

Use of English

Maximum score: 10

Choose the correct answer to fill in the gap. The exercise begins with an example.

Integrated Border Management, or IBM, is a concept of border management devised by 0 the European Union that was first applied in the context of the EU's support activities in the Western Balkans region during the period 2002-2006.

The need for agencies involved in 1 border management – such as the border police and customs – to coordinate their work at national and international levels became increasingly apparent in the light of 2 realities such as the expansion of the European Union (and Schengen zone) eastwards, the movement of migrants across borders in search of better socio-economic 3 conditions or in flight from conflict, and the globalization of crime and the international economy.

The EU moved quickly to meet 4 this need for greater coordination at its own external borders, and in 2004 created Frontex, an agency dedicated to 5 “the management of operational cooperation at the external borders of the Member States of the European Union.” Underpinning the idea of IBM is that individual border agencies are generally more effective when 6 cooperation is in place. That means cooperation within the agency itself (intra-agency); between the various agencies involved in border management in the same country (inter-agency); and cooperation with the border agencies of neighbouring countries (international). Conversely, when cooperation is lacking in any of these 7 three dimensions, effective border management is diminished.

IBM relies on striking the right balance between facilitation of legitimate movement of trade and travellers across borders, and controlling borders in order to identify and prevent cross-border crime 8. Ultimately, IBM should result in 9 smoother, hassle-free, border crossing for travellers.

The EU's own definition of IBM is: “National and international coordination and cooperation among all the relevant authorities and agencies involved in border security and trade facilitation to establish effective, efficient and coordinated border management, in order to reach the objective of open, but well controlled and secure 10 borders”.

0	A/ <i>devised by</i>	B/ <i>deployed in</i>	C/ <i>decision of</i>
1	A/ included in	B/ involved in	C/ implicated in
2	A/ in the light of	B/ with regard	C/ consequently
3	A/ higher living standard	B/ better social status	C/ better socio-economic
4	A/ meeting	B/ to meet	C/ to meeting
5	A/ dedicated to	B/ devoted for	C/ dealing in
6	A/ however	B/ while	C/ when
7	A/ all of that	B/ any of these	C/ any of them
8	A/ crime cross border	B/ across border crime	C/ cross-border crime
9	A/ has to succeed	B/ should result in	C/ would have targeted at
10	A/ secure	B/ security	C/ securing

HOW CYBERCRIMES CHALLENGE LAW ENFORCEMENT

The cyber-world brings global connections to local settings, transforming the ways we interact with one another. The benefits are many for each person and society. Barriers are bridged, and people have an easier time gaining access to information, connections, and a full range of legitimately offered goods and services. But there is a worrisome downside to the cyber-world as well, because it spreads illegal goods and services and makes it easier for criminals to operate across national boundaries as well as within them.

Cybercrimes add new dimensions to illegality and violent threats that law enforcement officials and policymakers struggle to address. Such crimes can be especially worrisome because they are often asymmetrical – in that one person or small group can wreak as much damage as it once took an entire army to cause. What is more, the offender does not have to be physically anywhere near the victim.

What are Cybercrimes?

Cybercrime is a broad term encompassing acts committed or facilitated by the use of computer technology.

- Some cybercrimes are simply new variants of traditional forms of wrongdoing – such as theft and fraud – where computers are used to steal personal identifications, passwords, and credit card information.
- In more sophisticated cybercrimes, computers may be sabotaged – as in denial of service attacks – or turned into agents of espionage. Viruses or other devices are often hidden in seemingly legitimate emails or advertisements on the web, which infect a computer once a user clicks on an email or link.
- In the case of “Trojan horse” attacks, the criminal hacker may be able to gain remote access to the computer system and view the user’s screen or web camera, or even take control of the entire computer from a remote location. Hackers typically use methods such as these to gain access to government computer systems and commercial databases.
- Cybercrimes can also involve illicit trade or the commissioning of criminal acts. Extremely serious crimes like murder for hire and killing to harvest organs are sometimes facilitated by the use of the “Deep Web,” which is also sometimes referred to as the “Dark Net.”

The Deep Web refers to information that a standard Internet search engine like *Google.com* or *Yahoo.com* cannot find. Anonymity is the name of the game, and special software is often needed to gain access. Some researchers have termed the Deep Web the “secret Internet for bad guys.” Much more remains to be learned about the extent to which organized criminal groups use the Deep Web to expedite and spread longstanding illegal activities such as drug trafficking, human trafficking, and manufacturing counterfeit products.

Special Concerns for Law Enforcement

The asymmetrical nature of cybercrime calls out for new approaches to combating crime. If one person can become as powerful as an entire army, countries can no longer rely solely on more reactive methods. Given the access and ease of the Internet, every person who has a computer, a Smartphone, or any other device that can connect to the Internet is

a potential point of entry into a country. Local police jurisdictions must also be alert to cybercriminals operating across state and regional lines. Security officials and law enforcement agencies alike must place a new emphasis on preventive intelligence to locate sources of potential cyber threats to the organizations and people they are supposed to protect.

Searching for the Right Balance

Policymakers struggle with what to do about dangerous or illicit information on the web. But does this mean national governments should limit their citizens' access to the Internet? Authoritarian countries such as China have already taken such steps, but democratic societies must find a more appropriate balance between personal freedoms and crime control. How this can be done remains to be seen, but there is no question that cybercrimes involving terrorism are at the forefront of concern for governments and law enforcement agencies around the world.

Example

0. the benefits of the cyber-world according to the author of the article (3)

0.1 connection with the whole world

0.2 quick and easy access to information

0.3 a wide range of goods and services

1. the dangers of the cyber-world according to the author of the article (2)

1 goods and services which are not legitimate can easily be sold and bought

2 criminals can communicate/operate easily both within their home country and abroad/worldwide

2. the disproportionate character of cybercrime (1)

3 a few criminals (or even one person) can cause enormous/extensive damage

3. the main types of cybercrime listed by the author (5)

4 theft and fraud of personal data

5 sabotage of computers

6 turning computers into means of spying

7 Trojan attacks (the criminal gains access to a remote computer)

8 trade and commissioning of criminal acts

4. the features of the Deep Web (2)

9 it cannot be reached by the common/standard search engines OR you need special software to get access to it

10 we do not know much about it/ there's a lot to investigate about it/we have very little information/knowledge about it

5. combating cybercrime, new approaches (2)

11 police forces must be alert to cybercrime without borders

12 emphasis on prevention / on locating the source of potential cybercrime

6. the difference in attitudes towards Internet access (2)

13 authoritarian countries: limited Internet access (1 point)

14 democratic societies: attempts to find a balance between personal freedom and cybercrime control (1 point)

NB. If the two types of countries are mixed up= 0 point

7. the most recent area of cybercrime governments are concerned about (1)

15 terrorism

Reading 2

Maximum score: 10

Fill in the gaps with the letters of the words/phrases given under the text. There are two extra letters, which you do not need. The exercise begins with an example (0).

Revealed: drug use figures and what they tell us about changing habits the latest

Every year, the UK Home Office invites a sample of 50,000 people to tell them __0__ any illicit drugs. Although you might wonder why anyone would willingly share __1__, most people agree to take part. [The survey](#) helps us to understand the trends in UK drug use and informs policy and service planning.

Overall, drug use at a population level remains stable. Cannabis continues to be __2__ illegal drug with 2.2m people using it in the last year. Although this seems like a large number, it's __3__ that 29m people drink alcohol every week and 9m continue to smoke.

Heroin and cocaine use remains stable generally although there was a slight increase __4__ of young people using cocaine over the last year.

But a significant increase in [anabolic steroid use](#) __5__, with 19,000 more young people using these types of drugs, reversing the previous trend of declining use.

In 2016, Novel Psychoactive Substances (NPS) were banned [in the UK](#) and this would appear to have significantly reduced their popularity. Only 0.4% of the sample __6__ this type of drug, compared to 0.7% last year.

But we cannot infer that fewer people are using NPS in the UK simply from a decrease in reported use of these drugs. This is mainly because NPS use is most prevalent in the groups that are __7__, such as homeless and prison populations.

Over recent decades, governments have continued to support a policy __8__ the demand for drugs and restrict supply. This year's survey might be viewed as an endorsement of such an approach. But the survey continues to show how fast __9__ in drug use can be.

It took the government seven years to update its __10__ – that's geological time in the world of drug use. An increase in anabolic steroid use among young people means that young people will need to access vital harm reduction services, such as specialist needle and syringe programmes, which are entirely lacking in the 2017 Drug Strategy.

A/ the UK's favourite; B/ that aims to reduce; C/; reported using D/ whether they have used;

E/ excluded from the survey; F/ in the proportion; G/ this type of information;

H/ worth remembering; I/ **vital harm** J/ some trends; K/; [drug strategy](#);

L/ **continue collecting drug use data**; M/ is concerning

0	1	2	3	4	5	6	7	8	9	10
D	G	A	H	F	M	C	E	B	J	K