Defense Information Network (DODIN).[38] In "Cyberspace and Electronic Warfare Operations," cyber electromagnetic activities (CEMA)[39] are defined as activities leveraged

to seize, retain, and exploit an advantage of friendly forces over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system of friendly forces, with the intention of acquiring the superiority in cyberspace and the domain of the electromagnetic spectrum. The conceptual diagram sorted by the U.S. Army is shown in Figure 8.

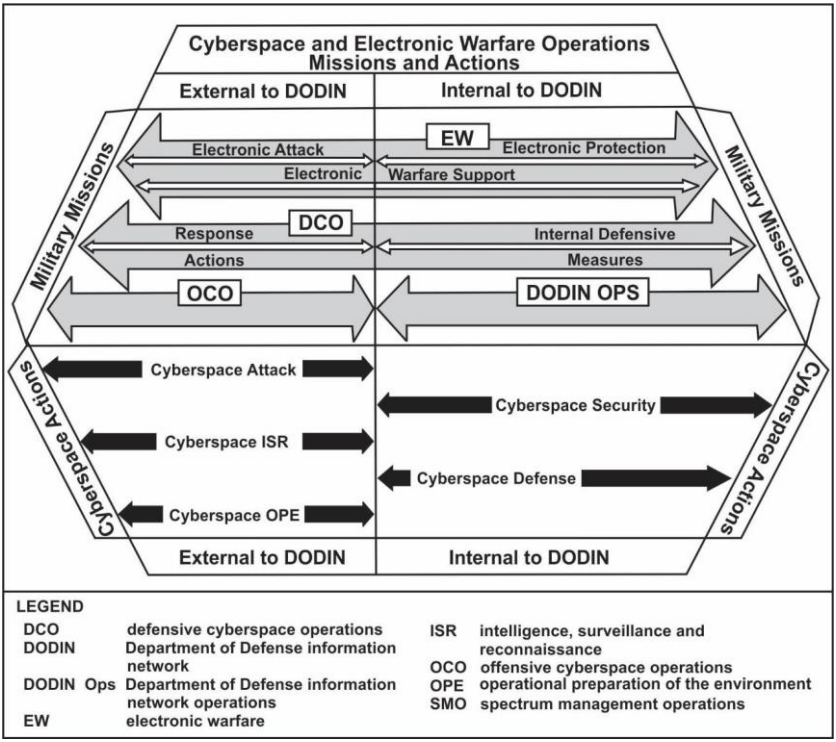

Figure 8 Missions and Actions in Cyberspace and Electronic Warfare Operations[40]

The diagram classifies cyberspace and electronic warfare operations as internal or external to the Department of Defense Information Network (DODIN), respectively, and defines activities in their respective domain.

5.3 Problems with Electromagnetic Spectrum Operations

As “Joint Publication 6-1 Joint Electromagnetic Spectrum Management

Operations" classifies users of electromagnetic waves into "Friendly" (including own forces), "Adversary" and "Neutral" (private sector, commercial, etc.),[41] electromagnetic waves by unknown users should not be ignored. Today, electromagnetic waves from low frequency (LF) to extremely high frequency (EHF) are used widely for a variety of communications and radars, regardless of the public or private sectors. In fact, a lot of electromagnetic waves are flying about in Japan and on its perimeters to form the complex electromagnetic spectrum environment, subjecting electromagnetic spectrum activities to a variety of restraints.

On the other hand, the digitization of various information in theaters of operations is resulting in an explosive increase in demand for communications. In the Iraq war, the U.S. forces reportedly arranged for over 20,000 frequencies.[42] In the war, the U.S. forces and allied forces made use of private-sector satellite communications to meet their communication requirements. The Defense Information System Agency (DISA)[43] reported these requirements accounted for as much as 84% of the entire military requirements.[44] The current situation is that it is indispensable for even military organizations to utilize communications infrastructures of the private sector. As communications requirements are expected to increase in large volumes, the satisfaction of such requirements for the execution of operations should require an increase in lines of communication, or an expansion of utilization of the electromagnetic spectrum.

In light of the dual conditions of the complex electromagnetic spectrum environment and expanding communications requirements, it would not be an easy task to deny an enemy's electromagnetic cyberattacks and electronic attacks while ensuring the freedom and safety of electromagnetic spectrum activities. In order to realize such task, it would also require activities to understand the electromagnetic

spectrum environment not only in times of operations but also under normal circumstances. For this reason, in the United States, the Defense Spectrum Organization (DSO) of the DISA has built a massive database related to the status of utilization of the electromagnetic spectrum, and also developed the system to enable the smooth planning of electromagnetic spectrum activities by getting a handle on the electromagnetic spectrum environment in areas of operations in advance through the electromagnetic spectrum management on a global scale.[45] It appears that Japan also needs to develop and improve its preparedness to manage the electromagnetic spectrum under normal circumstances to acquire the superiority that allows it to secure its own actions while disrupting actions by a potential enemy in preparation for possible combat in the domain of the electromagnetic spectrum.

5.4 How to Respond to EMP

As pointed out earlier, an EMP attack has yet to actually become a reality unlike electromagnetic cyberattacks. However, in view of a potentially massive impact on electronic equipment and the existence of simple and actually usable devices, it would be more necessary than ever to take measures against electromagnetic waves in various platforms and at facilities of command centers. Furthermore, since targets of EMP attacks and cyberattacks are not restricted only to defense systems, military responses alone are apparently not sufficient.

The loss of functions of power stations and other electricity infrastructures located around military bases or military posts and the means of transportation due to EMP attacks or electromagnetic cyberattacks would surely have no small impact on base operations. In particular, when such loss of functions persists for a long period of time, it is expected to cause great troubles in maintaining the base functions and the smooth engagement, including agile deployment of forces, and

may even create a situation where it becomes extremely difficult to continue operations.

In view of the potentiality of such circumstances, the U.S. forces revived the EMP protection program and entered into a contract worth $700 million in April 2015 in order to enhance the electronic device protection performance of the program. In addition, despite the earlier abolition of the EMP protection program
, the U.S. forces have already instituted HEMP protection standards for each category of equipment and facilities, including the common standards and individual standards for onshore Command, Control, Communications, Computers, and Intelligence (C4I) facilities, military aircraft and surface vessels.[46] Thus, the U.S. forces have had the basis for promoting EMP countermeasures from the very beginning. In addition, in view of the fact that power networks, communications and other critical infrastructures have not been reinforced for EMP protection, the U.S. government has appropriated $2 billion for EMP protection for the national power grid in the FY2017 budget. Though conditional upon Congressional approval, the U.S. government is likely to push ahead with similar measures.[47]

It can be argued that Japan, by using U.S. policy measures as a reference, needs to make national efforts to defend not only the bases and platforms of the Self-Defense Forces (SDF) but also electric power and other critical infrastructures against EMP attacks and electromagnetic cyberattacks by adversary forces.

6. Summary

The notion of system of systems was developed from the strategy that combines various command and reconnaissance/surveillance systems with sophisticated offensive weapons, which led to the great success in the Gulf War. The notion of system of systems then led to the creation

of the concept of NCW. At present, the U.S. forces and forces of major countries have built the networks in areas of operations and made NCW-based combat an ordinary state. While NCW-based combat has now become nothing new, efforts to seek an optimum combination of sensors and shooters have continued, resulting in the development of networks, including NIFC-CA, IFDL and MADL.

On the other hand, following the networking of forces of major countries, the NCW-proposed superiority in the networking over enemy forces has been undermined, requiring responses to combat between the networked units. In combat between the networked units, in addition to conventional attacks on the platforms, the networks themselves become subject to attacks. Thus, the handling and management of vulnerabilities of the networks become focal points, presumably increasing the importance of protection against electromagnetic cyberattacks and EMP attacks and the management of the electromagnetic spectrum. In other words, the protection of ISR and networks becomes indispensable for securing air superiority and the establishment of superiority in space and cyberspace becomes essential.

While cyber protection is beginning to become the basis of research and development of defense equipment, moves are observed to sort out the operations and relationships of cyber warfare and electronic warfare. The concept of electromagnetic maneuver warfare (EMW) envisioned by the U.S. forces is designed to capture the electromagnetic spectrum of friendly and adversary forces in theaters of operations, remove impediments in an appropriate and expeditious manner, and create an environment for friendly forces to use the electromagnetic spectrum.[48] The concept is based on the perception that the success or failure of the management of the electromagnetic spectrum that constitutes networks has the game in its hands.

At present, defense equipment that can keep track of the status of

utilization of the electromagnetic spectrum in theaters of operations in real time has yet to emerge. But such equipment is expected to become indispensable to create a superior environment in the offense and defense between the networks. Furthermore, the use of artificial intelligence in the search and identification of the electromagnetic spectrum has been proposed.[49] In the not-too-distant future, the conditions for the offense and defense over the electromagnetic spectrum may undergo a significant change.

The building of networks in an air space of operations has been pursued heretofore not only by the U.S. forces but also by the Air Self-Defense Force (ASDF). In fact, the ASDF is equipped with the Japan Aerospace Defense Ground Environment (JADGE), which plays an important role in air-defense operations and ballistic missile defense, as well as tactical data links for information sharing between platforms, enhancing its abilities to execute operations in areas surrounding Japan while securing the interoperability with the U.S. forces.[50] Furthermore, aside from the ASDF, the Ground Self-Defense Force (GSDF) has been striving to expand the scope of defense by connecting ground-to-air missiles and anti-ship missiles to the networks with JADGE at the core. On top of this, the Electronic Systems Research Center of the Acquisition, Technology & Logistics Agency (ATLA) is conducting research on an adaptive control millimeter-wave network system to respond to expanding communications requirements. The Ministry of Defense has also been striving to steadily develop the networks and enhance their performance.[51]

In the present day when controlled operations by military units are supported by the complex and diversified networks and communications between them, safeguarding the the networks is synonymous with the securing of the command and control, and operational capabilities. And what is necessary to use the networks in a

stable manner is the sufficient level of defense against cyberattacks and EMP attacks as well as securing of the superiority in the domain of the electromagnetic spectrum. For this reason, Japan, inclusive of the private sector, is being called upon to enhance its resistance to cyberattacks and EMP attacks and develop its systems necessary in the domain of the electromagnetic spectrum.

---

[1] Joint Surveillance Target Attack Radar System, which detects ground targets with the E-8 airborne radar and commands and controls attacks. It was jointly planned by the U.S. Air Force and the U.S. Army.

[2] Arthur K. Cebrowski, "Network-Centric Warfare: Its Origin and Future," http://www.kinection.com/ncoic/ncw_origin_future.pdf

[3] The Office of Force Transformation (OFT) was established on October 29, 2001, as the office to promote the transformation of the U.S. military, and Vice Admiral Arthur K. Cebrowski was appointed as its first director.

[4] Effect Based Operation (EBO)

[5] National Defense Panel, "Transforming Defense National Security in the 21st Century," December 1997.

[6] Secretary of Defense, "Transformation Planning Guidance," April 2003, p. 4.

[7] The term used in the original text is "knowledgeable entities," which this author liberally translated as military forces. U.S. Department of Defense, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004, p4.

[8] Clay Wilson, "CRS Report for Congress," RL32411, March 15, 2007.

[9] Robert M. Gates, "A Balanced Strategy," *Foreign Affairs*, January/February 2009.

[10] Air-Sea Battle Office, "AIR-SEA BATTLE: Service Collaboration to Address Anti-Access & Area Denial Challenges," May 2013; http:// archive defense. gov/pubs/ASB-Concept Implementation-Summary-May-2013.pdf
Ahead of the announcement by the Department of Defense, the Center for Strategic and Budgetary Assessments (CSBA) announced ASB in 2010.

[11] Kris Osborn, "Navy to Integrate F-35 with Beyond-the-Horizon Technology," *DEFENSETECH*, January 22, 2015;

http://www.defensetech.org/2015/01/22/navy-to-integrate-f35-with-beyond-the-horizon-technology/

[12] Jeffrey H. McConnell, "Naval Integrated Fire Control–Counter Air Capability‐Based System of Systems Engineering," Naval Surface Warfare Center, November 14, 2013.

[13] The MQM-170 cruising missile target and the PAAT ballistic missile target were launched simultaneously. Based on target intelligence obtained by the AN/MPQ-53 Patriot radar and the AN/MPQ-64 Sentinel radar by tailing the multiple targets, IBCS identified and assessed the threats, selected PAC-2 and PAC-3 as the most suitable shooters for the respective targets, and succeeded in intercepting both missiles almost simultaneously. "US Army Uses Northrop

Grumman-Built System to Destroy Multiple Targets in Air and Missile Defense Test,"GLOBE NEWSWIRE, April 18, 2016; http://www.globenewswire.com/newsarchive/noc/press/pages/news_release.html?d=10161904

[14] "The F-35: A New Era of International Cooperation," Lockheed Martin, June 15, 2015; http://www.lockheedmartin.com/us/news/features/2014/f35-new-era-of-internati onal-coopration.html

[15] John Keller, "DARPA wants new ideas to create reconfigurable aircraft networking in battlefield condition," Military Aerospace, October 19,2015; http://www.militaryaerospace.com/articles/2015/10/aircraft-networking-interoper ability.html

[16] https://www.darpa.mil/DDM_Gallery/DyNAMO%20Update-619x316.png

[17] Yashuhiro Oshima, Yoshiyuki Miyauchi, Kazuhiko Furumoto, Noriyuki Yoshida, Hiroshi Iwashita, Akira Sato and Kentaro Ohe, Beikoku no Toransufomeishon to Wagakuni no Boeiryoku no Arikata [U.S. Force Transformation and the Concept of Japan's Defense Capability], National Institute for Defense Studies (NIDS), ed., *Boei Kenkyujo Kiyo* [*NIDS Security Studies*], Volume 10, No. 1, September 2007, p. 52.

[18] Solar-Terrestrial Environment Laboratory, Nagoya University, STEL Newsletter No. 28, April 2002, p. 3.

[19] Tesla is the unit of the magnetic flux density that shows the measurement of the density of a magnetic field obtained by multiplying the strength of a magnetic field by the magnetic permeability. Nano means "one billionth," and 10^{-9}T=1nT. Generally, EMP is said to be caused by rapid changes in the magnetic flux density. It appears that the larger an amount of change per unit time, the larger the impact on electronic circuits.

[20] Electric Infrastructure Security Commission, "Report: USSR Nuclear EMP Upper Atmosphere Kazakhstan Test 184".

[21] Sukeyuki Ichimasa, Burakkuauto Jitai ni Itaru Denji Parusu (EMP) Kyoi no Shoso to Sono Tenbo [Various Aspects of the Threat of Electromagnetic Pulse (EMP) Leading to the Blackout Situation and the Outlook], *Boei Kenkyujo Kiyo* [*NIDS Security Studies*], Volume 18, No. 2, February 2016, pp. 7-8.; "Radio Frequency Weapons and the Next Phase of Terrorism," http://www. 123helpme. com/veiw.asp?id-7737

[22] "Millions Will Die In The First Month - EMP Attack On America Part2," All News Pipe Line, August 11, 2015; http://allnewspipeline.com/Millions_Will_Die_In_The_First_Month.php

[23] Yoshio Kajiwara, A2/AD Jokyoka deno Denshisen [Electronic Warfare under the A2/AD Situation], *Denshi Joho Tsushin Gakkai Gijutsu Kenkyu Houkoku* [*Institute of Electronics, Information and Communication Engineers (IEICE) Technology Research Report*], April 24, 2015, pp. 20-21.; "Iran shows film of captured US drone," BBC, December 8, 2011; http://www.bbc.com/news/world-middle-east-16098562

[24] Hatsuo Kimura, A2/AD Kankyoka ni Okeru Saibaa Denjisen no Saishin Doko (Zenpen) [Latest Trend of Cyber Electromagnetic War under the A2/AD Environment (First Part)], *Gekkan JADI* [*Monthy JADI*], June 2016, p. 41.

[25] Ibid., p. 41.
[26] A type of cyberattacks. The Information-Technology Promotion Agency, Japan （IPA）defines APT attacks as follows: “Persistent attacks that take advantage of vulnerabilities, combine multiple existing forms of attack, and target particular companies or individuals by means of social engineering, which are very hard to deal with.”
[27] “USSC, 2011 Report to Congress of the U.S.-China Economic and Security Review Commission,” November 2011.
[28] Clay Dillow, “Video: Iran Puts Its Captured RQ-170 Drone on Display,” POPULAR SCIENCE, December 9, 2011; http://www.popsci.com/technology/article/2011-12/video-iran-puts-its-captured-rq-170-drone-display
[29] “Joint Publication 3-12(R) Cyberspace Operation,” February 5, 2013.
[30] Ibid.
[31] “Saibaa Tero Semaru Kyoi…Bei Hakkaa Kokusai Kaigi” [Looming Threat of Cyberterrorism…U.S. Hackers’ International Conference], YOMIURI ONLINE, September1, 2015; http://www.yomiuri.co.jp/scienence.feature/CO017291/20150901-OYT8T50152.html
[32] Pierluigi Paganini, “The System Aware Secure Sentinel against drones hacking, “ Security Affairs, December 7, 2014; http://securityaffairs.co/wordpress/30885/security/system-aare-secure-sentinel-drone.html
[33] John Keller, “DARPA releases formal solicitation for HACMS cyber security initiative for military vetronics,” Military &Aerospace, February 26, 2012; http://www.militaryaerospace.com/article/2012/02/darpa-release-formal-solicitation-for-hacms-cyber-security-formilitary-vetronics.html
[34] http://www.sercuarc.org/wp-content/uploads/2014/11/SERC-RT-115-Security-Engineering-Pilot-Final-Report-SERC-2013-TR-036-4-Parts-1a-1b-3-4-20150131.pdf
[35] http://lunaticoutpost.com/thread-663121.html
[36] Admiral Jonathan W. Greenert,” “Imminent Domain,” *Proceedings Magazine*, December 2012; http://www.usni.org/magazines/proceedings/2012-12/imminent-domain
[37] Bryan Clark, Mark Gunzinger, “Winning the Airwaves,” CSBA, 2015.
[38] “CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS FM 3-12,” Headquarters, Department of the Army, April 2017.
[39] “CYBER ELECTROMAGNETIC ACTIVITIES FM 3-38,” Headquarters, Department of the Army, February 2014.
[40] Ibid.
[41] According to “Joint Publication 6-01 Joint Electromagnetic Spectrum Management Operations,” the Electromagnetic Operation Environment consists of Friendly EOB, Adversary EOB and Neutral EOB.
[42] Masatake Niimi, Jitsuryoku toha 21 Tushin Shuhasuu Kanri [Real Abilities 21 Communications and Frequency Management], *Air World*, December 2005 Issue, pp. 130-134.
[43] The Defense Information System Agency (DISA) is the internal bureau of the U.S. Department of Defense. The DISA manages the military-related

communications and electromagnetic spectrum, with over 7.2 million pieces of data in five databases placed under its management. A total of about 6,000 employees and over 1,500 men and women in uniform manage them.

[44] Julian C. Cheater, "Accelerating The Kill Chain via Future Unmanned Aircraft," USAF, April 2007.

[45] "DEFENSE SPECTRUM ORGANIZATION," DISA; http://disa.mil/Mission-support/Spectrum

[46] As the common standards, the U.S. forces have MIL-STD-2169B (High Altitude Electromagnetic Pulse (HEMP) Environment) issued in December 1993; MIL-STD-461F (Electromagnetic interference characteristics requirements for subsystems and equipment) issued in December 2007; MIL-STD-464C (Electromagnetic environmental effects requirements for systems) issued in December 2010; MIL-STD-188-125-1 (HEMP protection for ground-based C4I facilities stationary facilities) issued in July 1998; MIL-STD-3023(HEMP protection for military aircraft) issued in November 2011; and MIL-STD-4023(HEMP protection for military surface ships) issued in January 2016.

[47] Hatsuo Kimura, A2/AD Kankyoka ni Okeru Saibaa Denjisen no Saishin Doko (Zenpen) [Latest Trend of Cyber Electromagnetic War under the A2/AD Environment (First Part)], *Gekkan JADI* [*Monthy JADI*], July 2016, p. 29.

[48] "Information Dominance Roadmap 2013-2028," U.S. NAVY, pp. 9-10.

[49] Sydney J. Freedberg Jr, "Faster Than Thought: DARPA, Artificial Intelligence, & The Third Offset Strategy," Breaking Defense; http:// breaking defense.com/2106/02/faster-than-thought-darpa-artificial-inteligence-the-thirad-offset-strategy/

[50] *Defense of Japan 2015*, Ministry of Defense, pp. 229-230, pp. 240-242.

[51] http://www.mod.go.jp/atla/densouken.html