Chapter 9

Electronic Intelligence Warfare

North Korea conducts electronic intelligence warfare (EIW) as part of all operations. This chapter covers the 11 different components of EIW and how North Korea uses it in conjunction with combat operations. North Korea conducts EIW to obtain information on its enemies, to deceive them, and to achieve effects against them. While much of North Korean EIW is conducted above the tactical level on the battlefield, EIW at all levels will affect the tactical units.

TACTICAL-LEVEL ELECTRONIC INTELLIGENCE WARFARE

9-1. The Korean People's Army (KPA) defines *chonja chinungjon*, or electronic intelligence warfare (EIW), as specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The primary goals of EIW are to—

- Influence an enemy's decision making through its collected and available information, information systems, and information-based processes.
- Retain the ability to employ friendly information and information-based processes and systems.

9-2. Information and its management, dissemination, and control are critical to the successful conduct of tactical missions. Given today's advancements in information and information systems technology, this importance is growing in scope, impact, and sophistication. The KPA recognizes the unique opportunities EIW gives tactical commanders, and it continuously strives to incorporate EIW activities in all tactical missions and battles.

9-3. EIW may help degrade or deny effective enemy communications and blur or manipulate the battlefield picture. In addition, EIW helps the KPA achieve the goal of dominating the tempo of combat. Using a combination of perception management activities, deception techniques, and electronic warfare (EW), the KPA can effectively slow or control the pace of battle. For example, the KPA may select to destroy lucrative enemy targets through the execution of EW. It may also execute a perception management activity that weakens the enemy's international and domestic support, causing hesitation or actual failure of the operation. The KPA executes deception plans to confuse the enemy and conceal its true intentions. More-traditional EW activities also contribute to the successful application of EIW at the tactical level by challenging the enemy's quest for information dominance.

9-4. EIW also supports the critical mission of counterreconnaissance at the tactical level. The KPA constantly seeks ways to attack, degrade, or manipulate the enemy's reconnaissance, intelligence, surveillance, and target acquisition (RISTA) capabilities. All enemy target acquisition systems and sensors are potential targets.

ELECTRONIC INTELLIGENCE WARFARE TACTICAL TASKS

9-5. The effects of EIW can be multidimensional and at times hard to pinpoint. The KPA, however, highlights the following tasks and associated effects as critical to the application of EIW at the tactical level: destroy, degrade, disrupt, deny, deceive, exploit, and influence.

DESTROY

9-6. Destruction tasks physically render an enemy's information systems ineffective. They are most effective when timed to occur before the enemy executes a command and control (C2) function or when focused on a resource-intensive target that is hard to reconstitute. Neutralizing or destroying the opponent's information capability can be brought about by physical destruction of critical communications nodes and links.

DEGRADE

9-7. Degradation attempts to reduce the effectiveness of the enemy's information infrastructure, systems, and collection means.

DISRUPT

9-8. Disruption activities focus on interrupting enemy observation and sensor capabilities at critical times and locations. Disruption impedes the enemy's ability to observe and collect information and to obtain or maintain information dominance.

DENY

9-9. Denial activities attempt to limit the enemy's ability to collect or disseminate information on the KPA or deny its collection efforts.

DECEIVE

9-10. Deception activities strive to mislead the enemy's decision makers and manipulate its overall understanding of KPA activities. Deception manipulates perception and causes disorientation among decision makers within their decision cycle.

EXPLOIT

9-11. Exploitation activities attempt to use the enemy's C2, communications, or RISTA capabilities to the advantage of the KPA. The KPA also uses its various EIW capabilities to exploit any enemy vulnerability.

INFLUENCE

9-12. Influencing information affects an enemy's beliefs, motives, perspectives, and reasoning capabilities in order to support North Korean objectives. This may be done through misinformation or by manipulating information.

SYSTEMS WARFARE

9-13. In the systems warfare approach to combat (see chapter 1), the KPA will focus on attacking C2, communications, RISTA, logistics units, or other critical components of selected combat systems belonging to enemy forces. It is often more feasible to attack such targets than to directly engage the enemy's combat or combat support forces. Tactical-level EIW can be a primary means of attacking these assets, either on its own or in conjunction with other components of the KPA's own combat system.

WINDOWS OF OPPORTUNITY

9-14. To conduct successful actions against a more-powerful force enjoying a technological overmatch, the KPA will exploit windows of opportunity. Sometimes these windows occur naturally, as a result of favorable conditions in the operational environment. Most often, however, the KPA will have to create its own opportunities for offensive or defensive action. EIW can contribute to this by executing effective deception techniques, EW, and physical destruction, including—

- Destroying or disrupting enemy C2, communications, and RISTA assets.
- Deceiving enemy imagery and signals sensors.
- Selectively denying situational awareness.
- Slowing the tempo of enemy operations by overloading or confusing enemy leaders with too much or contradictory information.

- Isolating key units of the enemy force.
- Putting information on the Internet that draws people, including deception operations, "click bait," and "honey traps."
- Using its peasant class as both a direct and indirect influencer of the operational environment (deception operations, ruses, and decoys).

COMPETITION AND THE HUMAN DIMENSION

9-15. Three components compose the human dimension component during periods of conflict—cognitive, physical, and social. EIW normally attacks the cognitive and social aspects of the enemy's soldiers. War has normally been a clash of wills between at least two sides, but has risen to new heights in the current global environment. North Korea will use all aspects of EIW to attack its enemy before any shots are actually fired on the battlefield.

COMPONENTS OF ELECTRONIC INTELLIGENCE WARFARE

9-16. North Korean EIW should not be confused with the U.S. view of EW or information operations. North Korean EIW contains a number of components that are part of U.S. information operations, including EW, but also includes several activities that the U.S. does not normally associate with these terms. Integrated within North Korean EIW doctrine are the following components:

- EW.
- Deception.
- Physical destruction.
- Protection and security measures.
- Perception management.
- Information attack.
- Computer warfare.
- Reconnaissance.
- Cryptanalysis.
- Intelligence collection.
- Disinformation operations.

9-17. These components do not exist in isolation from one another and are not mutually exclusive. The overlapping of functions, means, and targets requires all components to be integrated into a single, cohesive EIW plan. Effective execution of EIW, however, does not necessary involve the use of all components concurrently. In some cases, one component may be enough to successfully execute a tactical EIW action. Nevertheless, using one component, such as camouflage, does not by itself necessarily constitute an application of EIW.

9-18. The use of EIW components is determined by the tactical situation and support to the overall operational objective. The size and sophistication of an enemy force also determines the extent to which the KPA employs the various components of EIW. The KPA commander may mix and match components to best suit tactical needs, within the bounds of guidance from higher authority.

9-19. Tools for waging EIW can include, but are not limited to—

- Conventional physical and electronic destruction means.
- Malicious software.
- Denial-of-service attacks.
- The Internet.
- The media.
- International public opinion.
- Communications networks.
- Various types of reconnaissance, espionage, and eavesdropping technologies.

9-20. The KPA can employ EIW tools from both civilian and military sources and from assets of third-party actors. Information links, such as transmitters, communications devices, and protocols, will be targeted. The KPA is extremely adaptive and will employ the best option available to degrade, manipulate, influence, use, or destroy an information link. See table 9-1 for typical examples of EIW objectives and targets.

Table 9-1. Electronic intelligence warfare objectives

Mission	*Objectives*	*Possible Targets*
Electronic warfare	Exploit, disrupt, deny, and degrade the enemy's use of the electromagnetic spectrum.	Command and control and RISTA assets and networks.
Deception	Mislead enemy decision makers. Cause confusion and delays in the decision making process. Persuade local population or international community to support North Korea's objectives.	Key military decision makers. General enemy populace and international media outlets and Internet sites.
Physical destruction	Destroy the enemy's information infrastructure.	Command and control nodes and links, RISTA assets, telecommunications, and power sources.
Protection & security measures	Protect critical information assets.	Enemy RISTA assets.
Perception management	Distort reality or manipulate information to support North Korea's goals.	Enemy RISTA assets. Local populace and leaders. Media outlets, both international and domestic.
Information attack	Alter or deny key information.	Decision makers and other information users. Systems reliant on accurate information.
Computer warfare	Disrupt, deny, or degrade the enemy's computer networks and information flow.	Enemy command and control unit, RISTA assets, and computer networks.
Reconnaissance	Obtain key information on the enemy to achieve positive results on the battlefield.	Enemy units and leaders.
Cryptanalysis	Decode the enemy's coded message traffic.	Enemy written and electronic communications.
Intelligence collection	Obtain key information as directed by the KPA unit leader.	Enemy units and leaders.
Disinformation operations	Deliberately release false information, causing the enemy to make a wrong decision.	Enemy political and military leaders.
KPA Korean People's Army RISTA reconnaissance, intelligence, surveillance, and target acquisition		

ELECTRONIC WARFARE

9-21. The KPA employs both lethal and nonlethal means of EW. Nonlethal methods range from signals reconnaissance and electronic jamming to the deployment of corner reflectors, protective countermeasures, and deception jammers. The KPA can employ low-cost Global Positioning System jammers to disrupt enemy precision munitions targeting, sensor-to-shooter links, and navigation. Lethal EW activities include the physical destruction of high-priority targets supporting the enemy's decision-making process, such as reconnaissance sensors, command posts (CPs), and communications systems. They also include activities such as lethal air defense suppression measures. If available, precision munitions can degrade or eliminate high-technology C2 and communications assets and associated links.

9-22. EW activities often focus on the enemy's advanced C2 and communications systems, developed to provide real-time force synchronization and shared situational awareness. The enemy relies on the availability of force composition and locations for both sides, digital mapping displays, and automated targeting data. By targeting vulnerable communications links, the KPA can disrupt the enemy's ability to digitally transfer and share such information. The KPA enhances its own survivability through disrupting the enemy's ability to mass fires with dispersed forces while increasing enemy crew and staff workloads and disrupting enemy fratricide-prevention measures.

9-23. EW is a perfect example of the integrated nature of KPA EIW components. It overlaps significantly with protection and security measures, deception, and physical destruction. Reconnaissance, aviation, air defense, artillery, and engineer support may all contribute to successful EW for EIW purposes. See Appendix E for additional information on KPA EW operations.

Signals Reconnaissance

9-24. Signals reconnaissance is action taken to detect, identify, locate, and track high-value targets through the use of the electromagnetic spectrum. It includes both intercept and direction finding, which may enable a near-real-time attack on the target. KPA commanders determine the priorities for signals reconnaissance by determining which high-value targets must be found in order to have the best chance for success. If the collected intelligence is of higher value than the destruction of the target, the KPA commander determines the best tactical course of action: destroy the target, jam it, or continue to exploit the collected information.

9-25. Signals reconnaissance targets must be detectable in some manner in the electromagnetic spectrum. The KPA operates available system(s) that perform this type of detection. Some high-value targets do not generate an electromagnetic signature and must be detected by other means. Those sought by signals reconnaissance efforts are specific to the battle, the KPA's plan and capabilities, and the enemy's plan and capabilities. Typical targets of KPA signals reconnaissance efforts include enemy—

- Maneuver unit CPs.
- Forward air controllers.
- Logistics CPs.
- Fire support and tactical aviation networks.
- Target acquisition systems.
- Reconnaissance and sensors networks.
- Battlefield surveillance radars.

9-26. Signals reconnaissance information is fused with information obtained from other sources. For example, the KPA can use trained reconnaissance units to—

- Put "eyes on" targets and objectives.
- Collect required information.
- Provide early warning.
- Monitor lines of communications and movement corridors in a target area.

9-27. Such reconnaissance could possibly include a signals reconnaissance capability.

Electronic Attack

9-28. KPA electronic attack supports the disaggregation of enemy forces. The primary form of electronic attack is jamming—interference with enemy signals links in order to prevent their proper use. Jamming priorities are similar to those for signals reconnaissance. The KPA jams maneuver units in order to disrupt coordination between and within units, especially when enemy units are achieving varying degrees of success. The KPA also will attack reporting links between reconnaissance and engineering units and their supported maneuver units, since these units attempt to exploit any KPA weaknesses detected.

Targets

9-29. The KPA can and will conduct electronic attack on virtually any system connected by signals transmitted in the electromagnetic spectrum. This includes both communications and noncommunications signals and data. As with signals reconnaissance, the choice of which links to disrupt varies with the scheme of maneuver, the impact of the disruption, the enemy's sophistication, and the availability of KPA electronic attack assets. A limited but representative list of possible targets includes—

- C2 and communications links between a key unit and its higher command.
- The link between a Global Positioning System satellite and a receiver.
- The link between a firing system and its fire direction center.
- The link between a missile or munition and its targeting system.
- Computer data links of all types.

Distributive Jamming

9-30. Instead of wide-band barrage jamming using large semifixed jammers, the KPA often fields small distributive jammers. These may be either dispersed throughout the battle area or focused on one or more select targets, and may be either fixed or mobile. Mobility can be by ground vehicle or aircraft. Jammers can be controlled though civilian cellular phone networks or by local forces. Along with known military frequencies, the KPA can target civilian radios or cellular phones of a regional neighbor, nongovernmental organizations, or other civilians from outside the region. Distributive jamming can cause—

- Loss of Global Positioning Systems, communications, and non-communications data links, such as Blue Force and personal or unit communications.
- Degradation of situational awareness and common operational picture.
- Disruption of tempo.
- Reduction of intelligence feeds to and from CPs.
- Opportunities for ambush, which is recorded and used for perception management operations.
- Units forced to use alternative, less secure communications.

Expendable Jammers

9-31. The KPA can take advantage of the time prior to an enemy attack to emplace expendable jammers, which can disrupt enemy communications nets. When used in conjunction with terrain—such as at natural chokepoints, mountain passes, or valleys—the jammers can achieve significant results despite their short range and low power. The KPA can also use them to support a deception plan without risking expensive vehicle-based systems. While limited in number, artillery-delivered expendable jammers may be employed. These jammers are especially useful in those areas where support is not available from more-powerful vehicle-mounted jammers.

Proximity Fuse Jammers

9-32. Proximity fuses used on some artillery projectiles rely on return of a radio signal reflected from the target in order to detonate the round within lethal range. Proximity fuse jammers cause the round to instead explode at a safe distance. The KPA may deploy such jammers to protect high-value assets within range of enemy indirect fire weapons.

DECEPTION

9-33. The KPA integrates deception into every tactical action. It does not plan deception measures and activities in an ad hoc manner; rather, the deception plan is typically a major portion of the KPA's overall EIW plan. The extent and complexity of the deception depend on the amount of time available for planning and preparation. The KPA formulates its plan of action and the overall EIW plan, including the deception plan, concurrently.

9-34. The KPA attempts to deceive the enemy concerning the exact strength and composition of its forces, their deployment and orientation, and their intended manner of employment. When successfully conducted, deception activities ensure the KPA achieves tactical surprise while enhancing force survivability. All deception measures and activities are continuously coordinated with deception plans and operations at higher levels. Affiliated forces may assist in executing deception activities.

9-35. The KPA employs all forms of deception, ranging from physical decoys and electronic devices to tactical activities and behaviors. The key to deception activities is both realism and consistency with the deception story. Due to the sophistication and variety of sensors available to the enemy, successful deception requires a multispectral effort. The KPA must provide false or misleading thermal, visual, acoustic, and electronic signatures.

9-36. When creating the picture of the battlefield that the KPA wants the enemy to perceive, deception planners have two primary objectives. The first is to cause the enemy to commit forces and act in a manner favoring the KPA's plan. The second—and the focus of deception activities when time is limited—is to minimize friendly-force signatures, which limits detection and destruction by the enemy.

9-37. Integral to the planning of deception activities is the KPA's identification of the deception target. This will be an individual, organization, or group with the necessary decision-making authority to take actions (or neglect to do so) in line with the KPA's deception objective. On the tactical battlefield, this target is typically the enemy commander, although the KPA recognizes the importance of focusing actions to affect specific staff elements.

9-38. Successful deception activities depend on the identification and exploitation of enemy information systems and networks, as well as other conduits for introducing deceptive information. Knowing how the conduits receive, process, analyze, and distribute information allows for the provision of specific signatures meeting the conduits' requirements. On the tactical battlefield, the enemy reconnaissance system is the primary information conduit and therefore receives the most attention from KPA deception planners. The international media and Internet sites may also be a target for deceptive information at the tactical level. The KPA can feed the enemy false stories and video portraying tactical-level actions with the goal of influencing operational or even strategic decisions.

Deception Units

9-39. The KPA battle plan or EIW plan may call for the creation of one or more deception units, meaning that nonexistent or partially existing formations attempt to present the illusion of real or larger units. When the EIW plan requires units to take some action, such as a feint or demonstration, they are designated as deception units in close-hold executive summaries of the plan. Wide-distribution copies of the plan make reference to these units according to the functional designations given them in the deception story.

9-40. The KPA deception unit is typically given its own command structure. The purpose of this is both to replicate the organization(s) necessary to the deception story and to execute the multidiscipline deception required to replicate an actual or larger military organization. The headquarters of a KPA unit that has lost all of its original subordinates to task organization is an excellent candidate for use as a deception unit.

Deception Activities

9-41. Deception units may use a series of feints, demonstrations, ruses, or decoys. All activities must fit the overall deception story and provide a consistent, believable, and multidiscipline representation. Basic tactical camouflage, concealment, cover, and deception (C3D) techniques are used to support all types of deception.

9-42. The KPA conducts deception activities to confuse the enemy to the extent that it is unable to distinguish between legitimate and false targets, units, activities, and future intentions. Inserting false or misleading information at any point in the enemy decision-making process can lead to increased KPA survivability and the inability to respond appropriately to KPA tactical actions. Manipulation of the electromagnetic spectrum is often critical to successful deception activities as the KPA responds to the challenge posed by advances in enemy C2 and communications systems and sensors. Some example deception activities for the KPA may include—

- Executing feints and demonstrations to provide a false picture of where the main effort will be.
- Creating the false picture of a major offensive effort.

- Maximizing protection and security measures to conceal movement.
- Creating false high-value assets.

Feints

9-43. Feints are offensive in nature and require engagement with the enemy in order to show the appearance of an attack. The goal is to support the mission and ultimately mislead the enemy. Feints can be used to force the enemy to—

- Employ its forces improperly. A feint may cause enemy forces to move away from the main attack, or it may be used to fix enemy follow-on forces.
- Shift its supporting fires from the main effort.
- Reveal its defensive fires locations by causing premature firing.

Demonstrations

9-44. Demonstrations are a show of force on a portion of the battlefield where no decision is sought, for the purpose of deceiving the enemy. They are similar to feints, but contact with the enemy is not required. Advantages of demonstrations include—

- Absence of contact with the enemy.
- The possibility of using simulation devices in lieu of real items to deceive the enemy's reconnaissance capabilities.
- Use of a smaller force due to lack of contact with the enemy.

Ruses

9-45. Ruses are tricks designed to deceive the enemy in order to obtain a tactical advantage. They are characterized by deliberately exposing false information to enemy collection means. Information attacks, perception management actions, and basic C3D measures all support this type of deception.

Decoys

9-46. Decoys are physical imitations of KPA systems or deception positions made detectable to enemy RISTA assets in order to confuse the enemy. The goal is to deceive enemy resources into reporting or engaging false targets. It is not necessary to have specially manufactured equipment for this type of visual deception. Decoys are used to attract an enemy's attention for a variety of tactical purposes. Their main use is to draw enemy fire away from high-value assets.

9-47. Decoys are generally expendable. They can be either elaborate or simple, and either prefabricated or made from field-expedient materials. Their design depends on several factors, such as the target to be mimicked, a unit's tactical situation, its available resources, and the time available. Except for selected types, prefabricated decoys are not widely available. A typical unit can construct effective, realistic decoys to replicate its key equipment and features through imaginative planning and a working knowledge of its electromagnetic signature emissions.

9-48. The two most important factors regarding decoy employment are location and realism. Logically placing decoys can greatly enhance their plausibility. They are usually placed close enough to the real target to convince an enemy that it has found the correct target. They must be far enough away, however, to prevent collateral damage to the real target when the decoy draws enemy fire. Proper spacing between target and decoy depends on target size, expected enemy target acquisition sensors, and type of enemy munitions likely to be used.

9-49. Decoys must include target features an enemy will recognize. The most effective decoys are those closely resembling the real target in terms of electromagnetic signatures. Completely replicating the signatures of some targets, particularly large and complex ones, can be difficult. Therefore, decoy construction should address the electromagnetic spectral region in which the real target is most vulnerable.

9-50. Smart decoys are designed to present a high-fidelity simulation of a real vehicle or other system. They may present heat, electromagnetic, electro-optical, audio, or visual signatures. They are distributed, controlled decoys. Computerized controls turn on decoy signatures to present a much more valid signature than previous-generation “rubber duck” decoys. Smart decoys can be placed close to prohibited targets, such as churches, mosques, schools, or hospitals, and civilian populations. If the enemy engages them, the KPA can exploit resulting civilian damage in follow-on perception management activities. Smart decoys cause—

- Loss of situational awareness.
- A flood of false targets, bogging down the enemy’s targeting process.
- Expenditure of limited munitions on false targets.
- Negation of multispectral RISTA assets, such as night vision goggles, infrared scopes, and other electro-optical devices.
- Negation of critical targeting planning and allocation of assets.

9-51. The KPA EIW plan may also call for employing deception CPs. These are complex, multisensor-affecting sites that are integrated into the overall deception plan. They can assist in achieving battlefield opportunity by forcing the enemy to expend C2 and communications warfare effort against meaningless positions.

9-52. The KPA attempts to deny the enemy the ability to accurately identify its force dispositions and intentions by using false deployments. Knowing it cannot totally hide its forces, the KPA tries to blur the boundaries and composition of forces while providing indications of deception units and false targets. Specific KPA tactical actions taken to hide the exact composition and deployment of forces may include—

- Establishing deception assembly areas or defensive positions supported by decoy vehicles.
- Establishing security zones to conceal the actual battle line of friendly defensive positions.
- Concealing unit and personnel movement or maneuver.
- Creating the perception of false units and their associated activity.
- Creating false high-value assets.

9-53. By providing the appearance of units in false locations, the KPA attempts to induce the enemy to attack into areas most advantageous to itself. When the deception is successful, enemy forces may decide to attack where the KPA can take maximum advantage of terrain. False thermal and acoustic signatures, decoy and actual vehicles, and corner reflectors, supported by false radio traffic, all contribute to the appearance of a unit where in fact none exists.

9-54. The reduction of KPA electromagnetic signatures is critical to the success of any deception plan. Minimizing the thermal, radar, acoustic, and electronic signatures of people, vehicles, and supporting systems is critical to ensuring deception of the enemy and enhanced survivability. The KPA makes extensive use of a variety of signature-reduction materials, procedures, and improvised methods to provide protection from enemy sensors and target acquisition systems operating throughout the electromagnetic spectrum.

Electronic Deception

9-55. Electronic deception is used to manipulate, falsify, and distort signatures received by enemy sensors. It must be conducted in such a way as to replicate realistic signatures. Electronic deception can take the form of manipulative, simulative, imitative, or non-communications deception. The KPA may use one or all of these types of electronic deception.

Manipulative Electronic Deception

9-56. Manipulative electronic deception seeks to counter enemy jamming, signals intelligence, and target acquisition efforts by altering the electromagnetic profile of friendly forces. North Korean specialists modify the technical characteristics and profiles of emitters that could provide an accurate picture of KPA intentions to its enemies. The objective is to have enemy analysts accept the profile or information as valid, and therefore arrive at an erroneous conclusion concerning KPA activities and intentions.

9-57. Manipulative electronic deception uses communications or other types of signals to convey indicators to mislead the enemy. It can cause the enemy to fragment its intelligence and EW efforts to the point where they lose effectiveness. It can also cause the enemy to misdirect its assets and therefore cause fewer problems for KPA communications.

Simulative Electronic Deception

9-58. Simulative electronic deception seeks to mislead the enemy as to the actual composition, deployment, and capabilities of the friendly force. The KPA may use controlled breaches of security to add credence to its simulative electronic deception activities. There are a number of techniques the KPA may use. With unit simulation, the KPA establishes a network of radio and radar emitters to emulate those emitters and activities found in the specific unit or activity type. The KPA may reference the false unit designator in communications traffic and may use false unit call signs. In capability or system simulation, the KPA projects an electronic signature of new or differing equipment to mislead the enemy into believing a new capability is in use on the battlefield. To add realism and improve the effectiveness of the deception, the KPA may make references to "new" equipment designators on related communications nets. To provide a false unit location, the KPA projects an electronic signature of a unit from a false location while suppressing the signature from the actual location. Radio operators may make references to false map locations near the false unit location, such as hill numbers, a road junction, or a river. This would be in accordance with a script as part of the deception plan.

Imitative Electronic Deception

9-59. Imitative electronic deception injects false or misleading information into enemy communications and radar networks. The communications imitator gains entry as a bona fide member of the enemy communications system and maintains the role until it passes the desired false information to the enemy.

9-60. In imitative electronic deception, the KPA imitates enemy electromagnetic emissions in order to mislead its opponent. Examples include entering the enemy's communications nets by using its call signs and radio procedures, then giving its commanders instructions to initiate actions. Targets for imitative electronic deception include any enemy receiver, ranging from cryptographic systems to simple, plain-language tactical nets. Among other effects, imitative electronic deception can cause an enemy unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts are intended to cause decisions based on false information that appears to have come from the enemy's own side.

Noncommunications Deception

9-61. The KPA continues to develop and field dedicated tactical noncommunications means of electronic deception. It can simulate troop movements by such means as use of civilian vehicles to portray the movement of military vehicles to radar, and marching refugees to portray movement of marching troops. Simple, inexpensive radar corner reflectors provide masking by approximating the radar cross sections of military targets such as bridges, tanks, aircraft, and even navigational reference points. Corner reflectors bouncing waves back at the source can be quite effective when used in conjunction with other EW systems, such as ground-based air defense jammers.

PHYSICAL DESTRUCTION

9-62. Another method for disrupting enemy control is physical destruction of the target. The KPA integrates all types of conventional and precision weapons systems to conduct destructive fires, to include—

- Fixed- and rotary-wing aviation.
- Cannon artillery.
- Multiple rocket launchers.
- Surface-to-surface missiles.

9-63. In some cases, the destruction may be accomplished by ground attack. The KPA can also utilize other means, such as explosives delivered by special operations forces (SOF) or North Korean sympathizers.

9-64. Physical destruction measures focus on destroying critical components of the enemy force. Enemy C2 and communications nodes and target acquisition sensors are a major part of the KPA fire support plan during physical destruction actions. KPA priority targets typically include—

- Battalion, brigade, and division CPs.
- Area communications distribution system centers and nodes.

- Artillery fire direction centers.
- Forward air controllers.
- Weapons system-related target acquisition sensors.
- Jammers and signals intelligence systems.

9-65. The KPA may integrate all forms of destructive fires, especially artillery and aviation, with other EIW activities. Physical destruction activities are integrated with jamming to maximize their effects. Specific missions are carefully timed and coordinated with the EIW plan and actions of the supported units.

9-66. The KPA gives special emphasis to destruction of its enemy's RISTA capabilities prior to an expected enemy attack on KPA defensive positions. Once the attack begins, the KPA heavily targets the enemy C2 and communications nodes responsible for the planning and conduct of the attack, along with supporting communications. Of note, destruction of these nodes prior to the attack may allow the enemy time to reconstitute control. Targeting the nodes once forces are committed to the attack, however, may cause a far greater disruptive effect.

9-67. The KPA does not possess the smart bombs of other modern militaries and would likely use "strap-on" guidance systems to increase the accuracy of its missiles. North Korea's missile inaccuracy is a major issue for the KPA when conducting attacks against EIW-related targets that require precision and timing. Due to the mobility and fleeting nature of its enemy's information operations targets, North Korea will likely focus its limited missile arsenal against high-priority targets.

9-68. The KPA continues to research and develop directed-energy weapons, to include radio-frequency weapons and high-power lasers. While North Korea has fielded no dedicated directed-energy weapons systems whose sole role is to conduct laser attacks, it may employ low-power laser rangefinders and laser target designators in a sensor-blinding role.

PROTECTION AND SECURITY MEASURES

9-69. Protection and security measures encompass a wide range of activities and incorporate some components of deception and EW. Successful protection and security measures significantly enhance tactical survivability and preserve combat power. The KPA will attempt to exploit the large number and superior technology of enemy sensors. For example, it may employ software at the tactical level to analyze the enemy's satellite intelligence collection capabilities and warn friendly forces of the risk of detection. The use of signature-reducing and signature-altering devices, along with diligent application of operational security measures, supports deception activities in addition to denying information.

9-70. At the tactical level, protection and security measures focus primarily on—

- Counterreconnaissance.
- C3D.
- Information and operational security.

9-71. These and other protection and security measures may overlap the realms of EW or deception.

Counterreconnaissance

9-72. Winning the counterreconnaissance battle is important to the KPA, since it can limit what information the enemy is able to collect and use in operational planning and execution. KPA tactical commanders realize the enemy's operations hinge on situational awareness. Therefore, counterreconnaissance efforts focus on destruction and deception of enemy sensors in order to limit the enemy's ability to understand the KPA battle plan.

9-73. The KPA recognizes that, when facing a powerful opponent, it will often be impossible to destroy enemy standoff RISTA means to observe KPA forces. While the KPA may execute missions to do so, it often uses C3D as the method of choice for degrading the capability of such systems. The KPA also recognizes the reluctance of enemy commanders to operate without human confirmation of intelligence due to the relative ease with which imagery and signals sensors may be deceived. A high priority for all defensive preparations is to deny enemy ability to maintain reconnaissance contact on the ground. KPA tactical commanders consider ground reconnaissance by enemy SOF as a significant threat, and therefore focus considerable effort to ensure the destruction of SOF reconnaissance units.

Camouflage, Concealment, Cover, and Deception

9-74. The KPA gives particular attention to protective measures aimed at reducing its enemy's ability to target and engage KPA systems with precision munitions. Knowing the enemy cannot attack what its RISTA systems do not find, the KPA employs a variety of C3D techniques throughout the security and defense zones. These techniques range from the simplest and least-expensive methods of hiding from observation to the most modern multispectral signature-reducing technologies.

9-75. The KPA dedicates extensive effort to employing C3D to protect its defensive positions and high-value assets. All units are responsible for providing protective measures for themselves with their own assets, with possible support from engineering units. The KPA employs a variety of signature-reducing or signature-altering materials and systems, to include infrared-absorbing and radar-absorbing camouflage nets and paints.

9-76. The KPA declared 2004 as the "Year of Camouflage," demonstrating how important C3D are to the survival of its military. A KPA manual smuggled out in 2010 discussed the failure of the U.S. Air Force to destroy Yugoslavian tanks due to the deception caused by false equipment. Instead of hitting the actual military weapons, the U.S. destroyed decoy tanks, antiaircraft guns, missile launcher sites, and aircraft made of logs, plywood, and cloth. Shortly before the November 2010 artillery bombardment of the South Korean island of Yeonpyeong-do, the KPA deployed painted plywood or inflatable 122-mm and 240-mm rocket launchers around its real launchers in an attempt to increase the difficulty of the enemy's counterartillery fire.

Information and Operational Security

9-77. Information and operational security can protect the physical and intellectual assets used to facilitate KPA C2 and communications. Security must function continuously to be effective. It must conceal not only the KPA commander's intentions and current locations, configurations, and actions of tactical units, but also obscure the tactics and techniques for employment and operation of information systems.

9-78. The KPA clearly understands the importance of information and operational security. Commanders understand their vulnerability to being attacked through their own information systems and develop means to protect these systems. In addition, the KPA must be capable of isolating attacks on its information systems while maintaining the ability to execute. In order to reduce its vulnerability, the KPA emphasizes strong communications, computer, and transmissions security. The KPA may even resort to using runners to avoid interception of electronic communications by enemy forces.

Perception Management

9-79. Perception management involves measures aimed at creating a perception of truth best suited to the KPA's objectives. It integrates a number of widely differing activities using a combination of true, false, misleading, and manipulated information to steer its enemy's commanders and staffs towards a preconceived idea. Targeted audiences range from enemy military forces, to the South Korean populace, to regional or world popular opinion.

9-80. At the tactical level, the KPA seeks to undermine an enemy's ability to conduct combat operations through psychological warfare and other perception management activities aimed at deterring, inhibiting, and demoralizing the enemy and influencing civilian populations. The various perception management activities include efforts conducted as part of—

- Psychological warfare.
- Direct action.
- Public affairs.
- Media manipulation and censorship.
- Statecraft.
- Public diplomacy.

9-81. The last three components, while not usually conducted at the tactical level, can certainly have a great impact on how and where the KPA conducts tactical-level perception management activities. These activities must be consistent with, and contribute to, the KPA's operational and strategic goals.

Psychological Warfare

9-82. Psychological warfare is a major contributor to perception management during pre-combat, combat, and post-conflict stages of a war. Targeting enemy military forces, psychological warfare attempts to influence the attitudes, emotions, motivations, aggressiveness, tenacity, and reasoning of enemy personnel. Specialists plan psychological warfare activities at all levels of command. In addition to enemy military forces, North Korea also conducts psychological warfare against its own people to control them.

9-83. North Korean specialists also concentrate on manipulating the local South Korean population and international media in favor of the KPA, turning opinion against its enemies' objectives. KPA planners focus special emphasis on highlighting enemy casualties and lack of success. KPA planners also highlight enemy mistakes, especially those causing civilian casualties. The South Korean population will be a major target of these activities due to the criticality of South Korean public support for military activities.

9-84. **Example: North Korea Blames U.S. for American Student's Death**. In January 2016, an American student visited North Korea as part of an organized tour group. As he was departing the country, the student took down a propaganda poster and attempted to smuggle it out of the country. The North Korean Government arrested him and sentenced him to 15 years' hard labor in prison just two months later. Early in his sentence, the student suffered a severe neurological injury and the North Korean Government released him in June 2017 on "humanitarian grounds." The student returned to the U.S., but died a week later.

9-85. North Korea attempted to deflect its culpability in the student's death in a number of ways, both domestically and internationally. First, the student confessed publicly on television to breaking North Korea's laws, reading from a handwritten script at the prompting of a local Methodist church and a university secret society. Second, the North Korean Government claimed the student was sent to the country to break its laws at the behest of the U.S. Government, doing so both before the trial and after the student's death. Third, North Korea stated the U.S. Government was trying to exploit the student's death for internal political purposes. Fourth, The North Korean Government denied any allegations that the student was tortured while in its country, and he had fallen into a coma due to a combination of botulism and sleeping pills. The U.S. doctor's noninvasive autopsy did not prove the student was tortured. Lastly, North Korea released three other Americans in May 2018 to demonstrate the country's willingness to negotiate with the U.S.

9-86. Through a variety of outlets, North Korea attempted to manage the perception of the student's death to the people living in North Korea, the U.S., and the international community. North Korea attempted to control the message as much as it could to create the impression that the student's death was not due to anything government officials did or failed to do while the student was in prison.

9-87. The KPA attempts to employ media and other neutral players, such as nongovernmental organizations, to further influence public and private perceptions. If North Korea perceives the presence of nongovernmental organizations to be detrimental to its objectives, the Kim government will attempt to hinder their efforts to provide humanitarian assistance to the populace, thus discrediting them.

Public Affairs

9-88. The KPA may conduct public affairs actions aimed at winning the favor or support of the South Korean leadership and populace in the event that North Korea decides to invade South Korea. This civil support from the KPA might take many forms, such as public information and community relations. It could involve providing money, schools, medical support or hospitals, religious facilities, security, other basic services, or hope—as seen from the North Korean perspective. The KPA would accompany these support activities with the message or impression that, if North Korea loses the war or leaves the area, the local population will lose these benefits and the security provided by the KPA.

Media Manipulation

9-89. Perception management targeting the media is aimed at influencing both domestic and international public opinion. The purpose is to build public and international support for North Korea's actions and to dissuade an adversary from pursuing policies perceived to be adverse to its interests. The willingness of the local South Korean population to either support or to oppose the KPA military effort will be critical to North Korea's success. While most aspects of media manipulation are applicable to levels well above the tactical, the trickle-down effect can have a major effect on the KPA tactical fight.

9-90. North Korea exploits the international media's willingness to report information without independent and actual confirmation. For example, South Korean and other international media reports state North Korea has ended its nuclear testing and has closed down its test facility. This is based on reports given to the media by the country and inviting the media, who are not knowledgeable about nuclear testing, to visit the nuclear test facility.

Note. North Korea employs media censorship to control its own population's access to information and perception of reality. Successful preparation of the population significantly enhances public support for the KPA's military actions. As part of this, North Korea prepares its forces and population for enemy information operation activities.

Target Audiences

9-91. North Korean perception management activities seek to define events in the minds of decision makers and populations in terms of North Korea's choosing. Successful perception management consists of two key factors: speed and connection. Speed means reaching the target audience before the other side can provide the correct information, thus altering the perception of events. Connection means having the right media to provide the story to the target audience in a way that it will find credible and memorable. World opinion is a primary target of perception management, either to gain support for North Korean causes or to turn world opinion and support against potential foes. Reinforcement of its message (preferably by different sources) is also a powerful tool North Korea uses to convince the target audience of the veracity of its position.

INFORMATION ATTACK

9-92. Information attack focuses on the intentional disruption or distortion of information in a manner to support KPA mission completion. Unlike computer warfare attacks targeting the information systems, information attacks target the information itself. Attacks on the commercial Internet by civilian hackers have demonstrated the vulnerability of cyberspace and information systems to innovative and flexible penetration, disruption, or distortion techniques. North Korean cyberspace attackers learn from and expand upon these methods. The KPA recognizes the increasing dependence of modern armies on tactical information systems. It therefore attempts to preserve the advantages of such systems for its own use while exploiting the enemy's reliance on them.

9-93. Information attack is a critical component of EIW, offering a powerful tool for North Korea. For example, an attacker may target an information system for electronic sabotage or to manipulate and exploit information. This may involve altering data, stealing data, or forcing a system to perform a function for which it was not intended, such as creating false information in a targeting or airspace control system.

9-94. Data manipulation is potentially one of the most dangerous techniques available to North Korea. It involves covertly gaining access to an enemy information system and altering key data items without detection. The possibilities are endless with this technique. Some examples are—

- **Navigation**. Altering position data for enemy units, soldiers, and systems, making them think they are in the right place when they are not.
- **Blue Force Tracking**. Altering position data of enemy units, soldiers, and systems to make other units, soldiers, and systems believe them to be in one place where they are not or to lose track of them entirely. Alternatively, data manipulation can make KPA units appear as enemy forces or vice versa.

- **Battlefield Information Systems**. Enhancing KPA tactical success by the ability to mitigate or influence enemy activities controlled via battlefield information systems.
- **Survey and Gun or Mortar Alignment**. Causing enemy weapons to fire on the wrong target location.
- **Targeting and Sensors**. Misdirecting sensors to have false reads, locate false targets, or identify the enemy's own units as KPA targets.
- **Weapon Guidance**. Sending enemy weapons to the wrong location or target.
- **Timing**. Changing internal clocks, thereby disrupting synchronization.
- **Logistics Tracking**. Sending logistics packages to the wrong place or delaying their arrival. This can be done by altering bar codes on equipment or by hacking and altering logistics (delivery or request) data.
- **Aviation Operations**. Changing altimeter readings, position location data, or identification, friend or foe codes.

9-95. North Korea attempts to inject disinformation through trusted networks. The KPA tries to make its enemies distrust their RISTA and situational awareness assets by injecting incorrect information. Attacks could take the form of icon shifting (blue to red) or moving the icon's location. Fire missions and unit control would require significant human interaction, thus slowing the enemy's target engagement cycle.

9-96. Likely targets for an information attack are information residing in the critical tactical systems of the enemy. Such targets include—

- Telecommunications links and switches.
- Fire control.
- Logistics automation.
- RISTA downlinks.
- Situational awareness networks.
- C2 and communications systems.

Computer Warfare

9-97. North Korea conducts computer warfare for three primary reasons—

- Countering the superior conventional military strength of its enemies.
- As a low-cost/low-risk means of targeting enemy computer vulnerabilities.
- In peacetime, as a method to upset the status quo with little fear of retaliation.

9-98. Computer warfare consists of attacks focusing specifically on computer systems, networks, or nodes. This includes a wide variety of activities, including—

- Unauthorized access (hacking) of information systems for intelligence-collection purposes.
- Insertion of malicious software (viruses, worms, logic bombs, or Trojan horses).

9-99. Such attacks concentrate on the denial of service, disruption, or manipulation of the integrity of the information infrastructure. Distributed denial-of-service attacks use a network of slave computers to overwhelm target computers with packets of data and deny them outgoing access to networks. Such attacks could disrupt logistics, communications, intelligence, and other functions. North Korea may attempt to accomplish any of these activities through the use of agents or third-party individuals with direct access to enemy information systems. The country can also continually access and attack systems at great distances via communications links such as the Internet.

9-100. North Korea can employ various types of malicious software or "malware" on enemy computers to slow operations, extract data, or inject data. Poor enemy operational procedures can enable this type of attack, with significant loss of capability or spillage of data to North Korea. These attacks also cause the enemy to waste data time and cycles in prevention and remediation. Malware could affect internal clocks (creating positional errors and communications difficulties) and slow the functional speed of computing. Any Internet-capable or networkable system is at potential risk.

9-101. North Korean computer warfare activities may be conducted prior to or during a military action. For example, by damaging or destroying networks related to an enemy's projected force deployments and troop movements, the KPA can effectively disrupt planning and misdirect movement, producing substantial confusion and delays. As modern armies increasingly rely on "just-in-time" logistics support, targeting logistics-related computers and databases can produce delays in the arrival of important materiel such as ammunition, fuel, and spare parts during critical phases of a conflict.

9-102. North Korea can successfully conduct invasive computer warfare activities from the safety of its own territory. It has the distributed ability to reach targeted computers anywhere in the world, as long as they are connected to the Internet. North Korea has the capability to continuously exploit the highly integrated information systems of an adversary.

9-103. The primary organization responsible for computer warfare in North Korea is Bureau 121, which fielded at least 1,000 elite hackers in 2010 who focused on other countries' computer systems. This number is likely much higher now: as of 2009, North Korea's Mirim College was graduating approximately 100 cyberspace hackers per year for the KPA.

Reconnaissance

9-104. The KPA considers reconnaissance to be a component of its EIW campaign. At its core, *reconnaissance* is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 2-0). See chapter 5 for details on the KPA use of reconnaissance.

Cryptanalysis

9-105. Cryptanalysis is the art or process of deciphering coded messages without the key. Most of this work will be done above the KPA division level or in other offices within the North Korean Government, such as the Reconnaissance Bureau. The results of cryptanalysis could be used at the tactical level.

Intelligence Collection

9-106. Intelligence collection is the systematic process used by the KPA to meet its intelligence requirements through the tasking of all available resources to gather and provide pertinent information within a required time limit. For additional information on intelligence collection, see the RISTA section of chapter 5.

Disinformation Operations

9-107. Disinformation operations is the process whereby the KPA will deliberately release false information in order to deceive the enemy. The KPA may use black propaganda as part of this campaign, which is false information and material supposedly from an enemy source, but actually from North Korea. Black propaganda is often used to misrepresent, embarrass, or disparage the KPA's enemies. The disinformation may be directed at an enemy's military forces, its media, or a third party.