普通高等教育“十一五”国家级规划教材

Advanced English: A Multimodal Video Course

多模态 高级英语视听读说教程

戴　劲　马薇娜　编著

教师用书

上海外语教育出版社
外教社 SHANGHAI FOREIGN LANGUAGE EDUCATION PRESS
www.sflep.com

普通高等教育“十一五”国家级规划教材

Advanced English: A Multimodal Video Course

多模态
高级英语视听读说教程

戴 劲 马薇娜 编著

教师用书

上海外语教育出版社
外教社 SHANGHAI FOREIGN LANGUAGE EDUCATION PRESS

图书在版编目（CIP）数据

多模态高级英语视听读说教程/戴劲，马薇娜编著. —上海：上海外语教育出版社，2010
教师用书
ISBN 978-7-5446-2043-7

Ⅰ.①多… Ⅱ.①戴… ②马… Ⅲ.①英语－听说教学－高等学校－教学参考资料 Ⅳ.①H319.9

中国版本图书馆CIP数据核字（2010）第194179号

出版发行：上海外语教育出版社
（上海外国语大学内） 邮编：200083
电　　话：021-65425300（总机）
电子邮箱：bookinfo@sflep.com.cn
网　　址：http://www.sflep.com.cn http://www.sflep.com
责任编辑：曹　娟

印　　刷：上海叶大印务发展有限公司
开　　本：787×1092 1/16 印张 16.5 字数 451 千字
版　　次：2010 年 12 月第 1 版 2010 年 12 月第 1 次印刷
印　　数：1 000 册

书　　号：ISBN 978-7-5446-2043-7 / H・0888
定　　价：33.00 元

本版图书如有印装质量问题，可向本社调换

前 言

从多模态教学理论角度看，英语视听说教学带有鲜明的多模态特征：它通常为学习者创造一种集音、像、图等多种语言模态形式呈现教学语料，并促使学习者启用视、听、说多种感官进行口语交际技能训练的教学环境。因此，以“多模态”冠名更能彰显本教程特色。

此外，与同类教程相比，本教程在名称上还多了一个“读”字，亦“点睛”出教程的一大创新：将“读”引入视听说教学。认知学研究表明，读和听之间尽管存在种种差异，但由于同属理解维度，两者间存在着相通性和重合性，而正是这种相通性和重合性为我们探索更有效的英语视听说教学方法提供了特殊启示。众所周知，我国学生各英语单项技能普遍存在着发展极不均衡的问题，突出地表现为阅读技能远远优于其他技能，进而衍生出一系列与“读”相关的问题，例如，“能读不能写”、“能读不能说”、“读得懂却听不懂”等现象。编者对“读得懂却听不懂”现象作了一些专门的探讨，并结合英语视听说教学进行了一些认真的思考。所有这些都成为本教程编写的创新之源。

“读得懂却听不懂”现象的确反映出学生英语阅读能力与听力能力之间存在的巨大差距，但不容否认的是，这种差距形成的原因与我们在英语视听说教学中忽略读、听之间的相通性和重合性不无关系。意识到这一点能帮助我们找到一种全新的视角来审视并解决这一问题。读、听之间的相通性和重合性实际上说明两者间存在着一种内在的关联性；“读得懂”说明学习者已具备相当的阅读能力；“听不懂”虽为一种被动状况，但它毕竟是暂时的，是可改变的。因此，一个值得我们思考的问题是：能否创造一种全新的视听说教学环境，让学生能借助自身的阅读优势去弥补并消除暂时的听力劣势？

经过反复探索和不断尝试，编者提出“以读助听，以读促听”的新的英语视听说教学理念，并在此基础上推出“多模态英语视听读说教学法”，即：借助英语影视字幕独特的语言教学功能，并通过视、听、读相结合的教学方式，为学生营造一个能借助自身阅读优势弥补暂时听力劣势的教学氛围和环境，逐步缩小英语听力水平与阅读水平之间的差距，实现由“听不懂”到“听得懂”的成功过渡和跨越；与此同时，还通过视、听、读、说紧密结合教学方式，使学生的英语口语交际能力获得稳步提高。

本教程所选视听材料均属于真实语料，类型为反映英语国家真实事件的纪实片。全书由十四个单元构成。每个单元包括“视前阅读”（Pre-viewing Reading）、“视前准备”（Pre-viewing Preparatory Work）、“边听边看边记”（During-viewing Activity）以及“视后练习”（Post-viewing Exercises）四个部分。前两部分属于准备阶段。“视前阅读”选出一篇与视听片内容相关但不雷同的文章供学生视前阅读，从背景知识和语言内容方面为后续的视听活动作准备。

每篇阅读文章后面还配有三个问答题，用以检测学生的阅读理解。“视前准备”包括生词语、专有名词、背景知识这三项内容，简要地讲解、介绍视听片中出现的生词语、人名、地名或事件名称以及重要的背景性知识。“边听边看边记”要求学生在视听过程中将某些信息（如重要数字、人名、地名、日期等）用笔快速记下来，没听清或没听懂的词语则可以用音标的形式记下来，供后续练习和学习用。这项训练能培养学生有目的、有重点地用英语做笔记的意识和技能，强化学生在视听过程中的专注力。“视后练习”包括视听理解练习和口语训练两项内容。视听理解由对错判断、多项式选择、完整段落填空、给词填空、给句组段等题型构成，从较微观的词语层面到较宏观语篇层面检测学生对相关词语的掌握和运用能力、对视听语篇的理解和认知状况。口语训练由复述、看图讲解、小组讨论和字幕电影配音等题型组成，其中“看图讲解”和“字幕电影配音”是本课程的另外两项创新。编者从每个单元的视听片中精心截选出五幅图片，要求学生根据自己的听力理解和记忆，运用所学词语对图片进行讲解；“字幕电影配音”则通过采用英语电影精彩对白中/英字幕的方式为学生创造一个集视译、表述和表演为一体的独特口语训练平台。

本教程适合高等院校英语专业视听说课程使用，也可供非英语专业硕士和博士研究生视听说课程使用；本教程尤其适合有志于看懂和听懂英语纪实片的广大英语学习者。本教程配备有供教学使用的影、音资料。

编者在此对美籍教师Ronald Broce教授、何继红博士在本教程的文字校对、影像资料编辑等方面给予的帮助深表感谢。

不足、不当之处，敬请本教程使用者、学界同仁批评指正。

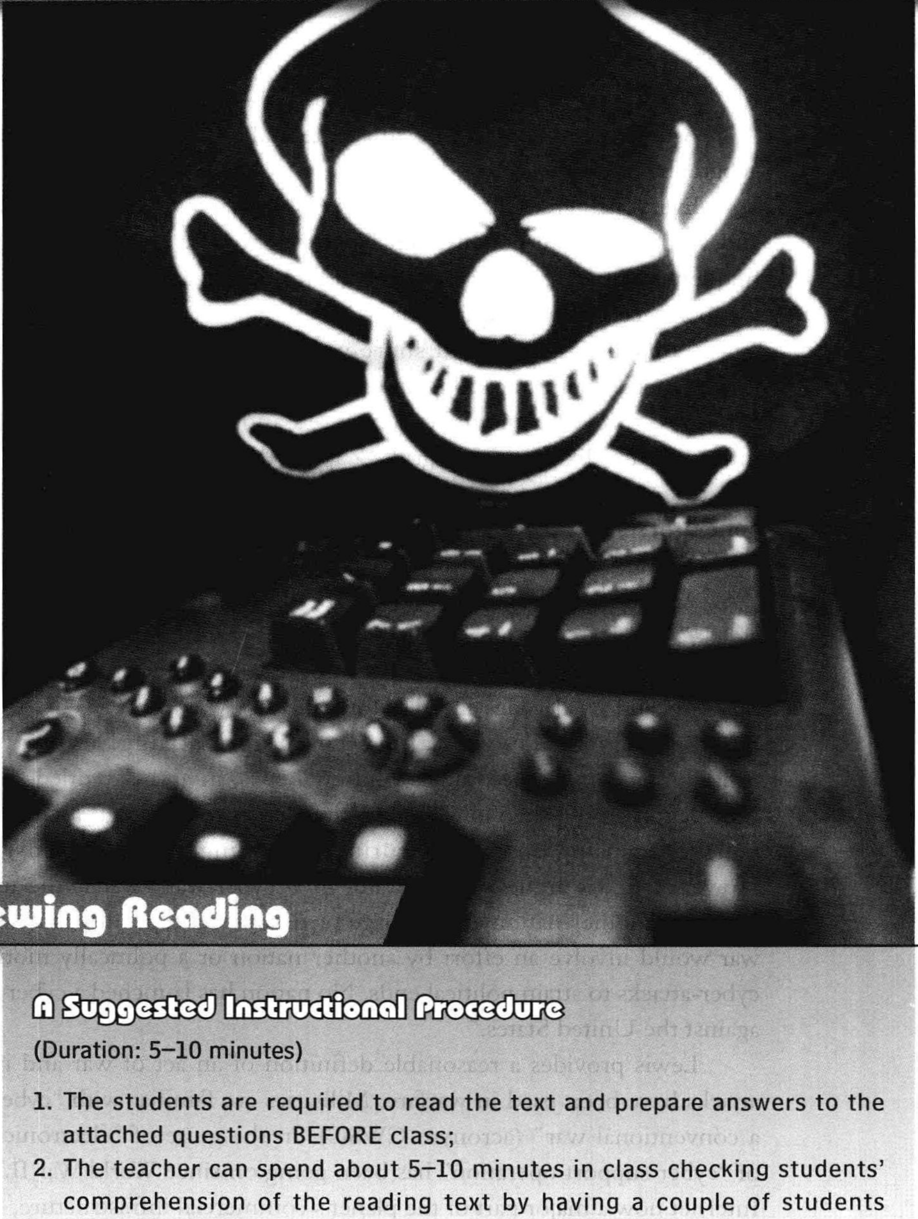
编者
2010年7月

此为试读，需要完整PDF请访问：www.ertongbook.com

CONTENTS

Unit 1

Cyber Warfare



I. Pre-viewing Reading

A Suggested Instructional Procedure

(Duration: 5–10 minutes)

1. The students are required to read the text and prepare answers to the attached questions BEFORE class;
2. The teacher can spend about 5–10 minutes in class checking students' comprehension of the reading text by having a couple of students provide answers orally in class.

Has the Cyber-War Begun?

Austin Bay

A battle rages over the definition of war — war in cyberspace, that is.

A definition matters because the stakes are already enormous in this "new geography of warfare."

Everyone agrees The First Great Cyber-War (a decisive struggle over the Internet and within the Internet) has not been fought — yet. Cyber-skirmishing, however, is frequent and fierce, a second-by-second form of digital probing and parrying (挡开) that is cyberspace's combat equivalent.

Computers store and share vast quantities of data — economic, military, intelligence, communications and politically sensitive information are obvious targets for spies, thieves, vandals, competitors and enemies. Digital systems control key infrastructure, like electrical grids. Zap (攻击) a central computer with digital viruses, and the grid is damaged until the viruses are identified and removed. Repairing generators and power lines after an aerial bomb attack is an analog. The viruses, however, don't leave high-explosive craters (弹坑).

And there's the rub (困难). Is a cyber-intrusion that disrupts and destroys an "armed attack," which under international law would permit armed retaliation? Technology and techniques have once again outpaced political adaptation, rendered military doctrine obsolete, and are decades ahead of formal law.

Strategists, lawyers and warriors are struggling with these complex, multidimensional issues. James Andrew Lewis, in an essay titled "The Cyber-War Has Not Begun" (published in March by the Center for Strategic and International Studies), believes focusing on cyber-security (protecting digital systems) "is a good thing." However, Lewis argues, "We are not in a 'cyber-war.' War is the use of military force to attack another nation and damage or destroy its capability and will to resist. Cyber-war would involve an effort by another nation or a politically motivated group to use cyber-attacks to attain political ends. No nation has launched a cyber-attack or cyber-war against the United States."

Lewis provides a reasonable definition of an act of war and its goals. Cyber-like attacks have been used in warfare. Militaries are familiar with "cyber-war in support of a conventional war" (acronym CWSC). In the guise of "electronic warfare," this type of "cyber support operation" has been going on since World War II. However, with the Internet now a major part of the planet's commercial infrastructure, "electronic warfare" has moved to another level. CWSC can now attack strategic targets (e.g., international lending and trading systems), not just the electronic weapons and communications of the combat forces.

Lewis recognizes a non-state actor ("politically motivated group") can wage cyber-war. He also asserts no nation (i.e., a nation-state) has launched a cyber-attack on the U.S., allowing the possibility of attempts to wage cyber-war by terrorists. Lewis argues that no nation-state has waged cyber-war or even launched a cyber-attack "to attain political ends" because the U.S. can trace these attacks to their source.

Guaranteed exposure is a deterrent because the attacker would risk retaliation of some sort — political, economic, military or, presumably, cyber. I hope he is right, though even the most informed speculations in this field are haunted by the "unknown unknowns" that time and actual warfare inevitably reveal at high cost.

Lewis discusses four types of cyber-threats and warns against conflating (混合) them: 1) economic espionage (theft of proprietary business and economic data, and intellectual property); 2) political and military espionage (traditional spying carried into cyberspace); 3) cyber-crime (e.g., theft of money from bank accounts); and 4) cyber-war. In Lewis' view, cyber-attacks in cyber-war are "just another weapons system" for hitting targets.

The categories suggest structural responses. Police, trade and legal institutions, linked to international agreements, become the mechanisms for addressing economic espionage and cyber-crime. Defense and diplomatic organizations address cyber-espionage and cyber-warfare. Lewis advocates creating international "norms" and understandings for what constitutes an attack, and "an international framework" to establish "potential consequences for differing levels of hostile action."

However, determining levels of hostility as a crisis emerges and escalates is a very stiff requirement. History is riddled with surprise attacks whose devastating effects took time to assess. The categories are really not so discrete.

In "real space" crime and terror, and crime and rebellion all too easily mesh (交织在一起). Separating criminal from rebel is often a tough judgment call. In my own view, skirmishing is warfare. In cyberspace we are witnessing the potshots(乱射) by light cavalry(轻骑兵) prior to a larger clash, where opponents, at a calculated pace, probe for vulnerabilities and seek decisive advantage.

(726 words)

(From: *The Patriot Post*. April 14, 2010)

Questions

1) What is "the rub" about?

The rub is that people don't know exactly how to respond to a devastating cyber-intrusion, since there hasn't been any formal law dealing with such an event. Here, technology and techniques have outpaced existing policies and military doctrine.

2) Which four types of cyber-threats does Lewis identify?

The four types are economic espionage, political and military espionage, cyber-crime, and cyber-war.

3) Why does the author view skirmishing as warfare?

He believes that in cyberspace, a small clash often evolves into a larger clash.

II. Pre-viewing Preparatory Work

A Suggested Instructional Procedure

(Duration: 15–20 minutes)

1. The students should complete the following tasks before class.
   1) studying the listed new words and phrases, in terms of meaning and usage;
   2) familiarizing themselves with the listed proper nouns;
   3) reading through the background notes.
2. The teacher will provide answers to whatever questions the students may raise.
3. The students are asked to skim all the comprehension questions before the viewing.

1. New Words & Phrases

lethal /'li:θəl/ *a.* sufficient to cause death

e.g. These chemicals are lethal to fish.

hack /hæk/ *v.* (to hack into sth.) to gain unauthorized access to a computer network

e.g. He managed to hack into the company's central database.

strand /strænd/ *v.* to bring into or leave in a difficult or helpless position

infrastructure /'ɪnfrə'strʌktʃə/ *n.* 基础设施

crumble /'krʌmbl/ *v.* to lose power, become weak, or fail

e.g. The Empire began to crumble during the 13th century.

stop in one's tracks to prevent sb. from continuing doing sth.

e.g. The memo was supposed to stop the protest in its tracks.

vulnerable /'vʌlnərəb(ə)l/ *a.* (of a place, thing, or idea) easy to attack or criticize

e.g. The fort was vulnerable to attack from the north.

the click of a mouse used to show how quickly sth. can be done on a computer

e.g. Your photos can be viewed with the click of a mouse.

consensus /kən'sensəs/ *n.* an opinion that everyone in a group agrees with or accepts

e.g. The EU Council of Finance Ministers failed to reach a consensus on the pace of integration.

intruder /ɪn'tru:də/ *n.* sb. who illegally enters a building or area, usually in order to steal sth.

track /træk/ *v.* to search for a person or animal by following the marks they leave behind them on the ground, their smell, etc.

e.g. Police have been tracking the four criminals all over central America.

national security paradigm /'pærədaɪm/ *n.* 国家安全范例

vigilant /'vɪdʒɪlənt/ *a.* giving careful attention to what is happening, so that you will notice any danger or illegal activity

e.g. Please remain vigilant at all times and report anything suspicious.

deterrent /dɪ'tɜ:rənt/ *n.* 威慑物，制止物

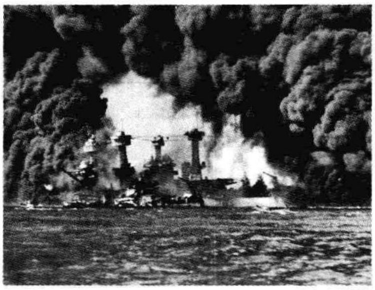
e.g. Do you think the death penalty acts as a deterrent to murderers?

2. Proper Nouns

Winn Schwartau: the author of *Cybershock*
Dr. Daniel Keel: an information warfare strategy expert
Daniel Kuehl Ph.D of: National Defense University
Colonel James Massaro: U.S. Air Force Commander 67th Intelligence Wing
ASEM: a digital detective program developed by the U.S. Air Force

3. Background Notes

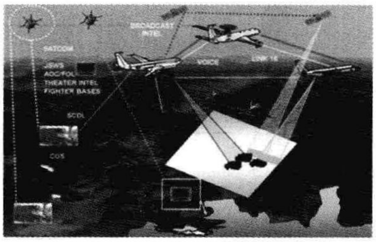
1) The attack on Pearl Harbor



The attack was an unannounced military strike conducted by the Japanese navy against the United States naval base at Pearl Harbor, Hawaii on the morning of December 7, 1941, causing personnel losses of 2,402 killed and 1,282 wounded. It was intended as a preventive action in order to keep the U.S. Pacific Fleet from influencing the war that the Empire of Japan was planning in Southeast Asia, against Britain and the Netherlands, as well as the U.S. in the Philippines. This attack resulted in the United States' entry into World War II.

2) Information warfare

Information warfare is the use and management of information in pursuit of a competitive advantage over an opponent. It may involve collection of tactical information, assurance(s) that one's own information is valid, spreading of disinformation to demoralize the enemy and the public, undermining the quality of opposing force information and denial of information-collection opportunities to opposing forces.



3) National Defense University (NDU)

The National Defense University is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. Most students are officers and selected civilians in Washington. Students take classes in advanced strategic methods and diplomacy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

此为试读，需要完整PDF请访问：www.ertongbook.com

III. During-viewing Activity

A Suggested Instructional Procedure

(Duration: the same as the video duration)

The students are asked to jot down in the provided space, while watching the video, some key words, lexical phrases, important figures, names of important people, place, and time, etc.

Jot down whatever you feel important while viewing the video.

IV. Post-viewing Exercises

Section A Comprehension

A Suggested Instructional Procedure

(Duration: 20–30 minutes)

1. The number of viewing times should be flexible, depending on the students' comprehension of the video.
2. Once the students have gone through all the comprehension questions, the teacher can ask the students to report their answers orally.
3. Whenever the students have disagreement on the comprehension questions, the teacher should give the floor to the students and encourage them to engage in debate. The teacher may hold his/her explanation or the correct answer(s) until an appropriate time.

1. Decide whether each of the following statements is true (T) or false (F).

1) The cyber warfare the U.S. is waging is aimed at locating computer terrorists. (*F*)
The cyber warfare the U.S. is waging is aimed at stopping computer terrorists in their tracks.

2) According to Mr. Schwartau, a cyber terrorist must be a computer expert. (*F*)
According to Mr. Schwartau, a cyber terrorist doesn't need to be an expert computer programmer to hack into our critical systems.

3) Dr. Kuehl believes that a militarily weaker enemy is more likely to launch a cyber-war , rather than a conventional war, against the U.S. (*T*)
"If another country is militarily weak, conventionally, and we are strong in that area, they are going to oppose us some other way, perhaps using information warfare."

4) Dr. Kuehl's words indicate that it may have been fairly easy for hackers to break into the computer systems of key government agencies. (*T*)
"The Department of Defense's computer systems have been broken into tens of thousands of times by foreign and domestic hackers."

5) The U.S. military is capable of defending against every cyber terrorist. (*F*)
The U.S. military can't defend against every cyber terrorist.

2. Choose the best answer that completes each statement.

1) _______ is not cited as an example to illustrate how heavily Americans rely on computer networks.

a. Navigation [✓ b.] Teaching
c. Banking d. Telecommunications

Cited examples include transportation, finance, and telecommunications.

2) Mr. Schwartau would not agree that ______.

[✓ a.] the U.S. is invulnerable to an electronic attack

b. a country's computers today constitute its critical infrastructure

c. today's world can hardly function, to a large extent, without computers

d. a computer system is very liable to attack

...is vulnerable to

3) The following statements are true except that ______.

a. Dr. Keel is an authority in cyber warfare strategy

b. Dr. Keel thinks it is urgent for the U.S. to take immediate actions in preparing for cyber warfare

[✓ c.] a small and poor country could do little harm to a power like the U.S. in a hypothetical cyber-war

d. both a and b

...even the smallest and poorest nation could pose a threat to the U.S.

4) The description that does not fit the Air Intelligence Agency (AIA) is ______.

a. protecting all the computers throughout the Air Force

b. the nerve center of the Air Force's battle against cyber enemies

c. being staffed by a team of cyber experts

[✓ d.] its computer database being intruded 24 hours a day, seven days a week

... a highly skilled cyber team is on the lookout for any intruder ... into the Air Force's computer database

5) Mr. Schwartau would not agree that cyber experts can ______.

a. identify who the hacker at the other end of the wire is

b. find out the age of a hacker

c. locate the hacker

[✓ d.] all of the above

One of the problems that we have with this is identifying who's the bad guy at the other end of the wire.

3. Fill in each blank with the EXACT word whose initial letter is already given, according to what you have watched.

But the military's best-kept secrets are not all 1) *decades* old. Some involve 2) *events* that are yet to come. In the war of the future, the United States will not only be attacked with planes, bombs, and bullets, but also with an 3) *invisible* lethal weapon: digital data that will come directly through our phone lines. When an enemy 4) *hacks* into our computer systems, 5) *financial* institutions will suddenly 6) *collapse*. 911 emergency calls will go 7) *unanswered*. Air traffic control systems will break down, 8) *stranding* airplanes in the sky. And, city by city, the nation's electronic 9) *infrastructure* will crumble. Could it happen? 10) *Incredibly*, the answer is, yes.

4. Complete the following sentences with the given phrases and expressions. Make changes where necessary.

to hack/break into (a system)
to stop one in one's tracks
to be vulnerable to
to serve as a deterrent to
to go unanswered
to be on the lookout for
in a sense
to be linked to
in some case
to learn the hard way about

1) Life is *in a sense* a battle.
2) The question stopped Alice *in her tracks*.
3) All rooms *are linked to* the main switchboard.
4) Police *are on the lookout for* those boat thieves.
5) *In some case*, these crossover dreams may be justified.
6) Budgets promote efficiency and *serve as a deterrent to* waste.
7) These dwellings are especially *vulnerable to* landslips during the heavy rainfall.
8) Travelers are *learning the hard way about* international carry-on rules of what can and cannot be brought onto a plane.
9) Once the books are open or the computer is booted up, phone calls *will go unanswered*, TV shows unwatched, snacks ignored.
10) Police say a 9-year-old McLean boy *hacked/broke into* the Blackboard Learning System used by the county school system to change teachers' and staff members' passwords, change or delete course content, and change course enrollment.

5. Form a comprehensible and coherent paragraph by arranging the following sentences in a proper order.

1) Each day, there are between 800 and 1,000 alerts.
2) This top-secret program monitors every Air Force base in the world.
3) To assist in the search for electronic terrorists, the Air Force has developed a digital detective program, known as ASEM.
4) But, not all of them pose a threat.
5) Immediately, they begin to track the intruder.
6) If an electronic invasion occurs, the team is alerted within 30 seconds.

3 → *2* → *6* → *5* → *1* → *4*

Section B Speaking

A Suggested Instructional Procedure

1. The teacher may prepare the students for the retelling and still-explaining tasks by letting them watch the video one more time. The students are asked to practise in pairs.
2. The teacher will ask the students to conduct group discussion over the prepared topics. By the end of the discussion, each group will have a spokesperson to report their views briefly to the whole class.
3. The teacher may prepare the students for the movie-dubbing task by providing the students with a movie summary and by showing the movie segment; then the students are given a few minutes of time to practise in pairs with the English/Chinese scripts; after that, the teacher will let the students practise a couple of times with the movie segment on; finally, the teacher may encourage as many pairs as possible to practise in front of the whole class, within the remaining class time.

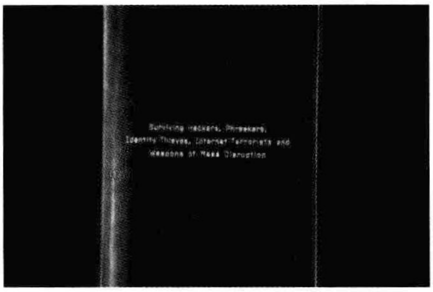
1. Find a partner and retell the report by using as many lexical phrases listed below as possible.

to hack/break into a system
to fight a secret war
to get things together
a futuristic war room
in some case
to be on the lookout for
in a sense
at the other end of the wire
to launch a counter attack

electronic infrastructure
to break down
a nerve center
to be vulnerable to
from all different angles
a national consensus that
to learn the hard way about
to pose a threat to
to serve as a deterrent to

to go unanswered
to stop sb. in their tracks
to be linked to
at all different sides
the click of a mouse
an electronic invasion
information warfare
to be all in this thing together
maximum-security

2. Explain to your partner the content of the selected stills.


Surviving Hackers, Phreakers,
Identity Thieves, Internet Terrorists and
Weapons of Mass Disruption

Still 1

And, the nation's top information security analyst, Winn Schwartau, believes that the U.S. is vulnerable to an electronic attack.

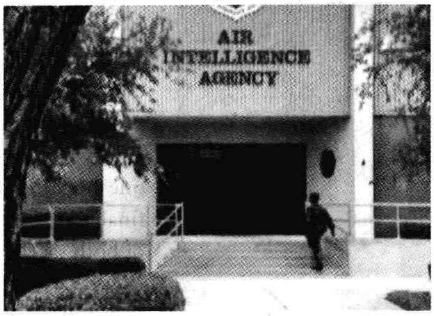
Schwartau: The nation's computers today, the critical infrastructures, the very blood that makes this country and a good part of, portion of the world operate and function today, are very poorly protected.

Still 2

Schwartau says a foreign adversary or cyber terrorist doesn't even need to be an expert computer programmer to hack into our critical systems. In some case, it can be done with nothing more than the click of a mouse.

Still 3

We've been granted a special access to a heavily guarded facility called the Air Intelligence Agency. It's the maximum-security nerve center of the Air Force's battle against information warfare.

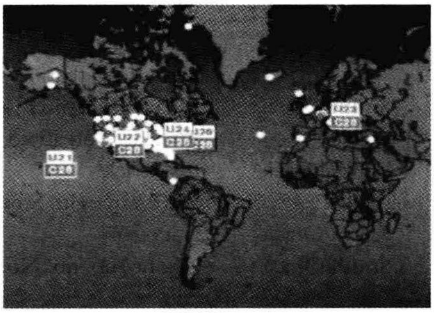


Still 4

24 hours a day, seven days a week, a highly skilled cyber team is on the lookout for any intruder that attempts to break into the Air Force's computer database.

Still 5

To assist in the search for electronic terrorists, the Air Force has developed a digital detective program, known as ASEM. This top-secret program monitors every Air Force base in the world. If an electronic invasion occurs, the team is alerted within 30 seconds. Immediately, they begin to track the intruder. Each day, there are between 800 and 1,000 alerts. But, not all of them pose a threat.



3. Questions for Discussion

1) What do you know about information warfare?
2) Tell a story about electronic invasion and its damage.

此为试读，需要完整PDF请访问：www.ertongbook.com