МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ

«НОВОРОССИЙСКИЙ КОЛЛЕДЖ РАДИОЭЛЕКТРОННОГО ПРИБОРОСТРОЕНИЯ»

Учебное пособие

на тему «Радиоэлектронная борьба (РЭБ): радиоэлектронное подавление, электромагнитное поражение и радиоэлектронная защита»
для специальности 11.02.02
Техническое обслуживание и ремонт радиоэлектронной техники

2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
КРАСНОДАРСКОГО КРАЯ

«НОВОРОССИЙСКИЙ КОЛЛЕДЖ РАДИОЭЛЕКТРОННОГО ПРИБОРОСТРОЕНИЯ»

УЧЕБНОЕ ПОСОБИЕ

на тему «Радиоэлектронная борьба (РЭБ): радиоэлектронное подавление, электромагнитное поражение и радиоэлектронная защита»

по дисциплине «**Иностранный язык**»
(английский)

для специальности 11.02.02
Техническое обслуживание и ремонт радиоэлектронной техники
3 курс

2 0 16

СОГЛАСОВАНО
На заседании Совета по методическим вопросам от 15 04 2016 г.
протокол № 7
Председатель Совета по методическим вопросам
_____ Е.В. Заслонова

УТВЕРЖДАЮ
Зам. директора по УР
_____ Т.В. Трусова
16 04 2016 г.

Рассмотрено на заседании УМО филологических дисциплин
от 1 03 2016 г.
протокол № 7
Председатель УМО _____ М.А.Марарь

Организация – разработчик: государственное бюджетное профессиональное образовательн учреждение Краснодарского края «Новороссийский колледж радиоэлектронно приборостроения» (ГБПОУ КК НКРП)

Разработчик:
Преподаватель высшей квалификационной ГБПОУ КК НКРП _____ М.А. Марарь

Рецензент:
Колосова Н.С. Преподаватель высшей квалификационной категории ГБПОУ КК НКРП

Задорожная Е.А. преподаватель высшей квалификационной категории ГБПОУ КК НСПК

Рецензия

на учебное пособие по иностранному языку (английский)

«Радиоэлектронная борьба (РЭБ): радиоэлектронное подавление, электромагнитное поражение и радиоэлектронная защита»

преподавателя Марарь Марины Александровны

ГБПОУ КК НКРП

Учебное пособие «Радиоэлектронная борьба (РЭБ): радиоэлектронное подавление, электромагнитное поражение и радиоэлектронная защита» преподавателя М.А. Марарь рассчитано для студентов 3 курса специальности 11.02.02 «Техническое обслуживание и ремонт радиоэлектронной техники». Количество страниц – 66.

Автор акцентирует внимание на том, что учебное пособие направлено на развитие индивидуальной траектории образования каждого обучающегося. Пособие аккумулирует важные процессы радиоэлектронной борьбы, подавления, электромагнитного поражения и защиты по учебной дисциплине «иностранный язык (английский)».

Актуальность и педагогическая целесообразность данного учебного пособия заключается в развитии умений и навыков у обучающихся по дисциплине «иностранный язык». В системе образования данное учебное пособие связано с другими дисциплинами, изучаемыми в СПО: инженерная графика, электротехника, метрология, стандартизация и сертификация, электронная техника, материаловедение, электрорадиоматериалы и радиокомпоненты, электрорадиоизмерения.

Основная идея разработанного учебного пособия заключается в привитии обучающимся навыков профессии посредством иностранного языка, что позволит студентам в будущем ориентироваться в документах, схемах, таблицах не только на родном языке, но и на изучаемом языке, на который ориентируется большинство производителей. Грамматические и лексические упражнения, которые предоставляются автором в пособии, делают этот материал интересным и оптимальным для восприятия студентов старших курсов.

Учебное пособие обладает практической значимостью: ряд заданий после рассматриваемой темы стимулирует интеллектуальную, поисковую и коммуникативную активность и, как следствие, формирует новые навыки студентов, которых, возможно, ранее у них не было (накопление запаса слов, логически правильное построение перевода, т.д.)

Рецензируемое учебное пособие актуально для системы образования, интересно по содержанию, будет доступно и понятно как преподавателю, так и студентам-старшекурсникам, которые осваивают специальность в теории и на практике.

Таким образом, данное пособие учебной дисциплины «Иностранный язык (английский)» может быть рекомендовано для использования в образовательном учреждении ГБПОУ КК «Новороссийский колледж радиоэлектронного приборостроения».

Рецензент:

Задорожная Е.А.

(Ф.И.О. рецензента)

зам. директора по учебно методической работе, ГБПОУ КК НКРПК

(должность, место работы)

преподаватель иностранного языка

(квалификация по диплому)

3 марта 2016 г.

Рецензия

Настоящее учебное пособие «Радиоэлектронная борьба (РЭБ): радиоэлектронное подавление, электромагнитное поражение и радиоэлектронная защита» предназначена для работы учащихся 3 курса специальности 11.02.02 «Техническое обслуживание и ремонт радиоэлектронной техники».

Основа для учебного пособия была заимствована из научно-публицистической литературы, в частности, научной книги Росса Андерсона «Инженерная безопасность» глава 19 – Радиоэлектронная борьба – и является частью учебного материала, изучаемого студентами по данной теме, рассчитанной на 4 часа (или на два учебных занятия).

Все тексты данного учебного пособия профессионально направлены. Во избежание языковых трудностей и трудностей перевода предусмотрена поэтапная работа с текстами, ряд упражнений и заданий для их последовательного разбора по частям, а также выявления сути и краткого изложения на изучаемом языке. Учебное пособие включает в себя:

- Тексты - «Communications Systems», «Signals Intelligence Techniques», «Attacks on Communications», «Protection Techniques», «Frequency Hopping», «DSSS», «Burst Communications», «Combining Covertness and Jam Resistance», «Interaction Between Civil and Military Uses», «Surveillance and Target Acquisition», «Types of Radar», «Jamming Techniques», «Advanced Radars and Countermeasures», «Other Sensors and Multisensor Issues», «IFF Systems», «Improvised Explosive Devices», «Directed Energy Weapons», «Information Warfare», «Definitions», «Doctrine», «Potentially Useful Lessons from Electronic Warfare», «Differences Between E-war and I-war», «Summary. Research Problems»;
- Новую лексику;
- Лексические упражнения;
- Грамматические упражнения.

Применение данного пособия на практике способствует решению следующих задач:

- развитие навыков чтения текста и его понимание;
- использование навыков чтения изучающего и поискового характера;
- развитие диалогической и монологической речи;
- развитие логического мышления обучаемых;
- закрепление грамматических навыков, полученных в процессе обучения.

Требования к результатам освоения материала учебного пособия конкретизированы и соответствуют требованиям к знаниям и умениям базовой подготовки по специальности.

Практические задачи обучения направлены на развитие составляющих коммуникативной компетентности студентов (речевой, языковой, социокультурной, компенсаторной и учебно-познавательной).

Предлагаемое учебным пособием содержание практических заданий носит профессионально ориентированный характер, обеспечивает приобретение обучаемыми требуемых умений и навыков.

Рецензент: _____ УЧЕБНАЯ ЧАСТЬ

Н.С. Колосова, преподаватель
(Ф.И.О. рецензента)
высшей квалификационной
(должность, место работы)
кафедры ГБПОУ КК НКРП

24 02 2016 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное учебное пособие «Радиоэлектронная борьба (РЭБ): радиоэлектронное подавление, электромагнитное поражение и радиоэлектронная защита» предназначено для студентов образовательных организаций, в программу которых входит изучение радиоэлектронной техники и приборостроения. Пособие соответствует базовому этапу подготовки иностранного языка и обеспечивает коммуникативную и профессиональную направленность в обучении языку в неязыковой образовательной организации.

Все компоненты учебного пособия построены на единых методических принципах, развивают все виды иноязычной речевой деятельности, позволяют организовать аудиторную и самостоятельную работу по овладению английским языком и формирование межкультурной компетенции будущих специалистов.

Целью учебного пособия является формирование умения беседовать на профессиональные темы, развитие умения читать специальную литературу средней и повышенной степени трудности и извлекать из нее информацию. Для достижения этого в пособии предусмотрена регулярная, от текста к тексту, учебная деятельность по созданию словаря активной лексики, включающего употребительные в данной специальности термины и слова общего значения.

Материалы, входящие в пособие, отобраны из оригинальной литературы, точнее, из книги Росса Андерсона «Инженерная безопасность», глава 19 «Радиоэлектронная борьба». Последовательность текстов имеет логическую направленность, соответствующую логике развития данной отрасли. Учебное пособие включает в себя 21 текст с послетекстовыми практическими заданиями на отработку понятой информации технических текстов. Тематика текстов соответствует реально существующим направлениям подготовки специалистов профиля техническое обслуживание и ремонт радиоэлектронной техники на основе знаний по электронной технике, электротехнике, материаловедения, электрорадиоматериалов и радиокомпонентов, а также электрорадиоизмерений.

При разработке системы заданий использованы элементы функционально-коммуникативного обучения иностранному языку, при котором явления языка (лексика и грамматика) рассматриваются не только как система языковых правил, но и как система коммуникативных функций. Такие функции типичны для текстов профиля техническое обслуживание и ремонт радиоэлектронной техники и находят свое отражение в типичных грамматических моделях и типичном наборе лексических единиц и словосочетаний. Также данное пособие включает дополнительную теоретическую информацию по тематике на английском и русском языках.

TEXT 1.

ELECTRONIC WARFARE

For ***decades***, electronic ***warfare*** has been a separate subject from computer security, even though they have some common technologies (such as cryptography). This is starting to change as elements of the two disciplines ***fuse*** to form the new subject of information warfare. The military's ***embrace*** of information warfare as a slogan over the last years of the twentieth century has ***establish***ed its importance—even if its concepts, theory, and doctrine are still ***underdeveloped***.

There are other ***reasons*** why a knowledge of electronic warfare is important to the security professional. Many technologies originally developed for the ***warrior*** have been adapted for commercial use, and there are many instructive parallels. In addition, the ***struggle*** for control of the electromagnetic spectrum has ***consume***d so many clever people and so many tens of billions of dollars that we find ***deception*** strategies and tactics of a unique ***depth*** and ***subtlety***. It is the one area of electronic security to have experienced a ***lengthy*** period of ***coevolution*** of attack and defense involving capable motivated opponents.

Electronic warfare is also our main teacher when it comes to service ***denial*** attacks, a topic that computer security people have largely ignored, but that is now center stage thanks to distributed denial-of-service attacks on commercial Web sites. As I develop this discussion I'll try ***to draw out*** the parallels. In general, while people say that computer security is about confidentiality, ***integrity*** and ***availability***, electronic warfare has this reversed and ***back-to-front***. The priorities are:

1. Denial of service, which includes ***jamming***, ***mimicry*** and physical ***attack***.
2. ***Deception***, which may be ***target***ed at automated systems or at people.
3. ***Exploitation***, which includes not just ***eavesdrop***ping but obtaining any operationally valuable information from the enemy's use of his electronic systems.

The ***goal*** of electronic warfare is to control the electromagnetic spectrum. It is generally considered to consist of:

- *Electronic attack*, such as jamming enemy communications or radar, and ***disrupt***ing enemy equipment using high-power microwaves.
- *Electronic protection*, which ranges from designing systems resistant to jamming, through hardening equipment to resist high-power microwave attack, to the destruction of enemy jammers using ***anti-radiation missiles***.
- *Electronic support* which supplies the necessary intelligence and ***threat recognition*** to allow effective attack and protection. It allows commanders to search for, identify and locate sources of intentional and unintentional electromagnetic energy. (Schleher)

The traditional topic of cryptography, namely *communications security* (Comsec), is only a small part of electronic protection, just as it is becoming only a small part of information protection in more general systems. Electronic support includes *signals intelligence* (Sigint), which consists of *communications intelligence* (Comint) and *electronic intelligence* (Elint). The ***former*** collects enemy communications, including both message content and traffic data about which units are communicating, while the latter concerns itself with recognizing ***hostile*** radars

and other non-communicating sources of electromagnetic energy.

Deception is central to electronic attack. The goal is ***to mislead*** the enemy by manipulating his ***perceptions*** in order to degrade the ***accuracy*** of his intelligence and target ***acquisition***. Its effective use depends on ***clarity*** about who (or what) is to be deceived, about what and how long, and—where the targets of deception are human—the exploitation of ***pride***, ***greed***, laziness, and other vices. Deception can be extremely cost-effective and is also ***relevant*** to commercial systems.

Physical destruction is an important part of the mix; while some enemy sensors and communications links may be neutralized by jamming (*soft kill*), others will often be destroyed (*hard kill*). Successful electronic warfare depends on using the available ***tools*** in a coordinated way.

Electronic weapon systems are like other ***weapon***s in that there are *sensors*, such as radar, infrared and sonar; *communications* links, which take sensor data to the command and control center; and *output devices* such as ***jammer***s, lasers, and so on. I'll discuss the communications system issues first, as they are the most ***self-contained***, then the sensors and associated jammers, and finally other devices such as electromagnetic pulse generators. Once we're done with e-war, we'll look at the lessons we might ***take over*** to i-war.

Language Study

1. Give the meanings of the words by variants. Check yourselves according to the dictionary.

Decades, warfare, fuse, embrace, establish, underdeveloped, reasons, warrior, struggle, consume, deception, depth and ***subtlety, lengthy, coevolution, denial, to draw out***, ***integrity*** and ***availability, back-to-front, jamming***, ***mimicry*** and physical ***attack, target, exploitation, eavesdrop, goal, disrupt, anti-radiation missiles, threat recognition, hostile, former, to mislead, perceptions, accuracy, acquisition, clarity, pride***, ***greed, relevant, tools, weapon, jammer, self-contained, take over.***

2. Fill in the text the missing words:

This is starting … as elements of the two disciplines fuse to form the new subject of ... . The military's embrace of information warfare as … over the last years of the twentieth century has established its importance—even if its … , theory, and doctrine are still ... .

Underdeveloped; information warfare; a slogan; concepts; to change.

3. a) Write out from the text the main goal and priorities.
b) Of what does the electromagnetic spectrum consist? What is, in author's opinion, a part of electronic protection and signals intelligence? Into what notions is the phrase "Physical destruction" subdivided? What kinds of electronic weapon systems are?
c) Write a summary of the text.

TEXT 2.

Communications Systems

Military communications were dominated by physical ***dispatch*** until about 1860, then by the telegraph until 1915, and then by the telephone until recently. Nowadays, a typical command and control structure is made up of various tactical and strategic radio networks, that support data, voice, and images, and operate over point-to-point links and ***broadcast***. Without situational ***awareness*** and the means to direct forces, the commander is likely to be ineffective. But the need to secure communications is much more ***pervasive*** than one might at first realize, and the ***threats*** are much more ***diverse***.

- One ***obvious*** type of traffic is the communications between fixed sites such as army ***headquarters*** and the political leadership. The main threat here is that the ***cipher*** security might be ***penetrated***, and the orders, situation reports and so on compromised. This might result from ***cryptanalysis*** or—more likely—equipment sabotage, ***subversion*** of personnel, or theft of key material. The ***insertion*** of deceptive messages may also be a threat in some ***circumstances.*** But ***cipher*** security will often include protection against traffic analysis (such as by link encryption) as well as of the transmitted message confidentiality and authenticity. The secondary threat is that the link might be ***disrupt***ed, such as by destruction of cables or relay stations.

- There are more ***stringent*** requirements for communications with ***covert*** assets such as agents in the field. Here, in addition to cipher security issues, location security is important. The agent will have to take steps to minimize the risk of being caught as a result of communications monitoring. If she sends messages using a medium that the enemy can monitor, such as the public telephone net- work or radio, then much of her ***effort*** may go into ***frustrating*** traffic analysis and radio direction finding.

- Tactical communications, such as between HQ and a ***platoon*** in the field, also have more stringent (but slightly different) needs. Radio direction finding is still an issue, but jamming may be at least as important; and deliberately deceptive messages may also be a problem. For example, there is equipment that enables an enemy air controller's voice commands to be captured, cut into phonemes and spliced back together into deceptive commands, in order to gain a tactical advantage in air combat. As voice-morphing techniques are developed for commercial use, the risk of ***spoof***ing attacks on unprotected communications will increase. Therefore, cipher security may include authenticity as well as confidentiality and/or covertness.

- Control and telemetry communications, such as signals sent from an aircraft to a missile it has just launched, must be protected against jamming and modification. It would also be desirable if they could be covert (so as not to ***trigger*** a target aircraft's warning receiver), but that is in ***tension*** with the power levels needed to ***defeat*** defensive jamming systems.

The protection of communications will require some mix, depending on the circumstances, of content secrecy, ***authenticity***, resistance to traffic analysis and radio direction finding, and resistance to various kinds of jamming. These interact in some rather unobvious ways. For example, one radio

designed for use by dissident organizations in Eastern Europe in the early 1980s operated in the radio bands normally occupied by the Voice of America and the BBC World Service—and routinely jammed by the Russians. The idea was that unless the Russians were prepared to turn off their jammers, they would have great difficulty doing direction finding.

Attack also generally requires a combination of techniques, even where the ***objective*** is not analysis or direction finding but simply denial of service. Owen Lewis summed it up succinctly: according to Soviet doctrine, a ***comprehensive*** and successful attack on a military communications infrastructure would involve destroying one third of it physically, denying effective use of a second third through techniques such as jamming, ***trojans*** or deception, and then allowing one's ***adversary*** to ***disable*** the remaining third in attempting to pass all his traffic over a third of the installed capacity. This applies even in ***guerilla*** wars: in Malaya, Kenya, and Cyprus, the ***rebels*** managed to degrade the telephone system enough to force the police to set up radio nets.

Language Study

1. Give the Russian equivalents to the missing words. Write out the phrases from the Text 2 with the given words.

Military – военные, войска, военная сила; ***dispatch - …; broadcast. - …; awareness*** – осознанность, осведомлённость***; pervasive - …; threats - …; diverse - …; obvious - …; headquarters*** – главное управление, штаб-квартира,главное командование***; penetrated*** – проникший; ***cipher*** – шифр; шифровать, вычислять; ***cryptanalysis - …; subversion - …; insertion - …; circumstances*** – обстоятельства, условия***; disrupt*** – разрушать; разрывать; срывать, подрывать; ***stringent - …; covert - …; effort - …; frustrating - …; platoon*** – взвод, отряд, группа; ***spoof*** – обманывать; обман, мистификация; ***trigger - …; tension - …; defeat - …; authenticity*** – подлинность, достоверность***; comprehensive - …; trojans*** – нечестные люди, с подвохом; ***adversary - …; disable - …; guerilla*** – партизан, партизанская война***; rebels - … .***

2. Look through the text once more. Answer the questions, using the information from the text:

1. During what time were military communications dominated?
2. How matters nowadays?
3. What are the threats now? List them.
4. On what does the protection depend?
5. For what is it necessary a combination of techniques?

3. Write the main idea of the Text 2 in five sentences.

TEXT 3.

Signals Intelligence Techniques

Before communications can be attacked, the enemy's network must be ***mapped***. The most expensive and critical task in signals intelligence is identifying and extracting the interesting material from the ***cacophony*** of radio signals and the huge mass of traffic on systems such as the telephone network and the Internet. The technologies in use are extensive and largely classified, but some aspects are public.

In the case of radio signals, communications intelligence agencies use receiving equipment, that can recognize a huge variety of signal types, to maintain extensive databases of signals—which stations or services use which frequencies. In many cases, it is possible to identify individual equipment by signal analysis. The ***clues*** can include any unintentional frequency modulation, the shape of the transmitter turn-on ***transient***, the ***precise*** center frequency, and the final-stage amplifier ***harmonics***. This *RF finger-printing* technology was declassified in the mid-1990s for use in identifying cloned cellular telephones, where its makers claim a 95% success rate. It is the direct ***descendant*** of the World War II technique of recognizing a wireless operator by his *fist*—the way he sent Morse code.

Radio direction finding (RDF) is also critical. In the old days, this involved ***triangulating*** the signal of interest using directional antennas at two monitoring stations. ***Spies*** might have at most a few minutes to send a message home before having to move. Modern monitoring stations use *time difference of arrival* (TDOA) to locate a suspect signal rapidly, accurately, and automatically by comparing the phase of the signals received at two sites. Nowadays, anything more than a second or so of transmission can be a ***giveaway***.

Traffic analysis—looking at the number of messages by source and destination—can also give very valuable information, not just about imminent attacks (which were signaled in World War I by a greatly increased volume of radio messages) but also about unit movements and other routine matters. However, traffic analysis really comes into its own when ***sifting*** through traffic on public networks, where its importance (both for national intelligence and police purposes) is difficult to overstate.

If you suspect Alice of espionage (or drug dealing, or whatever), you note everyone she calls and everyone who calls her. This gives you a list of dozens of ***suspects***. You ***eliminate*** the likes of banks and doctors, who receive calls from too many people to analyze (your *whitelist*), and repeat the procedure on each remaining number. Having done this procedure ***recursively*** several times, you have a mass of thousands of contacts, which you sift for telephone numbers that appear more than once. If (say) Bob, Camilla, and Donald are Alice's contacts, with Bob and Camilla in contact with Eve, and Donald and Eve in touch with Farquhar, then all of these people

are considered to be suspects. You now ***draw*** a *friendship tree*, which gives a first approximation to Alice's network, and ***refine*** it by ***collating*** it with other intelligence sources.

This is not as easy as it sounds. People can have several numbers; Bob might get a call from Alice at his work number, then call Eve from a phone booth. (In fact, if you're running an IRA cell, your signals officer should get a job at a dentist's or a doctor's or some other place that will be called by so many different people that they will probably be whitelisted. But that's another story.) Also, you will need some means of ***correlating*** telephone numbers to people. Even if you have ***access*** to the phone company's database of unlisted numbers, prepaid mobile phones can be a serious headache, as can clone phones and hacked PBXs. I'll discuss these in the chapter on telecoms security; for now, I'll just remark that anonymous phones aren't new. There have been public phone ***booths*** for generations. But they are not a universal answer for the ***crook***, as the discipline needed to use them properly is beyond most criminals, and in any case causes severe disruption.

Signals collection is not restricted to agreements with phone companies for access to the content of phone calls and the communications data. It also involves a wide range of specialized facilities ranging from expensive fixed installations, which copy inter- national satellite links, through temporary tactical ***arrangements***. A book by Nicky Hager describes the main fixed collection network operated by the United States, Canada, Britain, Australia, and New Zealand. Known as *Echelon*, this consists of a number of collection stations that monitor international phone, fax, and data traffic using computers called *dictionaries.* These search the passing traffic for interesting phone numbers, network addresses, and machine-readable content; this is driven by search strings entered by intelligence analysts. The fixed network is supplemented by tactical collection facilities as needed; Hager describes, for example, the dispatch of Australian and New Zealand navy ***frigate***s to monitor domestic communications in Fiji during military coups in the 1980s. Egmont Koch and Jochen Sperber discuss U.S. and German installations in Germany in; David Fulghum describes ***airborne*** signals collection in satellites are also used to collect signals, and there are covert collection facilities that are not known to the host country.

Despite this huge capital investment, the most difficult and expensive part of the whole operation is traffic selection, not collection. Thus, contrary to naïve expectations, cryptography can make communications more ***vulnerable*** rather than less (if used incompetently, as it usually is). If you just ***encipher*** all the traffic you consider to be important, you have thereby marked it for collection by the enemy. On the other hand, if everyone encrypted all their traffic, then hiding traffic could be much easier (hence the push by signals intelligence agencies to prevent the widespread use of cryptography, even if it's freely available to individuals). This brings us to the topic of ***attacks***.

Language Study

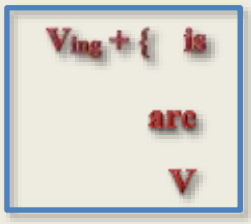
1. Translate the next words and word combinations into Russian. Find the international words:

Cacophony, clues, transient, precise, mapped, harmonics, descendant, triangulating, spies, giveaway, sifting, suspects, eliminate, recursively, draw, refine, collating, correlating, access, booths, crook, arrangements, frigate**s, **airborne, vulnerable, encipher, attacks.

2. Find in the text the sentences with subordinate clauses. Write them out and give the

translation.

3. Find the Gerund grammar constructions from the next boxes in the text. Translate them.



4. Read the example of Alice's network with other intelligence sources. For what did the author set in this illustration? Prove your answer.

TEXT 4. Attacks on Communications

Once you have mapped the enemy network, you may wish to attack it. People often talk in terms of "codebreaking," but this is a gross ***oversimplification***.

First, although some systems have been broken by pure cryptanalysis, this is fairly rare. Most production attacks have involved theft of key material as when the U.S. State Department code book was stolen during World War II by the ***valet*** of the U.S. ***ambassador*** to Rome or errors in the manufacture and distribution of key material as in the U.S. "Venona" attacks on Soviet diplomatic traffic. Even where attacks based on cryptanalysis have been possible, they have often been made much easier by errors such as these, an example being the U.K./U.S. attacks on the German Enigma traffic during World War II. The ***pattern*** continues to this day. A recent history of Soviet intelligence during the Cold War ***reveal***s that the technological advantage of the United States was largely ***nullified*** by Soviet skills in "using Humint in Sigint support"—which largely consisted of recruiting ***traitors*** who sold key material, such as the Walker family.

Second, access to ***content*** is often not the desired result. In tactical situations, the goal is often to detect and destroy ***nodes***, or to jam the traffic. Jamming can involve not just noise insertion but active deception. In World War II, the ***Allies*** used German speakers as ***bogus*** controllers to send German night fighters confusing instructions, and there was ***a battle of wits*** as authentication techniques were invented and defeated. More recently, as I noted in the chapter on biometrics, the U.S. Air Force has deployed more sophisticated systems based on voice morphing. I mentioned in an earlier chapter the tension between intelligence and operational units: the former want to listen to the other side's traffic, and the latter to deny them its use. Compromises between these goals can be hard to find. It's not enough ***to jam*** the traffic you can't read, as that tells the enemy what you can read!

Matters can, in fact, be simplified if the opponent uses cryptography—even in a competent way. This removes the ops/intel tension, and you switch to RDF or link destruction as

appropriate. This can involve the hard-kill approach of digging up cables or bombing telephone exchanges (both of which the allies did during the Gulf War), the soft-kill approach of jamming, or whatever combination of the two is economic. Jamming is a useful expedient where a link is to be disrupted for a short period, but is often expensive; not only does it tie up facilities, but the jammer itself becomes a target. (There are cases where it is more effective, such as against some satellite links where the uplink can be jammed using a tight beam from a hidden location using only a modest amount of power.)

The increasing use of civilian infrastructure, and in particular the Internet, raises the question of whether systematic ***denial-of-service attacks*** might be used to jam traffic. (There are anecdotes of Serbian information warfare cells attempting such attacks on NATO Web sites.) This threat is still considered real enough that many Western countries have separate ***intranets*** for government and military use.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C).

Oversimplification, valet, ambassador, pattern, reveal, nullify, traitors, content, nodes, Allies, bogus, a battle of wits, to jam, appropriate, denial-of-service attacks, intranets.

2. Translate the sentences into Russian. Say what forms of non-personal form of the verb (Participle or Gerund) they are:

1. People often talk in terms of ***"codebreaking"***. **2.** They have often been made much easier by errors such as these, an example ***being*** the U.K./U.S. attacks on the German Enigma traffic during World War II. **3.** The technological advantage of the United States was largely nullified by Soviet skills in "***using*** Humint in Sigint support"—which largely consisted of ***recruiting*** traitors who sold key material. **4.** ***Jamming*** can involve not just noise insertion but active deception. **5.** ***Bogus*** controllers to send German night fighters ***confusing*** instructions, and there was a battle of wits as authentication techniques were invented and defeated. **6.** Air Force has deployed more sophisticated systems based on voice ***morphing***.**7.** This can involve the hard-kill approach of ***digging*** up cables or ***bombing*** telephone exchanges, the soft-kill approach of ***jamming***. **8.** There are cases where it is more effective, such as against some satellite links where the uplink can be jammed ***using*** a tight beam from a hidden location ***using*** only a modest amount of power. **9.** The ***increasing*** use of civilian infrastructure raises the question of whether systematic denial-of-service attacks might be used to jam traffic. **10.** There are anecdotes of Serbian information warfare cells ***attempting*** such attacks.

3. What sentences correspond the content of the text? All the false sentences should be corrected:

1. Some systems have been broken by pure cryptanalysis, this is fairly rare. **2.** State Department code book wasn't stolen during World War I by the valet of the U.S. ambassador to Rome. **3.** A recent history of Soviet intelligence during the Cold War reveals that the technological advantage of the United States was largely nullified by Soviet skills. **4.** Access to content is often the desired result.**5.** The tension was between intelligence and operational units: the former want to match to the other side's traffic, and the latter to cover them its use. **6.** Compromises between these three goals can be easy to find.**7.** This threat is still considered real enough that many Western countries have separate intranets for government and military use.

TEXT 5.

Protection Techniques

As should be clear from the above, ***communications security techniques*** involve not just protecting the ***authenticity*** and confidentiality of the content—which can be achieved in a relatively ***straightforward*** way by encryption and authentication protocols—but also preventing traffic analysis, direction finding, jamming and physical destruction. Encryption can stretch to the first of these if applied at the link ***layer***, so that all links appear to have ***a pseudorandom*** bit stream on them at all times, regardless of whether there is any message traffic. But link-layer encryption alone is not in general enough, as ***enemy capture*** of a single node might put the whole network at risk.

Encryption alone cannot protect against interception, RDF, jamming, and the destruction of links or nodes. For this, different technologies are needed. The obvious ***solutions*** are:

- ***Dedicated*** lines or optical fibers.
- Highly directional transmission links, such as optical links using ***infrared*** lasers or microwave links using highly directional antennas and extremely high frequencies, 20 GHz and up.
- *Low-probability-of-intercept* (LPI), *low-probability-of-position-fix* (LPPF), and antijam radio techniques.

The first two of these ***options*** are fairly ***straightforward*** to understand, and where ***feasible***, they are usually the best. Cabled networks are very hard to destroy completely, unless the enemy knows where the cables are and has physical access to cut them. Even with massive artillery ***bombardment***, the telephone network in Stalingrad remained in use (by both sides) all through the ***siege***.

The third option is a substantial subject in itself, which I will now describe (***albeit*** only briefly).

There are a number of LPI/LPPF/***antijam*** techniques that go under the ***generic name*** of *spread spectrum* communications. They include *frequency hoppers*, *direct sequence spread spectrum* (DSSS), and *burst transmission.* From beginnings around World War II, spread-spectrum has ***spawn***ed a substantial industry, and the technology (especially DSSS) has been applied to numerous other problems, ranging from high-resolution ranging (in the GPS system) through copyright marks in digital images (which I'll discuss later). Let's look at each of these three approaches ***in turn***.

Language Study

1. Combine all words on parts of speech - N, Adj, V, Adv or W/C (word combinations):

Communications security techniques, authenticity, straightforward, layer, pseudorandom, enemy capture, dedicated, solutions, infrared, options, feasible, bombardment, albeit, antijam, generic name, spawn, in turn.

2. Give all w/c in the meaning of "protection".

3. Change the defined words with the used ones from the text:

1. confidentiality of the content—which can be **taken** in a relatively **plain** way by **encoding** and authentication protocols; **2.** all **ties** appear to have a pseudorandom bit **flow** on them at all times; **3.** enemy **catch** of a single **knot** might put the whole network at risk; **4. various** technologies are **necessary; 5.** Cabled **webs** are very **difficult** to **frustrate totally**.

4. Define what sentences are from the text:

1. Encryption can stretch to the first of these if applied at the link layer; **2.** But link-layer encryption alone is in general enough, as enemy contribution to the military actions; **3.** Encryption alone cannot protect against interception, RDF, jamming, and the destruction of links or nodes. **4.** Even with massive artillery bombardment, the telephone network in Moscow remained in use all through the siege. **5.** They include frequency hoppers, direct sequence spread spectrum (DSSS), and burst transponders.

TEXT 6.

Frequency Hopping

Frequency ***hoppers*** are the simplest spread-spectrum systems to understand and to ***implement***. They do exactly as their name ***suggest***s: they hop rapidly from one frequency to another, with the sequence of frequencies determined by a pseudorandom sequence known to the authorized ***principals***. Hoppers were invented, famously, over dinner in 1940 by actress Hedy Lamarr and screenwriter George Antheil, who devised the technique as a means of controlling ***torpedos*** without the enemy detecting them or jamming their transmissions. A frequency-hopping radar was independently developed at about the same time by the Germans; in response to steady improvements in British jamming, German technicians adapted their equipment to change frequency daily, then hourly, and finally, every few seconds.

Hoppers are resistant to jamming by an opponent who doesn't know the hop sequence. Such an opponent may have to jam much of the ***band***, and thus needs much more power than would otherwise be necessary. The ***ratio*** of the input signal's bandwidth to that of the transmitted signal is called the *process gain* of the system; thus, a 100 bit/sec signal spread over 10 MHz has a process gain of $10^7/10^2 = 10^5 = 50$ dB.

The *jamming margin*, which is defined as the maximum tolerable ratio of jamming power to signal power, is essentially the process gain ***modulo*** implementation and other losses (strictly speaking, process gain divided by the minimum bit ***energy-to-noise*** density ratio). The optimal jamming strategy, for an opponent who can't ***predict*** the hop sequence, is *partial band jamming*—to jam enough of the band to introduce an unacceptable error rate in the signal.

Although hoppers can give a large jamming ***margin***, they give little protection against an opponent who ***merely*** wants to detect their ***existence***. A signal analysis receiver that ***sweep***s across the frequency band of interest will often intercept them. (Depending on the relevant ***bandwidth***s, sweep rate, and dwell time, it might intercept a hopping signal several times).
However, because frequency hoppers are simple to implement, they are often used in combat networks, such as ***man-pack radios***, with slow hop rates of 5 0–500 per second. To disrupt their communications, the enemy will need a fast or powerful jammer, which is inconvenient for the ***battlefield***. Fast hoppers (defined in theory as having hop rates ***exceeding*** the bit rate; in practice, with hop rates of 10,000 per second or more) can pass the limit of even large jammers.

Language Study

1. Translate all the words in next order:

a) N; b) V; c) Adj; d) Adv (if they are)

Hoppers, implement, suggest, principals, torpedos, band, ratio, modulo, energy-to-noise, predict, margin, merely, existence, sweep, bandwidth, man-pack, battlefield, exceeding.

2. Join the next pairs of simple sentences by means of next conjunctions: <u>who, and, thus, which, that</u> following the next scheme: a+b, a+b+c, a+b+c+d

1. (a) Hoppers were invented, famously, over dinner in 1940
(b) by actress Hedy Lamarr
(c) screenwriter George Antheil
(d) devised the technique as a means of controlling torpedos without the enemy detecting them;

2. (a) Hoppers are resistant to jamming
(b) by an opponent
(c) doesn't know the hop sequence;

3. (a) Such an opponent may have to jam much of the band
(b) thus needs much more power than would otherwise be necessary;

4. (a) The ratio of the input signal's bandwidth to that of the transmitted signal is called the *process gain* of the system
(b) a 100 bit/sec signal spread over 10 MHz;

5. (a) The jamming margin
(b) is defined as the maximum tolerable ratio of jamming power to signal power, is essentially the process gain modulo implementation;

6. (a) The optimal jamming strategy, for an opponent
(b) can't predict the hop sequence is partial band jamming

7. (a) A signal analysis receiver
(b) sweeps across the frequency band of interest will often intercept them;

8. (a)To disrupt their communications

(b) the enemy will need a fast or powerful jammer

(c) is inconvenient for the battlefield.

3. Choose the right preposition:

1. They do exactly as their name suggests: they hop rapidly … one frequency … another, … the sequence … frequencies determined … a pseudorandom sequence known … the authorized principals. (with, from, to, of, by, to)

2. Hoppers were invented, famously, … dinner … 1940 … actress Hedy Lamarr and screenwriter George Antheil. (by, in, over)

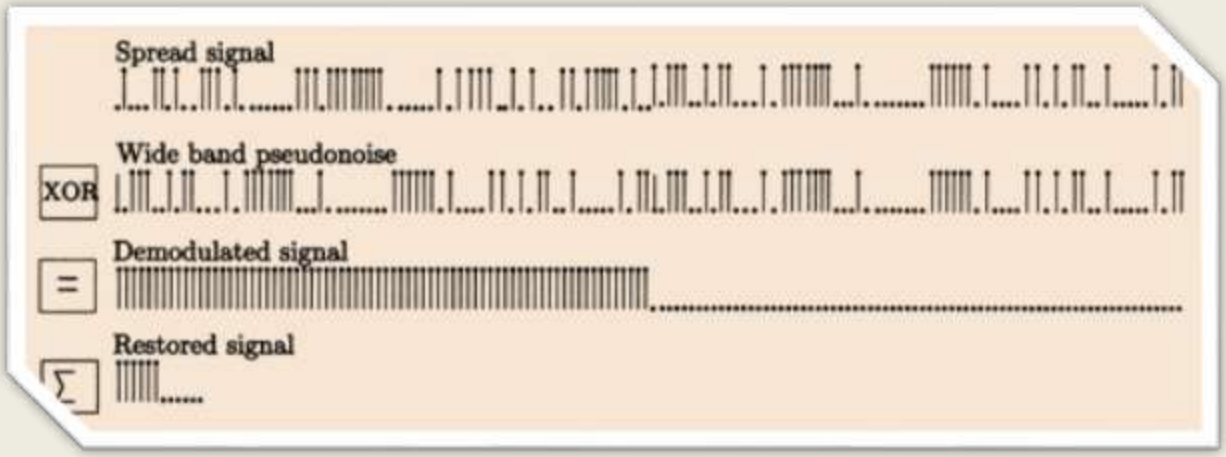
3. The frequency hoppers are simple … implement, they are often used … combat networks, such as man-pack radios, … slow hop rates … 5 0–500 … second. (of, in, per, with, to)

TEXT 7.

DSSS

In direct ***sequence*** spread spectrum, we ***multiply*** the information-bearing sequence by a much higher-rate pseudorandom sequence, usually generated by some kind of stream cipher. This spreads the spectrum by increasing the bandwidth (Figure 16.1). The technique was first described by a Swiss engineer, Gustav Guanella, in a 1938 patent application, and developed extensively in the United States in the 1950s. Its first ***deployment*** in ***anger*** was in Berlin in 1959. Like hopping, DSSS can give substantial jamming margin (the two systems have the same theoretical performance). But it can also make the signal significantly harder to ***intercept***. The trick is to arrange things so that at the intercept location, the signal strength is so low that it is lost in the noise floor unless you know the spreading sequence with which to recover it. Of course, it's harder to do both at the same time, since an ***antijam*** signal should be high power and an LPI/LPPF signal low power; the usual modus operandi is to work in LPI mode until detected by the enemy (for example, when coming within radar ***range***), then ***boost*** transmitter power into antijam mode.

Figure 16.1 *Spreading in DSSS (courtesy of Roche and Dugelay).*



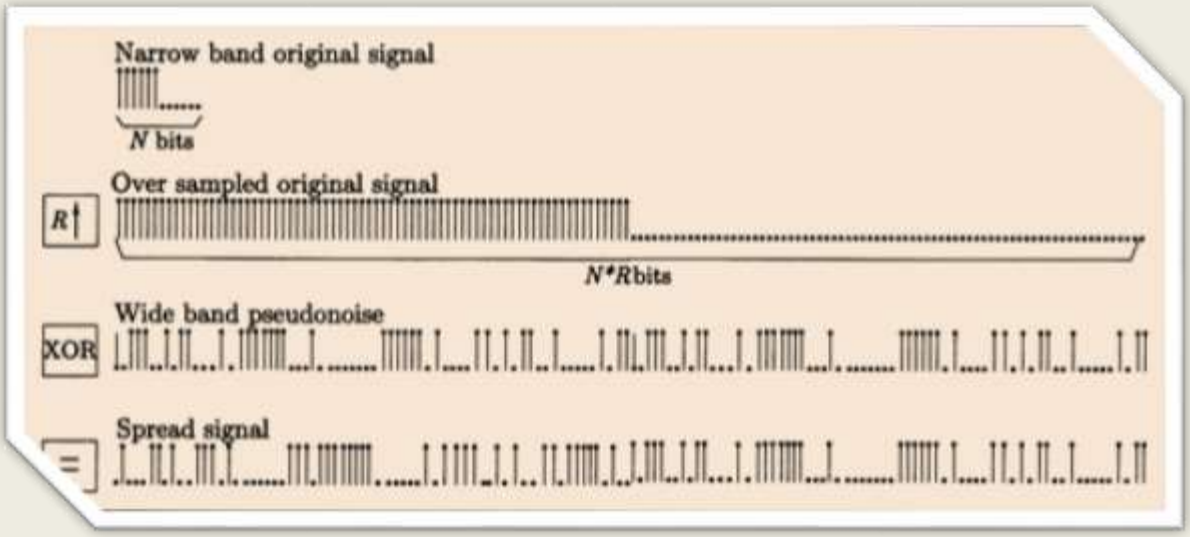


Figure 16.2 *Unspreading in DSSS (courtesy of Roche and Dugelay).*

There is a large literature on DSSS; and the techniques have now been taken up by the commercial world as *code division multiple* ***access*** (CDMA) in various mobile radio and phone systems. DSSS is sometimes referred to as "encrypting the RF," and it comes in a number of variants. For example, when the underlying modulation scheme is FM rather than AM, it's called ***chirp***. (The classic introduction to the underlying mathematics and technology is.) The engineering complexity is higher than with frequency ***hop***, for various reasons. For example, synchronization is particularly critical. Users with access to a reference time signal (such as GPS or an atomic clock) can do this much more easily; of course, if you don't control GPS, you may be open to synchronization attacks; and even if you do, the GPS signal might be jammed. (It has recently been reported that the French jammed GPS in Greece in ***an attempt*** to sabotage a British ***bid*** to sell 250 tanks to the Greek government, a deal in which France was ***a competitor***. This caused the British tanks to get lost during ***trials***. When the ***ruse*** was discovered, the Greeks found it all rather amusing.) Another strategy is to have your users take turns at providing a reference signal.

Language Study

1. Translate all the words in next order:

a) N; b) V; c) Adj; d) Adv (if they are)

Sequence, multiply, deployment, anger, intercept, range, boost, antijam, access, chirp, hop, attempt, bid, competitor, trials, ruse.

2. Insert the blanks with the right word:

The technique was first … *(written, said, described)* by a Swiss engineer, Gustav Guanella, in a 1938 … *(pattern, patent, model)* application, and … *(developed, constructed, defined)* extensively in the … *(UK, United States, China)* in the 1950s. Its first deployment in anger was in Berlin in … *(1940, 1959, 1961)*. Like hopping, … *(DSSS, LAN, PSSS)* can give substantial jamming margin (the two systems have the same theoretical performance). But it can also make the … *(signal,*

sound, mode) significantly harder to intercept. The trick is to … *(amplify, arrange, notify)* things so that at the intercept … *(location, modulation, altitude)*, the signal strength is so … *(high, low, fast, slow)* that it is lost in the noise floor unless you know the spreading … *(sequence, cover, introduction)* with which to recover it.

3. Translate the next sentences. Find the wrong sentences going against the point of the text:

1. The trick is to arrange things so that at the intercept location, the signal strength is so low that it is lost in the noise floor unless you know the spreading sequence with which to recover it. 2. When the underlying introduction scheme is FM rather than AM, it's called access. 3. Users with bandwidth to a reference period signal (such as GLONASS or an atomic clock) can do this much more easily; of course, if you don't control GPS, you may be open to modulation attacks; and even if you do, the GPS transmission might be jammed. 4. This caused the British tanks to get lost during trials. 5. But it can also make the signal significantly harder to intercept.

4. Express your relation using the next clichés:

That's right!	**I'm afraid you're wrong.**
I quite agree with you.	**I don't think so.**
I believe (suppose)…	
In my opinion…	

a) In direct sequence spread spectrum, we multiply the information-bearing sequence by a much higher-rate pseudorandom sequence, usually generated by some kind of stream cipher.
b) It's harder to do both at the same time, since an antijam signal should be high power and an LPI/LPPF signal low power.
c) The classic introduction to the underlying mechanical drawing and technology is.
d) Another strategy is to have your users take turns at providing a reference modulation.
e) If you don't control GPS, you may be open to synchronization attacks; and even if you do, the GPS signal might be jammed.

TEXT 8.

Burst Communications

Burst communications, as their name ***suggest***s, involve compressing the data and transmitting it in short bursts at times ***unpredictable*** by the enemy. They are also known as ***time-hop.*** Usually, they are not so jam-resistant (except ***insofar*** as the higher data rate spreads the spectrum), but they can be difficult to intercept; if the duty cycle is low, a ***sweep*** receiver can easily ***miss*** them. They are often used in radios for special forces and intelligence agents.

An interesting variant is ***meteor burst*** transmission (also known as ***meteor scatter***). This relies on the billions of micrometeorites that strike the Earth's atmosphere each day, each leaving a long ***ionization trail*** that persists for about a third of a second, and providing a temporary transmission path between a "mother station" and an area that might be a hundred miles long and a few miles wide. The mother station transmits continuously, and whenever one of the "daughters" hears mother, it starts to send packets of data at high speed, to which mother replies. With the low power levels used in covert operations, it is possible to achieve an ***average data*** rate of about 50 bps, with an average ***latency*** of about 5 minutes and a range of 500–1,500 miles. With higher power levels, and in higher ***latitude***s, average data rates can rise into the tens of kilo- bits per second.

As well as special forces, the U.S. Air Force in Alaska uses meteor scatter as ***backup*** communications for early warning radars. It's also used in civilian applications such as monitoring ***rainfall*** in Lesotho, Africa. In niche markets, where low bit rates and high latency can be ***tolerate***d, but where equipment size and cost are important, meteor scatter can be hard to beat.

Language Study

1. Combine all words on parts of speech - N, Adj, V, Adv or W/C (word combinations):

Burst communications, suggest, unpredictable, time-hop, insofar, sweep, miss, meteor burst/ scatter, ionization, trail, average, latency, latitude, backup, rainfall, tolerate.

2. Find the English equivalents to the Russian ones:

Название предполагает, быть помехоустойчивым, наносить удар атмосфере Земли, оставлять ионизационный след, материнская станция, на высокой скорости, одна из дочерних станций "слышит" материнскую (станцию), низкий уровень мощности, задержка в среднем 5 минут, резервная связь радаров быстрого реагирования, мониторинг осадков, трудно преодолеть метеоритную туманность.

3. Fill in the blanks choosing corresponding words from the brackets:

1. Burst *(communications, transmission, conduction, reception)* as their name suggests, involve compressing the data and transmitting it in short bursts at times unpredictable by the enemy. 2. The mother *(station, card, modulation, conduction)* transmits continuously, and whenever one of the *("dads", "broths", "granddaughters", "grandpas", "daughters")* hears mother, it starts to send packets of data at high speed, to which mother replies.3. With the low *(energy, power, strength, force)* levels used in covert operations, it is possible to achieve an average data rate of about 50 bps. 4. In niche markets, where low bit *(ratios, rates, levels, speeds)* and high latency can be tolerated.

4. Find the sentence which is said about the mother and daughters. Write the point of these idea in two sentences.

TEXT 9.

Combining Covertness and Jam Resistance

There are some rather complex ***trade-offs*** between different LPI, LPPF, and jam resistance technologies, and other aspects of performance such as their resistance to ***fad***ing and multipath, and the number of users that can be ***accommodate***d simultaneously. They also ***behave*** differently in the face of specialized jamming techniques such as ***swept-frequency jamming*** (where the jammer sweeps ***repeatedly*** through the target frequency band) and ***repeater jamming*** (where the jammer follows a hopper as closely as it can). Some types of jamming translate; for example, an opponent with insufficient power to block a signal completely can do ***partial time jamming*** on DSSS by emitting pulses that cover most of its utilized spectrum, and on frequency hop by partial band jamming.

There are also engineering trade-offs. For example, DSSS tends to be about twice as efficient as frequency ***hop*** in power terms, but frequency hop gives much more jamming margin for a given complexity of equipment. On the other hand, DSSS signals are much harder to locate using

direction-finding techniques.
System ***survivability*** requirements can impose further constraints. It may be essential to prevent an opponent who has captured one radio and extracted its current key material from using this to jam a whole network.
A typical modern military system will use some combination of ***tight beams***, DSSS, hopping and burst.

- The Jaguar tactical radio used by U.K. armed forces hops over one of nine 6.4 MHz bands, and has an antenna with a steerable null that can be pointed at a jammer or at a hostile intercept station.
- Both DSSS and hopping are used with *Time Division Multiple Access* (TDMA) in the *Joint Tactical Information Distribution System* (JTIDS), a U.S. data link system used by AWACS—the Airborne Warning and Control System—to communicate with fighters. TDMA separates transmission from ***reception***, and lets users know when to expect their ***slot***. The DSSS signal has a 57.6 KHz data rate and a 10 MHz chip rate (and so a jamming margin of 36.5 dB), which hops around in a 255 MHz band with a minimum jump of 30 MHz. The hopping code is available to all users, while the spreading code is limited to individual circuits. The rationale is that if an equipment capture leads to the compromise of the spreading code, this would allow jamming of only a single 10 MHz band, not the full 255 MHz.
- MILSTAR is a U.S. satellite communications system with 1-degree beams from a geostationary orbit (20 GHz down, 44 GHz up). The effect of the narrow beam is that users can operate within three miles of the enemy without being detected. Jam protection is from hopping; its channels hop several thou- sand times a second in bands of 2 GHz.
- A system designed to control MX ***missiles*** (but not in the end deployed) is described in and gives an example of extreme survivability engineering. To be able to ***withstand a nuclear*** first ***strike***, the system had to withstand significant levels of ***node*** destruction, jamming, and atmospheric noise. The design ***adopt***ed was a frequency hopper at 450 KHz with a dynamically ***reconfigurable*** network.
- French tactical radios have ***remote controls***. The soldier can use the ***handset*** a hundred meters from the radio. This means that attacks on the high-power emitter don't ***endanger*** the ***troop***s so much.

There are also some system-level tricks, such as ***interference cancellation***, where the idea is to communicate in a band you are jamming and whose jamming waveform is known to your own radios, so they can cancel it out or hop around it. This can make jamming harder for the enemy by forcing him to spread his available power over a larger bandwidth, and can make signals intelligence harder, too.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns and W/C.

Trade-offs, fade, accommodate, behave, swept-frequency jamming, repeatedly, repeater jamming, partial time jamming, hop, direction-finding, survivability, tight beams, reception, slot, missiles, withstand, a nuclear strike, node, adopt, reconfigurable, remote controls, handset, endanger, troop, interference cancellation.

2. Read the title of the text and suppose about what is the text.

a) Write out the text the information about *repeater jamming, partial time jamming* and substantiate their meanings in the "jam resistance"

b) In the paragraph four the aspects of some combination of tight beams, DSSS, hopping and burst are listed. How many aspects have you counted?

c) Find the sentence where the main idea of the text is defined.

3. Find in the text all "doers" and write them down. Use the prompt: V + -er (-or) → do+ -er →*doer*

4. Define the "processes" taking place in the text. Use the frame: V + -ing → *process*

TEXT 10. Interaction Between Civil and Military Uses

Civil and military uses of communications are increasingly ***intertwine***d. Operation Desert Storm (the Gulf War against Iraq) made extensive use of the Gulf States' civilian infrastructure: a huge tactical communications network was created in a short space of time using satellites, radio links, and leased lines. Experts from various U.S. armed services ***claim*** that the effect of communications capability on the war was absolutely ***decisive***. It appears ***inevitable*** that both military and substate groups will attack civilian infrastructure to deny it to their opponents. Already, satellite links are particularly vulnerable to uplink jamming. Satellite-based systems such as GPS have been jammed as an exercise; and there is some discussion of the systemic vulnerabilities that result from ***overreliance*** on it. Another example of growing ***interdependency*** is given by the Global Positioning System, GPS. This started as a U.S. military navigation system, and had a ***selective availability*** feature that limited the ***accuracy*** to about a hundred yards unless the user had the relevant cryptographic key. This had to be turned off during Desert Storm as there weren't enough military GPS sets to go around, and civilian equipment had to be used instead. As time went on, GPS ***turn***ed ***out*** to be so useful, particularly in civil aviation, that the FAA helped find ways to defeat selective availability that give an accuracy of about three yards, compared with a claimed eight yards for the standard military receiver. Finally, in May 2000, President Clinton announced the ***cessation*** of selective availability. (***Presumably***, this preserves its usability in wartime.)

The civilian infrastructure also provides some defensive systems of which government organizations (especially in the intelligence field) can make use. I mentioned the prepaid mobile phone, which provides a fair degree of ***anonymity***; secure Web servers offer some possibilities; and another example is the ***anonymous remailer***, a device that accepts encrypted email, decrypts it, and sends it on to a ***destination*** contained within the outer encrypted ***envelope***. I'll discuss this technology in more detail in Section 20.4.3; one of the pioneers of anonymous networking was the U.S. Navy. Conspiracy theorists suspect that public use of the system provides cover ***traffic*** for classified messages.

Although communications security on the Net has, until now, been interpreted largely in terms of message confidentiality and authentication, it looks likely that the future will become much more

like military communications, in that various kinds of service denial attacks, anonymity, and deception plays will become increasingly important. I'll return to this theme later. For now, let's look at the aspects of electronic warfare that have to do with target ***acquisition*** and ***weapon guidance***, as these are where the arts of jamming and ***deception*** have been most highly developed. (In fact, although there is much more in the open literature on the application of electronic attack and defense to radar than to communications, much of the same material clearly applies to both.)

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Adjectives and Verbs:

Intertwine, claim, decisive, inevitable, overreliance, selective availability, anonymity, anonymous remailer, destination, turn out, envelope, traffic, cessation, weapon guidance, acquisition, deception.

2. a) Rephrase the next sentence fragments following the pattern and translate them. Then find the sentences in the text and translate them in full.
b) Some sentences are not corresponded the model. Find them and give a translation, too.

substate groups will attack civilian infrastructure ***to deny*** it = substate groups will attack civilian infrastructure which ***should be denied***

1) Satellite links are particularly vulnerable ***to uplink*** jamming… .
2) Navigation system had a selective availability feature that limited the accuracy ***to*** about a hundred yards… .
3) This had ***to be*** turned off during Desert Storm… .
4) As time went on, GPS turned out ***to be*** so useful… .
5) There weren't enough military GPS sets ***to go*** around, and civilian equipment had ***to be used*** instead… .
6) I'll return ***to*** this theme later… .
7) Electronic warfare that have ***to do*** with target acquisition and weapon guidance… .
8) Much of the same material clearly applies ***to*** both… .

3. a) Find in the text the sentences formed by the model → **have + V_{ed}**
b) Write them out the text and translate in a written way.

TEXT 11.

Surveillance and Target Acquisition

Although some sensor systems use passive direction finding, the main methods used to detect ***hostile*** targets and guide weapons to them are ***sonar***, radar, and ***infrared***. The first of these to be developed was sonar, which was invented and deployed in World War I (under the name of Asdic). Except in ***submarine*** warfare, the key sensor is radar. Although radar was invented by

Christian Hülsmeyer in 1904 as a maritime ***anti-collision*** device, its serious development only ***occur***red in the 1930s, and it was used by all major participants in World War II. The electronic attack and protection techniques developed for it ***tend*** to be better developed than, and often ***go over to***, systems using other sensors. In the context of radar, "electronic attack" usually means jamming (though in theory it also includes stealth technology), and "electronic protection" refers to the techniques used to ***preserve*** at least some radar capability.

TEXT 12. Types of Radar

A very wide range of systems are in use, including search radars, ***fire-control*** radars, ***terrain-following*** radars, counter bombardment radars, and weather radars. They have a wide variety of signal characteristics. For example, radars with a low RF and a low ***pulse repetition frequency*** (PRF) are better for search, while high-frequency, high PRF devices are better for tracking. A good textbook on the technology is by Schleher.

Simple radar designs for search applications may have a ***rotat***ing antenna that emits a sequence of pulses and detects ***echoe***s. This was an easy way to ***implement*** radar in the days before digital electronics; the sweep in the display tube could be mechanically rotated in ***synch*** with the antenna. Fire-control radars often used ***conical scan****;* the beam would be ***track***ed in a circle around the target's position, and the amplitude of the returns could drive positioning ***servos*** (and weapon controls) directly. Now the beams are often generated electronically using multiple antenna elements, but tracking loops remain central. Many radars have a ***range gate***, ***circuitry*** that focuses on targets within a certain range of distances from the antenna; if the radar had to track all objects between, say, 0 and 100 miles, then its pulse repetition frequency would be limited by the time it takes radio waves to travel 200 miles. This would have consequences for angular ***resolution*** and for tracking performance generally.

Doppler radar measures the ***velocity*** of the target by the change in frequency in the return signal. It is very important in ***distinguish***ing moving targets from ***clutter***, the returns reflected from the ground. Doppler radars may have ***velocity gates*** that restrict attention to targets whose radial speed with respect to the antenna is within certain limits.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Verbs:

Hostile, sonar, infrared, submarine, anti-collision, occur, tend, go over to, preserve, fire-control, terrain-following, pulse repetition frequency, rotate, echo, implement, synch, conical scan, track, servos, range gate, circuitry, resolution, velocity, distinguish, clutter, velocity gates.

2. Find in the text the predicative formed by the model to be + V_{ed} and say of the fact its

using.

3. Translate the next sentences into Russian taking into account the meaning of the verbal forms:

1. Although some sensor systems use passive direction finding, the main methods used to detect hostile targets and guide weapons to them are sonar, radar, and infrared. **2.** The first of these to be developed was sonar, which was invented and deployed in World War I. **3.** A very wide range of systems are in use, including search radars, fire-control radars, terrain-following radars**. 4.** Simple radar designs for search applications may have a rotating antenna that emits a sequence of pulses and detects echoes. **5.** Fire-control radars often used conical scan; the beam would be tracked in a circle around the target's position, and the amplitude of the returns could drive positioning servos directly. **6.** If the radar had to track all objects between 0 and 100 miles then its pulse repetition frequency would be limited by the time it takes radio waves to travel 200 miles.

4. Define the sentences which correspond the point of the text:

1. Radar was invented by Christian Hülsmeyer in 1906 as a maritime collision device.
2. Radar's serious development only occurred in the 1930s, and it was used by all major participants in World War II.
3. "Jamming" usually means electronic attack (though in theory it also includes phantom technology), and "ionic protection" refers to the techniques used to preserve at least some radar capability.
4. The beam would be tracked in a circle around the target's position, and the amplitude of the returns could drive positioning servos (and weapon controls) directly.
5. For example, radars with a high RA and a high pulse repetition frequency (HRF) are better for rest, while low-frequency, high PRF devices are better for tracking.
6. This was an easy way to implement radar in the days before digital electronics; the sweep in the screen tube could be automatically rotated in synch with the aerial.
7. Now the beams are often generated electronically using multiple antenna elements, but tracking loops remain central.
8. This would have consequences for triangle resolution and for searching performance generally.

Jamming Techniques

TEXT 13.

Electronic attack techniques can be passive or active. The earliest ***countermeasure*** to be widely used was ***chaff***—thin strips of conducting ***foil*** cut to a half the wavelength of the target signal, then ***dispersed*** to provide a false return. Toward the end of World War II, ***allied*** aircraft were dropping 2,000 tons of chaff a day to degrade German air defenses. Chaff can be dropped directly by the aircraft attempting to ***penetrate*** the defenses (which isn't ideal, as they will then be at the ***apex*** of an elongated signal) or by support aircraft, or fired forward into a suitable pattern using rockets or shells. The main ***counter-countermeasure*** against chaff is the use of Doppler radars; the chaff is very light, so it comes to rest almost at once and can be distinguished fairly easily from ***moving targets***.

Other techniques include small ***decoys*** with active repeaters that retransmit radar signals, and larger decoys that simply reflect them; sometimes one ***vehicle*** (such as a helicopter) acts as a decoy for another more valuable one (such as an aircraft ***carrier***). The principles are quite general. Weapons that home using RDF are decoyed by special drones that emit ***seduction*** RF signals, while infrared guided missiles are ***divert***ed using ***flare***s.

The passive countermeasure in which the most money has been invested is ***stealth***, reducing the ***radar cross-section*** (RCS) of a vehicle so that it can be detected only at very much shorter range. This means, for example, that the ***enemy*** has to place his air defense radars closer together, so he has to buy a lot more of them. Stealth includes a wide range of techniques, and a proper discussion is well beyond the ***scope*** of this book. Some people think of it as "extremely expensive black paint," but there's more to it than that. Because an aircraft's RCS is typically a function of its aspect, it may have a ***fly-by-wire*** system that continually ***exhibit***s an aspect with a low RCS to identified hostile emitters.

Active countermeasures are much more diverse. Early jammers simply generated a lot of noise in

the range of frequencies used by the target radar; this technique is known as *noise jamming* or ***barrage*** *jamming*. Some systems used systematic frequency patterns, such as pulse jammers, or swept jammers which traversed the frequency range of interest (also known as *squidging oscillators*). But such a signal is fairly easy to block—one trick is to use a *guard band* receiver, a receiver on a frequency ***adjacent*** to the one in use, and to blank the signal when this receiver shows a jamming signal. It should also be noted that jamming isn't restricted to one side. As well as being used by the radar's opponent, the radar itself can also send suitable ***spurious*** signals from an auxiliary antenna to ***mask*** the real signal or simply to overload the defenses.

At the other end of the ***scale*** lie hard-kill techniques such as *anti-radiation missiles* (ARMs), often fired by support aircraft, which home in on the sources of hostile signals. Defenses against such weapons include the use of decoy transmitters, and blinking transmitters on and off.

In the middle lies a large ***toolkit*** of *deception jamming* techniques. Most jammers used for self-protection are deception jammers of one kind or another; barrage and ARM techniques tend to be more suited to use by support vehicles.

The usual goal with a self-protection jammer is to deny range and bearing information to attackers. The basic trick is *inverse gain jamming* or *inverse gain amplitude modulation.* This is based on the observation that the directionality of the attacker's antenna is usually not perfect; in addition to the main beam, it has ***sidelobes*** through which energy is also transmitted and received, ***albeit*** much less efficiently. The sidelobe response can be mapped by observing the transmitted signal, and a jamming signal can be generated so that the net emission is the ***inverse*** of the antenna's directional response. The effect, as far as the attacker's radar is concerned, is that the signal seems to come from everywhere; instead of a "***blip***" on the radar screen you see a circle centered on your own antenna. Inverse gain jamming is very effective against the older conical-scan fire-control systems.

More generally, the technique is to retransmit the radar signal with a systematic change in delay and/or frequency. This can be either noncoherent, in which case the jammer is called a ***transponder***, or coherent—that is, with the right waveform—when it's a *repeater*. (It is now common to store received waveforms in *digital radio frequency memory* (DRFM) and manipulate them using signal processing chips.)

An elementary countermeasure is *burn-through*. By lowering the pulse repetition frequency, the ***dwell*** time is increased, so the return signal is stronger—at the cost of less ***precision***. A more sophisticated countermeasure is *range gate pull-off* (RGPO). Here, the jammer transmits a number of fake pulses that are stronger than the real ones, thus capturing the receiver, and then moving them out of phase so that the target is no longer in the receiver's range gate. Similarly, with Doppler radars the basic trick is *velocity gate pull-off* (VGPO). With older radars, successful RGPO would cause the radar to break lock and the target to disappear from the screen. Modern radars can ***reacquire*** lock very quickly, so RGPO must either be performed repeatedly or combined with another technique—commonly, with inverse gain jamming to break angle tracking at the same time.

An elementary counter-countermeasure is to ***jitter*** the pulse repetition frequency. Each outgoing pulse is either delayed or not, depending on a *lag sequence* generated by a stream cipher or random number generator. This means that the jammer cannot ***anticipate*** when the next pulse will arrive, and so has to follow it. Such *follower jamming* can only make false targets that appear to be further away. The (counter)-measure is for the radar to have a *leading-edge tracker*, which responds only to the first return pulse; and the (counter)-measures can include jamming at such a high power that the receiver's automatic gain control circuit is captured, or *cover jamming* in which the jamming pulse is long enough to cover the maximum jitter period.

The next ***twist*** of the ***screw*** may involve tactics. Chaff is often used to force a radar into Doppler

mode, which makes PRF jitter difficult (as continuous waveforms are better than pulsed for Doppler), while leading-edge trackers may be combined with frequency agility and smart signal processing. For example, true target returns ***fluctuate***, and have realistic ***acceleration***s, while simple transponders and repeaters give out a more or less steady signal. Of course, it's always possible for designers to be too clever; the ***Mig-29*** could ***decelerate*** more rapidly in level flight by a rapid ***pull-up*** than some radar designers had anticipated, and so pilots could use this ***maneuver*** to break radar lock. And now, of course, enough MIPS are available to manufacture realistic false returns.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Adjectives and Verbs:

Countermeasure, chaff, foil, dispersed, allied, penetrate, counter-countermeasure, moving targets, decoys, vehicle, carrier, seduction, divert, flare, stealth, radar cross-section, exhibit, barrage, adjacent, spurious, mask, scale, toolkit, sidelobes, albeit, inverse, blip, transponder, dwell, precision, reacquire, jitter, anticipate, twist, screw, fluctuate, acceleration, Mig-29, decelerate, pull-up, maneuver.

2. Join the two parts of the sentence using next conjunctions. Translate the formed sentences:

a) then
The earliest countermeasure to be widely used was chaff. Dispersed to provide a false return.

b) as
Chaff can be dropped directly by the aircraft attempting to penetrate the defenses (which isn't ideal. They will then be at the apex of an elongated signal).

c) that, while
Weapons. Home using RDF are decoyed by special drones that emit seduction RF signals. Infrared guided missiles are diverted using flares.

d) in which, so that
The passive countermeasure. The most money has been invested is stealth, reducing the radar cross-section (RCS) of a vehicle. It can be detected only at very much shorter range.

e) that, so
This means… the ***enemy*** has to place his air defense radars closer together. He has to buy a lot more of them.

d) or, as well as
Being used by the radar's opponent … the radar itself can also send suitable spurious signals from an auxiliary antenna to mask the real signal … simply to overload the defenses.

f) which, such as
At the other end of the scale lie hard-kill techniques … anti-radiation missiles (ARMs), often fired by support aircraft, … home in on the sources of hostile signals.

g) that
The directionality of the attacker's antenna is usually not perfect. This is based on the observation.

h) so that, and
The sidelobe response can be mapped by observing the transmitted signal. A jamming signal can be generated. The net emission is the inverse of the antenna's directional response.

3. Find in the text and write down 5 conjunctionless sentences. Translate them in a written way.

TEXT 14. Advanced Radars and Countermeasures

A number of ***advanced techniques*** are used to give an edge on the jammer. ***Pulse compression***, first developed in Germany in World War II, uses a kind of direct sequence spread-spectrum pulse, filtered on return by a matched filter to compress it again. This can give processing gains of 10–1,000. Pulse compression radars are resistant to transponder jammers, but are vulnerable to repeater jammers, especially those with digital radio frequency memory. However, the use of LPI waveforms is important if you do not wish the target to detect you first.

Pulsed Doppler is much the same as Doppler, and sends a series of phase ***stable*** pulses. It has come to dominate many high-end markets, and is widely used, for example, in ***look-down shoot-down systems*** for air defense against low-flying intruders. As with elementary pulsed tracking radars, different RF and pulse repetition frequencies have different characteristics: we want low-frequency/PRF for ***unambiguous*** range/velocity and also to reduce ***clutter***—but this can leave many blind spots. Airborne radars that have to deal with many threats use high PRF and look only for velocities above some ***threshold***, say 100 ***knots***—but are weak in tail chases. The usual compromise is medium PRF—but this ***suffer***s from severe range ambiguities in airborne operations. Also, search radar requires long, diverse ***bursts***, whereas tracking needs only short, tuned ones. An advantage is that pulsed Doppler can discriminate some very specific signals, such as modulation provided by turbine ***blades*** in jet engines. The main ***deception strategy*** used against pulsed Doppler is velocity gate pull- off, although a new variant is to excite multiple velocity gates with deceptive returns.

Monopulse is becoming one of the most popular techniques. It is used, for example, in the Exocet missiles that proved so difficult to jam in the Falklands war. The idea is to have four linked antennas so that azimuth and elevation data can be ***compute***d from each return pulse using interferometric techniques. Monopulse radars are difficult and expensive to jam, unless a design defect can be exploited; the usual techniques involve tricks such as formation jamming and terrain bounce. Often the preferred defensive strategy is just to use towed decoys.

One of the more recent tricks is *passive coherent location.* Lockheed's Silent Sentry system has no emitters at all, but rather utilizes reflections of commercial radio and television broadcast signals to detect and track airborne objects. The receivers, being passive, are hard to locate and attack; and knocking out the system entails destroying major civilian infrastructures, which

opponents will often prefer not to do for various propaganda reasons. This strategy is moderately effective against some kinds of stealth technology.
The ***emergence*** of digital radio frequency memory and other software radio techniques holds out the prospect of much more complex attack and defense. Both radar and jammer waveforms may be adapted to the tactical situation with much greater ***flexibility*** than before. But fancy combinations of spectral, temporal, and ***spatial*** characteristics will not be the whole story. Effective electronic attack is likely to continue to require the effective coordination of different passive and active tools with weapons and tactics. The importance of intelligence, and of careful deception planning, is likely to increase.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns and Adjectives:

Advanced techniques, pulse compression, stable, look-down shoot-down systems, unambiguous, clutter, thresholds, knots, suffer, bursts, deception strategy, monopulse, compute, emergence flexibility, spatial.

2. What of Russian equivalents will be more corresponding to the defined English construction?

1. Pulse compression, first developed in Germany in World War II, uses a kind of direct sequence spread-spectrum pulse *(прямую последовательность импульсов с расширенным спектром; прямую импульсную последовательность расширенного спектра)*, filtered on return by a matched filter to compress it again.
2. Pulse compression radars are resistant to transponder jammers, but are vulnerable to repeater jammers *(уязвимые глушители ретрансляторов; уязвимы для ретрансляторов глушителей)*, especially those with digital radio frequency memory.
3. Airborne radars that have to deal with many threats use high PRF and look only for velocities above some threshold *(выискивают скорость выше некоего порога; ищут скорости превышающие пороговое значение)*, say 100 knots—but are weak in tail chases.
4. The idea is to have four linked antennas so that azimuth and elevation data can be computed from each return pulse using interferometric techniques. *(могут быть вычислены из каждого отражённого импульса с использованием интерферометрических методов; могут быть вычислены от каждого отражённого импульса, используя интерферометрические методы).*
5. Monopulse radars are difficult and expensive to jam, unless a design defect can be exploited; the usual techniques involve tricks such as formation jamming and terrain bounce *(обычные методы включают приемы, такие как образование и заклинивания местности отскока; обычные методы включают приемы, такие как образование взаимных помех при приёме и их земное отражение)*.
6. Lockheed's Silent Sentry system has no emitters at all, but rather utilizes reflections of commercial radio and television broadcast signals *(не имеет излучатели на всех, а скорее использует отражения коммерческих радио- и телевизионных вещательных сигналов; вовсе не имеет излучателей, а скорее использует отражение коммерческих транслируемых радио- и телесигналов)* to detect and track airborne objects.

3. Define the English sentence which is the equivalent to the Russian one:

Используется ряд передовых методов, применяемых преимущественно на глушителях.

1. A number of advanced techniques are used to give an edge on the jammer.
2. Advanced techniques are used to give an edge on the jammer.
3. New technologies are used only for jamming.
4. A new technology are applied to the jammer band.

Преимущество состоит в том, что импульсная доплеровская частота может различать некоторые очень специфические сигналы, такие как модуляция, производимая турбинными лопастями реактивных двигателей.

1. Pulsed Doppler can discriminate some very specific signals, such as modulation provided by turbine blades in jet engines.
2. An advantage is that pulsed Doppler can discriminate some very specific signals, such as modulation provided by turbine blades in jet engines.
3. The Doppler can discriminate specific signals, such as modulation made by turbine blades in jet engines.
4. An advantage is that jammer can discriminate some very important signals, such as amplitude provided by turbine blades in jet engines.

TEXT 15. Other Sensors and Multisensor Issues

Much of what was said about radar earlier applies to sonar as well, and a fair amount applies to ***infrared***. Passive ***decoy***s—***flares***—worked very well against early ***heat-seeking missiles*** that used a mechanically ***spun*** detector, but are less effective against modern detectors that incorporate signal processing. Flares are like ***chaff*** in that they ***decelerate*** rapidly with respect to the target, so the attacker can filter on velocity or acceleration. Flares are also like repeater jammers in that their signals are relatively stable and strong compared with real targets.

Active infrared jamming is harder, and thus less widespread, than radar jamming. It tends to ***exploit*** features of the hostile sensor by pulsing at a rate or in a pattern that causes confusion. Some infrared defense systems are starting to employ lasers to disable the sensors of incoming weapons; and it has recently been admitted that a number of UFO sightings were actually due to various kinds of jamming (both radar and infra- red).

One growth area is ***multisensor data fusion***, whereby inputs from radars, infrared sensors, video cameras, and even humans are combined to give better target identification and tracking than any could individually. The Rapier air defense missile, for example, uses radar to acquire ***azimuth*** while tracking is carried out optically in visual ***conditions***. Data fusion can be harder than it seems. Combining two alarm systems will generally result in improving either the false alarm or the missed alarm rate, while making the other worse. If you ***scramble*** your fighters when you see

a ***blip*** on either the radar or the infrared, there will be more false alarms; but if you scramble only when you see both, it will be easier for the enemy to jam you or to ***sneak through***.
System issues become more complex where the attacker himself is on a platform that's vulnerable to counterattack, such as a fighter bomber. He will have systems for threat recognition, direction finding, and missile approach warning; and the receivers in these will be deafened by his jammer. The usual trick is to turn the jammer off for a short "look-through" period at random times.
With multiple friendly and hostile platforms, things get much more complex still. Each side might have specialist support vehicles with high-power dedicated equipment, which makes it to some extent an energy battle—"he with the most watts wins." A SAM ***belt*** may have multiple radars at different frequencies to make jamming harder. The overall effect of jamming (as of stealth) is to reduce the effective range of radar. But the jamming ***margin*** also matters, and who has the most vehicles, and the tactics employed.
With multiple vehicles engaged, it's also necessary to have a reliable way of distinguishing friend from foe.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns, Adjectives and Verbs:

Infrared, decoy, heat-seeking missiles, spun, flare, chaff, decelerate, multisensor data fusion, azimuth, conditions, scramble, blip, scramble, sneak through, belt, margin.

2. Complete the next sentences with the corresponded endings from the right column:

1. Passive flares worked very well against early heat-seeking missiles that used a mechanically spun detector, …

2. Flares are also like repeater jammers in that …

3. It tends to exploit features of the hostile sensor by pulsing at a rate or in a pattern …

4. ..., there will be more false alarms.

5. …, which makes it to some extent an energy battle.

---

a) their signals are relatively stable and strong compared with real targets.

b) that causes confusion.

c) but are less effective against modern detectors that incorporate signal processing.

d) if you scramble your fighters when you see a blip on either the radar or the infrared…

e) each side might have specialist support vehicles with high-power dedicated equipment…

3. Fill in the blanks choosing one of the offered variants:

One growth area is … (*multisensor, sensor, insensor*) data fusion, whereby inputs from radars, infrared sensors, video cameras, and even humans are combined to give better target identification and tracking than any could individually. The Rapier air defense … (*missile, rocket, jet-propelled projectile*) for example, uses radar to acquire azimuth while tracking is carried out optically in visual conditions. Data … (*fusion, confluence, alloy*) can be harder than it seems. Combining two … (*alarm, alert, trouble*) systems will generally result in improving either the false alarm or the missed alarm rate, while making the other worse. If you … (*scramble, bout, struggle*) your fighters when you see a blip on either the radar or the infrared, there will be more false alarms; but if you scramble only when you see both, it will be easier for the enemy to jam you or … (*to sneak, slink, scrounge*) through.

TEXT 16.

IFF Systems

The technological innovations of World War II—and especially jet aircraft, radar, and missiles—made it impractical to identify targets visually, and ***imperative*** to have an automatic way to ***identify friend or foe*** (IFF). Early IFF systems ***emerge***d during that war, using a vehicle serial number or "code of the day"; but this is open to ***spoof***ing. Since the 1960s, U.S. aircraft have used the Mark XII system, which has cryptographic protection as discussed in Section 2.3. Here, it isn't the cryptography that's the hard part, but rather the protocol and operational problems.

The Mark XII has four ***mode***s, of which the secure mode uses a 32-bit challenge and a 4-bit response. This is a precedent set by its predecessor, the Mark X; if ***challenge***s or responses were too long, the radar's pulse repetition frequency (and thus it ***accuracy***) would be degraded. The Mark XII sends a series of 12–20 challenges at a rate of one every four milliseconds. In the original ***implementation***, the responses were displayed on a screen at a position offset by the arithmetic difference between the actual response and the expected one. The effect was that while a foe had a null or random response, a friend would have responses at or near the center screen, which would light up. Reflection attacks are prevented, and MIG-in-the-middle attacks made much harder, because the challenge uses a focused antenna, while the receiver is ***omnidirectional***. (In fact, the antenna used for the challenge is typically the fire control radar, which in older systems was conically scanned).

I mentioned in Section 2.3 that cryptographic protection alone isn't ***bulletproof***: the enemy might record and replay valid challenges, with a view to using your IFF signal for direction finding purposes. This can be a real problem in dense operational areas with many vehicles and emitters, such as on the border between East and West Germany during the Cold War, and parts of the Middle East to this day. There, the return signal can be degraded by overlapping signals from nearby aircraft—an effect known as ***garbling***. In the other direction, aircraft transponders subjected to many challenges may be unable to decode them properly—an effect known as ***fruiting***. Controlling these phenomena means minimizing the length of challenge and response signals, which limits the usefulness of cryptographic protection. As a result, the Royal Air Force resisted American demands to make the Mark XII a NATO requirement and continues using the

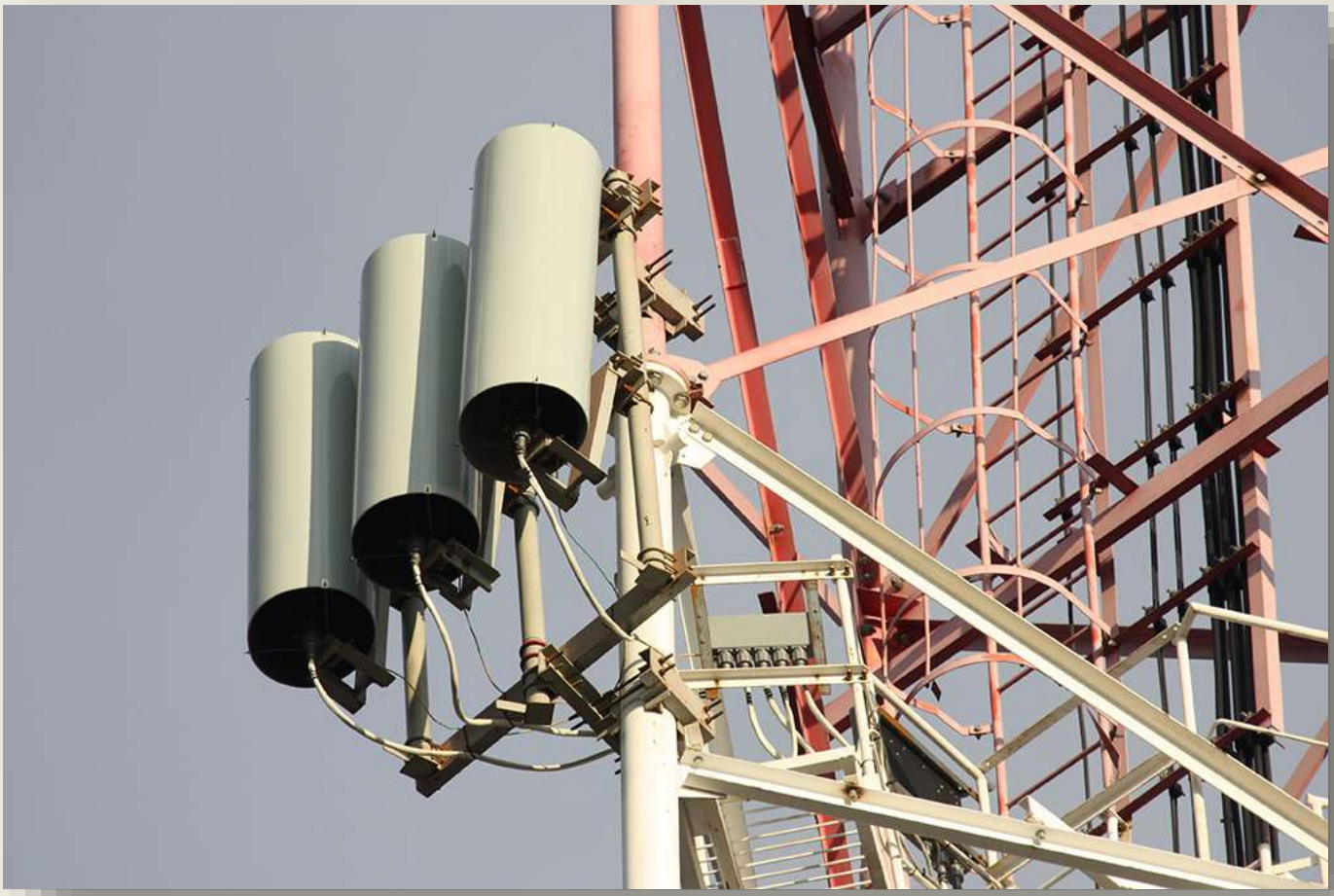
World-War-II-vintage Mark X, changing the codes every 30 minutes. (The details of Mark X and Mark XII, and the R.A.F.-U.S.A.F. debate, can be found in. This is yet another example of the surprising difficulty of getting cryptography to add value to a system design.
The system-level issues are even less tractable. The requirement is to identify enemy forces, but an IFF system ***reliant*** on cooperation from the target can only identify friends positively. Neither neutrals, nor friends with defective or incorrectly set transponders, can be ***distinguish***ed from enemies. So while IFF may be used as a primary mechanism in areas where neutrals are excluded (such as in the ***vicinity*** of naval task forces at sea in wartime), its more usual use is as an adjunct to more traditional methods, such as correlation with flight plans. In this role it can still be very valuable.
Since the Gulf war, in which 25% of Allied troop ***casualties*** were caused by "friendly fire", a number of experimental systems have been developed that extend IFF to ground troops. One U.S. system combines laser and RF components. Shooters have lasers, and soldiers have transponders; when the soldier is illuminated with a suitable challenge, his equipment broadcasts a "don't shoot me" message using frequency- hopping radio. An extension allows aircraft to broadcast targeting intentions on millimeter wave radio. This system was due to be fielded in the year 2000. Britain is developing a cheaper system called ***MAGPIE***, in which friendly vehicles carry a low- probability-of-intercept millimeter wave transmitter, and shooters ***carry*** a directional receiver. (Dismounted British foot soldiers, unlike their American counterparts, have no protection.) Other countries are developing yet other systems.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns and Verbs:

Imperative, identify friend or foe, emerge, spoof, mode, challenge, accuracy, implementation, omnidirectional, bulletproof, garbling, fruiting, reliant, distinguish, casualties, MAGPIE, carry.

2. Translate the next sentences and define their conformity and discrepancy to the text content:
Since the 1960s, U.S. aircraft *have used* the Mark XII system, which has cryptographic protection as *discussed* in Section 2.3. Here, it isn't the cryptography that's the hard part, but rather the protocol and operational problems.
The Mark XII has four modes, of which the secure mode uses a 32-bit challenge and a 4-bit response. This is a precedent set by its predecessor, the Mark X; if challenges or responses were too long, the radar's pulse repetition frequency (and thus it accuracy) *would be degrading*. The Mark XII sends a series of 12–20 challenges at a rate of one every four milliseconds. In the original implementation, the responses *were displaying* on a screen at a position offset by the arithmetic difference between the actual response and the expected one. The effect was that while a foe had a null or random response, a friend *would have* responses at or near the center screen, which *would lighting* up. Reflection attacks *are prevented*, and MIG-in-the-middle attacks made much harder, because the challenge uses a focused antenna, while the receiver is omnidirectional. (In fact, the antenna used for the challenge is typically the fire control radar, which in older systems *was* conically *be scanning*).



3. Find the English equivalents to the Russian lexis in the text:

Технические нововведения; реактивный самолёт; сделать непрактичным для визуального обнаружения цели; идентифицировать друга или врага; быть открытым для подмен; иметь шифровальную защиту; отображённые на экране ответы в смещённом положении; тогда как приёмник всенаправлен; шифровальная защита не является пуленепробиваемой; для пеленгационных целей; отражённый сигнал может быть подавлен перекрывающими сигналами; может оказаться не в состоянии расшифровать их правильно; положительно распознавать друзей; у стрелков имеются лазеры, у солдат – транспондеры; солдаты подсвечиваются соответствующим сообщением, что их оборудования транслируют "не стреляйте в меня", используя радио скачкового распространения радиоволн.

TEXT 17.

Directed Energy Weapons

In the late 1930s, there was panic in Britain and America on ***rumors*** that the Nazis had developed ***a high-power radio beam*** that would burn out vehicle ignition systems. British scientists studied the problem and concluded that this was ***infeasible***. They were correct—given the relatively low-powered radio transmitters, and the simple but ***robust*** vehicle electronics, of the 1930s.

Things started to change with the arrival of the atomic bomb. The detonation of a nuclear device creates a large pulse of gamma-ray photons, which in turn displace electrons from air molecules

by *Compton scattering*. The large induced currents give rise to ***an electromagnetic pulse*** (EMP), which may be thought of as a very high amplitude pulse of radio waves with a very short rise time.

Where ***a nuclear explosion*** occurs within the earth's atmosphere, the EMP energy is predominantly in the VHF and UHF bands, though there is enough energy at lower frequencies for a *radio flash* to be observable thousands of miles away. Within a few tens of miles of the explosion, the radio frequency energy may ***induce*** currents large enough to damage most electronic equipment that has not been hardened. The effects of ***a blast*** outside the earth's atmosphere are believed to be much worse (although there has never been a test). The gamma photons can travel thousands of miles before they strike the earth's atmosphere, which could ionize to form an antenna on a continental scale. It is ***reckon***ed that most electronic equipment in Northern Europe could be burned out by a one megaton blast at a height of 250 miles above the North Sea. For this reason, critical military systems are carefully shielded.

Western concern about EMP grew after the Soviet Union started a research program on non-nuclear EMP weapons in the mid-80s. At the time, the United States was ***deploy***ing "neutron bombs" in Europe—***enhanced radiation*** weapons that could kill people without ***demolish***ing buildings. The Soviets portrayed this as a "capitalist bomb" which would destroy people while leaving property intact, and responded by threatening a "socialist bomb" to destroy property (in the form of electronics) while leaving the surrounding people intact.

By the end of World War II, the invention of the ***cavity*** magnetron had made it possible to build radars powerful enough to damage unprotected electronic circuitry for a range of several hundred yards. The move from valves to transistors and integrated circuits has increased the vulnerability of most commercial electronic equipment. A terrorist group could in theory mount a radar in a truck and drive around a city's financial sector wiping out the banks. For battlefield use, a more compact form factor is preferred, and so the Soviets are said to have built high-energy RF (HERF) devices from capacitors, magneto hydrodynamic generators and the like.

By the mid-1990s, the concern that terrorists might get hold of these weapons from the former Soviet Union led the agencies to try to sell commerce and industry on the idea of electromagnetic shielding. These efforts were dismissed as ***hype***. Personally, I tend to agree. The details of the Soviet HERF bombs haven't been released, but physics suggests that EMP is limited by the dielectric strength of air and the ***cross-section*** of the antenna. In nuclear EMP, the effective antenna size could be a few hundred meters for an end atmospheric blast, up to several thousand kilometers for an ***exoatmospheric*** one. But in "ordinary" EMP/HERF, it seems that the antenna will be at most a few meters. NATO planners concluded that military command and control systems that were already hardened for nuclear EMP should be unaffected.

As for the civilian infrastructure, I suspect that a terrorist can do a lot more damage with an old-fashioned truck bomb made with a ton of ***fertilizer*** and fuel oil, and he doesn't need a PhD in physics to design one! Anyway, the standard reference on EMP is.

Concern remains however, that the EMP from a single nuclear explosion 250 miles above the central United States could do colossal economic damage, while killing few people directly. This potentially gives a blackmail weapon to countries such as Iran and North Korea, both of which have nuclear ambitions but primitive infrastructures. In general, a massive attack on electronic communications is more of a threat to countries such as the United States that depend heavily on

them than on countries such as North Korea, or even China, that don't. This observation goes across to attacks on the Internet as well, so let's now turn to information warfare.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Adjectives and Word Combinations and Verbs:

Rumors, a high-power radio beam, infeasible, an robust, electromagnetic pulse, a nuclear explosion, induce, a blast, reckon, enhanced radiation, deploy, demolish, cavity, hype, cross-section, exoatmospheric, fertilizer.

2. Find the second part of the sentence according the point of the text:

1. In the late 1930s, there was panic in Britain and America on rumors that the Nazis had developed a high-power radio beam...
2. The detonation of a nuclear device creates a large pulse of gamma-ray photons, …
3. The large induced currents give rise to an electromagnetic pulse (EMP), …
4. … that has not been hardened.
5. … , which could ionize to form an antenna on a continental scale.

_____

a) which may be thought of as a very high amplitude pulse of radio waves with a very short rise time.

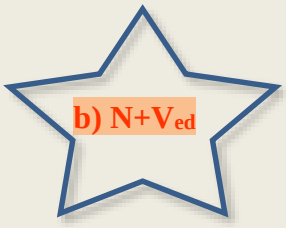
b) which in turn displace electrons from air molecules by Compton scattering.

c) within a few tens of miles of the explosion, the radio frequency energy may ***induce*** currents large enough to damage most electronic equipment…

d) that would burn out vehicle ignition systems. British scientists studied the problem and concluded that this was infeasible.

e) the gamma photons can travel thousands of miles before they strike the earth's atmosphere

3. Translate the word combinations built by the next models:



A high-power radio beam developed by the Nazis, given the relatively low-powered radio transmitters they were correct, started to change things, the large induced currents, has not been hardened electronic equipment, displaced electrons from air molecules by Compton scattering, may be thought of an electromagnetic pulse as a very high amplitude pulse of radio waves with a very short rise time, carefully shielded critical military systems, enhanced radiation weapons, hype dismissed these efforts, bomb made with a ton of fertilizer.

TEXT 18.

Information Warfare

Since about 1995, the phrase ***information warfare*** has come into wide use. Its popularity appears to have been catalyzed by operational experience in Desert Storm. There, air power was used to ***degrade*** the Iraqi defenses before the land attack was launched; and one ***goal*** of NSA personnel supporting the ***allies*** was to enable the initial attack to be made without ***casualties***—even though the Iraqi air defenses were at that time intact and alert. The attack involved a mixture of standard e-war techniques, such as jammers and ***antiradiation missiles***; cruise missile attacks on command centers; attacks by special forces, who sneaked into Iraq and dug up lengths of communications cabling from the desert; and, ***allegedly***, the use of hacking tricks to disable computers and telephone exchanges. (By 1990, the U.S. Army was already calling for bids for virus production.) The operation successfully achieved its mission of ensuring zero Allied casualties on the first night of the ***aerial bombardment***. Military planners and think tanks started to consider how the success could be extended.

There is little agreement about definitions. The conventional view, arising out of Desert Storm, was expressed by Major Yu Lin Whitehead:

*The strategist . . . should employ [the **information weapon**] as a **precursor weapon** to blind the enemy prior to conventional attacks and operations.*

The more aggressive view is that properly conducted information operations should ***encompass*** everything from signals intelligence to propaganda; and, given the ***reliance*** that modern societies place on information, it should ***suffice*** to break the enemy's will without fighting.

Definitions

In fact, there are ***roughly*** three views on what information warfare means:

- It is just a remarketing of the stuff that the agencies have been doing for decades anyway, in an attempt to maintain the agencies' budgets post-Cold-War.
- It consists of the use of hacking ***in a broad sense***—network attack tools, computer viruses, and so on—in conflict between states or substate groups, in order to deny critical military and other services, whether for operational or propaganda purposes. It has been observed, for example, that the Internet, though designed ***to withstand thermonuclear bombardment***, was knocked out by the Morris worm.
- It extends the electronic warfare doctrine of controlling the electromagnetic spectrum to control of all information relevant to the conflict. It thus extends traditional e-war techniques, such as radar jammers, by adding assorted hacking techniques, but also incorporates propaganda and news management.

The first of these views was the one taken by some ***cynical*** defense insiders to whom I've spoken. The second is the popular view found in newspaper articles, and also Whitehead's. It's the one I'll use as a guide in this section, but without taking a position on whether it actually contains anything really new, either technically or doctrinally.

The third finds expression in a book by Dorothy Denning, whose definition of information warfare is, "operations that target or ***exploit*** information media in order to win some advantage over an ***adversary***." Its interpretation is so broad that it includes not just hacking but all of electronic warfare and all existing ***intelligence-gathering*** techniques (from ***sigint*** through satellite imagery to spies), and propaganda, too. In a later article, she's discussed the role of the Net in the propaganda and activism surrounding the Kosovo war. However the ***bulk*** of her book is given over to computer security and ***related*** topics.

A similar view of information warfare, and from a writer whose background is defense planning rather than computer security, is by Edward Waltz. He defines ***information superiority*** as "the capability to collect, process and ***disseminate an uninterrupted flow of information*** while exploiting or denying an adversary's ability to do the same". The theory is that such superiority will allow the conduct of operations without effective opposition. The book has less technical detail on computer security matters than Denning's, but sets forth a first attempt to formulate a military doctrine of information operations.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns, Adjectives and Verbs:

Information warfare, degrade, goal, allies, casualties, antiradiation missiles, allegedly, aerial bombardment, information weapon, precursor weapon, encompass, reliance, suffice, roughly, in a broad sense, to withstand thermonuclear bombardment, cynical, exploit, adversary, intelligence-gathering, sigint, bulk, related, information superiority, disseminate an uninterrupted flow of information.

2. Find in the text the word combinations with the given words and translate them. Give the words with the opposite meaning:

Popularity, attack, a mixture, dig up, ensuring, bids, conventional, stuff, relevant, view, propaganda, denying, detail.

3. Insert the appropriate to the point of the sentence conjunction into the sentences:

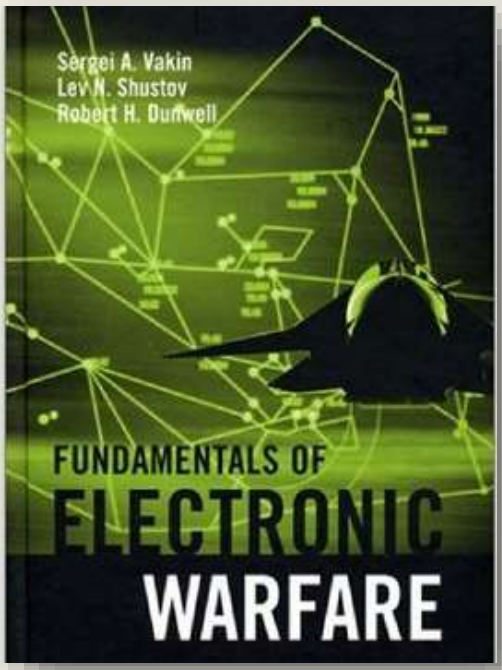
1. Air power was used to degrade the Iraqi defenses … the land attack was launched. (what, that, if, before)
2. The attack involved a mixture of standard e-war techniques, such as jammers and antiradiation missiles; attacks by special forces, … sneaked into Iraq and dug up lengths of communications cabling from the desert. (how, who, whether)
3. It consists of the use of hacking in a broad sense—network attack tools, computer viruses, and so on—in conflict between states or substate groups, … deny critical military and

other services, … for operational or propaganda purposes. (in order to, that, while; which, after, whether)

4. It thus extends traditional e-war techniques, such as radar jammers, by adding assorted hacking techniques, … also incorporates propaganda and news management. (because, what, that's why, but)
5. The third finds expression in a book by Dorothy Denning, … definition of information warfare is, "operations … target or exploit information media in order to win some advantage over an adversary." (whose, that, which; while, that, if)

TEXT 19.

Doctrine



When writers such as Denning and Waltz include propaganda operations in information warfare, the cynical defense insider may remark that nothing has changed. From Roman and Mongol efforts to promote a ***myth of invincibility***, through the use of propaganda radio stations by both sides in World War II and the Cold War, to the bombing of Serbian TV during the Kosovo campaign and ***denial-of-service*** attacks on Chechen Web sites by Russian agencies—the tools may change but the game remains the same.

But there is a ***twist***, perhaps thanks to government and military leaders' lack of ***familiarity*** with the Internet. When teenage kids deface a U.S. government department Web site, an experienced computer security professional is likely to see it as the equivalent of graffiti ***scrawl***ed on the wall of a public building. After all, it's easy enough to do, and easy enough to remove. But the information warfare community can ***paint*** it as ***undermining*** the ***posture*** of information ***dominance*** that a country must project in order to ***deter*** aggression.

So there is a fair amount of debunking to be done before the political and military leadership can start to think clearly about the ***issues***. For example, it's often stated that information warfare provides casualty-free way to win wars: "just hack the Iranian power ***grid*** and watch them sue for peace."

The three obvious comments are as follows:

- The denial-of-service attacks that have so far been conducted on information systems without the use of physical force have mostly had a ***transient effect***. A computer goes down; the operators find out what happened; they ***restore*** the system from backup and restart it. An ***outage*** of a few hours may be enough to let a wave of bombers get through unscathed, but it appears unlikely to bring a country to its knees. In this context, the failure of the Millennium Bug to cause the expected damage may be a useful warning.

- ***Insofar*** as there is a ***vulnerability***, developed countries are more ***expose***d. The power grid in the United States or Britain is much more computerized than that in the ***average*** developing country.

- Finally, if such an attack causes the deaths of several dozen people in Iranian hospitals, the Iranians aren't likely to see the matter much differently from a conventional military attack that killed the same number of people. Indeed, if information war targets ***civilians*** to greater extent than the alternatives, then the attackers' leaders are likely to be portrayed as ***war criminals***. The Pinochet case, in which a former head of government only escaped extradition on health grounds, should give ***pause*** for thought. Having made these points, I will ***restrict*** discussion in the rest of this section to technical matters.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns, Adjectives and Word Combinations:

Myth of invincibility, denial-of-service, twist, familiarity, scrawl, paint, undermining, posture, dominance, deter, issues, grid, transient effect, restore, outage, insofar, vulnerability, expose, average, civilians, war criminals, pause, restrict.

2. Translate the given sentences into Russian language:

1. From Roman and Mongol efforts to promote a myth of invincibility, through the use of propaganda radio stations by both sides in World War II and the Cold War, to the bombing of Serbian TV during the Kosovo campaign and denial-of-service attacks on Chechen Web sites by Russian agencies—the tools may change but the game remains the same.

2. When teenage kids deface a U.S. government department Web site, an experienced computer security professional is likely to see it as the equivalent of graffiti scrawled on the wall of a public building. After all, it's easy enough to do, and easy enough to remove. But the information warfare community can paint it as undermining the posture of information dominance that a country must project in order to deter aggression.

3. So there is a fair amount of debunking to be done before the political and military leadership can start to think clearly about the issues. For example, it's often stated that information warfare provides casualty-free way to win wars: "just hack the Iranian power grid and watch them sue for peace."

3. Finish the next sentences choosing the appropriate word combinations from the underneath list:

1. A computer goes down; the operators find out what happened; they restore _____ and restart it. An outage of a few hours may be _____ get through unscathed, but it appears unlikely _____ .
2. _____ in the United States or Britain is much more computerized than that in the _____.
3. If such an attack causes the deaths of _____ in Iranian hospitals, the Iranians aren't

likely to see the matter much differently from _____ that killed the same number of people.

4. If _____ targets civilians to greater extent than the alternatives, then the attackers' leaders are likely to be portrayed as _____ .

---

1. The power grid; average developing country; **2.** the system from backup; enough to let a wave of bombers; to bring a country to its knees; **3.** information war; war criminals **4.** several dozen people; a conventional military attack

TEXT 20. Potentially Useful Lessons from Electronic Warfare

Perhaps the most important policy lesson from the world of electronic warfare is that conducting operations that involve more than one service is very much harder than it looks. Things are bad enough when army, navy, and air force units have to be coordinated—during the U.S. ***invasion*** of Grenada, a ground commander had to go to a pay phone and call home using his credit card in order ***to call down an air strike***, as the different services' radios were incompatible. (Indeed, this was the ***spur*** for the development of software radios). Things are even worse when intelligence services are involved, as they don't train with warfighters in peacetime, and so take a long time to become productive once the fighting starts. ***Turf*** fights also get in the way: under current U.S. rules, the air force can decide to bomb an enemy telephone exchange but has to get permission from the NSA and/or CIA to hack it. The U.S. Army's communications strategy is now taking account of the need to communicate across the traditional command ***hierarchy***, and to make extensive use of the existing civilian infrastructure.

At the technical level, many *concepts* may go across from electronic warfare to information protection in general.

- The electronic warfare community uses guard band receivers to detect jamming, so it can be filtered out (for example, by blanking receivers at the precise time a sweep jammer passes through their frequency). Using ***bait addresses*** to detect spam is essentially the same concept.
- There is also an analogy between virus ***recognition*** and radar signal recognition. Virus writers may make their code ***polymorphic***, in that it changes its form as it ***propagate***s, to make life harder for the virus scanner vendors. Similarly, radar designers use very diverse ***waveforms*** to make it harder to store enough of the waveform in digital radio frequency memory to do ***coherent*** jamming effectively.

- Our old friends, the false accept and false reject rate, will continue to dominate tactics and strategy. As with ***burglar*** alarms or radar jamming, the ability to cause many false alarms (however crudely) will always be worth something: as soon as the false alarm rate ***exceed***s about 15%, operator performance is degraded. As for filtering, it can usually be ***cheat***ed.

- The limiting economic factor in both attack and defense will increasingly be the software cost, and the speed at which new tools can be created and deployed.

It is useful, when subjected to jamming, not to let the jammer know whether, or how, his attack is succeeding. In military communications, it's usually better to respond to jamming by dropping the bit rate rather than by boosting power; similarly, when a nonexistent credit card number is presented at your Web site, you might say, "Sorry, bad card number, try again," but the second time it happens you should take a different line (or the attacker will keep on trying). Something such as, "Sorry, the items you have requested are temporarily out of stock and should be mailed within five working days" may do the trick.

- Although defense in ***depth*** is in general a good idea, you have to be careful of interactions between the different defenses. The classic case in e-war is when ***chaff*** dispensed by a warship to defend against an incoming cruise missile knocks out its anti-aircraft guns. The side effects of defenses can also be exploited. The most common case on the Net is the mail bomb: an attacker forges offensive newsgroup messages, which appear to come from the victim, who then gets subjected to a ***barrage of abuse*** and attacks.

- Finally, some perspective can be drawn from the differing roles of hard kill and soft kill in electronic warfare. Jamming and other ***soft-kill attacks*** can be cheaper in the short term; they can be used against multiple threats; and they have reduced political consequences. But damage assessment is hard, and you may just ***divert*** the weapon to another target. As most i-war is soft kill, these comments can be expected to go across, too.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns, Verbs and Word Combinations:

Invasion, call down an air strike, turf, hierarchy, concepts, bait addresses, recognition, propagate, polymorphic, waveforms, coherent, burglar, exceed, cheat, depth, chaff, barrage of abuse, soft-kill attacks, divert.

2. Finish the sentences:

1. The electronic warfare community uses guard band receivers … .
2. Virus writers may make their code polymorphic, in that it changes its form as it propagates, … .
3. The limiting economic factor in both attack and defense will increasingly be the software cost, and the speed at which new tools ... .
4. The classic case in e-war is when chaff dispensed by a warship to defend against an incoming cruise missile … .
5. The most common case on the Net is the mail bomb: an attacker forges offensive newsgroup messages, which appear to come from the victim, who then … .
6. Damage assessment is hard, and you may just … .

---

1. to make life harder for the virus scanner vendors; **2.** can be created and deployed; **3.** to detect jamming, so it can be filtered out; **4.** gets subjected to a barrage of abuse and attacks.

5. divert the weapon to another target; **6.** knocks out its anti-aircraft guns.

3. Translate the next word combinations finding one of the given Grammar models:

V+Adv | **V+N+Adv**

1. … to do coherent jamming effectively. **2.** … is very much harder than it looks. **3.** … take a long time to become productive once the fighting starts. **4. …** warfare community uses guard band receivers not effectively. **5.** … radar designers use very diverse waveforms to make it harder to store waveform. **6.** … bait addresses is essentially the same concept. **7.** … the ability to cause many false alarms however crudely will always be worth something.

TEXT 21.

Differences Between E-War and I-War

There are differences as well as similarities between traditional electronic warfare and the kinds of attack that can potentially be run over the Net.

- There are roughly two kinds of war: open war and ***guerilla*** war. Electronic warfare comes into its own in the former case, such as in air combat, most naval engagements, and the desert. In forests and mountains, the man with the AK-47 can still get a result against mechanized forces. Guerilla war has largely been ignored by the e-war community, except insofar as they make and sell radars to detect ***snipers*** and ***conceal***ed ***mortar batteries***.

In cyberspace, the "forests and the mountains" are likely to be the large numbers of insecure hosts belonging to friendly or neutral civilians and organizations. The distributed denial-of-service (DDoS) attack, in which hundreds of ***innocent*** machines are subverted and used to ***bombard*** a target Web site with traffic, has no real analogue in the world of electronic warfare. Nevertheless, it is the likely platform for launching attacks even on "open" targets such as large commercial Web sites. So it's unclear where the open countryside in cyberspace actually is.

- Another possible source of asymmetric advantage for the guerilla is ***complexity***. Large countries have many incompatible systems; this makes little difference when fighting another large country with similarly ***incompatible*** systems, but can leave them at a disadvantage to a small group that has built simple, coherent systems.
- Anyone trying to attack the United States is unlikely to repeat Saddam Hussein's mistake of trying to fight a tank ***battle***. Guerilla warfare will be the norm, and cyberspace appears to be fairly well suited for this.

- There is no electronic warfare ***analogue*** of "script kiddies," people who download attack scripts and launch them without really understanding how they work. That such powerful weapons are available universally, and for free, has few analogues in ***meat*** space. Perhaps the closest is in the lawless areas of countries such as Afghanistan, where all men go about with military weapons.

Summary

Electronic warfare is much more developed than most other areas of information security. There are many lessons to be learned, from the technical level up through the tactical level to matters of planning and strategy. We can expect that, as information warfare ***evolve***s from a fashionable concept to ***establish***ed doctrine, these lessons will become important for ***practitioner***s.

Research Problems

An interesting research problem is how to port techniques and experience from the world of electronic warfare to the Internet. This chapter is only a ***sketchy*** first attempt at setting down the possible parallels and differences.

Language Study

1. Study the next words and word combinations. Divide all words into four columns as Nouns, Adjectives, Verbs or Word Combinations (W/C). Translate only Nouns, Verbs and Word Combinations:

Guerilla, snipers, conceal, mortar batteries, complexity, incompatible, battle, analogue, meat, evolve, establish, practitioner, sketchy.

2. What sentences don't correspond to the point of the text?

1. In forests and mountains, the man with the KA-47 can still get a result against mechanized forces.
2. In cyberspace, the "woods and the mountains" are likely to be the small numbers of insecure hosts belonging to friendly or neutral civilians and organizations.
3. It is the likely platform for launching attacks even on "open" targets such as large commercial Web sites. So it's unclear where the open countryside in cyberspace actually is.
4. Guerilla warfare will be the norm, and cyberspace appears to be fairly well suited for this.
5. Electronic warfare is much more developed than most other areas of cyberspace security. There are many countries to be learned, from the technical level up through the tactical level to matters of planning and launching attacks.

3. Try to guess the words in the word combinations:

A_r co_bat, na_al engage_ents, me_anized fo_ces, n_tral civil_ns, a tar_et W_b s_te, "s_ript ki_dies", in_ompatible s_stems, elec_onic wa_are, ske_hy at_empt, po_erful w_pons

APPENDIX

THEORETIC DATA

Electronic warfare (**EW**) is any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or impede enemy assaults via the spectrum. The purpose of electronic warfare is to deny the opponent the advantage of, and ensure friendly unimpeded access to, the EM spectrum. EW can be applied from air, sea, land, and space by manned and unmanned systems, and can target humans, communications, radar, or other assets.

The electromagnetic environment

Military operations are executed in an information environment increasingly complicated by the electromagnetic (EM) spectrum. The electromagnetic spectrum portion of the information environment is referred to as the electromagnetic environment (EME). The recognized need for military forces to have unimpeded access to and use of the electromagnetic environment creates vulnerabilities and opportunities for electronic warfare (EW) in support of military operations. Within the information operations construct, EW is an element of information warfare; more specifically, it is an element of offensive and defensive counter information.

Electronic warfare applications

Electronic warfare is any military action involving the use of the EM spectrum to include directed energy (DE) to control the EM spectrum or to attack an enemy. This is not limited to radio or radar frequencies but includes IR, visible, ultraviolet, and other less used portions of the EM spectrum. This includes self-protection, standoff, and escort jamming, and antiradiation attacks. EW is a specialized tool that enhances many air and space functions at multiple levels of conflict. The purpose of EW is to deny the opponent an advantage in the EM spectrum and ensure friendly unimpeded access to the EM spectrum portion of the information environment. EW can be applied from air, sea, land, and space by manned and unmanned systems. EW is employed to support military operations involving various levels of detection, denial, deception, disruption, degradation, protection, and destruction. EW contributes to the success of information operations (IO) by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum. Expanding reliance on the EM spectrum increases both the potential and the challenges of EW in information operations. All of the core, supporting, and related information operations capabilities either directly use EW or indirectly benefit from EW. The principal EW activities have been developed over time to exploit the opportunities and vulnerabilities that are inherent in the physics of EM energy. Activities used in EW include: electro-optical, infrared and radio frequency countermeasures; EM compatibility and deception; communications jamming, radar jamming and anti-jamming; electronic masking, probing, reconnaissance, and intelligence; electronics security; EW reprogramming; emission control; spectrum management; and wartime reserve modes.

Subdivisions

Electronic warfare includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

Electronic attack (EA)

Electronic attack (EA) (previously known as Electronic Counter Measures (ECM)) involves the use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. In the case of EM energy, this action is referred to as jamming and can be performed on communications systems (see Radio jamming) or radar systems (see Radar jamming and deception).

Electronic Protection (EP)

Electronic Protection (EP) (previously known as electronic protective measures (EPM) or electronic counter countermeasures (ECCM)) involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Jamming is not part of EP, it is an EA measure.

The use of flare rejection logic on an Infrared homing missile to counter an adversary's use of flares is EP. While defensive EA actions and EP both protect personnel, facilities, capabilities, and equipment, EP protects from the *effects* of EA (friendly and/or adversary). Other examples of EP include spread spectrum technologies, use of Joint Restricted Frequency List (JRFL), emissions control (EMCON), and low observability or "stealth". An Electronic Warfare Self Protection (EWSP) is a suite of countermeasure systems fitted primarily to aircraft for the purpose of protecting the aircraft from weapons fire and can include among others: DIRCM (protects against IR missiles), Infrared countermeasures (protects against IR missiles), Chaff (protects against RADAR guided missiles), DRFM Decoys (Protects against Radar guided missiles), Flare(protects against IR missiles).

An Electronic Warfare Tactics Range (EWTR) is a practice range which provides for the training of aircrew in electronic warfare. There are two such ranges in Europe; one at RAF Spade Adam in the United Kingdom and the POLYGON range in Germany and France. EWTRs are equipped with ground-based equipment to simulate electronic warfare threats that aircrew might encounter on missions.

Antifragile EW is a step beyond standard EP, occurring when a communications link being jammed actually increases in capability as a result of a jamming attack, although this is only possible under certain circumstances such as reactive forms of jamming.

Electronic warfare support (ES)

Electronic Warfare Support (ES), is the subdivision of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic (EM) energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. These measures begin with systems designed and operators trained to make Electronic Intercepts (ELINT) and then classification and analysis broadly known as Signals intelligence from such detection to return information and perhaps actionable intelligence (e.g. a ship's identification from unique characteristics of a specific radar) to the commander.

The overlapping discipline, signals intelligence (SIGINT) is the related process of analyzing and identifying the intercepted frequencies (e.g. as a mobile phone or radar). SIGINT is broken into three categories: ELINT, COMINT, and FISINT. The parameters of intercepted are: communication equipment-: frequency, bandwidth, modulation, polarization etc. The distinction between intelligence and electronic warfare support (ES) is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. Electronic warfare support is achieved by assets tasked or controlled by an operational commander. The purpose of ES tasking is immediate threat recognition, targeting, planning and conduct of future operations, and other tactical actions such as threat avoidance and homing. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements. Where these activities are under the control of an operational commander and being applied for the purpose of situational awareness, threat recognition, or EM targeting, they also serve the purpose of Electronic Warfare surveillance (ES).

Borisoglebsk 2

Multifunctional EW system

In February 2015 the Russian army received their first set of the multifunctional electronic warfare system, known as Borisoglebsk 2.

A Russian blog describes Borisoglebsk 2 as "*The 'Borisoglebsk-2' when compared to its predecessors has better technical characteristics: wider frequency bandwidth for conducting radar collection and jamming, faster scanning times of the frequency spectrum, and higher precision when identifying the location and source of radar emissions, and increased capacity for suppression."*

Borisoglebsk 2 is a Russian, MT-LB ground vehicle mounted, multi-functional electronic warfare (EW) weapon system. It was developed by Sozvezdie over a six year period, beginning in 2004. Starting in February 2015, it has been manufactured and delivered by UIMC to the Russian armed forces. It is designed to disrupt communications and GPS systems. *Borisoglebsk 2* achieved initial operating capability in 2010, but was not ordered and delivered to Russian military until February 2015. Rossiyskaya Gazeta reported that Borisoglebsk 2 was the core system for electronic warfare in the Russian Army, controlling four types of jamming units from a single point. Experimentation and testing were conducted after the first deliveries to the Russian armed forces. It has been claimed that the system has caused difficulties for NATO, supposedly defeating GPS and mobile telephony systems in parts of that country. The United States military commander in Europe, general Frederick Hodges stated to Defense News, that Russia is conducting electronic warfare in eastern Ukraine that even NATO would have difficulties to resist, but did not mention Borisoglebsk 2. US advisers sent to Ukraine have learned about Russian electronic warfare from the Ukrainian Army, though Ukraine never has had access to this new EW-technology. The American advisers are nevertheless impressed even with earlier Russian EW-technology in the hands of the Ukrainian Army. Svenska Dagbladet claimed that the United States and NATO are worried that the F-35 fighter aircraft may not stand up against new Russian EW systems. Borisoglebsk 2 was given as an example of a new Russian system, but not directly compared to the F-35. As of August 2015, ten sets of this system have been

delivered to the Russian armed forces with another 14 sets follow. According to Rostec, Russia plans to deploy them along the Russian borders "from Kaliningrad to Blagoveshchensk".As of October 2015, these systems are also rumored to be active in Syria.

Electronic warfare support measures

In military telecommunications, the terms **Electronic Support** (ES) or **Electronic Support Measures** (ESM) describe the division of electronic warfare involving actions taken under direct control of an operational commander to detect, intercept, identify, locate, record, and/or analyze sources of radiated electromagnetic energy for the purposes of immediate threat recognition (such as warning that fire control RADAR has locked on a combat vehicle, ship, or aircraft) or longer-term operational planning. Thus, Electronic Support provides a source of information required for decisions involving Electronic Protection (EP), Electronic Attack (EA), avoidance, targeting, and other tactical employment of forces. Electronic Support data can be used to produce signals intelligence (SIGINT), communications intelligence(COMINT) and electronics intelligence (ELINT).

Electronic support measures gather intelligence through passive "listening" to electromagnetic radiations of military interest. Electronic support measures can provide (1) initial detection or knowledge of foreign systems, (2) a library of technical and operational data on foreign systems, and (3) tactical combat information utilizing that library. ESM collection platforms can remain electronically silent and detect and analyze RADAR transmissions beyond the RADAR detection range because of the greater power of the transmittedelectromagnetic pulse with respect to a reflected echo of that pulse. United States airborne ESM receivers are designated in the AN/ALR series. Desirable characteristics for electromagnetic surveillance and collection equipment include (1) wide-spectrum or bandwidth capability because foreign frequencies are initially unknown, (2) wide dynamic range because signal strength is initially unknown, (3) narrow bandpass to discriminate the signal of interest from other electromagnetic radiation on nearby frequencies, and (4) good angle-of arrival measurement for bearings to locate the transmitter. The frequency spectrum of interest ranges from 30 MHz to 50 GHz. Multiple receivers are typically required for surveillance of the entire spectrum, but tactical receivers may be functional within a specific signal strength threshold of a smaller frequency range.

Radar warning receiver

Radar warning receiver (**RWR**) systems detect the radio emissions of radar systems. Their primary purpose is to issue a warning when a radar signal that might be a threat (such as a police speed detection radar) is detected. The warning can then be used, manually or automatically, to evade the detected threat. RWR systems can be installed in all kind of airborne, sea-based, and ground-based assets (such as aircraft, ships, automobiles, military bases). This article is focused mainly on airborne military RWR systems; for commercial police RWR systems, see radar detector.

Depending on the market the RWR system is designed for, it can be as simple as detecting the presence of energy in a specific radar band (such as police radar detectors). For more critical situations, such as military combat, RWR systems are often capable of classifying the source of the radar by the signal's strength, phase and waveform type, such as pulsed wave or continuous wave with amplitude modulation or frequency modulation (chirped). The information about the signal's strength and waveform can then be used to estimate the most probable type of threat the detected radar poses. Simpler systems are typically installed in less expensive assets like automobiles, while more sophisticated systems are installed in mission critical assets such as military aircraft.

The RWR usually has a visual display somewhere prominent in the cockpit (in some modern aircraft, in multiple locations in the cockpit) and also generates audible tones which feed into the pilot's (and perhaps RIO/co-pilot/GIB's in a multi-seat aircraft) headset. The visual display often takes the form of a circle, with symbols displaying the detected radars according to their direction relative to the current aircraft heading (i.e. a radar straight ahead displayed at the top of the circle, directly behind at the bottom, etc.). The distance from the center of the circle, depending on the type of unit, can represent the estimated distance from the generating radar, or to categorize the severity of threats to the aircraft, with tracking radars placed closer to the center than search radars. The symbol itself is related to the type of radar or the type of vehicle that carries it, often with a distinction made between ground-based radars and airborne radars. Audible tones are usually assigned to each type of threat or type of radar and are fairly distinctive. The more serious the threat, the more shrill the tone. For example, an active missile seeker might be represented by a high pitched, almost continuous trill, whereas the radar of an obsolete fighter type or SAM system might be a low pitched, intermittent buzz.

The typical airborne RWR system consists of multiple wideband antennas placed around the aircraft which receive the radar signals. The receiver periodically scans across the frequency band and determines various parameters of the received signals, like frequency, signal shape, direction of arrival, pulse repetition frequency, etc. By using these measurements, the signals are first deinterleaved to sort the mixture of incoming signals by emitter type. These data are then further sorted by threat priority and displayed.

The RWR is used for identifying, avoiding, evading or engaging threats. For example, a fighter aircraft on a combat air patrol (CAP) might notice enemy fighters on the RWR and subsequently use its own radar set to find and eventually engage the bandit. In addition, the RWR helps identify and classify threats—it's hard to tell which blips on a radar console-screen are dangerous, but since different fighter aircraft typically have different types of radar sets, once they turn them on and point them near the aircraft in question it may be able to tell, by the direction and strength of the signal, which of the blips is which type of fighter.

A non-combat aircraft, or one attempting to avoid engagements, might turn its own radar off and attempt to steer around threats detected on the RWR. Especially at high altitude (more than 30,000 feet AGL), very few threats exist that don't emit radiation. As long as the pilot is careful to check for aircraft that might try to sneak up without radar, say with the assistance of AWACS or GCI, it should be able to steer clear of SAMs, fighter aircraft and high altitude, radar-directed AAA.

SEAD and ELINT aircraft often have sensitive and sophisticated RWR equipment like the U.S. HTS (HARM targeting system) pod which is able to find and classify threats which are much further

away than those detected by a typical RWR, and may be able to overlay threat circles on a map in the aircraft's multi-function display (MFD), providing much better information for avoiding or engaging threats, and may even store information to be analyzed later or transmitted to the ground to help the commanders plan future missions.

The RWR can be an important tool for evading threats if avoidance has failed. For example, if a SAM system or enemy fighter aircraft has fired a missile (for example, a SARH-guided missile) at the aircraft, the RWR may be able to detect the change in mode that the radar must use to guide the missile and notify the pilot with much more insistent warning tones and flashing, bracketed symbols on the RWR display. The pilot then can take evasive action to break the missile lock-on or dodge the missile. The pilot may even be able to visually acquire the missile after being alerted to the possible launch. What's more, if an actively guided missile is tracking the aircraft, the pilot can use the direction and distance display of the RWR to work out which evasive maneuvers to perform to outrun or dodge the missile. For example, the rate of closure and aspect of the incoming missile may allow the pilot to determine that if they dive away from the missile, it is unlikely to catch up, or if it is closing fast, that it is time to jettison external supplies and turn toward the missile in an attempt to out-turn it. The RWR may be able to send a signal to another defensive system on board the aircraft, such as a Countermeasure Dispensing System (CMDS), which can eject countermeasures such as chaff, to aid in avoidance.

Electromagnetic interference

Electromagnetic interference (**EMI**), also called **radio-frequency interference** (**RFI**) when in the radio frequency spectrum, is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction.[1] The disturbance may degrade the performance of the circuit or even stop it from functioning. In the case of a data path, these effects can range from an increase in error rate to a total loss of the data.[2] Both man-made and natural sources generate changing electrical currents and voltages that can cause EMI: automobile ignition systems, cell phones, thunder storms, the Sun, and the Northern Lights. EMI frequently affects AM radios. It can also affect cell phones, FM radios, and televisions. EMI can be used intentionally for radio jamming, as in electronic warfare

Susceptibilities of different radio technologies

Interference tends to be more troublesome with older radio technologies such as analogue amplitude modulation, which have no way of distinguishing unwanted in-band signals from the intended signal, and the omnidirectional antennas

used with broadcast systems. Newer radio systems incorporate several improvements that enhance the selectivity. In digital radio systems, such as Wi-Fi, error-correction techniques can be used. Spread-spectrum and frequency-hopping techniques can be used with both analogue and digital signalling to improve resistance to interference. A highly directional receiver, such as a parabolic antenna or a diversity receiver, can be used to select one signal in space to the exclusion of others.

The most extreme example of digital spread-spectrum signalling to date is ultra-wideband (UWB), which proposes the use of large sections of the radio spectrum at low amplitudes to transmit high-bandwidth digital data. UWB, if used exclusively, would enable very efficient use of the spectrum, but users of non-UWB technology are not yet prepared to share the spectrum with the new system because of the interference it would cause to their receivers (the regulatory implications of UWB are discussed in the ultra-wideband article).

Radar jamming and deception

Radar jamming and deception (Electronic countermeasure) is the intentional emission of radio frequency signals to interfere with the operation of a radar by saturating its receiver with noise or false information. There are two types of radar jamming: *Mechanical* and *Electronic jamming*.

Mechanical jamming

Mechanical jamming is caused by devices which reflect or re-reflect radar energy back to the radar to produce false target returns on the operator's scope. Mechanical jamming devices include chaff, corner reflectors, and decoys.

- **Chaff** is made of different length metallic strips, which reflect different frequencies, so as to create a large area of false returns in which a real contact would be difficult to detect. Modern chaff is usually aluminum coated glass fibers of various lengths. Their extremely low weight and small size allows them to form a dense, long lasting cloud of interference.
- **Corner reflectors** have the same effect as chaff but are physically very different. Corner reflectors are multiple-sided objects that re-radiate radar energy mostly back toward its source. An aircraft cannot carry as many corner reflectors as it can chaff.
- **Decoys** are maneuverable flying objects that are intended to deceive a radar operator into believing that they are actually aircraft. They are especially dangerous because they can clutter up a radar with false targets making it easier for an attacker to get within weapons range and neutralize the radar. Corner reflectors can be fitted on decoys to make them appear larger than they are, thus furthering the illusion that a decoy is an actual aircraft. Some decoys have the capability to perform electronic jamming or drop chaff. Decoys also have a deliberately sacrificial purpose i.e. defenders may fire guided missiles at the decoys, thereby depleting limited stocks of expensive weaponry which might otherwise have been used against genuine targets.

Electronic jamming

Electronic jamming is a form of electronic warfare where jammers radiate interfering signals toward an enemy's radar, blocking the receiver with highly concentrated energy signals. The two main technique styles are noise techniques and repeater techniques. The three types of noise jamming are spot, sweep, and barrage.

- **Spot jamming** occurs when a jammer focuses all of its power on a single frequency. While this would severely degrade the ability to track on the jammed frequency, a frequency agile radar would hardly be affected because the jammer can only jam one frequency. While multiple jammers could possibly jam a range of frequencies, this would consume a great deal of resources to have any effect on a frequency-agile radar, and would probably still be ineffective.
- **Sweep jamming** is when a jammer's full power is shifted from one frequency to another. While this has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. Although, depending on the error checking in the device(s) this can render a wide range of devices effectively useless.
- **Barrage jamming** is the jamming of multiple frequencies at once by a single jammer. The advantage is that multiple frequencies can be jammed simultaneously; however, the jamming effect can be limited because this requires the jammer to spread its full power between these frequencies, as the number of frequencies covered increases the less effectively each is jammed.
- **Base jamming** is a new type of Barrage Jamming where one radar is jammed effectively at its source at all frequencies. However, all other radars continue working normally.
- **Pulse jamming** produces noise pulses with period depending on radar mast rotation speed thus creating blocked sectors from directions other than the jammer making it harder to discover the jammer location.
- **Cover pulse jamming** creates a short noise pulse when radar signal is received thus concealing any aircraft flying behind the EW craft with a block of noise.
- **Digital radio frequency memory, or DRFM jamming**, or **Repeater jamming** is a repeater technique that manipulates received radar energy and retransmits it to change the return the radar sees. This technique can change the range the radar detects by changing the delay in transmission of pulses, the velocity the radar detects by changing the doppler shift of the transmitted signal, or the angle to the plane by using AM techniques to transmit into the sidelobes of the radar. Electronics, radio equipment, and antenna can cause DRFM jamming causing false targets, the signal must be timed after the received radar signal. By analysing received signal strength from side and backlobes and thus getting radar antennae radiation pattern false targets can be created to directions other than one where the jammer is coming from. If each radar pulse is uniquely coded it is not possible to create targets in directions other than the direction of the jammer
- **Deceptive jamming** uses techniques like "range gate pull-off" to break a radar lock.

Countermeasures

Constantly alternating the frequency that the radar operates on (frequency hopping) over a spread-spectrum will limit the effectiveness of most jamming, making it easier to read through it. Modern jammers can track a predictable frequency change, so the more random the frequency change, the more likely it is to counter the jammer.

- Cloaking the outgoing signal with random noise makes it more difficult for a jammer to figure out the frequency that a radar is operating on.
- Limiting unsecure radio communication concerning the jamming and its effectiveness is also important. The jammer could be listening, and if they know that a certain technique is effective, they could direct more jamming assets to employ this method.
- The most important method to counter radar jammers is operator training. Any system can be fooled with a jamming signal but a properly trained operator pays attention to the raw video signal and can detect abnormal patterns on the radar screen.

- The best indicator of jamming effectiveness to the jammer is countermeasures taken by the operator. The jammer does not know if their jamming is effective before operator starts changing radar transmission settings.
- Using EW countermeasures will give away radar capabilities thus on peacetime operations most military radars are used on fixed frequencies, at minimal power levels and with blocked Tx sectors toward possible listeners (country borders)
- Mobile fire control radars are usually kept passive when military operations are not ongoing to keep radar locations secret
- Active electronically scanned array (AESA) radars are innately harder to jam and can operate in Low Probability of Intercept (LPI) modes to reduce the chance that the radar is detected.
- A quantum radar system would automatically detect attempts at deceptive jamming, which might otherwise go unnoticed.

THE RUSSIAN ELECTRONIC WARFARE

Радиоэлектронная борьба

Радиоэлектронная борьба (РЭБ) — разновидность вооружённой борьбы, в ходе которой осуществляется воздействие радиоизлучениями (радиопомехами) на радиоэлектронные средства систем управления, связи и разведки противника в целях изменения качества циркулирующей в них военной информации, защита своих систем от аналогичных воздействий, а также изменение условий (свойств среды) распространения радиоволн.

Профессиональный праздник специалиста по радиоэлектронной борьбе в России отмечается 15 апреля.

Объекты и цели

Объектами воздействия в ходе РЭБ являются важные радиоэлектронные объекты (элементы систем управления войсками, силами и оружием, использующие радиосредства), нарушение или срыв работы которых приведёт к снижению эффективности применения противником своих вооружений.

Целями радиопомех являются радиолинии связи, управления, наведения, навигации. Помехи воздействуют, главным образом, на приёмную часть радиосредств. Для создания радиопомех используются активные и пассивные средства. К активным относятся средства, которые для формирования излучений используют принцип генерирования (например, передатчики, станции помех). Пассивные средства — используют принцип отражения (переизлучения) (например, дипольные и уголковые отражатели и др.).

В настоящее время РЭБ представляет собой комплекс согласованных мероприятий и действий войск, которые проводятся в целях:

- снижения эффективности управления войсками и применения оружия противника;
- обеспечения заданной эффективности управления войсками;
- применения своих средств поражения.

Достижение указанных целей осуществляется в рамках поражения систем управления войсками и оружием, связи и разведки противника путем изменения качества, циркулирующей в них информации, скорости информационных процессов, параметров и характеристик электронных средств; защиты своих систем управления, связи и разведки от поражения, а также охраняемых сведений о вооружении, военной технике, военных объектах и действиях войск от технических

средств разведки иностранных государств (противника) путем обеспечения заданных требований к информации и информационным процессам в автоматизированных системах управления, связи и разведки, а также свойств электронных средств.

В ходе РЭБ: поражение обеспечивается преднамеренным воздействием различными видами излучений на электронные средства, каналы получения и передачи информации, специальным программно-техническим воздействием на электронно-вычислительные средства противника; свои системы управления, связи и разведки защищаются от аналогичных воздействий противника, а также от непреднамеренных воздействий излучениями, возникающих вследствие совместного применения электронных средств; защита охраняемых сведений осуществляется их скрытием или (и) введением противника в заблуждение относительно их действительного содержания. Объектами РЭБ являются носители информации (поля и волны различной природы, потоки заряженных частиц), среда их распространения и электронные средства и системы. Таким образом, РЭБ является составной частью, технической основой информационной борьбы.

Составные части РЭБ

Составными частями РЭБ являются ***радиоэлектронное подавление*** и ***радиоэлектронная защита***.

Радиоэлектронное подавление

Радиоэлектро́нное подавле́ние (РЭП) — комплекс мероприятий и действий по снижению эффективности боевого применения противником радиоэлектронных систем и средств путём воздействия на их приёмные устройства радиоэлектронными помехами; составная часть радиоэлектронной борьбы. Включает радиотехническое, оптико-электронное и гидроакустическое подавление. РЭП обеспечивается созданием активных и пассивных помех, применением ложных целей, ловушек и другими способами.

Аппаратура

Р-330 — советский автоматизированный комплекс радиоэлектронного подавления.

- **«Лиман»** — советский/украинский наземный мобильный комплекс радиоэлектронного подавления линий наведения авиации.
- **БКО «Талисман»** — бортовой комплекс обороны для индивидуальной защиты боевых самолетов от управляемого ракетного оружия.
- **Алтаец**
- **Р-330МР**
- **Арбалет МР** (*Обслуживание самолётной станции радиопомех AN/ALQ-184)*

Радиоэлектронное подавление — комплекс мероприятий и действий по срыву (нарушению) работы или снижению эффективности боевого применения противником радиоэлектронных систем и средств путём воздействия на их приёмные устройства радиоэлектронными помехами. Включает радио-, радиотехническое, оптико-электронное и гидроакустическое подавление. Радиоэлектронное подавление обеспечивается созданием активных и пассивных помех, применением ложных целей, ловушек и другими способами.

Радиоэлектронная защита

Радиоэлектронная защита — совокупность мероприятий и действий войск (вооружённых сил) по устранению или ослаблению воздействия на свои радиоэлектронные объекты средств радиоэлектронного поражения противника, защите от поражения самонаводящимся на излучение оружием, защите от непреднамеренных взаимных радиопомех и от технических средств радиоэлектронной разведки противника.

В 70-х годах прошлого века в связи с активизацией иностранных технических разведок в составе Управления Начальника Связи Вооружённых Сил СССР создана специальная Служба безопасности связи. 1 сентября 1975 года приказом Министра Обороны СССР в составе Военной академии связи им. С. М. Будённого была создана общеакадемическая кафедра "Эффективности и радиоэлектронной защиты систем военной связи". В 1998 году в связи с реорганизацией создана кафедра "Радиоэлектронной защиты, безопасности связи и информации". Научные исследования в области радиоэлектронной защиты велись по следующим направлениям: защита от радиоэлектронного подавления (от преднамеренных помех); обеспечение электромагнитной совместимости (защита от непреднамеренных помех); защита от ионизирующего излучения и электромагнитного импульса; защита от самонаводящегося на источник излучения оружия. В 2008 году на национальном форуме информационной безопасности "ИНФОФОРУМ" Военной академии связи в лице кафедры "Радиоэлектронной защиты, безопасности связи и информации" вручены диплом и медаль "За вклад в подготовку специалистов в области информационной безопасности" Комитета Государственной думы по безопасности, Совета Безопасности Российской Федерации, Федерального агентства по информационным технологиям.

Радиоэлектронная защита — составная часть радиоэлектронной борьбы, направленная на обеспечение устойчивой работы радиоэлектронных средств (РЭС) в условиях воздействия преднамеренных радиопомех противника, электромагнитных излучений оружия функционального поражения, электромагнитных и ионизирующих излучений, возникающих при применении ядерного оружия, а также в условиях воздействия непреднамеренных радиопомех. Основу РЭЗ составляют: обеспечение электромагнитной совместимости (ЭМС) РЭС, комплекс организационных и технических мероприятий направленных на обеспечение помехоустойчивости РЭС в условиях воздействия на них непреднамеренных помех; защита РЭС от преднамеренных помех, комплекс организационных и технических мероприятий, направленных на обеспечение помехозащищённости РЭС в условиях воздействия на них преднамеренных помех; защита РЭС от электромагнитных и ионизирующих излучений, комплекс организационных и технических мероприятий по обеспечению надежности функционирования РЭС в условиях воздействия на них излучений, приводящих к функциональному поражению элементной базы; защита от воздействия ложных сигналов, комплекс организационных и технических мероприятий, направленных на воспрещение противнику возможности ввода в системы и средства информации (сообщений) при передаче им ложных сигналов.

Радиоэлектронная разведка

Радиоэлектронная разведка — сбор разведывательной информации на основе приёма и анализа электромагнитного излучения. Радиоэлектронная разведка использует как перехваченные сигналы из каналов связи между людьми и техническими средствами, так и сигналы работающих РЛС, станций связи, станций радиопомех и иных радиоэлектронных средств.

Комплексный технический контроль

Комплексный технический контроль — контроль за состоянием функционирования своих радиоэлектронных средств и их защиты от технических средств разведки противника. Осуществляется в интересах радиоэлектронной защиты. Включает радио-, радиотехнический,

фотографический, визуально-оптический контроль, а также контроль эффективности защиты информации от её утечки по техническим каналам при эксплуатации средств передачи и обработки информации.

Электромагнитное поражение

Электромагнитное воздействие (импульс), выводящее из строя электронное, коммуникационное и силовое оборудование противника. Поражающий эффект достигается за счёт наведения индукционных токов. Впервые отмечено при ядерных взрывах в атмосфере.

В настоящее время для создания поражающего импульса используются магнетроны. Электромагнитные системы поражения стоят на вооружении в США и других странах НАТО.

История

EA-6B «Праулер» — самолёт радиоэлектронной борьбы, используемый ВМС США.

Впервые радиоэлектронная борьба была применена силами ВМФ России в ходе Русско-японской войны. 15 апреля 1904 года во время артиллерийского обстрела, который японская эскадра вела по внутреннему рейду Порт-Артура, радиостанции российского броненосца «Победа» и берегового поста «Золотая гора» путём создания преднамеренных помех серьёзно затруднили передачу телеграмм вражеских кораблей-корректировщиков (считается очевидно первым в мире случаем).

Тем не менее радиосредства в то время в основном использовались для обеспечения связи, выявления каналов связи противника и перехвата передаваемой по ним информации. Предпочтение отдавалось перехвату радиопередач, а не их подавлению. Однако в годы Первой мировой войны радиопомехи стали эпизодически применяться для нарушения радиосвязи между штабами армий, корпусов и дивизий и между военными кораблями. Вместе с тем в германской армии уже тогда появились специальные станции радиопомех.

В период между мировыми войнами активно развивается радиосвязь, появляются средства радиопеленгации,радиоуправления и радиолокации. В результате кардинально меняется концепция управления и взаимодействия сухопутных войск, ВВС и ВМФ. Всё это привело к дальнейшему развитию способов и техники противодействия радиоэлектронным средствам противника.

Во время Второй мировой войны страны-участники активно использовали средства радиоэлектронного и гидроакустического подавления. Были сформированы и широко применялись для обеспечения боевых действий специальные части и подразделения радиопомех. Был накоплен большой опыт ведения разведки и создания радиопомех, а также радиоэлектронной защиты.

В послевоенное время продолжается развитие средств радиоэлектронной борьбы. Появляются новые средства радиопомех корабельного и авиационного базирования[4].

В современных войнах и военных конфликтах роль радиоэлектронной борьбы продолжает возрастать. Разработка и принятие на вооружение многих государстввысокоточного и высокотехнологичного оружия приводит к появлению новых объектов радиоэлектронного воздействия. Применение противорадиолокационных ракет значительно снижает живучесть современных радиоэлектронных средств (РЛС, комплексов ПВО), построенных на базе активных средств радиолокации. Широкое применение спутниковых систем разведки, связи и навигации вызывает необходимость их нейтрализации, в том числе, путём радиоэлектронного подавления. Разрабатываются портативные средства радиоэлектронной разведки и помех для борьбы с новыми средствами связи и навигации, поиска и нейтрализации радиофугасов и других устройств дистанционного подрыва. Средства РЭБ получили возможности системно-программного воздействия на АСУ и на другие вычислительные комплексы.

XXI век

Системы ЭМ оружия установлены на самолёте радиоэлектронной борьбы ВМФ США — EA-18 Growler. Оружие позволяет подавлять системы электронной коммуникации противника и при необходимости уничтожать их, а также выводить из строя электронные системы противника, в том числе системы наведения ПВО и электронные элементы управления самолётов противника. Впервые Growler был применен в операции НАТО в Ливии в 2011.

- ЭМ системой защиты от самонаводящихся ракет снабжен истребитель НАТО F-35. Действие системы основано на дистанционном разрушении электронных систем наведения ракет направленным электромагнитным импульсом.
- Системами индивидуальной защиты (бортовыми комплексами обороны, БКО) — БКО «Талисман» оснащены истребители МиГ-29 и штурмовики Су-25 ВВС Беларуси и самолёты Су-27УБМ2 ВВС Казахстана. Действие БКО «Талисман» основано на разрушении работы моноимпульсной пеленгации, что приводит к срыву наведения зенитной или авиационной управляемой ракеты.

Радиоэлектронная борьба в России

История

14 декабря 1942 года — Докладная народного комиссара внутренних дел Союза ССР Л. П. Берии председателю Государственного комитета обороны СССР И. В. Сталину о необходимости создания в Красной Армии «Службы по забивке немецких радиостанций, действующих на поле боя»

16 декабря 1942 И. Сталиным подписано Постановление Государственного Комитета Обороны № ГОКО 2633 сс «Об организации в составе Управления Войсковой разведки Генерального Штаба Красной Армии отдела по руководству работой радиостанций мешающего действия»

23 сентября 1953 в ГШ ВС СССР введена должность помощника начальника ГШ по вопросам радиотехнической разведки и помех

4 ноября 1953 — организован аппарат помощника начальника ГШ по вопросам радиотехнической разведки и помех

26 июня 1960 Аппарат помощника НГШ по вопросам радиопротиводействия преобразован в 9 отдел ГШ (борьбы с радиоэлектронными средствами противника).

22 апреля 1964 — 9 отдел ГШ включен в состав ГОУ ГШ.

22 января 1965 — 9 отдел выведен из состава ГОУ ГШ и определен как 9 отдел ГШ (борьбы с радиоэлектронными средствами противника).

8 июля 1968 — на базе 9 отдела ГШ и 8 отдела Управления ГШ сформирована Служба радиоэлектронного противодействия ГШ.

8 апреля 1972 — года служба радиоэлектронного противодействия ГШ реорганизована в 5 управление ГШ.

22 января 1974 — 5 управление ГШ реорганизовано в 1 управление 2 Главного управления ГШ.

13 мая 1977 — на базе 1-го управления организовано Управление РЭБ ГШ.

6 июня 1986 — Управление РЭБ ГШ преобразуется в Управление РЭБ Главного управления АСУ и РЭБ ГШ СССР.

3 июня 1989 — в связи с расформированием Главного управления АСУ и РЭБ ГШ Управление РЭБ ГШ выведено в самостоятельное управление.

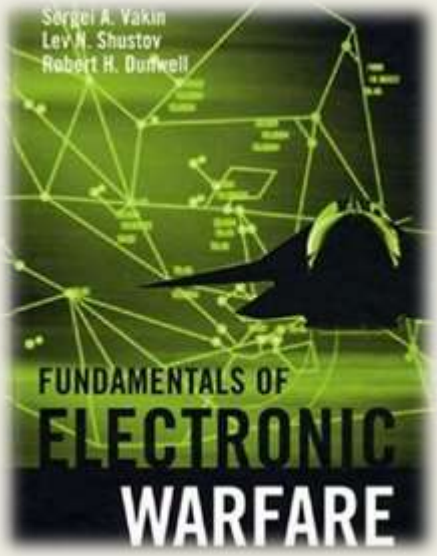
3 мая 1999 — учреждён День специалиста РЭБ, который отмечается ежегодно 15 апреля.

19 января 2009 — день образования Войск радиоэлектронной борьбы ВС РФ

По словам специалистов, если к 2020 году армия и флот должны будут перейти на новейшее вооружение на 70-75 %, то стратегический потенциал войск радиоэлектронного фронта будет обновлен на 100 %.

Комплексный технический контроль

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ:



1.***"Security Engineering – A Guide to Building Dependable Distributed Systems, 2nd edition" by Ross Anderson John Wiley & Sons 2008*** – ***Chapter 19*** – Electronic and Information Warfare.

This chapter covers topics that have been traditionally more interesting for the military, namely jamming and blocking electronic communications as well as countermeasures and surveillance. In essence the same as in the first edition with a few updates and more explanatory text. **(для пособия был заимствован 21 текст из данной книги):**

19.2 Basics

19.3 Communications Systems

19.3.1 Signals Intelligence Techniques

19.3.2 Attacks on Communications

19.3.3 Protection Techniques

19.3.3.1 Frequency Hopping

19.3.3.2 DSSS

19.3.3.3 Burst Communications

19.3.3.4 Combining Covertness and Jam Resistance

19.3.4 Interaction Between Civil and Military Uses

19.4 Surveillance and Target Acquisition

19.4.1 Types of Radar

19.4.2 Jamming Techniques 19.4.3 Advanced Radars and Countermeasures

19.4.4 Other Sensors and Multisensor Issues

19.5 IFF Systems

19.6 Improvised Explosive Devices

19.7 Directed Energy Weapons

19.8 Information Warfare

19.8.1 Definitions

19.8.2 Doctrine

19.8.3 Potentially Useful Lessons from Electronic Warfare

19.8.4 Differences Between E-war and I-war

19.9 Summary

Research Problems

Интернет-сайты:

1. Радиоэлектронная борьба

https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D0%B8%D0%BE%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%BE%D1%80%D1%8C%D0%B1%D0%B0

2. Electronic Warfare

https://en.wikipedia.org/wiki/Electronic_warfare

3. Radar navigation

https://en.wikipedia.org/wiki/Radar_navigation