Краснодарский университет МВД России

ЗАРУБЕЖНАЯ ПРАКТИКА ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ КАК ИНСТРУМЕНТОМ СОВРЕМЕННОГО ТЕРРОРИЗМА

Учебное пособие
по английскому языку

Краснодар
2020

УДК 811.111(075.8)
ББК 81.432.1
З-34

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *В. А. Гончарова, С. В. Борисова*

Рецензенты:
В. В. Посиделова, кандидат филологических наук (Ростовский юридический институт МВД России);
Б. Н. Селин, кандидат педагогических наук (Белгородский юридический институт МВД России имени И.Д. Путилина).

З-34 **Зарубежная практика правоохранительной деятельности** в борьбе с киберпреступлениями как инструментом современного терроризма : учебное пособие по английскому языку / сост.: В. А. Гончарова, С. В. Борисова. – Краснодар : Краснодарский университет МВД России, 2020. – 144 с.

ISBN 978-5-9266-1642-9

Содержатся современные аутентичные профессионально-ориентированные материалы на английском языке, способствующие углублению знаний обучающихся по темам: «Киберпреступления: понятия, виды», «Зарубежная практика правоохранительной деятельности в борьбе с терроризмом».

Для профессорско-преподавательского состава, курсантов и слушателей образовательных организаций МВД России.

УДК 811.111(075.8)
ББК 81.432.1

ISBN 978-5-9266-1642-9

Содержание

Introduction (Введение)……………………….……….………………4

Unit I. Introduction to the language of cybercrime: definitions and discussion……………………………………………………………...…6

Part 1. Definition of cybercrime…………………………..……...….6

Part 2. Legal definitions of cybercrime………………..……..………..15

Part 3. What is cybercrime ……………………….……………….. 16

Part 4. Europol on cybercrime …………………………….…………22

Part 5. Abbreviations …………………………………….…………..27

Part 6. Basic criminal law vocabulary ……………….………...……29

Part 7. Hackers. Hacktivists and cybercrime ……………….……….30

UNIT II. Cybercrime regulations, directives and organizations ……….....33

Part 1. The Internet organized crime threat assessment …………………. 33

Part 2. Acronyms and abbreviations …………………………..…..35

Part 3. Directive 2013/40 EU, vocabulary in context ………………..…37

Part 4. COE convention on cybercrime – extradition. Prepositions. …..….43

UNIT III. The language of cybercrime: Cases ……………….……..47

Part 1. Law Enforcement successes in cybercrime ……………..……47

Part 2. The Love-Bug virus 33 ……………………………...…..52

Part 3. US Employee sentenced for hacking and cybercrime ……………..58

UNIT IV. Foreign law-enforcement activity practice in fighting cybercrimes……………………………………………………………72

References …………………………………………..........…...93

Appendix (Supplementary Reading) …………………………..142

ВВЕДЕНИЕ

Методическая организация учебного пособия, предусматривает выполнение целевых установок программы – научить будущих профессионалов – сотрудников полиции понимать и обсуждать литературу, связанную со всеми аспектами деятельности, направленной на борьбу с терроризмом, воспринимать на слух иноязычную речь и объясняться в определенных ситуациях профессионального характера на изучаемом языке по данной теме.

Развитие умений и навыков устной речи, чтения и письма происходит параллельно, на одном тематическом материале, комплексно-дифференцированно. Методическая система учебного пособия позволяет при достижении той или иной цели осуществлять вариативность обучения путем концентрации внимания на соответствующих видах речевой деятельности. Основные особенности данной системы сосредоточены в профессиональной направленности текстов и упражнений; взаимодействии видов речевой деятельности, реализуемой через комплексно-дифференцированную организацию усвоения устной речи, чтения и письма; цикличности работы; научно обоснованном отборе языкового и речевого материала; определенной последовательности представления языковых явлений и речевых моделей, устной речи и чтения, внутри одного крупного грамматического явления; системой подачи материала в соответствии с языковой системой; обеспечении обратной связи – текущей и итоговой.

Учебное пособие «Зарубежная практика правоохранительной деятельности в борьбе с киберпреступлениями как инструментом современного терроризма» предполагает взаимосвязанное прохождение лексического и грамматического материала и развитие речевых умений и навыков. Каждый раздел пособия включает профессионально направленные аутентичные и адаптированные учебные тексты (для изучающего, ознакомительного, просмотрового и поискового чтения), лексико-грамматические комментарии и упражнения. Для будущих сотрудников ОВД представляется необходимым овладение всеми видами чтения литературы по специальности на английском языке с целью получения профессионально значимой информации, т. к. при решении ряда профессиональных задач как вид речевой деятельности чтение широко востребовано.

Наполнению разделов, содержащих лексические единицы, которые были введены в предыдущих разделах или вводятся в данном разделе, что снимает трудности в активизации новых лексико-грамматических единиц, уделено значительное внимание. Количество упражнений и разнообразие заданий способствуют совершенствованию навыков устной и письменной форм коммуникации.

Приложение (тексты для внеаудиторного чтения) предназначено для самостоятельной работы слушателей всех форм обучения (аудиторной, самостоятельной работы, внеаудиторной самостоятельной работы).

Аутентичные профессионально-ориентированные тексты юридической тематики на английском языке могут быть использованы профессорско-преподавательским составом, адъюнктами, курсантами и слушателями образовательных организаций МВД России как для работы в аудитории, так и для самоконтроля. Обращается особое внимание на профессиональную лексику, необходимую для будущих сотрудников ОВД.

UNIT 1
INTRODUCTION TO THE LANGUAGE OF CYBERCRIME: DEFINITIONS AND DISCUSSION

INTRODUCTION
The Language of the Law and Cybercrime in English
Michael S. Boyd

The language of law in English has been known to confound both laypeople and experts. There are a number of reasons for the apparent impenetrability of legal English, most of which are due to the rather exceptional history of the English language as well as the development of the law profession in England and Wales and later in the colonies in which the common law was adopted. In this short introduction to the language of cybercrime I, of course, do not have time to trace this fascinating history[1], but rather I will introduce some of the most important features of legal English, many of which can also be found in the texts presented in this handbook. To understand the apparent complexity of legal English, all we have to do is look at any type of legal document such as a contract or license – even for the most basic of services – and examine the long and seemingly unending sentences, technical words and expressions, Latin words and phrases, the wide use of certain grammatical forms (such as, e.g., shall and the subjunctive), as well as terms of art and common words that have very different meanings in legal contexts.

Since most of the people who will be reading this book will probably already have had some training in the law, be they judges, prosecutors or law enforcement agents, such “strange” uses of language in legal contexts will probably come as no surprise. Your own legal languages are most likely characterized by similar features. Yet, English legal language is different, which, as we have already said, is due to its history. Such differences are also the result of the different systems of law practiced in England, Wales, the United States, etc. (the so-called common law) as compared to those so-called civil or continental law systems as practiced on the European Continent (and elsewhere): “the modes of expression of legal English differ from those of the legal languages of continental Europe” (Mattila, 2006, p. 221). This also means that many legal terms that may look exactly the same in English and the languages of the continent may refer to completely different concepts. For example, a *sentence* in English law (i.e. the punishment assigned to a defendant who has been found guilty) is very different from a *sentenza* in Italian law, which is closer to the English *judgment* or *opinion*. The major differences in legal systems demonstrate that we cannot fully understand the legal language of one country without first accepting that “[e]ach society has different cultural, social and linguistic structures developed separately according to its own conditioning” (Cao, 2007, p. 24).

But why is it so difficult and so important to understand the meanings of words in legal English? Stubbs (1996, p. 106) provides the following (excellent) explanation: “Because the law relies on interpretation of language, the standards by which words are interpreted are inevitably different for the legal profession and the lay public, and it is inevitable that judge and jury will use language differently. People interpret discourse according to their own conventions, and it is therefore very likely that the jury are not always able to suspend their common-sense interpretations of language in ways the court may require of them.” While Stubbs focuses on the importance of the judge and jury in the Anglo-American adversarial system, the same “standards” can be implied to the reading of any text in a (foreign) legal language. Thus, when you approach the texts and language activities provided in this Handbook, you should always consider how your own “conventions” might be different from or similar to those presented herein. We should be interested in ascertaining what happens in the UK, the United States, the EU and the individual Member States when dealing with the legal language and issues of cybercrime.

Despite all of the characteristic features of legal English, one does not have to learn legal English separately from general English, as legal English is a mix of general English with a number of specific features of lexis, morphology, syntax, etc. Tiersma (1999, p. 49) notes that although legal English "follows the rules that govern English in general", it also "diverges in many ways from ordinary speech, far more than the technical languages of most other professions." Such features, then, are both what distinguish legal English as a distinct variety of English and what can make it complex both for native and foreign speakers of English. Understanding these features in general can help with general understanding of legal texts as well as the specific features encountered in cybercrime legal texts.

Finnegan (2012, p. 483) notes that the language of the law actually refers to different areas: (a) language that comes from statutory law; (b) the interpretation of such law in judicial opinions; (c) various forms of courtroom language, including opening statements and closing arguments, direct examination and cross-examination of witnesses, and jury instructions; (d) written contracts that create legal obligations, including rental agreements, insurance policies, wills, and liability waivers. In the present handbook we can find examples especially of (a) and (d), but that does not mean that (b) and (c) are any less important when studying the language of the law and cybercrime. Therefore, users of this handbook are encouraged to consult all such documents in the field of cybercrime.

We will now briefly take a look at some of the defining features that characterize legal English. What exactly are these features and how can they be categorized? Firstly, the most striking feature of legal English is certainly in its different types of lexis that we can find in legal texts. To better understand the different types of lexis and the problems that this might create for learners, we can classify legal vocabulary on the basis of the following categories:

1. legal homonyms
2. technical legal lexis
3. legal Latinisms
4. jurisdiction-specific legal words (e.g. US, England and Wales, EU)
5. proper names
6. acronyms
7. jargon

Of all of these categories probably the first requires the most explanation. The concept of "legal homonyms" was first introduced by Tiersma (1999), who with it refers to the use of seemingly everyday words that have specific, and often very different, meanings in legal contexts. These are words that "ordinary people use in their ordinary non-technical and non-legal conversations" (Schauer, 2015, p. 36). Examples of such words include *contract*, *trust*, *complaint*, and *assault*, as the legal meanings of such words will not necessarily be fully explained in a non-specialized dictionary. Such words, in fact, often need to be understood on the basis of their specific (legal) context and even then if the speaker or listener does not completely understand how the legal system works, they still may not be understood especially by non-professionals. Take, for example, the latter word, *assault*, which in its general meaning means "physical attack" but in a specialized online law dictionary is defined as "an intentional act by one person that creates an apprehension in another of an imminent harmful or offensive contact; often *assault and battery*: the crime of threatening a person together with the act of making physical contact with them".2 And even with such specialized definitions, in a field such as cybercrime, which is constantly changing with the development of more sophisticated technologies (and the criminals that exploit them), official dictionaries cannot always keep up with the pace of change. We will see many such examples in the exercises that follow in this book.

The second category from the list above, technical legal lexis, refers to words which are generally only found in legal contexts. While many of these words and expressions are widely understood by the general public, such as, for example, *defendant*, *judge* and *jury*, many, or even most, of them, such as *beyond (a) reasonable doubt*, *commital*, *counsel*, *felon/felony*, or *wrongful imprisonment*, may not be immediately understood by non-experts (Tiersma, 1999, p. 121). These words are considered technical because they "are found exclusively in the legal sphere and have no application outside it" (Alcaraz Varo & Hughes, 2002, p. 16). Legal English is full of such terms, which vary according to the specific area of law that is being dealt with. The third category, legal Latinisms, needs no explanation other than the fact that English, and to an even greater extent US legal documents are full of Latin words and expressions, such as *certiorari*, *quo warranto*, and *subpoena*. The fourth category, jurisdiction-specific lexis is also important to consider, especially in an area such as cybercrime, which, as noted above by Tatyana Tropina in her introduction, “knows no borders”. As we shall see in the documents in the language exercises that follow although most of the documents are from EU sources, there are also many examples from the US and England and Wales. The fifth category, proper names, is also interesting but probably not the most salient category for the current discussion. Gibbons (2002) describes this category as those proper names which are used to refer to a specific legal concept (that is associated to a person), as, e.g., the American usage of *Miranda*, as in *Miranda warning*, which is related to the duty of a member of the police to inform any person taken into custody of their right to have legal advice and to remain silent while they are being questioned.

The last two categories in the list, acronyms and jargon are probably the most important for the current discussion as they are both widely encountered in cybercrime legal texts. First, short forms, acronyms or abbreviations are widely used in legal English (Gibbons, 2002) as well as in the area of cybercrime as we shall see in the exercises that follow. Some general legal examples include *TRO*, which is used as a short form of *Temporary Restraining Order* and *UCC* for *Uniform Commercial Code*. Goźdź-Roszkowski (2011, p. 55) notes that the use of such acronyms is beneficial for “efficient professional communication and the knowledge of such forms may mark membership to the specialist group of legal professionals.”

The final category is distinguished by slang or jargon terms, which are used by members of the legal profession to refer to a part of their work in some way. Some examples of legal jargon provided by Tiersma (1999, p. 107) include, e.g., *arguendo*, *black-letter law*, *chilling effect*, *grandfather clause*, or *judge shopping*.

In addition to such purely legal jargon terms, one of the defining characteristics of cybercrime texts is the wide use of computer-related technical jargon such as, to name just a few, *botnet*, *brute force attack*, *crimeware*, *cryptocurrency*, *cyberbullying*, *grooming*, *hacktivism*, *moneymule* and *phishing*.

All of the latter terms have been created in relatively recent times through various forms of word derivation and neologisms that are often based on other terms that already exist as part of so-called computer-mediated interaction and the language forms that are used therein (often called 'netspeak').

The frequency of such terms in cybercrime legal documents (as amply demonstrated in the language activities that follow and the glossary found at the end of the Handbook) means that there should probably be an eighth category of lexical items above called specific cybercrime terms.

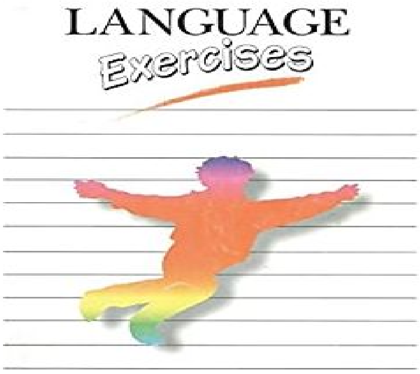
Before ending this short Introduction, it is important to recall briefly some of the other features typical of legal English, which, as we shall see, may or may not be found in the documents examined in this handbook depending on the type of document we encounter. First of all, we can find the use of multiword phrases, or complex function expressions such as *in pursuance of, in relation to*, during *the time that*, etc. Another oft-quoted feature of legal English is the use of binomials or trinomials, also called conjoined phrases, in which two similar words or ones with the same meaning are joined by a preposition, such as *devise and bequeath (*or *give, devise and bequeath*), *breaking and entering*, *acknowledge and confess*.

Although such expressions are quite common in legal documents such as contracts and wills, they are much less so in the type of documents we will be studying in this Handbook. One of the most noted grammatical peculiarities of legal English is the wide-spread use of modal verb *shall*, which differs from modern standard English usage. Rather than indicating the future, it is generally used as a command or obligation in legal documents or as a means of making a declaration, e.g. *This act shall be known as…* (Tiersma, 1999, p. 105). Another morphological feature of legal English are word pairs with the ending *–ee* and –*or*/*–er*, as in *lessee*, i.e. one who has been leased property, vs. *lessor*, i.e. one that lease property to somebody else. These endings clearly come from the (legal) French pairs. Legal experts, even today, are coining new words on this pattern, including *asylee, condemnee, detainee, expellee,* and *tippee*" (Tiersma, 2008, p. 11). Finally, written legal texts are almost always in the third person and very often impersonal, which is due to a number of different reasons. The first and second person pronouns such as *I*, *we*, and *you* are generally avoided due to the need to make legal documents applicable to a general audience and so that they address several different individual audiences at the same time (Tiersma, 1999, p. 67). In addition, the use of the third person gives an air of objectivity which is a desired for result for lawmakers and, for example, judges.

Finally, since many of the documents that serve as the basis for the linguistic activities that follow come from the European Union, it is important to point out a few of the most important features in EU discourse. First of all, as a legal system, EU law has a number of different origins that can best be described as a "hybrid, mixed law, in which the legal traditions of Europe increasingly intertwine" (Mattila, 2006, p. 108). The result of this hybridity, which mixes side by side elements of civil law and common law, has led to the creation of new terminology such as, e.g., *acquis communautaire* and the *principle of subsidiarity*, in order to express the original concepts of the EU. In the creation of new EU terminology "the aim is to avoid expression closely associated with the content of the legal order of any one Member State. This goal of neutrality sometimes results in the creation of somewhat complicated terms, or use of circumlocution" (Mattila, 2006, p. 118). Within EU legal language we can often find generic terms that are used in a specialized meaning, as for example *Union*, *Community*, *Council*, and *Court of Justice*. Furthermore, many (but not all) EU texts are characterized by the high frequency of a number of different features, which may include: (a) impersonalization, i.e. the use of the subject *it* and the absence of a subject; (b) negative constructions, which is often unnecessary; (c) standardized formulas for documents such as directives including a citation formula (often using the form *Having regard to*) and recital (general motivations on which the legal act is grounded); (d) nominalization, i.e. the use of nouns instead of verbs to express actions (*promotion*, *development*); (e) complex syntactic structure with widespread coordination and subordination. Such features can be found to varying degrees in a number of different EU documents, or genres, including **regulations** (the strongest act which is directly applicable in its entirety); **decisions** (an instrument which is focused at a particular person/group and is directly applicable); **recommendations and opinions** (which are non-binding declarations); **written declarations** (a document proposed by up to five MEPs on a matter within the EU's activities used to launch a debate on that subject), as well as **speeches/statements**, **codes of conduct/rules of procedure**, **presidency conclusions**, **Community Action Plans** and **reports** (Wodak and Weiss, 2005). Many of these genre types are reproduced in Chapter 2 of the Handbook.

While this short introduction has summarized a number of features of legal English and the language of cybercrime, it is by no means exhaustive. As you do the activities in this Handbook you should try to pay careful attention to the features that each document exhibits: were the features exhibited in the texts mentioned in these few pages or are there other salient features in the text that should be mentioned? In the next section, you will find a number of different activities dealing with the definition of cybercrime. These activities, as well as those that are found in Chapter 2 and Chapter 3 are aimed at improving your knowledge of English grammar and vocabulary, both in legal and in general contexts. They also should help you to improve your reading and listening skills. As you are doing the activities make sure that you look up any words that you do not know either in the Glossary at the end of the book or in a dictionary.

LANGUAGE EXCERCISES



I. DEFINITION OF CYBERCRIME

Read the different definitions of cybercrime below and do the following:

1. Choose the definition of cybercrime that you agree most with (A-H).

2. Give one reason for each of the other definitions that has made you decide they are not the best.

3. Three of these definitions come from official bodies, agencies or institutions. Can you spot them? What tricks can you use to spot "normative" definitions? In order to help you, here are a few of the typical features of formal language:

- It avoids conversational/idiomatic/colloquial expressions.

- It doesn't use contractions (don't, can't. etc.).

- It normally involves longer words or words with origins in Latin and Greek.

- It tends to place adverbs within the verb ('A solution can *then* be found' rather than

'*Then* a solution can be found')

- It doesn't use ellipsis (omission of elements; for instance, 'I saw Mary and I have a lot of things to tell you' rather than 'I saw Mary, lots to tell you')

A. Any criminal act that has to do with computers and networks; it also includes traditional crimes conducted through the Internet.

B. Any crime that is committed using a computer network or a hardware device.

C. Sophisticated attacks against computer hardware and software.

D. Any crime that involves a computer and a network.

E. Criminal acts that are committed online by using electronic communications networks and information systems.

F. Crimes which are directed at computers or other devices (for example, hacking), and where computers or other devices are integral to the offence.

G. Using a computer as an instrument for illegal ends, such as committing fraud, trafficking in child pornography and/or intellectual property, stealing people's identity, or violating privacy.

H. The violation of laws involving a computer or a network.

II LEGAL 'DEFINITIONS' OF CYBERCRIME

Read the text below and decide if the statements below (1-5) are true or false (T/F) with reference to the text. Remember that 'definitions' of cybercrime mostly depend upon the purpose of using the term.

A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime.

Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term.

Certain definitions are required for the core of cybercrime acts. However, a 'definition' of cybercrime is not as relevant for other purposes, such as defining the scope of specialised investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime' construct.

Statements:

1. The core of cybercrimes refers to a list of expressly defined crimes. T/F

2. Computer-related acts only fall within the scope of cybercrime if they result in causing personal harm. T/F

3. It is quite difficult to define acts that constitute cybercrimes. T/F

4. Without defining the individual cybercrimes precisely the scope of investigative powers cannot be specified. T/F

5. The core focus of the investigative and international cooperation powers is discovery of specific evidence of any criminal offence as such. T/F

III. WHAT IS CYBERCRIME

a) PART I: Collocations

Look at the pairs of words (Adjective + noun collocations) below and check if you know their meanings. Translate these expressions.

Remember that in English nouns are often used as adjectives, as e.g. "bank accounts". Then read the text below and complete the gaps with the correct collocations from the list. Remember to look for clues in the grammar to help you (e.g. singular and plural verb forms).

bank accounts	*sexual abuse*	*Framework Decision*
communications services	*child pornography*	*legislative actions*
information systems	*criminal sanctions*	*operational cooperation*
terrorist acts	*criminal acts*	

What is cybercrime?

Cybercrime consists of (A) ________________ ________________ that are committed online by using electronic communications networks and (B) ________________ ________________. It is a borderless problem that can be classified in three broad definitions: Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' (C) ________________ ________________).

• Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.

• Illegal online content, including child (D) ________________ ________________ material, incitement to racial hatred, incitement to (E) ________________ ________________ and glorification of violence, terrorism, racism and xenophobia.

EU response to Cybercrime

In order to combat cybercrime, the EU has implemented legislation and supported (F) ________________

________________, as part of the ongoing EU Cybersecurity Strategy.

Legislative Actions

Several EU (G) ________________ ________________ contribute to the fight against cybercrime. These include: • 2013 – A Directive on attacks against information systems, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher (H) ________________ ________________;

• 2011 – A Directive on combating the sexual exploitation of children online and (I) ________________ ________________, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse) 2002 – ePrivacy Directive, whereby providers of electronic (J) ________________ ________________ must ensure the security of their services and maintain the confidentiality of client information;

• 2001 – (K) ________________ ________________ on combating fraud and counterfeiting of non-cash means of payment, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences.

Reread the text in part b) and look at the specific cybercrime vocabulary. Do you understand their meanings? Are the meanings already provided in the text? If not, look them up in the glossary and review.

b) PART II: Verb Review

In this short activity you will review your knowledge of the verb tenses in English. Before we begin match the verb examples in the left column (1-6) with the tenses on the right (a-f). Write in the small letter in the boxes.

Example	*Answer*	*Tense*
1. this has been started		*a. present simple active*
2. they play a role		*b. past simple active*
3. it was launched		*c. present simple passive*
4. other people are involved		*d. past simple passive*
5. they acted immediately		*e. present perfect active*
6. he has finished		*f. present perfect passive*

Now complete the gaps in the second part of the text with the correct form of the following verbs. Please note that there is one extra verb that should not be used. Use the following tenses only once: present simple active, past simple active, present perfect active, present simple passive and past simple passive:

act	*finish*	*involve*
launch	*play*	*start*

EUROPEAN CYBERCRIME CENTRE (EC3)

The European Commission (A) ________________ a key role in the development of EC3, which (B)________________ operations in January 2013. EC3 (C) ________________as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary.

Working Together

- Global Alliance against Child Sexual Abuse Online: The Alliance (D) ________________ on 5 December 2012 and is a joint initiative by the EU and the US, gathering 54 countries from around the world to fight together Child Sexual Abuse.

- ENISA: The European Network and Information Security Agency (E) ________________ in supporting exchanges of good practices between EU States.

c) PART III: General framework for the types of crime

Read the text below and fill in the gaps with the letter or the missing phrases or words provided below:

a) measures to counteract cybercrime
b) minimum rules concerning definitions of criminal offences
c) legislative level
d) Information Security Agency
e) an ever- increasing threat
f) profit-driven cybercrime
g) operational level
h) combating the sexual abuse
i) EU approach to cyber-security
j) attacks against information systems

The EU has set out its approach against cybercrime with actions developed at strategic, legislative and operational levels.

At strategic level, the 2009 Stockholm Programme includes a number of (1) _________________.

Europol’s 2013 Serious and Organised Crime Threat Assessment (SOCTA) considers cybercrime to be (2)_____________________ to the EU in the form of large-scale data breaches, online fraud and child sexual exploitation, while (3)____________________ is becoming an enabler for other types of criminal activity.

At (4)____________________ , the creation of the European Network and (5)______________ (ENISA) in 2004 was followed more recently by the creation of the European Cybercrime Centre (EC3). Hosted by Europol, EC3 is intended to become the main point in the EU's fight against cybercrime, by supporting Member States and the European Union's institutions. I

The "Cyber-attacks" Directive

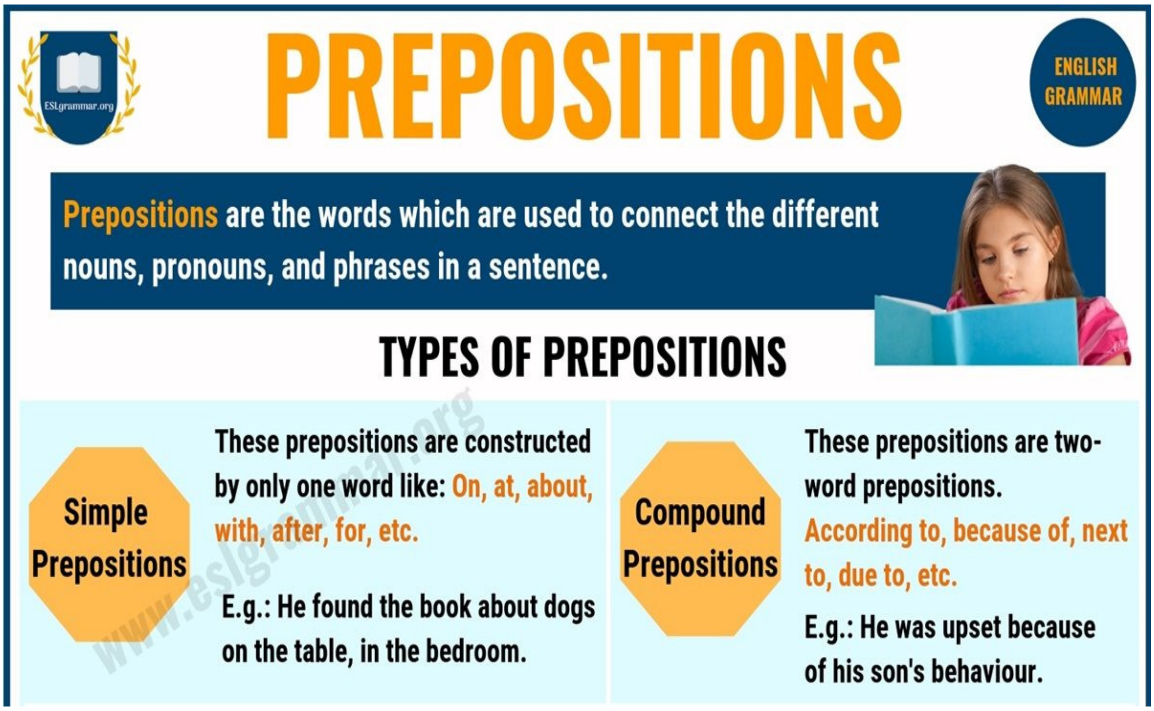
At (6) ____________________ , several measures against cybercrime have been adopted, such as the 2011 Directive on (7) ____________________ and sexual exploitation of children and child pornography.

Particularly relevant is the 2013 Directive on (8)____________________ , which replaces a 2005 Council Framework Decision and had to be transposed before 4 September 2015. This Directive sets out (9) ____________________ in this field and sanctions for those found guilty of them.

Now write the following grammatical explanations next to the words taken from the reading above with the part of speech and explanation:

1. to counteract	***A. a form of a verb that depending on where it stands in the sentence may be used as either an adjective or a noun, in this context it is used as a noun***
2. ever-increasing	***B. adjective formed by joining an adverb and an adjective***
3. profit-driven	***C. verb***
4. combating	***D. adjective formed by joining a noun and an adjective***
5. cyber-security	***E. a noun formed by joining an adjective and a noun***

d) PART IV: Prepositions and grammar



PREPOSITIONS

ENGLISH GRAMMAR

Prepositions are the words which are used to connect the different nouns, pronouns, and phrases in a sentence.

TYPES OF PREPOSITIONS

Simple Prepositions

These prepositions are constructed by only one word like: On, at, about, with, after, for, etc.

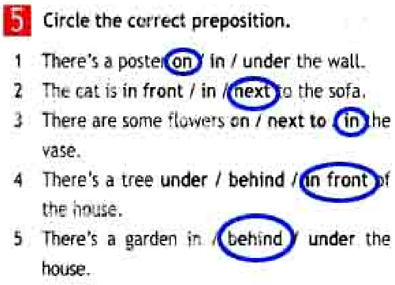
E.g.: He found the book about dogs on the table, in the bedroom.

Compound Prepositions

These prepositions are two-word prepositions. According to, because of, next to, due to, etc.

E.g.: He was upset because of his son's behaviour.

Read the continuation of the text from (c) Part III and circle the correct preposition to complete the sentences.



5 Circle the correct preposition.

1 There's a poster [✓ on] / in / under the wall.
2 The cat is in front / in / [✓ next] to the sofa.
3 There are some flowers on / next to / [✓ in] the vase.
4 There's a tree under / behind / [✓ in front] of the house.
5 There's a garden in / [✓ behind] / under the house.

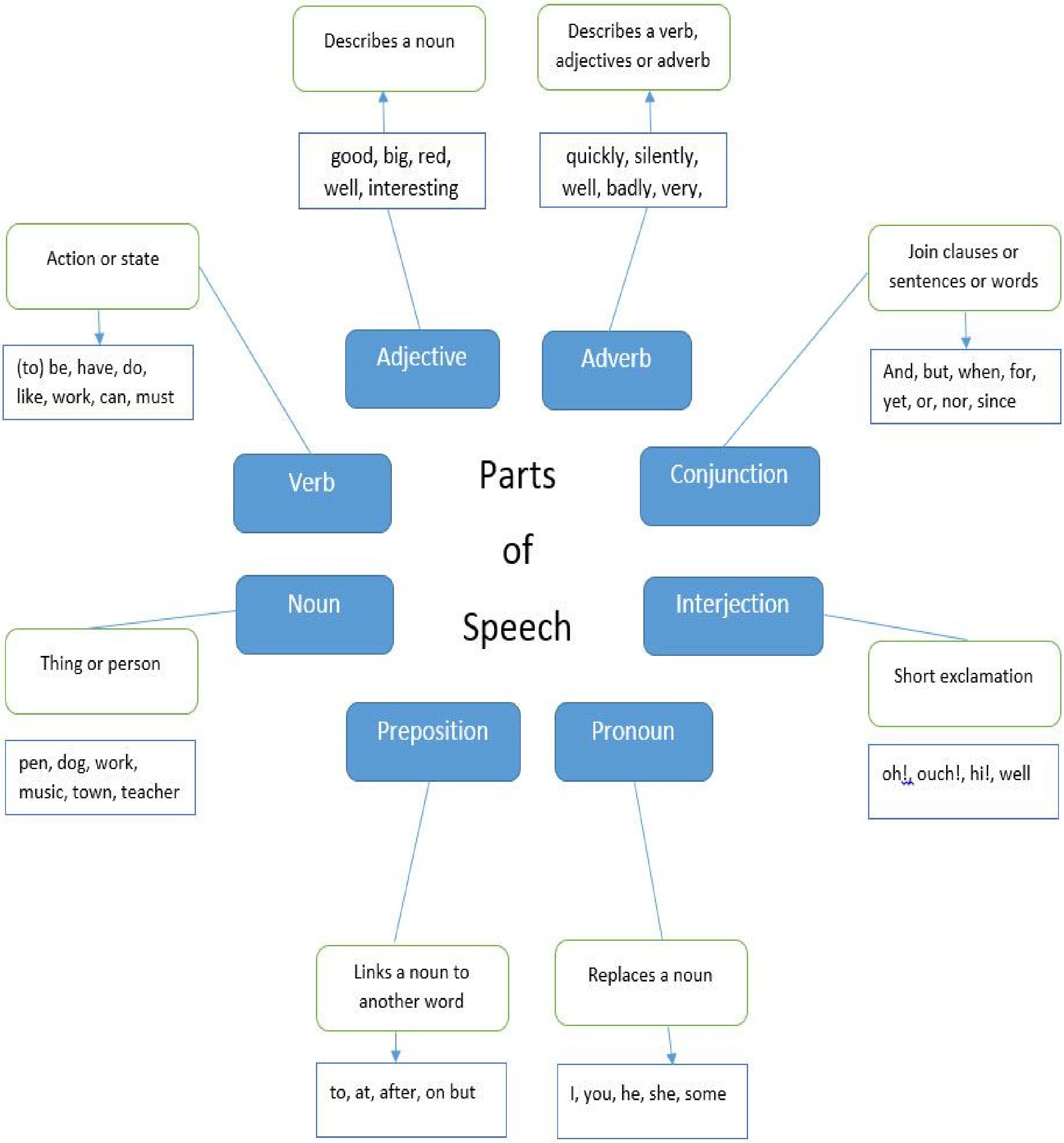
The main crimes defined in the Directive are illegal access **into / to / for** information systems, illegal interference systems or data, and illegal interception **of / to / for** data transmissions.

In / **With / For** particular, stricter criminal sanctions are required **for / to / by** so-called “botnet” attacks, in which a large number of computers is infected **by / to / in** order to control them remotely, performing tasks automatically without users’ knowledge. Large-scale cyber-attacks can thus spread rapidly **by / over / upon** the internet. Penalties can also be imposed on legal persons, such as companies, **for /to / in** case of criminal acts **from / by / for** which they benefit.

The Directive, however, aims to take a balanced approach so as to prevent possible over-criminalisation.

Bonus question: look at the examples below from the text and decide which parts of speech the words (marked in bold) represent. If you have any doubts about the parts of speech you can look at the chart below the examples:

- illegal interception **of** data transmissions
- in which a large number of computers is infected **in** order **to** control them remotely
- **thus** spread rapidly
- aims **to** take a balanced approach


Parts of Speech
Adjective
Describes a noun
good, big, red, well, interesting
Adverb
Describes a verb, adjectives or adverb
quickly, silently, well, badly, very,
Verb
Action or state
(to) be, have, do, like, work, can, must
Conjunction
Join clauses or sentences or words
And, but, when, for, yet, or, nor, since
Noun
Thing or person
pen, dog, work, music, town, teacher
Interjection
Short exclamation
oh!, ouch!, hi!, well
Preposition
Links a noun to another word
to, at, after, on but
Pronoun
Replaces a noun
I, you, he, she, some

IV. EUROPOL ON CYBERCRIME

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

a) PART I: Verbs

Read the text below which has been taken from the EUROPOL website and complete the gaps with the correct form of the verbs provided in square brackets. Look for clues in the text to help you decide which tense to use. Remember to check if the form should be an active verb (such as *generate***) or a passive one (***is/are generated***). *Please note that alternative verb forms are provided in parentheses.***

***The first one has been done for you*:**

Cybercrime is an EMPACT[10] priority for the policy cycle from 2013 to 2017: the aim is to combat cybercrimes that (A) *are committed (have been committed)* [***commit***] by organised crime groups and that (B) ____________________ [***generate***] large profits from such activities as online and payment card fraud, cybercrimes that cause serious harm to their victims such as child sexual exploitation, and cyberattacks, which (C) ____________________ [***affect***] critical infrastructure and information systems in the EU.

Technical innovation (D) can ____________________ [***harness***] for social good, but just as readily for nefarious[11] ends. This is truer of cybercrime than of perhaps any other crime area. And cybercriminals (E)___________________ [***get, also***] more aggressive. That's why Europol and its partner organisations (F)___________________ [***take***] the fight to them on all fronts.

According to the most recent Internet Organised Crime Threat Assessment (IOCTA), cybercrime (G)___________________ [***become***] more aggressive and confrontational. This (H) can ___________________ [***see***] across the various forms of cybercrime, including high-tech crimes, data breaches and sexual extortion.

Cybercrime is a growing problem for countries, such as EU Member States, in most of which internet infrastructure is well developed and payment systems are online. But it is not just financial data, but data more generally, that is a key target for cybercriminals. The number and frequency of data breaches are on the rise, and this in turn (I) ___________________ [***lead***] to more cases of fraud and extortion.

The sheer range of opportunities that cybercriminals (J) ___________________ [***seek***] to exploit is impressive. These crimes include:

• using botnets—networks of devices infected with malware without their users' knowledge— to transmit viruses that (K) ___________________ [***gain***] illicit remote control of the devices, steal passwords and disable antivirus protection;

• creating "back doors" on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets;

• creating online fora to trade hacking expertise;

• bulletproof hosting and creating counter-anti-virus services;

• laundering traditional and virtual currencies;

committing online fraud, such as through online payment systems, carding and social engineering;

• various forms of online child sexual exploitation, including the distribution online of child sex-abuse materials and the live-streaming of child sexual abuse

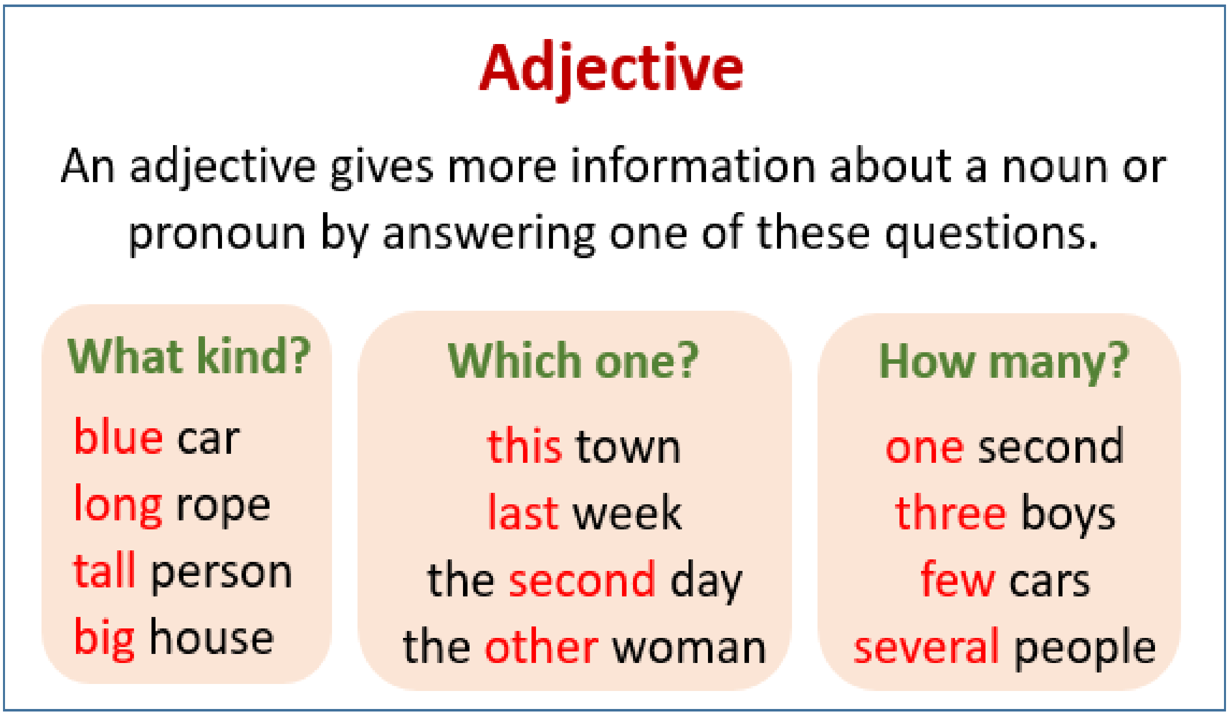
• the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services.

High-tech crimes

Malware, or malicious software, (L) __________________ [***infiltrate***] and (M) __________________ [***gain***] control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware, and they (N) *can* __________________ [***complement***] each other when performing an attack.

Reread the text in part a) and look at the underlined words. Do you understand their meanings? Are the meanings already provided in the text? If not, look them up.

b) PART II: Adjectives



Adjective

An adjective gives more information about a noun or pronoun by answering one of these questions.

What kind?	Which one?	How many?
blue car	this town	one second
long rope	last week	three boys
tall person	the second day	few cars
big house	the other woman	several people

Read the rest of the text from EUROPOL and complete the gaps with the correct adjectives from the list below. Make sure you know the meanings of the adjectives before you begin:

law	*intelligence-led*	*compromised*
notable	*large-scale*	*institutional*
joint	*innovative*	*cross-border*

The response: pursuing cybercriminals on all fronts

With such a range of activities being pursued with such inventiveness, the response of Europol and its partners must itself be comprehensive, dynamic and relentlessly (A) _______________. And it is. First, there's the (B) _______________ response. In 2013 Europol set up the European Cybercrime Centre (EC3) to bolster the response of (C) _______________ enforcement to cybercrime in the EU and help protect European citizens, businesses and governments.

Each year the EC3 issues the aforementioned Internet Organised Crime Threat Assessment (IOCTA), which sets priorities for the EMPACT Operational Action Plan in the areas of cybercrime that are the focus for that year.

The EC3 also hosts the Joint Cybercrime Action Taskforce (J-CAT). Its mission is to drive (D) _______________, coordinated action against key cybercrime threats through (E) _______________ investigations and operations by its partners.

These institutional arrangements have led to (F) _______________ successes at the operational level, including:

- the coordination of a (G) _______________ operation, including private-sector partners to target a botnet, Ramnit, that had infected millions of computers around the world;
- coordination with Eurojust in an operation targeting (H) _______________ malware attacks that originated in Ukraine and that were being investigated by a number of agencies — an operation that led to tens of arrests and continues to supply evidence that supports other cybercrime investigations;
- an operation targeting a major cybercriminal forum engaged in trading hacking expertise, malware and botnets, Zero Day Exploits, access to (I) _______________ servers, and matching partners for spam campaigns and malware attacks.

c) PART III: Vocabulary (Definitions)

Look at the words below. Do you know their meanings? Complete the gaps in the last part of the reading from Europol with one of the words from the list below starting with the ones you already know.

file infector	*infected code*
rootkit	*scareware*
remote-access trojan	*adware*
privileged access	*botnet*
trojan	*pop-ups*
Ransomware	*spyware*
distributed denial-of-service	*security threats*

• A (A) ___________________ (short for robot network) is made up of computers communicating with each other over the internet. A command and control centre uses them to send spam, mount (B) ___________________ (DDoS) attacks (see below) and commit other crimes.

• A (C) ___________________ is a collection of programmes that enable administrator-level access to a computer or computer network, thus allowing the attacker to gain root or (D) ______________ ___________ to the computer and possibly other machines on the same network.

• A worm replicates itself over a computer network and performs malicious actions without guidance. • A (E) ___________________poses as, or is embedded within, a legitimate programme, but it is designed for malicious purposes, such as spying, stealing data, deleting files, expanding a botnet, and performing DDoS attacks.

A (F) ___________________ infects executable files (such as .exe) by overwriting them or inserting (G) ___________________ that disables them.

• A backdoor/(H) ____________________ (RAT) accesses a computer system or mobile device remotely.

It can be installed by another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions, including:

monitoring actions

executing commands

sending files and documents back to the attacker

logging keystrokes

taking screen shots

• (I) ____________________ stops users from accessing their devices and demands that they pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.

• (J) ____________________ is fake anti-virus software that pretends to scan and find malware/ (K)____________________ on a user's device so that they will pay to have it removed.

• (L) ____________________is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party • (M) ____________________displays advertising banners or (N) ____________________ that include code to track the user's behaviour on the internet

V. ABBREVIATIONS

As in many genres of legal English the use of abbreviations is common in the language of cybercrime.

Look at the examples below and try to complete the missing words or letters (small spaces) in parentheses. Translate them.

1. AS (A _ _ _ _ s Server)

2. ATM (A____________ T___________Machine)

3. BT (B _ _ _ _ _ _ th)

4. BW (Band _ _ _ _ _)

5. CERT (Computer E__________R____________ Team)

6. CNP Transaction (C _ _ _ Not Present Transaction)

7. CPS (C_____________s per Second)

8. CSP (C _ _ _ _ Service Provider)

9. CSV (C _ _ _ _ -separated values)

10. DBMS (D _ _ _ _ _ _ e M___________ ment System)

11. DL (D _ _ _ _ _ ad)

12. DNS (D _ _ _ _ n Name System)

13. EFS (En _ _ _ _ _ ing File System)

15. FAQs (F____________ A_________ Q__________)

15. FxP (F _ _ _ Exchange P _ _ _ _ _ ol)

16. GB (________________)

17. IP (I___________ Protocol)

18. IS (I______________ Systems)

19. ISP (I__________ S__________ Provider)

20. IT (I___________ T____________)

21. LCD (L _ _ _ _ d C _ _ _ _ _ _ Display)

22. MB (________________)

23. MS (M _ _ _ _ _ Stick)

24. NFS (Network F _ _ _ System)

25. ODBC (O _ _ _ D _ _ _ _ _ se Connectivity)

26. OLTP (Online T_____________n Processing)

27. OS (O______________ System)

28. PDF (P _ _ _ _ _ le D _ _ _ _ _ nt Format)

29. RAS (R _ _ _ _ _ A _ _ _ _ _ Service)

30. RAM (R _ _ _ _ m A _ _ _ _ _ Memory)

31. RAT (R _ _ _ _ e Administration T _ _ l)

32. RC (R _ _ _ _ n Code)

33. ROM (R _ _ _ O _ _ _ Memory)

34. SMTP (S _ _ _ _ _ Mail T _ _ _ _ _ _ r Protocol)

35. SSD (Software Spe____________ Document)

36. TB (_______________)

37. URL (U ____________ Resource L _ _ _ tor)

38. VGA (Video Graphics Adapter)

39. VR (V___________ Reality)

40. WAN (W _ _ _ Area N _ _ _ _ _ k)

41. WAP (W _________ Access P _________)

42. WiFi (W___________ F _ _ _ _ _ _ y)

43. WLAN (W___________ L _ _ _ _ Area N______________)

44. WWW (________________________)

VI. BASIC CRIMINAL LAW VOCABULARY

Complete the following sentences with the verbs in italics, with the appropriate verb form. Once you have done so, rearrange the sentences so that they reflect the chronological order in which the events took place.

arrest	*acquit*	*charge*
convict	*find*	*interrogate*
plead	*quash*	*seize*
sentence	*try*	

1. He was _____________ to an eight-month juvenile term.

2. He was finally ____________ with criminal damage, but at the initial hearing, he _____________not guilty.

3. On appeal, the conviction was __________________.

4. Once at the police station, he was ___________ in the presence of counsel, but refused to answer most of the questions.

5. The conviction was quite surprising to him, since he expected to be _______________.

6. The judge ________ him guilty, although in most jurisdictions a jury would probably have not __________ him.

7. The judge who was __________ the case ________ most of the evidence presented by the prosecution.

8. The youth was __________ at his home, where computer equipment was _________ containing evidence of his illegally tampering with websites.

VII. HACKERS, HACKTIVISTS AND CYBERCRIMINALS

a) PART I: Definitions

Provide two features for the terms.

1. Hacker.

Feature 1:

Feature 2:

2. Hacktivist.

Feature 1:

Feature 2:

3. Cracker.

Feature 1:

Feature 2:

4. Cybercriminal.

Feature 1:

Feature 2:

5. Cyberterrorist.

Feature 1:

Feature 2:

Now read the following definitions and decide whether you agree with them or not. Write down the reasons. Then answer questions 6 and 7.

1. A **hacker** seeks and exploits weaknesses in a computer system or network. They may be acting for many reasons, such as profit, protest, fun or even to evaluate weaknesses and to assist in removing them.

Reasons to agree or to disagree:

2. A **hacktivist** hacks computer networks and systems as a form of political protest.

Reasons to agree or to disagree:

3. A **cracker** breaks into a computer system or network with no authorisation and with the intention of doing damage. Among the damage they can cause is the following: destruction of files, theft of personal information (credit card numbers, client data, etc.), virus infection of systems, etc.

Reasons to agree or to disagree:

4. A **cybercriminal** commits cybercrimes using computers either as a tool, as a target or as both.

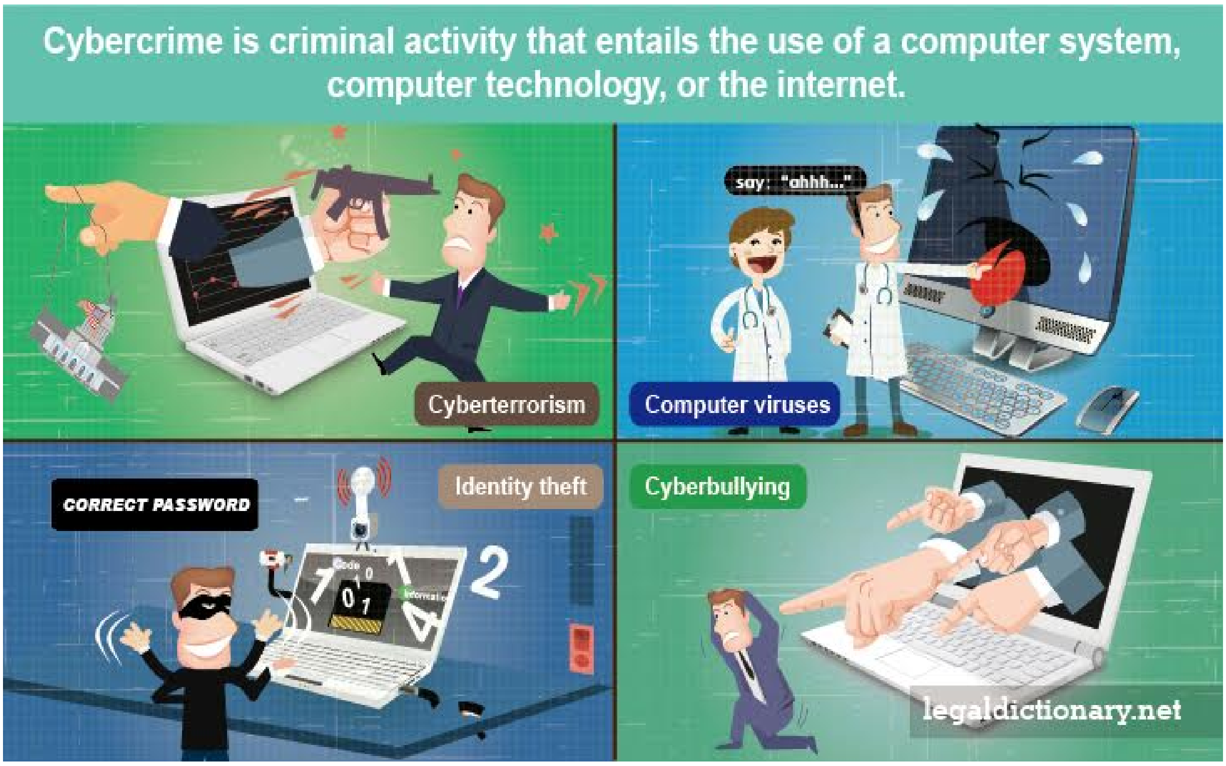
Reasons to agree or to disagree:

5. A **cyberterrorist** executes deliberate attacks and disruptions of computer networks using any means (computer viruses, malware, etc.) to attack individuals, agencies, governments, bodies or organizations.

Reasons to agree or to disagree:

6. Why do you think that people generally use the term “hacker” when they mean “cracker”?

7. What is, in your opinion, the difference between cybercriminals and cyberterrorists?



Cybercrime is criminal activity that entails the use of a computer system, computer technology, or the internet.

UNIT II

CYBERCRIME: REGULATIONS, DIRECTIVES & ORGANIZATIONS

LANGUAGE EXERCISES

I. THE INTERNET ORGANISED CRIME THREAT ASSESSMENT

Read the text and then fill in the numbered gaps with the missing word (a-c) from the list below.

The 2015 Internet Organised Crime Threat Assessment (IOCTA), the (1) ______ presentation of the cybercrime (2) ______ landscape by Europol's European Cybercrime Centre (EC3), covers the key developments, changes and emerging threats in the field of cybercrime for the period under consideration.

It offers a view predominantly from a law (3) ______ perspective, highlighting a number of operational successes, and is based on contributions by EU Member States and the expert input of Europol staff, which has been further enhanced and (4) ______ with input from private industry, the financial sector and academia.

The assessment highlights important developments in several areas of online crime:

• Cybercrime is becoming more (5) ______ and confrontational, suggesting changes in the profile of cybercrime offenders and increasing the psychological impact on victims.

• Malware, particularly (6) ______, remains a key threat for private citizens and businesses both in terms of quantity and impact.

• The lack of digital (7) ______ and security awareness contributes to the long lifecycle of exploit kits using well-known attack vectors but also provides new attack vectors as the number of devices in the Internet of Things grows.

• Growing Internet coverage in developing countries and the development of (8) ______ streaming solutions providing a high degree of anonymity to the viewer, are furthering the trend in the commercial live streaming of child sexual abuse.

• The use of anonymisation and encryption technologies is (9) ______. Attackers and abusers use these to protect their identities, communications, data and payment methods.

The report identifies a number of key recommendations to address these developments:

• The continuation of close law enforcement cooperation in (10) ______ the key criminal networks and criminal (11) ______ for cybercrime with a special focus on cross (12) ______ crime enablers such as bulletproof (13) ______ and laundering services.

• Law enforcement should seek to actively engage in and share the success of multi-stakeholder initiatives such as Europol’s Airline Action Days and E-commerce initiative.

• Adequate resources should be given to prevention strategies to raise (14) ______ of cybercrime and increase standards in online safety and information security.

• Law enforcement requires the tools, training and resources to effectively investigate complex cybercrime cases and the underlying criminal structures as well as to deal with (15) ______ crime.

• It is essential for law enforcement to build and develop working relationships with EU and non-EU partners in law enforcement, private industry and academia, and to promote the lawful exchange of information and intelligence in relation to criminal activity.

• In collaboration with the private sector and academia, law enforcement needs to explore (16) ______ and research opportunities related to emerging technologies such as decentralised marketplaces, artificial intelligence and (17) ______ technology.

(1) a) annual b) weekly c) currently

(2) a) trial b) jeopardy c) threat

(3) a) agency b) enforcement c) academy

(4) a) mixed b) confused c) combined

(5) a) aggressive b) aggression c) aggravate

(6) a) ransomware b) hacking c) viruses

(7) a) safeness b) hygiene c) scanning

(8) a) frequent b) pay-as-you-go c) legal

(9) a) wild b) wideness c) widening

(10) a) targeting b) focusing c) aiming

(11) a) helpers b) facilitators c) criminals

(12) a) cutting b) words c) dressing

(13) a) hacking b) scamming c) hosting

(14) a) awareness b) quality c) knowledge

(15) a) perfect b) high-volume c) high-quality

(16) a) investigative b) persuasive c) judicial

(17) a) modernised b) internet c) blockchain

Now underline any expressions you are unfamiliar with or have difficulty using or understanding and look them up in a dictionary.

EXPRESSION	DEFINITION

II. ACRONYMS AND ABBREVIATIONS

In the following activities you will review your knowledge of acronyms and abbreviations used in IOCTA,

organizations and authorities, and telecommunications. Write the letter next to the abbreviation.

a) PART I: IOCTA general abbreviations

1	APT	a) Internet service provider
2	APWG	b) European Money Mule Actions
3	AVC	c) Crime Abuse Material
4	CaaS	d) European Malaware Analysis System
5	CAM	e) Critical Infrastructure
6	CI	f) Advanced Persistent Threat
7	CVV	g) Domain Name System

8	DNS	h) Card Verification Value
9	EMAS	i)Crime-as-a-Service
10	EMMA	j) Anti-Phishing Working Group
11	IIP	k) Internet Protocol
12	ISP	l) Automated Vending Card
13	IP	m) Organised crime group
14	OCG	n) Invisible Internet Project

b) PART II: Organizations and authorities

1	CERT	a) European Cybercrime Centre
2	J-CAT	b) Serious and Organised Crime Threat Assessment
3	ENISA	c) Supervisory control and data acquisition systems
4	EC3	d) European Union Agency for Network and Information Security
5	EAST	e) Computer emergency response team
6	SCADA	f) Society for Worldwide Interbank Financial
7	SIENA	g) Computer Security Incident Response Team
8	SOCTA	h) Secure Information Exchange Network Application
9	SWIFT	i) European Association for Secure Transactions
10	CSIRT	j) Joint Cybercrime Action Taskforce

c) PART III: Telecommunications

1	THB	a) Transaction Authentication Number
2	Tor	b) Trafficking in human beings
3	URL	c) The Onion Router
4	TAN	d) Virtual private network
5	VoIP	e) Uniform resource locator
6	VPN	f) Voice-over-Internet Protocol

III. DIRECTIVE 2013/40 EU: VOCABULARY IN CONTEXT

Read the excerpts from Directive 2013/40/EU and choose the best word or expressions to complete the gaps.

DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/ JHA [Excerpts]

ARTICLE 1

Subject matter

This Directive establishes minimum rules concerning the definition of **(1)** ________________ _______________ and **(2)** _____________ in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between **(3)** _____________ and other competent authorities.

1	a. penal offences	b. criminal offenses	c. criminal offences
2	a. punishments	b. sanctions	c. sentences
3	a. judicial	b. judiciary	c. juridical

ARTICLE 3

Illegal access to information systems

Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is **(4)** ____________ as a criminal offence where committed by infringing a security measure, at least for cases which are not **(5)** ____________.

4	a. actionable	b. punishable	c. condemnable
5	a. lesser	b. petty	c. minor

ARTICLE 4

Illegal system interference

Member States shall take the necessary measures to ensure that seriously **(6)** ______________________ or interrupting the functioning of an information system by **(7)** ______________________ computer data, by transmitting, damaging, **(8)** ______________________, deteriorating, **(9)** ______________________ or suppressing such data, or by rendering such data **(10)** ____________________, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

1	a. hindering	b. bothering	c. interfering
2	a. inserting	b. inputting	c. implanting
3	a. wiping out	b. rubbing out	c. deleting
4	a. transforming	b. altering	c. amending
5	a. inaccessible	b. unattainable	c. unreachable

ARTICLE 6

Illegal interception

Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or **(11)** __________________ an information system, including electromagnetic **(12)** __________________ from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

11	a. at	b. in	c. within
12	a. emanations	b. emissions	c. issues

ARTICLE 7

Tools used for committing offences

Member States shall take the necessary measures to ensure that the intentional production, sale, **(13)** _________________ for use, import, distribution or **(14)** __________________ making available, of one of the following tools, without right and with the intention that it **(15)** _________________ used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, **(16)** _______________ code, or similar data (…).

13	a. procurement	b. appropriation	c. gain
14	a. contrariwise	b. likewise	c. otherwise
15	a. is	b. should be	c. be
16	a. access	b. accession	c. acceding

ARTICLE 8

Incitement, (**17**) ________________________ and attempt

1. Member States shall ensure that the incitement, or **(17bis)** ______________________, to commit an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

17	a. helping and abetting	b. aiding and abetting	c. assisting and abetting
17bis)	a. helping and abetting	b. aiding and abetting	c. assisting and abetting

ARTICLE 9

Penalties

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, **(18)** __________________ and dissuasive criminal penalties.

(18) a. proportionate b. equal c. proportional 4. Member States shall take the necessary measures to **(19)** ______________ that offences referred to in Articles 4 and 5 are punishable by a maximum **(20)** ______________________ of at least five years where:

(a) they are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;

(b) they cause **(21)** ____________________ damage; or;

(c) they are committed against a critical infrastructure information system.

19	a. insure	b. ensure	c. guarantee
20	a. term of imprisonment	b. period of imprisonment	c. time of imprisonment
21	a. grave	b. severe	c. serious

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by **(22)** _____________ the personal data of another person, with the aim of gaining the trust of a third party, thereby causing **(23)** ______________ to the rightful identity owner, this may, in accordance with national law, be regarded as **(24)** ________________ circumstances, unless those circumstances are already covered by another offence, punishable under national law.

(22) **a.** misusing **b.** misapplying **c.** maltreating
(23) **a.** bias **b.** perjudice **c.** prejudice
(24) **a.** worsening **b.** aggravating **c.** exacerbating

ARTICLE 10

(25) _________________ of legal persons

2. Member States shall take the necessary measures to ensure that legal **(26)** _____________ can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has allowed the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. The liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against **(27)** _____________ persons who are perpetrators or **(28)** _______________ of, or **(29)** _________ to, any of the offences referred to in Articles 3 to 8.

(25) **a**. responsibility **b**. liability **c.** accountability
(26) **a**. persons **b**. people **c**. individuals
(27) **a**. plain **b**. physical **c**. natural
(28) **a**. inciters **b**. incitors **c**. insitors
(29) **a.** accessories **b**. accomplices **c.** ancillaries

ARTICLE 11

Sanctions against legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(1) is punishable by effective, proportionate and **(30)** ________________ sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, such as:

(a) exclusion from **(31)** ___________ to public **(32)** ____________ or aid;

(b) temporary or permanent **(33)** __________ from the practice of commercial activities;

(c) placing under judicial supervision;

(d) judicial **(34)** _______________;

(e) temporary or permanent **(35)** _____________ of establishments which have been used for

committing the offence.

(30) **a**. dissuasory **b**. dissuasive **c**. dissuatorial
(31) **a**. entitlement **b**. accreditation **c**. allowance
(32**) a**. reliefs **b**. profits **c**. benefits
(33) **a**. disqualification **b**. inqualification **c**. unqualification
(34) **a.** winding-up **b**. up-winding **c**. wind-up
(35) **a**. shutting **b**. closure **c**. cessation

ARTICLE 12

Jurisdiction

2. When **(36)** ______________ jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where:

(a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system **(37)** _____________ its territory; or

(b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish jurisdiction **(38)** _____________ an offence referred to in Articles 3 to 8 committed outside its territory, including where:

(a) the offender has his or her **(39)** ______________ residence in its territory; or

(b) the offence is committed for the **(40)** ______________ of a legal person established in its territory.

(36) **a**. determining **b.** setting up **c**. establishing
(37) **a**. at **b**. on c. in
(38) **a**. over **b**. in **c**. for
(39) **a**. regular **b**. habitual **c**. usual
(40) **a**. benefit **b**. profit **c**. gain

IV. COE CONVENTION ON CYBERCRIME – EXTRADITION: PREPOSITIONS

Fill in the gaps with the correct prepositions from the list below. Please note that some prepositions may be used more than once.

at, between, by, for, from, in, on, over, to, under, with

CoE Convention on Cybercrime

ARTICLE 24 – EXTRADITION

1 a. This article applies to extradition (1) _________ Parties for the criminal offences established in accordance (2) _______ Articles 2 through 11 of this

Convention, provided that they are punishable (3) _______ the laws of both Parties concerned (4) _______ deprivation of liberty for a maximum period of at least one year, or (5) _______ a more severe penalty.

b. Where a different minimum penalty is to be applied (6) ________ an arrangement agreed (7) _______ the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for (8) _______ such arrangement or treaty shall apply. […]

3 If a Party that makes extradition conditional (9) __________ the existence of a treaty receives a request for extradition (10) _______ another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis (11) _______ extradition with respect to any criminal offence referred to in paragraph 1 of this article. [….]

6 lf. extradition for a criminal offence referred (12) _______ in paragraph 1 of this article is refused solely (13) ______ the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction (14) _______ the offence, the requested Party shall submit the case (15) ________ the request of the requesting Party to its competent authorities (16) ________ the purpose of prosecution and shall report the final outcome to the requesting Party (17) _______ due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature (18) _______ the law of that Party.

b) PART II: Grammar practice

Now look at the following examples and decide what meaning the structures convey. Then replace the structure with an equivalent structure that conveys the same meaning. The first one has been done for you.

1. The President is to make a further visit to New York next week. (FUTURE ARRANGEMENTS)

The President WILL make a further visit to New York next week.

2. You are to carry your ID at all times.

3. All students are to take a mental maths test at the end of the term.

4. The Secretary General was to speak to the Committee meeting.

5. You may go to John's birthday party but you are not to return later than 12pm.

6. If you are to work in Spain for longer than three months, you have to apply for a work permit.

7. Mr. Jones was to have spoken at the conference, but he didn't make it in time.

8. An employee of the firm is to appear in court today to give evidence about the alleged fraud.

9. If I were to lend you 80 euros, would you be able to return them by Monday?

10. No books or notes of any kind are to be taken into the examination room.

INSTRUCTIONS/ORDERS

11. You are not to leave the premises without parental permission.

UNIT 3
THE LANGUAGE OF CYBERCRIME: CASES

LAW ENFORCEMENT SUCCESSES IN CYBERCRIME

a) PART I: Reading comprehension

Read the questions below and scan the text for the correct answers. Read the text again and look up any of the words you do not understand.

1. Which is IOCTA's stated mission?

2. Why, in your view, does the article refer to cybercrime 'hitting home'?

3. What is the principal remit of ENISA?

4. What type of community is a 'CERT community'?

5. The term used to describe the ability cyber criminals have to quickly recover from change as a result of investigative police operations.

2017, the year when cybercrime hit close to home: Major law enforcement successes despite an increasingly professionalised cybercrime landscape.

27 September 2017.

The past 12 months have seen a number of unprecedented cyber-attacks in terms of their global scale, impact and rate of spread. Already causing widespread public concern, these attacks only represent a small sample of the wide array of cyber threats we now face. Europol's 2017 Internet Organized Crime Threat Assessment (IOCTA) identifies the main cybercrime threats and provides key recommendations to address the challenges.

Europol's Executive Director Rob Wainwright: "The global impact of huge cyber security events such as the WannaCry ransomware epidemic has taken the threat from cybercrime to another level. Banks and other major businesses are now targeted on a scale not seen before and, while Europol and its partners in policing and Industry have enjoyed success in disrupting major criminal syndicates operating online, the collective response is still not good enough. In particular people and companies everywhere must

do more to better protect themselves.”

The 2017 Internet Organized Crime Threat Assessment presents an in-depth assessment of the key developments, changes and emerging threats in cybercrime over the last year. It relies on contributions from the EU Member States, expert Europol staff and partners in private industry, the financial sector and academia. The report highlights important developments in several areas of cybercrime: Ransomware has eclipsed most other cyber-threats with global campaigns indiscriminately affecting victims across multiple industries in both the public and private sectors. Some attacks have targeted and affected critical national infrastructures at levels that could endanger lives. These attacks have highlighted how connectivity, poor digital hygiene standards and security practices can allow such a threat to quickly spread and expand the attack vector.

The first serious attacks by botnets using infected insecure Internet of Things (IoT) devices occurred.

Data breaches continue to result in the disclosure of vast amounts of data, with over 2 billion records related to EU citizens reportedly leaked over a 12 month period, often facilitated by poor digital hygiene and practices.

The Darknet remains a key cross-cutting enabler for a variety of crime areas. It provides access to, amongst other things: the supply of drugs such as Fentanyl and new psychoactive substances which internationally have directly led to many fatalities; the supply of firearms that have been used in terrorist acts; compromised payment data to commit various types of payment fraud; and fraudulent documents to facilitate fraud, trafficking in human beings and illegal immigration.

Offenders continue to abuse the Darknet and other online platforms to share and distribute child sexual abuse material, and to engage with potential victims, often seeking to coerce or sexually extort vulnerable minors.

Payment fraud affects almost all industries, having the greatest impact on the retail, airline and accommodation sectors. Several sectors are targeted by these fraudsters as the services they provide can be used for the facilitation of other crimes, including trafficking in human beings or drugs, and illegal immigration.

Direct attacks on bank networks to manipulate card balances, take control of ATMs or directly transfer funds, known as payment process compromise, represent one of the serious emerging threats in this area. Julian King, EU Commissioner for the security union, said: “This report shows online crime is the new frontier of law enforcement. We’ve all seen the impact of events like WannaCry: whether attacks are carried out for financial or political reasons, we need to improve our resilience and ensure cybercrime does not pay - last week the EU set out a package of concrete cybersecurity measures.”

Dimitris Avramopoulos, EU Commissioner for Migration, Home Affairs and Citizenship, added: “Crossborder Cyber threats today threaten not only our citizens and our economies, but also our democracies themselves. Cybercrime has become increasingly instrumental in geopolitics and conflicts. With a new EU cyber strategy, and a stronger role for European agencies, including ENISA and Europol, we will be better equipped to increase cybersecurity collectively, in Europe and beyond.”

Despite the growing threats and challenges for law enforcement, last year did see some tremendous operational successes, for example the takedown of two of the largest Darknet markets, AlphaBay and Hansa, the dismantling of the Avalanche network, and two successful Global Airport Action Days targeting those travelling on fraudulently-purchased airline tickets.

The IOCTA seeks to make recommendations for law enforcement, policy makers and regulators to allow them to act and plan accordingly, and respond to cybercrime in an effective and concerted manner.

Law enforcement must continue to focus on the actors developing and providing the cybercrime attack tools and services responsible for ransomware, banking Trojans and other malware, and suppliers of DDOS attack tools, counter-anti-virus services and botnets.

The international law enforcement community must continue to build trusted relationships with public and private partners, CERT communities, etc., so that it is adequately prepared to provide a fast and coordinated response in case of a global cyber-attack.

Company employees and the general public need to be educated to recognize and respond accordingly to changing criminal tactics like social engineering and spam botnets. EU Member States should continue to support and expand their engagement with Europol in the development of pan-European prevention and awareness campaigns.

While investigating online child sexual exploitation, EU Member States should ensure sufficient investigative tools and resources to fight this crime. Joint high-quality and multilingual EU-wide prevention and awareness activity needs to be maintained.

Law enforcement needs to develop a globally coordinated strategic overview of the threat presented by the Darknet. Such analysis would allow for future coordination of global action to destabilize and close down criminal marketplaces. It is also essential that investigators responsible for all crime areas represented on Darknet markets have the knowledge, expertise and tools required to effectively investigate and act in this environment.

The growing threat of cybercrime requires dedicated legislation that enables law enforcement presence and action in an online environment. The lack of adapted legislation is leading to a loss of both investigative leads and the ability to effectively prosecute online criminal activity.

b) PART II: Word formation 1

Change the adjectives into nouns:

1. professional a) ______________________

2. global b) ______________________

3. enforcing c) ______________________

4. expertise d) ______________________

5. criminal e) ________________________

6. equipped f) ________________________

7. wide g) ________________________

c) PART II: Word formation 2

Change the nouns into adjectives:

1. leader a) ________________________

2. threat b) ________________________

3. environment c) ________________________

4. awareness d) ________________________

5. coordination e) ________________________

6. ability f) ________________________

7. expansion g) ________________________

8. fraudster h) ________________________

d) PART IV: Definitions

Which word or phrase from the article in Part I is being described below?

1. The word for the group of people (3 or more) who get together for the sole objective of planning and carrying out criminal acts.

2. The cybercrime term for a place where all kinds of internet not indexed exchanges take place.

3. The phrase used for the request for 'tailor-made' reforms in the field of cybercrime.

4. The word used to refer to 'a person with professional experience'.

5. The word often used describe a person who carries out a crime.

6. A network of objects such as cars and other physical devices that are fixed with electronics, sensors, software and internet connectivity.

a) PART I: Press Release (Verbs)

Complete the gaps with the correct form of the verb provided in brackets. The number of gaps provided correspond to the words in the verb form.

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, July 15, 2015

Major Computer Hacking Forum Dismantled

As Part of Coordinated Law Enforcement Efforts in 20 Countries, United States Charges 12 Defendants

in Connection with Computer Fraud Conspiracy

The computer hacking forum known as Darkode (a)_______________ _______________ [***dismantle***] yesterday, and criminal charges (b) _______________ _______________ _______________ [***file***] in the Western District of Pennsylvania and elsewhere against 12 individuals associated with the forum, announced Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, U.S. Attorney David J. Hickton of the Western District of Pennsylvania and Deputy Director Mark F.

Giuliano of the FBI.

"Hackers and those who profit from stolen information (c) _______________ [***use***] underground Internet forums to evade law enforcement and target innocent people around the world," said Assistant Attorney General Caldwell. "This operation is a great example of what international law enforcement (d) **can** _______________ [***accomplish***] when we work closely together to neutralize a global cybercrime marketplace."

"Of the roughly 800 criminal internet forums worldwide, Darkode (e) _______________ [***represent***] one of the gravest threats to the integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world," said U.S. Attorney Hickton. "Through this operation, we (f) _______________

_______________ [***dismantle***] a cyber hornets' nest of criminal hackers which (g) _______________ _______________ [***believe***] by many, including the hackers themselves, to be impenetrable."

"This is a milestone in our efforts to shut down criminals' ability to buy, sell, and trade malware, botnets and personally identifiable information used to steal from U.S. citizens and individuals around the world," said Deputy Director Giuliano. "Cyber criminals (h) **should** _______________ _______________ [***have, not***] a safe haven to shop for the tools of their trade and Operation Shrouded Horizon shows we will do all we can to disrupt their unlawful activities."

As alleged in the charging documents, Darkode was an online, password-protected forum in which

hackers and other cyber-criminals (i) _______________ [***convene***] to buy, sell, trade and share information, ideas, and tools to facilitate unlawful intrusions on others' computers and electronic devices.

Before (j)_______________ [***become***] a member of Darkode, prospective members (k) _______________ **allegedly** _______________ [***vet***] through a process in which an existing member invited a prospective member to the forum for the purpose of presenting the skills or products that he or she could bring to the group. Darkode members allegedly used each other's skills and products to infect computers and electronic devices of victims around the world with malware and, thereby gain access to, and control over, those devices.

The takedown of the forum and the charges announced today are the result of the FBI's infiltration, as part of Operation Shrouded Horizon, of the Darkode's membership. The investigation of the Darkode forum is ongoing, and the U.S. Attorney's Office of the Western District of Pennsylvania (l) _______________ _______________ [***take***] a leadership role in conjunction with the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS).

The charges (m) _______________ [***announce***] today are part of a coordinated effort by a coalition of law enforcement authorities from 20 nations to charge, arrest or search 70 Darkode members and associates around the world. The nations (n) _______________ [***comprise***] the coalition include Australia, Bosnia and Herzegovina, Brazil, Canada, Colombia, Costa Rica, Cyprus, Croatia, Denmark, Finland, Germany, Israel, Latvia, Macedonia, Nigeria, Romania, Serbia, Sweden, the United Kingdom and the United States.

Today's actions represent the largest coordinated international law enforcement effort ever directed at an online cyber-criminal forum.

The Love-Bug virus33

a) PART I: grammar (verbs)

Read the first part of the article and complete the gaps with the correct form of the verb in brackets.

"Love-Bug" virus damage estimated at $10 billion:

More than 20 countries affected

Mike Ingram

10 May 2000

It is estimated that the so-called "Love-Bug" email virus (A) _______________ _______________ [***cause***] some $10 billion in losses in as many as 20 countries. The virus (B) _____________ originally ____________ [***distribute***] in an email with the subject line "I love you". The message contains the text "kindly check the attached LOVELETTER from me" and an attached file called LOVE-LETTER-FOR-YOU.TXT.

VBS. If this attachment (C) _____________ _____________ [***open***] it will replicate itself and be transferred to all addresses within a user's email address book. The virus also (D) _____________ [***delete***] graphic files ending with the letters jpg or jpeg, and alters music files ending in mp3 to make them inaccessible.

The victim's Internet browser (E) _____________ _____________ [***direct***]by the virus to visit four web sites in the Philippines, where another malicious program called WIN-BUGSFIX.EXE is downloaded. This program searches the victim's hard drive for password files and sends them to an Internet account in the Philippines, (F) _____________ [***manage***] by Access Net Inc., an Internet service provider.

Since the original attack last week, the virus (G) _____________ _____________ [***continue***] to circulate in new and particularly dangerous variants calculated to cause the maximum damage. One such new message has the subject heading "Virus warning" and another is marked "Mother's Day Order Confirmation." The latter tells the recipient that $326.92 (H) _________ ___________ _____________ [***charge***] to his credit card for a "diamond special" and urges him to review the attached invoice, which contains the virus.

It is estimated that there are at least 10 new variants of the virus in circulation. A new virus with the title "Friend Message" and containing the file FRIEND_MESSAGE.TXT.vbs is also in circulation. The results of this are the same as the LoveLetter virus but the code (I) ___________ __________ completely _____________ [***rewrite***]. Virus detection software upgraded to detect the original "Love-Bug" will not detect this new and no less destructive version.

Security experts and systems administrators (J) _____________ [***warn***] that all email attachments from unknown sources should (K) _____________ _____________ [***regard***]with suspicion and that files with the VBS extension should never be opened.

The search for the author of the virus, which shut down the email service of the British parliament and attacked the computers of the Pentagon and CIA in the US, focused on the Philippines, after security experts (L) _____________ [***scritinise***] the code of the virus.

b) PART II: Vocabulary and reading for detail

Read the rest of the article and try to guess the meanings of the underlined words. Look them up in a dictionary to make sure that you understand their meanings in context. Then answer the multiple choice questions (about the entire article) and short answer questions (about the second part of the article).

Initial reports that the author had used the name “spider” proved to be misleading. The references to “spider” in the software code were, in fact, references to the author of the password collection software used in the file “WIN-BUGSFIX.EXE”, which infected computers were directed to download. Stolen passwords were emailed to accounts at Access Net in the Philippines with the message, “Barok... e.mail. passwords.sender.Trojan-by spyder.”

Barok is the name of popular password-stealing software and “spyder” is the name used by the hacker who created it. Barok is currently at version 2.1 and was released on underground Internet sites about a month ago. An earlier version of the software included a reference to Amable Mendoza Aguiluz Computer College (AMACC) in the Philippines. The words “Manila, Philippines” were also found elsewhere in the virus code.

As the details of the computer code were revealed, experts feared that the clues were so numerous that they could have been left deliberately as false tips, to throw investigators off track. “This may be somebody putting us on, and the reality is, he might be sitting in his boxer shorts in New Jersey having a good laugh at us,” warned Elias Levy, chief technology officer at SecurityFocus.Com of San Mateo,

California.

A computer expert in Sweden said Saturday that he believed the attack was the responsibility of an 18-year-old German exchange student in Australia who had hacked into computers in the Philippines, but Australian Federal Police say they have been given no firm evidence to back up the allegation.

Despite conflicting opinions as to the validity of the details left in the computer code, a full-scale hunt for the authors of the virus has focused on the Phillipines.

Over the weekend of May 6-7, the Philippines National Bureau of Investigations (NBI), accompanied by officers of the US Federal Bureau of Investigations (FBI), arrested 27-year-old Reomal Ramones following a surveillance operation outside his home in the Bagong Barangay suburb of Manila. Irene de Guzman, said to be Ramones’ live-in girlfriend, is also sought by police.

It is by no means certain that Ramones or de Guzman, both bank workers, were involved in the attacks.

Security experts say that even if the attacks were traced to a computer in the house, this could also have been the work of hackers who used the computer to launch the attacks without the knowledge of the owners. Attorneys for both Ramones and Guzman say they deny any involvement in the virus attacks.

Ramones was released Tuesday after Philippine prosecutors ruled that police did not have enough evidence to hold him.

Investigators were led to the Bagong Barangay house after Access Net examined chat room logs containing incriminating references to hacking and the creation of viruses. These were traced back to an email account said to belong to either Ramones or de Guzman.

It was revealed that Ramones and Guzman both attended courses at AMACC and the college has now become the focus of further investigations. NBI officer Elfren Meneses said some eight other people with links to the school could be involved in the spread of the virus. He told reporters there were 10 coded names found embedded in the virus. “There were reports from the FBI that the names are from an called AMACC,” he said.

Whoever turns out to be behind the virus attacks and whatever their motives, acts of vandalism such as these serve no positive political or social purpose. The justifiable and widespread concerns that these attacks generate are used by governments to instigate new police powers and more intrusive forms of control over the Internet. This is already illustrated by the massive police operation under way in the Philippines and the sensationalised media coverage it is receiving.

Multiple choice questions (about the whole text)

1. The so-called “Love-Bug” email virus led to losses

a) amounting to $10 million in losses in Philippines

b) amounting to $10 million in losses in many more countries

c) amounting to $10 million in losses in each of the 20 countries.

2. The message requests the user

a) to send a letter to a person he or she loves

b) to open and read a love letter

c) to delete the letter and its attachment

3. The virus

a) deletes all files

b) replicates itself and deletes addresses

c) replicates itself and deletes some specific types of files

4. The affected internet browser

a) can only be fixed in Philippines

b) is re-directed to Philippines to be scanned for viruses

c) is attacked by another virus and scanned for passwords

5. The virus

a) was fairly harmless

b) kept being upgraded

c) contained a Mother's Day Card

6. The virus detection software

a) detected the Friend Message within the Love Bug virus

b) could not detect any of those viruses

c) would not detect the upgraded variations of the virus

7. The virus

a) shut down the email service of the British parliament

b) did not attack the computers of the Pentagon and CIA in the US,

c) was only active if you had IP address in Philippines

8. The author of the virus

a) called the virus “spider”

b) studied at the Computer Colleague in Philippines

c) left numerous clues

9. The author of the virus

a) was believed to be German but living in Philippines

b) was difficult to track and opinion varied

c) was caught by the Australian Federal Police

10. The people suspected and sought as authors

a) were both arrested

b) admitted they were guilty

c) worked in a bank

Short answer questions (about the second part of the article).

1. What did “spider” refer to?
2. What are “barok” and “spyder”?
3. Why were experts worried about the number of clues?
4. Where was Reomal Ramones arrested?
5. Where did Ramones and his girlfriend work?
6. Why was Ramones released?
7. How did police find Ramones’ house?
8. How many other people could be involved in the attacks?
9. What, according to the article, do such attacks lead governments to do? How is this being illustrated at the moment?

U.S. EMPLOYEE SENTENCED FOR HACKING AND CYBERCRIMES

Read the text and look up any words that you do not understand. Then do the activities.

U.S. employee sentenced to 57 months for hacking and cybercrimes

A former U.S. State Department employee was sentenced today to 57 months in prison for perpetrating a widespread, international e-mail phishing, computer hacking and cyberstalking scheme against hundreds of victims in the United States and abroad. […] Michael C. Ford, 36, of Atlanta, was sentenced today by U.S. District Judge Eleanor L. Ross of the Northern District of Georgia. On Dec. 9, 2015, Ford pleaded guilty to nine counts of cyberstalking, seven counts of computer hacking to extort and one count of wire fraud in connection with his ongoing criminal scheme. The names of the victims are being withheld from the public to protect their privacy.

According to the plea document, Ford admitted that between January 2013 and May 2015, while employed by the U.S. Embassy in London, he used various aliases to commit a widespread, international computer hacking, cyberstalking and "sextortion" campaign designed to force victims to provide Ford with personal information as well as sexually explicit videos of others. Ford targeted young females, some of whom were students at U.S. colleges and universities, with a particular focus on members of sororities and aspiring models.

Posing as a member of the fictitious "account deletion team" for a well-known e-mail service provider, Ford sent thousands of phishing e-mails to thousands of potential victims, warning them that their e-mail accounts would be deleted if they did not provide their passwords. Ford admitted he then used the passwords to hack into at least 450 e-mail and social media accounts belonging to at least 200 victims, where he searched for sexually explicit photographs and for victims' personal identifying information (PII), including their home and work addresses, school and employment information, and names and contact information of family members, among other things. Using both the photos and PII, Ford admitted that he then e-mailed at least 75 victims, threatening to release those photos unless they took and sent him sexually explicit videos of "sexy girls" undressing in changing rooms at pools, gyms and clothing stores.

When the victims refused to comply, threatened to go to the police or begged Ford to leave them alone, Ford escalated his threats, according to the plea agreement. For example, Ford admitted that he wrote in one e-mail "don't worry, it's not like I know where you live," followed by another e-mail with her home address and threatened to post her photographs to an "escort/hooker website" along with her phone number and home address. On several occasions, Ford followed through with his threats, sending his victims' sexually explicit photographs to family members and friends, according to the plea.

Additionally, at sentencing, the government presented evidence that Ford engaged in a related scheme targeting aspiring models beginning in 2009. Posing as a model scout, Ford convinced young women to send their personal information, to include dates of birth and measurements, as well as topless photos for consideration for fictitious modeling opportunities. During this ruse, Ford obtained topless and partially nude photos from hundreds of women, including several minors. He also attempted to entice a minor to take voyeuristic videos of her peers in her school locker room. Some of his early model-scout victims became the first victims of his charged cyberstalking scheme.

"Michael Ford hacked hundreds of email accounts, particularly targeting young women so he could extort them into sending him sexually explicit images," said Assistant Attorney General Caldwell. "He preyed on vulnerable victims, leaving them with indelible emotional scars. His sentence is a necessary step in holding him to account for his crimes and helping his victims move forward with their lives."

"This case unfortunately shows that cyber-stalkers have the ability to torment victims from any corner of the globe," said U.S. Attorney Horn.

"Hopefully, Ford's victims can be reassured that he will serve a significant sentence for his conduct. Members of the public must be extremely careful about disclosing their logins and passwords to anyone, even when the person on the other end of an e-mail or instant message appears to be legitimate."

"The Diplomatic Security Service is proud of the hard work of everyone involved in the investigation including our partners at the FBI and the Department of Justice," said Director Miller. "When a public servant in a position of trust commits crimes like cyberstalking and computer hacking on such a large scale, we will vigorously investigate those crimes and ensure they are brought to justice. We hope that this sentence will provide some closure for the victims."

"Today's sentencing of Mr. Ford will not only hold him accountable for his despicable criminal conduct but will also deny him the ability to further victimize others," said Special Agent in Charge Johnson. "The FBI is proud of the role that it played in bringing this case forward for investigation, apprehension, and federal prosecution and it is hoped that those who were victimized by Mr. Ford will find some relief with this sentencing." […]

a) Part I: True or False.

Decide whether the following statements True or False?

1. A foreign State Department civil servant was caught hacking people's computers. T/F

2. The perpetrator was found guilty of setting up a 24/7 complex cybercrime scheme. T/F

3. The victims of Ford's crime scheme were unattractive loners with low IQs. T/F

4. Mr. Ford operated with no criminal purpose in mind. He simply was lonely and in need of new friends. T/F

5. Ford posed as a legitimate expert ready to save people with computer security problems. T/F

6. The DSS is satisfied with the work done ferreting out the perpetrator. T/F

7. The punishment for crimes committed by Ford amounted to 6 years in federal prison. T/F

b) PART II: Definitions

Write the word/phrase described in the gap

1. The reconciliation with the events suffered by the victims of crime. ___________________

2. The act of convincing someone to do something that is wrong or damaging to others. ___________________

3. The act of taking pictures or spying on one's friends, peers or family with the sole purpose of using or exposing the information collected. ___________________

4. The act of pursuing repressed sexual arousal or dominance towards a vulnerable person by adopting hunting practices for the purpose of instilling fear and instability on victims.

____

5. The state of permanent harm caused by another or by a traumatic event. ___________________ 6. The act of increasing one's attempt to make others do something they are reluctant to do by persuading or instilling fear. ___________________

c) PART III. Working with synonyms.

Find near-synonyms for the words or expressions that are underlined.

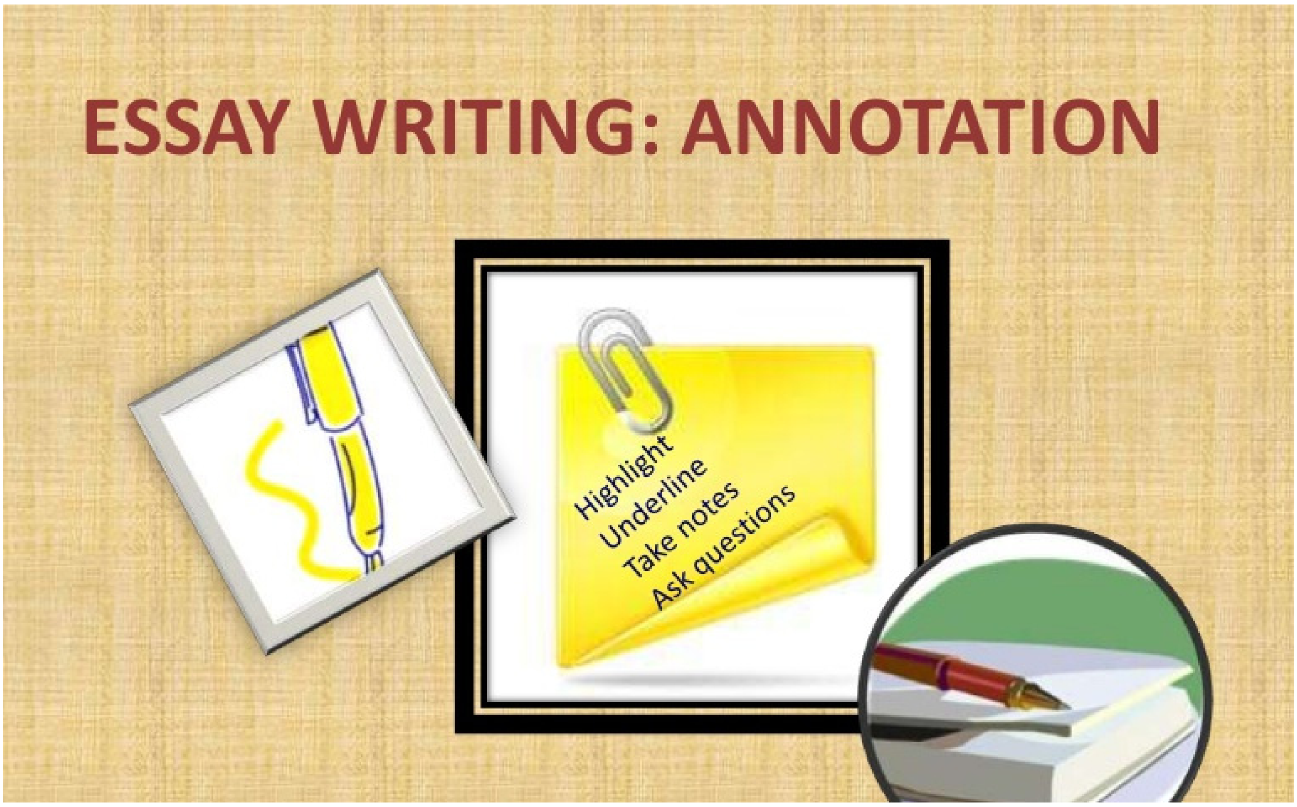
1. A former U.S. State Department employee was sentenced today.

2. His sentence is a necessary step in holding him to account for his crimes.

3. “Today’s sentencing of Mr. Ford will not only hold him accountable for his despicable criminal conduct but will also deny him the ability to further victimize others.”

4. Ford sent thousands of phishing e-mails to thousands of potential victims.

5. Posing as a model scout, Ford convinced young women to send their personal information, to include dates of birth and measurements.



Summarizing English Scientific Literature

Язык аннотации

К аннотациям как на русском, так и на английском языке предъявляются следующие требования:

1. Лаконичность языка, т.е. использование простых предложений (глаголы употребляются всегда в настоящем времени в действительном или страдательном залоге. Модальные глаголы, как правило, отсутствуют).

2. Строгая логическая структура аннотации.

3. Обязательное введение в текст аннотации безличных конструкций и отдельных слов, например: «Сообщается…», «Подробно описывается», «Кратко рассматривается…», «Излагаются…», «Комментируются…» и др., с помощью которых происходит введение и описание текста оригинала.

4. Недопущение повторений в заглавии и тексте аннотации.

5. Точность в передаче заглавия оригинала, отдельных формулировок и определений.

6. Использование общепринятых сокращений слов, таких, как напр., и т.д., и т.п., и др.

7. Единство терминов и обозначений.

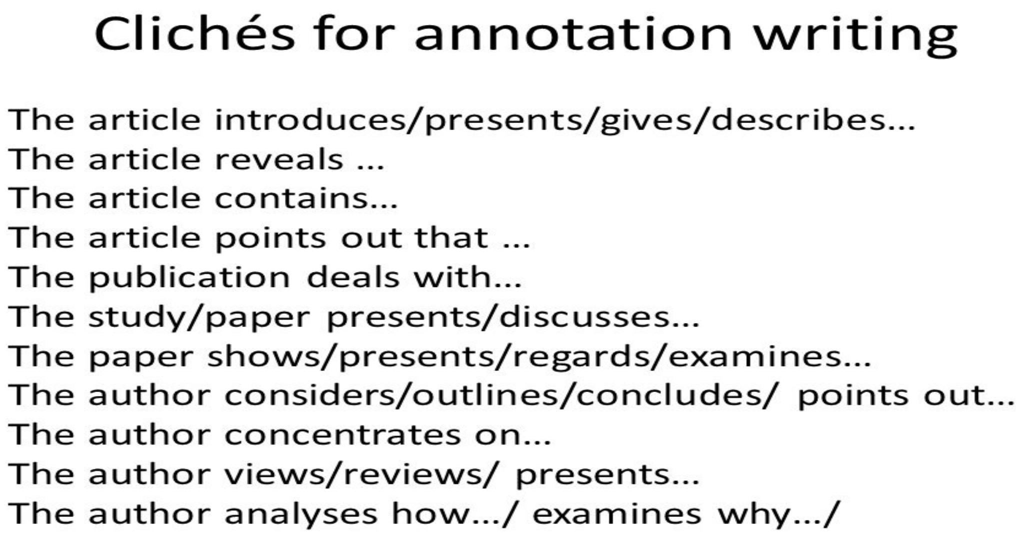
Текст аннотации должен быть максимально кратким, от 500 до 1000 печатных знаков.

Основные штампы (key-patterns) аннотаций на английском и русском языках:

1. The article (paper, book, etc.) deals with…	1. Эта статья (работа, книга и т.д.) касается…
2. As the title implies the article describes…	2. Согласно названию, в статье описывается…
3. It is specially noted…	3. Особенно отмечается…
4. A mention should be made…	4. Упоминается…
5. It is spoken in detail…	5. Подробно описывается…
6. …are noted	6. Упоминаются…
7. It is reported…	7. Сообщается…
8. The text gives a valuable information on…	8.Текст дает ценную информацию…
9. Much attention is given to…	9. Большое внимание уделяется…
10. The article is of great help to …	10. Эта статья окажет большую помощь…
11. The article is of interest to…	11. Эта статья представляет интерес для…
12. It (the article) gives a detailed analysis of …	12. Она (статья) дает детальный анализ…
13. It draws our attention to…	13. Она (статья, работа) привлекает наше внимание к…
14. The difference between the terms…and…should be stressed	14. Следует подчеркнуть различие между терминами …и…
15. It should be stressed (emphasized) that…	15. Следует подчеркнуть, что…

16. …is proposed	16. Предлагается…
17. …are examined	17. Проверяются (рассматриваются)
18. …are discussed	18. Обсуждаются…
19. An option permits…	19. Выбор позволяет…
20. The method proposed … etc.	20. Предлагаемый метод… и т.д.

Первые два штампа в основном используются при устном аннотировании и кратком изложении содержания оригинала.



Clichés for annotation writing

The article introduces/presents/gives/describes...
The article reveals ...
The article contains...
The article points out that ...
The publication deals with...
The study/paper presents/discusses...
The paper shows/presents/regards/examines...
The author considers/outlines/concludes/ points out...
The author concentrates on...
The author views/reviews/ presents...
The author analyses how.../ examines why.../

Обратите внимание!

Научная статья обычно состоит из следующих частей:

1. Заголовок (Title). 2. Аннотация (Abstract or Summary). 3. Введение (Introduction). 4. Общая часть (Methods, Materials, Procedures). 5. Результаты, обсуждение результатов, заключение (выводы) и рекомендации (Results, Discussions, Conclusion, Recommendations). 6. Использованная литература (References, Literature, Bibliography).

PLAN OF ANNOTATION

A) **Headline of the text**

I'd like to present the article headlined...

I"m going to speak about the article under the headline...

b) **Source**

- The article is (comes) from...
- The article was carried (published) by...
- It is of the 1-st of October, 2012
- The author of the article is... The article is by...

c) **Theme**

- The article is about...
- It deals with... It covers...
- The text traces (presents, describes, focuses on)...

d) **Idea**

- The author of the article stresses (urges, makes it clear) that...
- The main idea of the author is that...
- The author's aim is... The author aims at...

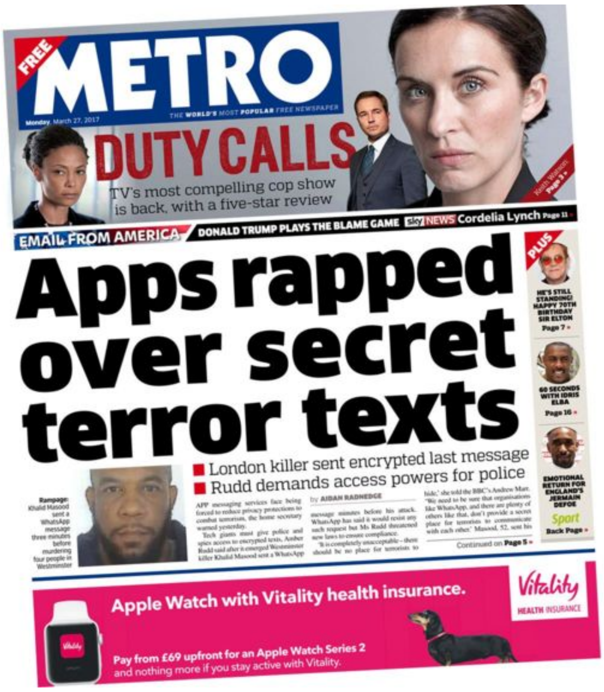
e) **Judgment**

It seems to me that...

I think (suppose, believe) that...

It is clear to me...It is obvious that..,

To my mind... In my opinion...



FREE METRO

THE WORLD'S MOST POPULAR FREE NEWSPAPER

Monday, March 27, 2017

DUTY CALLS

TV's most compelling cop show is back, with a five-star review

EMAIL FROM AMERICA DONALD TRUMP PLAYS THE BLAME GAME sky NEWS Cordelia Lynch Page 11

Apps rapped over secret terror texts

- London killer sent encrypted last message
- Rudd demands access powers for police

Rampage: Khalid Masood sent a WhatsApp message three minutes before murdering four people in Westminster

by AIDAN RADNEDGE

Continued on Page 5

PLUS HE'S STILL STANDING! HAPPY 70TH BIRTHDAY SIR ELTON Page 7

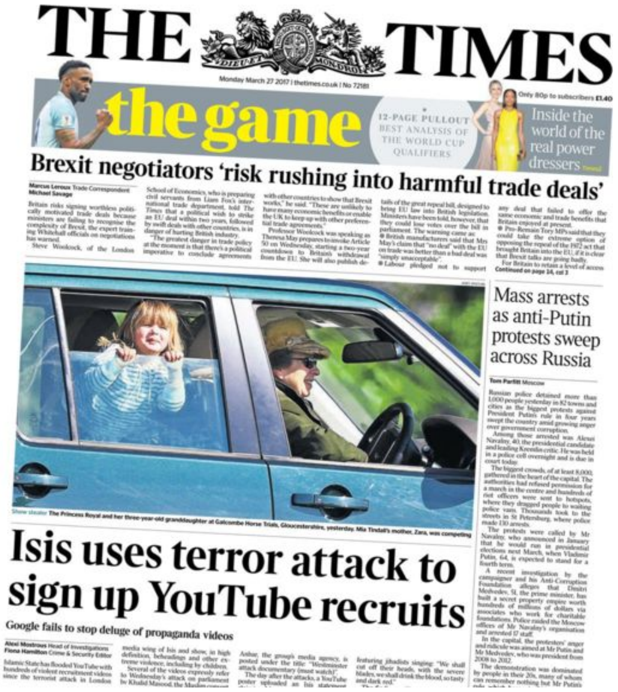
60 SECONDS WITH IDRIS ELBA Page 16

EMOTIONAL RETURN FOR ENGLAND'S JERMAIN DEFOE Sport Back Page

Apple Watch with Vitality health insurance.

Vitality HEALTH INSURANCE

Pay from £69 upfront for an Apple Watch Series 2 and nothing more if you stay active with Vitality.



THE TIMES

Monday March 27 2017 | thetimes.co.uk | No 72181

Only 80p to subscribers £1.40

the game

12-PAGE PULLOUT BEST ANALYSIS OF THE WORLD CUP QUALIFIERS

Inside the world of the real power dressers

Brexit negotiators 'risk rushing into harmful trade deals'

Marcus Leroux Trade Correspondent
Michael Savage

Continued on page 14, col 3

Mass arrests as anti-Putin protests sweep across Russia

Tom Parfitt Moscow

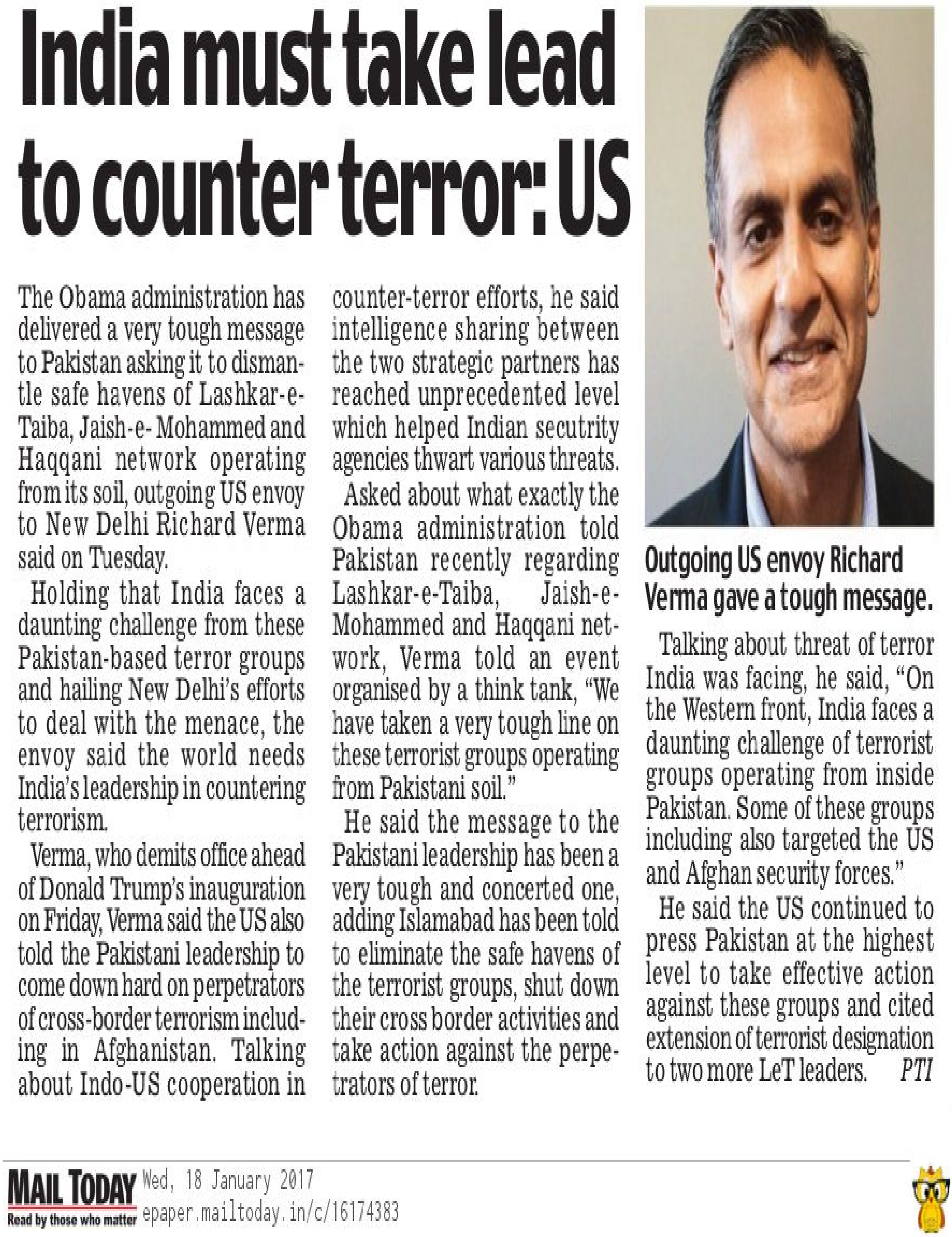
Show stealer The Princess Royal and her three-year-old granddaughter at Gatcombe Horse Trials, Gloucestershire, yesterday. Mia Tindall's mother, Zara, was competing

Isis uses terror attack to sign up YouTube recruits

Google fails to stop deluge of propaganda videos

Alexi Mostrous Head of Investigations
Fiona Hamilton Crime & Security Editor

Practice yourself in writing an annotation



India must take lead to counter terror: US

The Obama administration has delivered a very tough message to Pakistan asking it to dismantle safe havens of Lashkar-e-Taiba, Jaish-e- Mohammed and Haqqani network operating from its soil, outgoing US envoy to New Delhi Richard Verma said on Tuesday.

Holding that India faces a daunting challenge from these Pakistan-based terror groups and hailing New Delhi's efforts to deal with the menace, the envoy said the world needs India's leadership in countering terrorism.

Verma, who demits office ahead of Donald Trump's inauguration on Friday, Verma said the US also told the Pakistani leadership to come down hard on perpetrators of cross-border terrorism including in Afghanistan. Talking about Indo-US cooperation in counter-terror efforts, he said intelligence sharing between the two strategic partners has reached unprecedented level which helped Indian secutrity agencies thwart various threats.

Asked about what exactly the Obama administration told Pakistan recently regarding Lashkar-e-Taiba, Jaish-e-Mohammed and Haqqani network, Verma told an event organised by a think tank, "We have taken a very tough line on these terrorist groups operating from Pakistani soil."

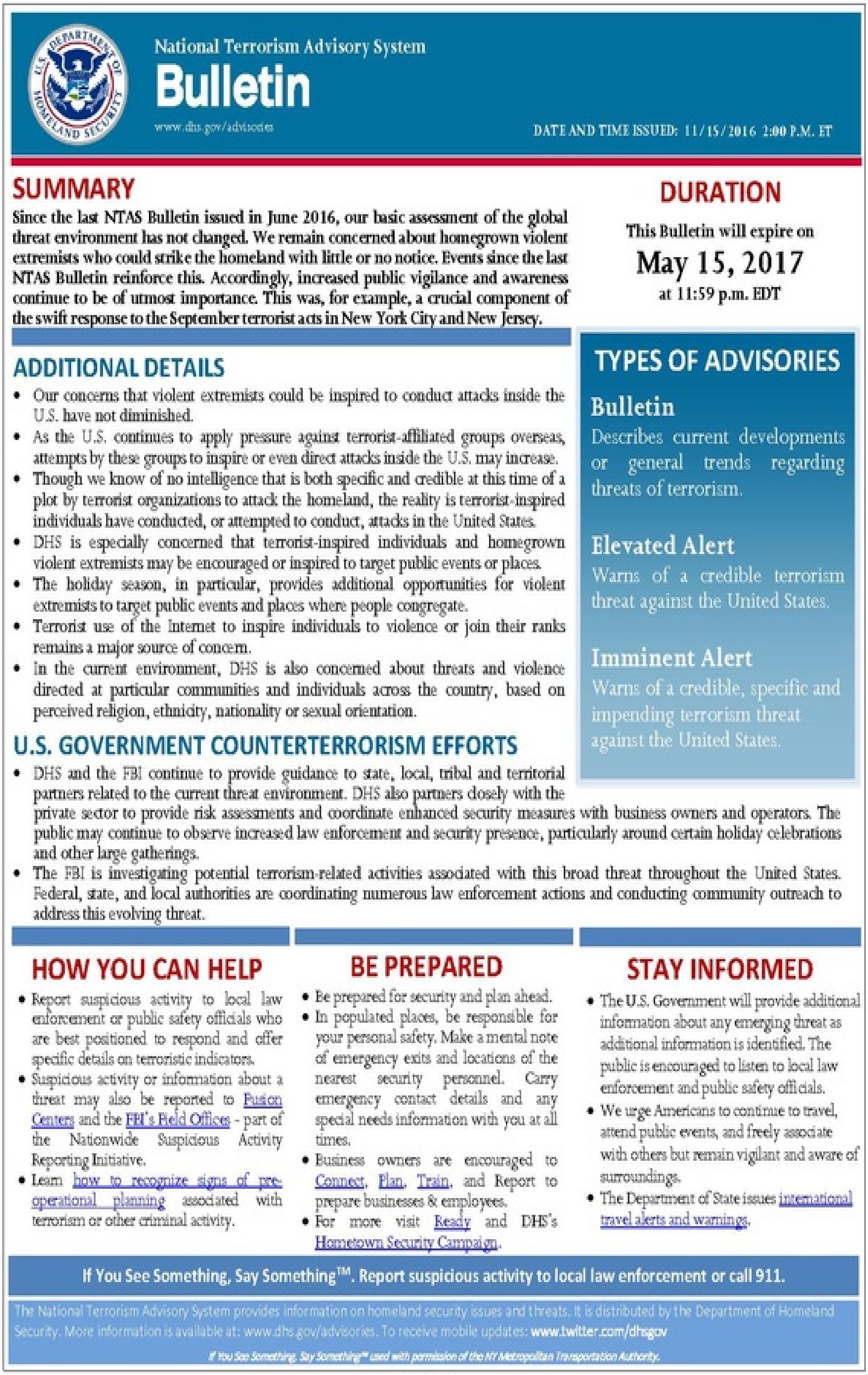
He said the message to the Pakistani leadership has been a very tough and concerted one, adding Islamabad has been told to eliminate the safe havens of the terrorist groups, shut down their cross border activities and take action against the perpetrators of terror.

Outgoing US envoy Richard Verma gave a tough message.

Talking about threat of terror India was facing, he said, "On the Western front, India faces a daunting challenge of terrorist groups operating from inside Pakistan. Some of these groups including also targeted the US and Afghan security forces."

He said the US continued to press Pakistan at the highest level to take effective action against these groups and cited extension of terrorist designation to two more LeT leaders. *PTI*

MAIL TODAY
Read by those who matter
Wed, 18 January 2017
epaper.mailtoday.in/c/16174383



National Terrorism Advisory System

Bulletin

www.dhs.gov/advisories

DATE AND TIME ISSUED: 11/15/2016 2:00 P.M. ET

SUMMARY

Since the last NTAS Bulletin issued in June 2016, our basic assessment of the global threat environment has not changed. We remain concerned about homegrown violent extremists who could strike the homeland with little or no notice. Events since the last NTAS Bulletin reinforce this. Accordingly, increased public vigilance and awareness continue to be of utmost importance. This was, for example, a crucial component of the swift response to the September terrorist acts in New York City and New Jersey.

DURATION

This Bulletin will expire on

May 15, 2017

at 11:59 p.m. EDT

ADDITIONAL DETAILS

- Our concerns that violent extremists could be inspired to conduct attacks inside the U.S. have not diminished.
- As the U.S. continues to apply pressure against terrorist-affiliated groups overseas, attempts by these groups to inspire or even direct attacks inside the U.S. may increase.
- Though we know of no intelligence that is both specific and credible at this time of a plot by terrorist organizations to attack the homeland, the reality is terrorist-inspired individuals have conducted, or attempted to conduct, attacks in the United States.
- DHS is especially concerned that terrorist-inspired individuals and homegrown violent extremists may be encouraged or inspired to target public events or places.
- The holiday season, in particular, provides additional opportunities for violent extremists to target public events and places where people congregate.
- Terrorist use of the Internet to inspire individuals to violence or join their ranks remains a major source of concern.
- In the current environment, DHS is also concerned about threats and violence directed at particular communities and individuals across the country, based on perceived religion, ethnicity, nationality or sexual orientation.

TYPES OF ADVISORIES

Bulletin

Describes current developments or general trends regarding threats of terrorism.

Elevated Alert

Warns of a credible terrorism threat against the United States.

Imminent Alert

Warns of a credible, specific and impending terrorism threat against the United States.

U.S. GOVERNMENT COUNTERTERRORISM EFFORTS

- DHS and the FBI continue to provide guidance to state, local, tribal and territorial partners related to the current threat environment. DHS also partners closely with the private sector to provide risk assessments and coordinate enhanced security measures with business owners and operators. The public may continue to observe increased law enforcement and security presence, particularly around certain holiday celebrations and other large gatherings.
- The FBI is investigating potential terrorism-related activities associated with this broad threat throughout the United States. Federal, state, and local authorities are coordinating numerous law enforcement actions and conducting community outreach to address this evolving threat.

HOW YOU CAN HELP

- Report suspicious activity to local law enforcement or public safety officials who are best positioned to respond and offer specific details on terroristic indicators.
- Suspicious activity or information about a threat may also be reported to Fusion Centers and the FBI's Field Offices - part of the Nationwide Suspicious Activity Reporting Initiative.
- Learn how to recognize signs of pre-operational planning associated with terrorism or other criminal activity.

BE PREPARED

- Be prepared for security and plan ahead.
- In populated places, be responsible for your personal safety. Make a mental note of emergency exits and locations of the nearest security personnel. Carry emergency contact details and any special needs information with you at all times.
- Business owners are encouraged to Connect, Plan, Train, and Report to prepare businesses & employees.
- For more visit Ready and DHS's Hometown Security Campaign.

STAY INFORMED

- The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials.
- We urge Americans to continue to travel, attend public events, and freely associate with others but remain vigilant and aware of surroundings.
- The Department of State issues international travel alerts and warnings.

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides information on homeland security issues and threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/advisories. To receive mobile updates: **www.twitter.com/dhsgov**

If You See Something, Say Something™ used with permission of the NY Metropolitan Transportation Authority.

NTAS ADV SORY 2016.002.3-8

Counter-terrorism from Canada to ISIS:

An Insider's Discussion of All Things Jihadist.

Mubin **Shaikh**

Mubin Shaikh is a former extremist who de-radicalized after studying Islam in Syria and was recruited as an undercover counter-terrorism operative for the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, Integrated National Security Enforcement Team (INSET). He conducted infiltration operations in human and online networks and has testified as a fact witness at the Superior Court of Ontario in five legal hearings over four years, obtaining a Master of Policing, Intelligence and Counter Terrorism in the meantime. Shaikh continued his professional research with the rise of ISIS, tracking and engaging with ISIS fighters and propagandists in real-time online. He is now an international, external Subject Matter Expert in national security and counter-terrorism to the United Nations Security Council and the Command Staff of CENTCOM, and trains various intelligence, police, and special operations forces on countering the terrorist threat.

Wed.March.14th
6:30 to 8:30pm

FREE ADMISSION

ENG103
George Vari Computing and Engineering Centre
245 Church St, Toronto,

The IID is committed to accessibility for persons with
disabilities. Please contact us at 416-979-5000 ext. 6206
at least one week in advance of this event if you have accommodation requirements,
and we will do our very best to assist.

UNIT IV
FOREIGN LAW-ENFORCEMENT ACTIVITY PRACTICE IN FIGHTING CYBERCRIMES

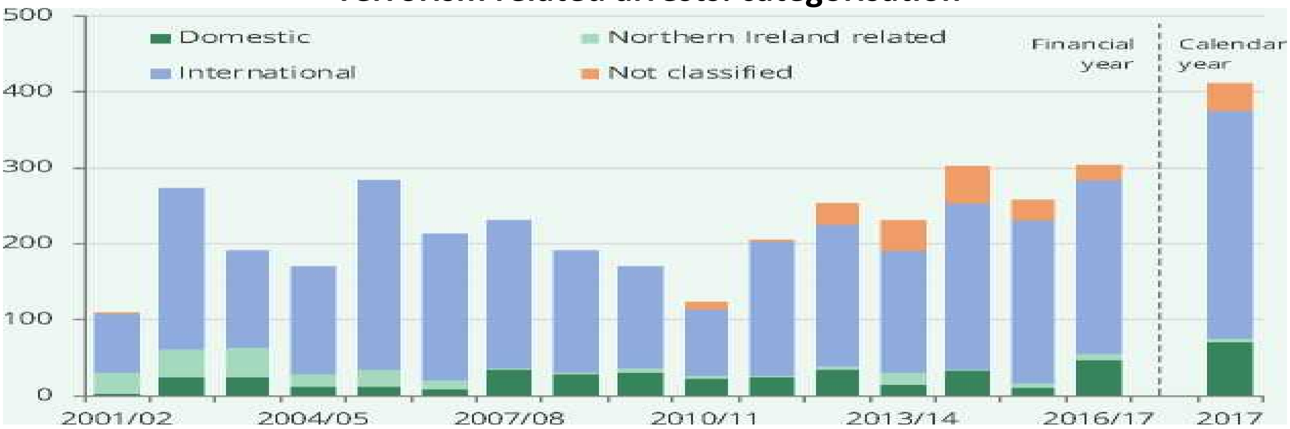
In line with measures taken by our allies, the Government of Canada is implementing legislation

ping our law enforcement and national security agencies stop those who mote the commission of terrorism offences in general, such as calling for cks on Canadians.

The ***Anti-Terrorism*** *Act*, 2015 received Royal Assent on June 18, 2015. ough this legislation, the Government of Canada is taking action to prevent orist travel, thwart efforts to use Canada as a recruiting ground and prevent nned attacks on our soil

Terrorism in Great Britain: the statistics

Terrorism related arrests: categorisation



Note: Data for 2001/02 is for 11 September 2001 onwards.

Source: Home Office, Operation of Police powers under the Terrorism Act 2000 and subsequent legislation: 31 March 2017, table A.13; Home Office, Operation of Police powers under the Terrorism Act 2000 and subsequent legislation: quarterly update to December 2017, table QA.13

The majority of terrorism related arrests made since 11 September 2001 have been classified by ACTCC as being related to international terrorism (79%).

In the year ending 31 December 2017, 73% (300) of arrests were classified by ACTCC as being

related to international terrorism.

POLICE SERVICES

The objective of the different community awareness programs implemented by police services is to engage all communities in the social problem-solving process to ensure the safety and security of the Canadian public. In Canada, the successful Community Mobilization Prince Albert program (Saskatchewan, Canada) is an example of this.

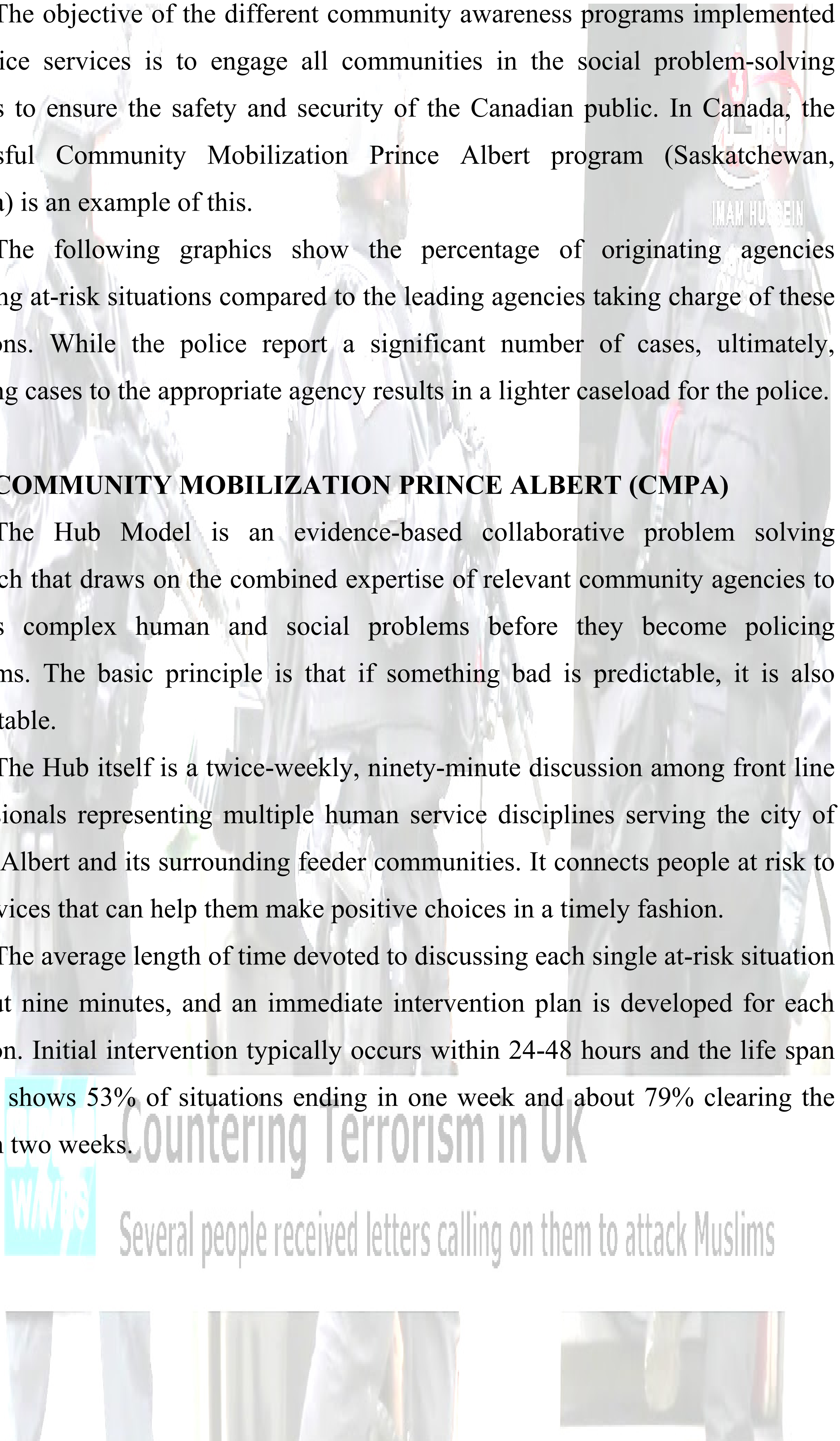
The following graphics show the percentage of originating agencies reporting at-risk situations compared to the leading agencies taking charge of these situations. While the police report a significant number of cases, ultimately, referring cases to the appropriate agency results in a lighter caseload for the police.

COMMUNITY MOBILIZATION PRINCE ALBERT (CMPA)

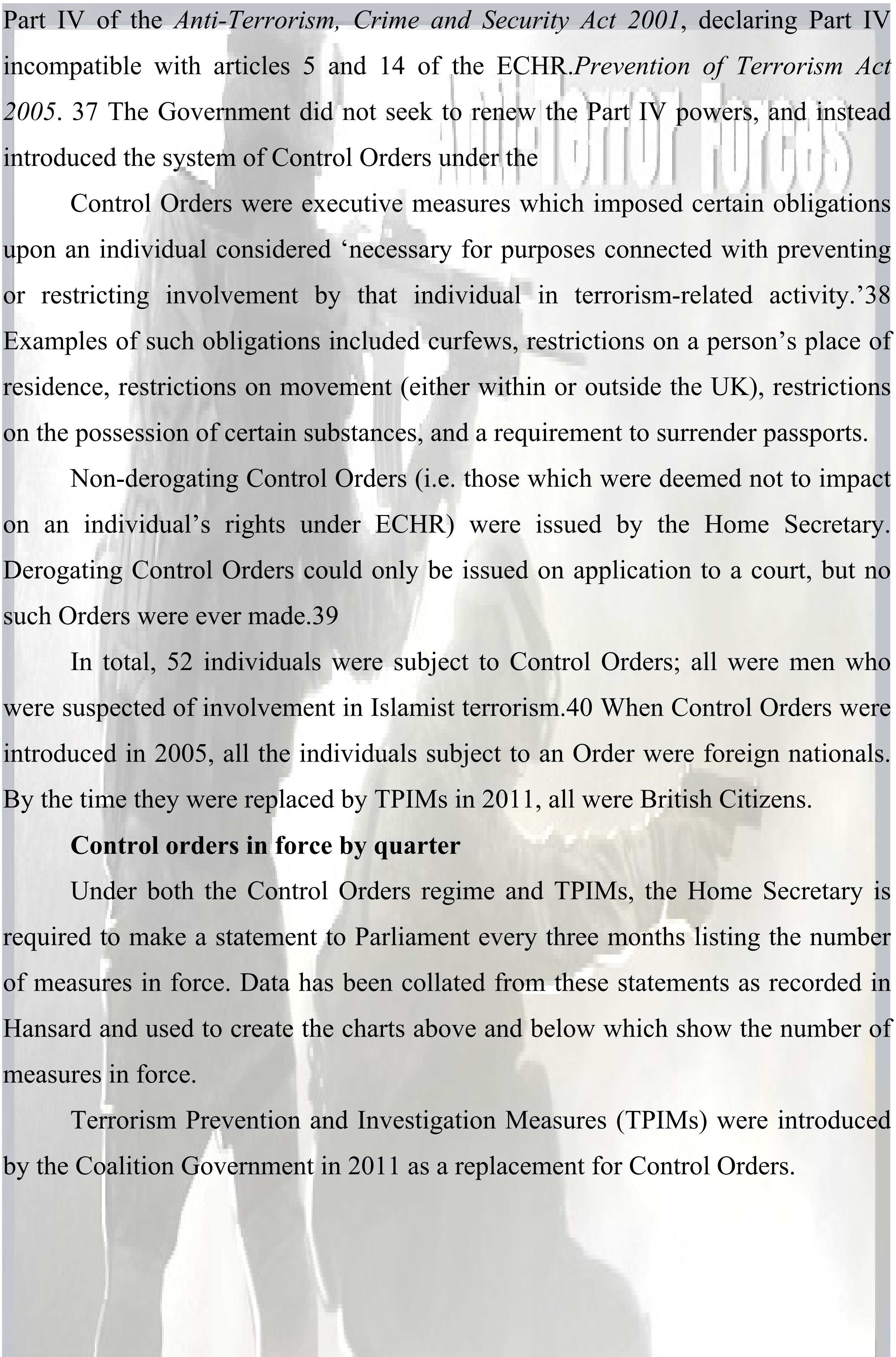
The Hub Model is an evidence-based collaborative problem solving approach that draws on the combined expertise of relevant community agencies to address complex human and social problems before they become policing problems. The basic principle is that if something bad is predictable, it is also preventable.

The Hub itself is a twice-weekly, ninety-minute discussion among front line professionals representing multiple human service disciplines serving the city of Prince Albert and its surrounding feeder communities. It connects people at risk to the services that can help them make positive choices in a timely fashion.

The average length of time devoted to discussing each single at-risk situation is about nine minutes, and an immediate intervention plan is developed for each situation. Initial intervention typically occurs within 24-48 hours and the life span pattern shows 53% of situations ending in one week and about 79% clearing the table in two weeks.


IMAM HUSSEIN
Countering Terrorism in UK
Several people received letters calling on them to attack Muslims

Control Orders in the UK



In 2004, a House of Lords ruling quashed the derogation order in relation to Part IV of the *Anti-Terrorism, Crime and Security Act 2001*, declaring Part IV incompatible with articles 5 and 14 of the ECHR.*Prevention of Terrorism Act 2005*. 37 The Government did not seek to renew the Part IV powers, and instead introduced the system of Control Orders under the

Control Orders were executive measures which imposed certain obligations upon an individual considered 'necessary for purposes connected with preventing or restricting involvement by that individual in terrorism-related activity.'38 Examples of such obligations included curfews, restrictions on a person's place of residence, restrictions on movement (either within or outside the UK), restrictions on the possession of certain substances, and a requirement to surrender passports.

Non-derogating Control Orders (i.e. those which were deemed not to impact on an individual's rights under ECHR) were issued by the Home Secretary. Derogating Control Orders could only be issued on application to a court, but no such Orders were ever made.39

In total, 52 individuals were subject to Control Orders; all were men who were suspected of involvement in Islamist terrorism.40 When Control Orders were introduced in 2005, all the individuals subject to an Order were foreign nationals. By the time they were replaced by TPIMs in 2011, all were British Citizens.

Control orders in force by quarter

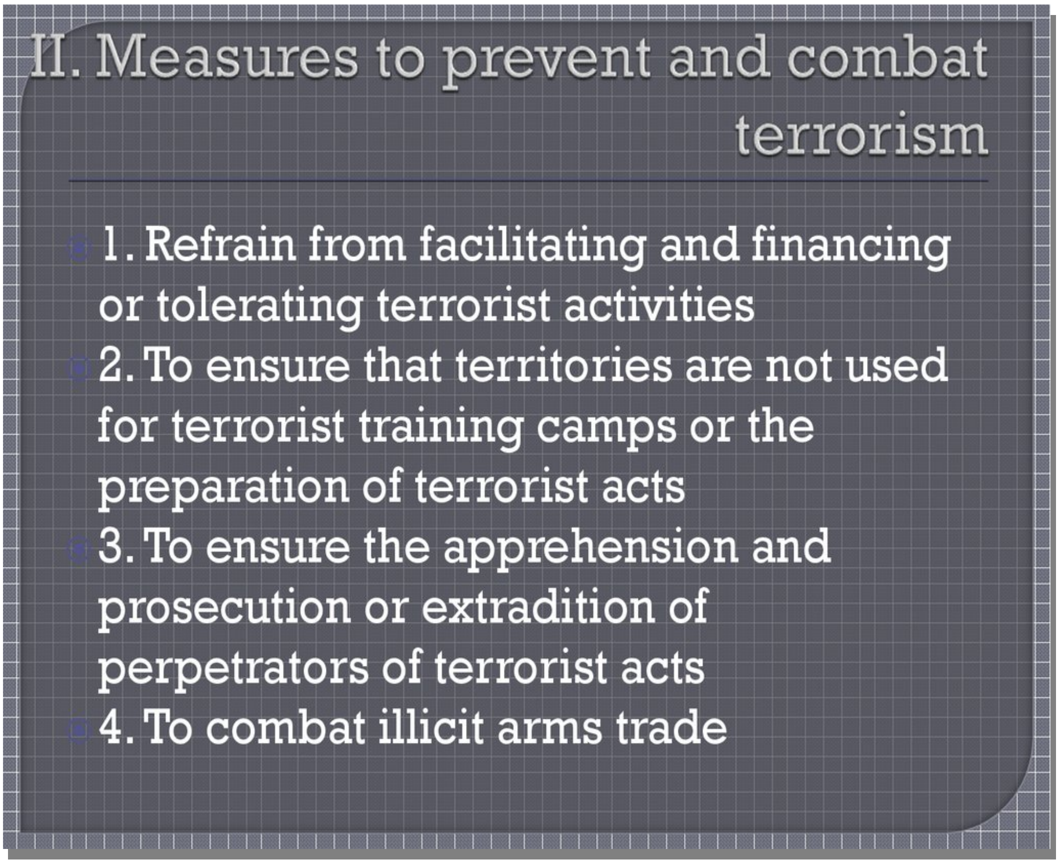
Under both the Control Orders regime and TPIMs, the Home Secretary is required to make a statement to Parliament every three months listing the number of measures in force. Data has been collated from these statements as recorded in Hansard and used to create the charts above and below which show the number of measures in force.

Terrorism Prevention and Investigation Measures (TPIMs) were introduced by the Coalition Government in 2011 as a replacement for Control Orders.

Like Control Orders, TPIMs are issued by the Home Secretary. They may also place certain obligations on an individual but are restricted to 12 measures listed in Schedule 1 of the 2011 Act. **TPIMS in force by quarter**

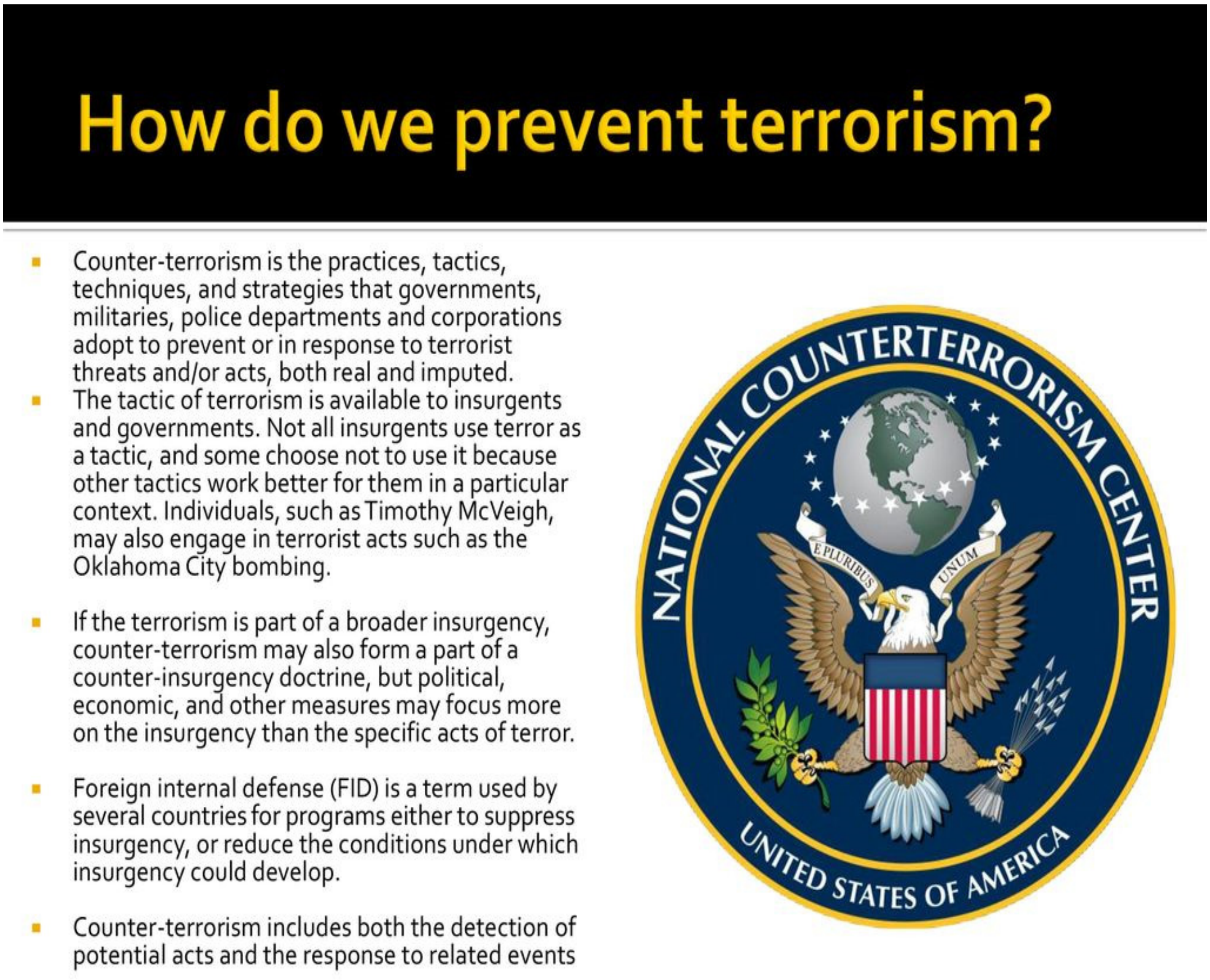
There are currently seven TPIMs in force; considerably fewer than at the peak when 20 Control Orders were in force in June 2009. One notable trend is the reduction in the number of measures issued against foreign nationals over the years with a contrasting increase in those issued against British Citizens.

IMAM HUSSEIN 3
SHIA WAVES
Shia World News
Countering Terrorism in UK
Several people received letters calling on them to attack Muslims



II. Measures to prevent and combat terrorism

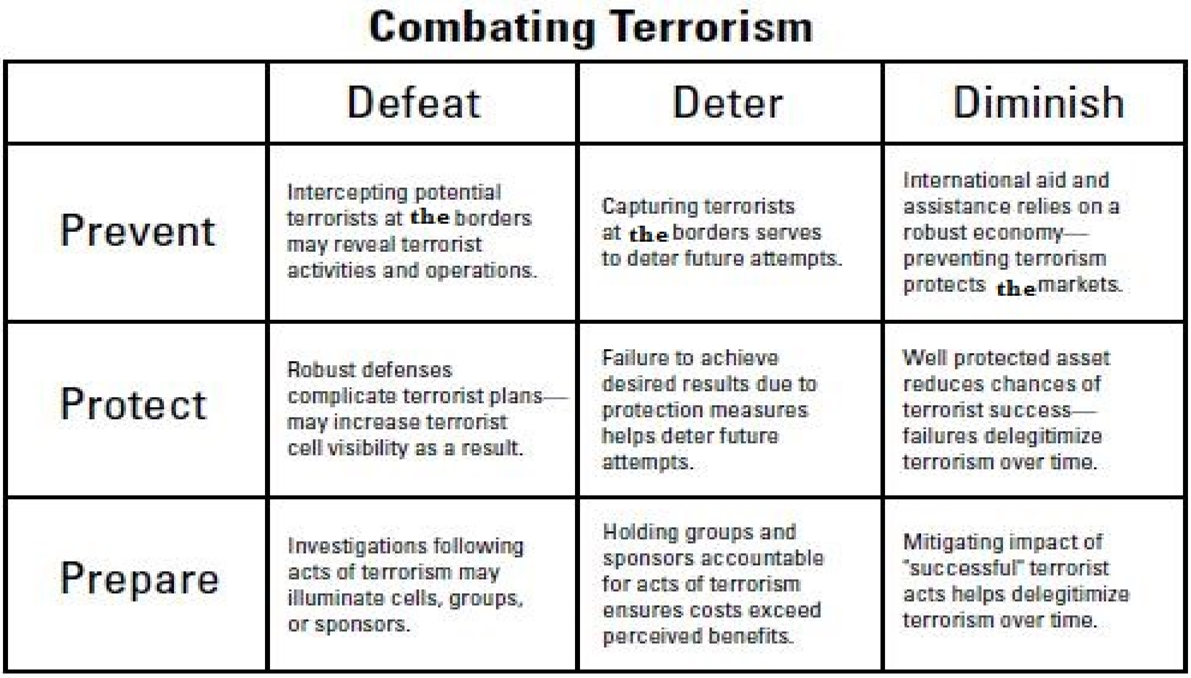
- 1. Refrain from facilitating and financing or tolerating terrorist activities
- 2. To ensure that territories are not used for terrorist training camps or the preparation of terrorist acts
- 3. To ensure the apprehension and prosecution or extradition of perpetrators of terrorist acts
- 4. To combat illicit arms trade



How do we prevent terrorism?

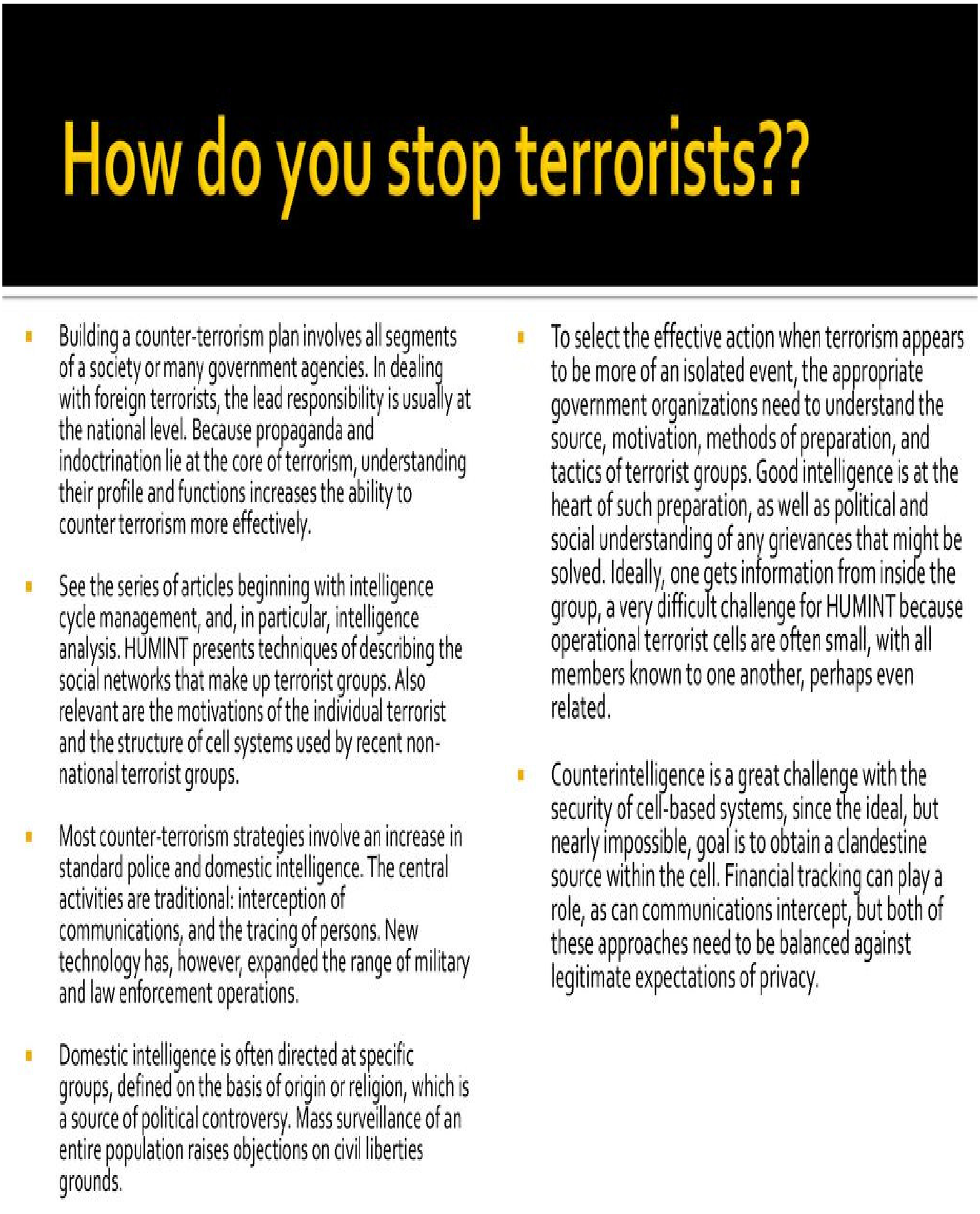
- Counter-terrorism is the practices, tactics, techniques, and strategies that governments, militaries, police departments and corporations adopt to prevent or in response to terrorist threats and/or acts, both real and imputed.
- The tactic of terrorism is available to insurgents and governments. Not all insurgents use terror as a tactic, and some choose not to use it because other tactics work better for them in a particular context. Individuals, such as Timothy McVeigh, may also engage in terrorist acts such as the Oklahoma City bombing.
- If the terrorism is part of a broader insurgency, counter-terrorism may also form a part of a counter-insurgency doctrine, but political, economic, and other measures may focus more on the insurgency than the specific acts of terror.
- Foreign internal defense (FID) is a term used by several countries for programs either to suppress insurgency, or reduce the conditions under which insurgency could develop.
- Counter-terrorism includes both the detection of potential acts and the response to related events

NATIONAL COUNTERTERRORISM CENTER
E PLURIBUS UNUM
UNITED STATES OF AMERICA



Combating Terrorism

	Defeat	Deter	Diminish
Prevent	Intercepting potential terrorists at the borders may reveal terrorist activities and operations.	Capturing terrorists at the borders serves to deter future attempts.	International aid and assistance relies on a robust economy—preventing terrorism protects the markets.
Protect	Robust defenses complicate terrorist plans—may increase terrorist cell visibility as a result.	Failure to achieve desired results due to protection measures helps deter future attempts.	Well protected asset reduces chances of terrorist success—failures delegitimize terrorism over time.
Prepare	Investigations following acts of terrorism may illuminate cells, groups, or sponsors.	Holding groups and sponsors accountable for acts of terrorism ensures costs exceed perceived benefits.	Mitigating impact of "successful" terrorist acts helps delegitimize terrorism over time.



How do you stop terrorists??

- Building a counter-terrorism plan involves all segments of a society or many government agencies. In dealing with foreign terrorists, the lead responsibility is usually at the national level. Because propaganda and indoctrination lie at the core of terrorism, understanding their profile and functions increases the ability to counter terrorism more effectively.

- See the series of articles beginning with intelligence cycle management, and, in particular, intelligence analysis. HUMINT presents techniques of describing the social networks that make up terrorist groups. Also relevant are the motivations of the individual terrorist and the structure of cell systems used by recent non-national terrorist groups.

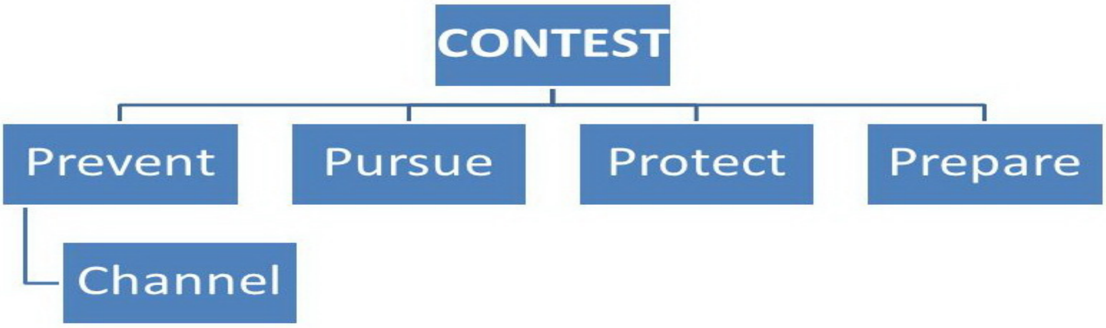
- Most counter-terrorism strategies involve an increase in standard police and domestic intelligence. The central activities are traditional: interception of communications, and the tracing of persons. New technology has, however, expanded the range of military and law enforcement operations.

- Domestic intelligence is often directed at specific groups, defined on the basis of origin or religion, which is a source of political controversy. Mass surveillance of an entire population raises objections on civil liberties grounds.

- To select the effective action when terrorism appears to be more of an isolated event, the appropriate government organizations need to understand the source, motivation, methods of preparation, and tactics of terrorist groups. Good intelligence is at the heart of such preparation, as well as political and social understanding of any grievances that might be solved. Ideally, one gets information from inside the group, a very difficult challenge for HUMINT because operational terrorist cells are often small, with all members known to one another, perhaps even related.

- Counterintelligence is a great challenge with the security of cell-based systems, since the ideal, but nearly impossible, goal is to obtain a clandestine source within the cell. Financial tracking can play a role, as can communications intercept, but both of these approaches need to be balanced against legitimate expectations of privacy.

UK Counter-terrorism strategy



CONTEST

Prevent

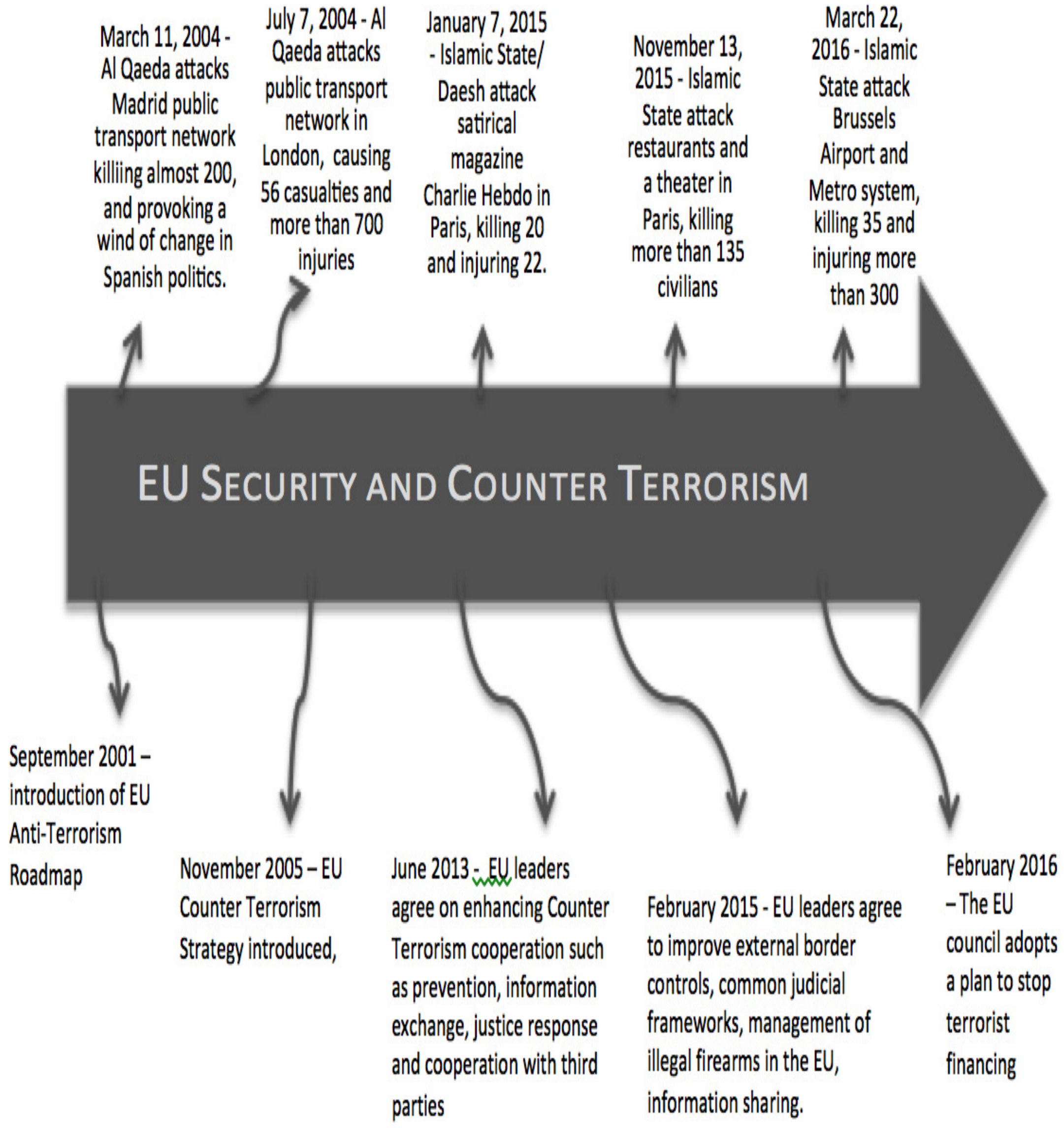
Pursue

Protect

Prepare

Channel

- Channel is a local monthly multi-agency meeting which considers the referrals made to Prevent. A preliminary assessment is made and a support plan is created. This is all pre-criminal and requires consent.



EU Security and Counter Terrorism

March 11, 2004 - Al Qaeda attacks Madrid public transport network killiing almost 200, and provoking a wind of change in Spanish politics.

July 7, 2004 - Al Qaeda attacks public transport network in London, causing 56 casualties and more than 700 injuries

January 7, 2015 - Islamic State/ Daesh attack satirical magazine Charlie Hebdo in Paris, killing 20 and injuring 22.

November 13, 2015 - Islamic State attack restaurants and a theater in Paris, killing more than 135 civilians

March 22, 2016 - Islamic State attack Brussels Airport and Metro system, killing 35 and injuring more than 300

September 2001 – introduction of EU Anti-Terrorism Roadmap

November 2005 – EU Counter Terrorism Strategy introduced,

June 2013 - EU leaders agree on enhancing Counter Terrorism cooperation such as prevention, information exchange, justice response and cooperation with third parties

February 2015 - EU leaders agree to improve external border controls, common judicial frameworks, management of illegal firearms in the EU, information sharing.

February 2016 – The EU council adopts a plan to stop terrorist financing

Conversation Questions

Terror

- Why do people use terror?
- What terror actions do you remember?
- What should be done to prevent terror?
- Are you afraid of traveling because of terror?
- Why is terror used more in some countries than others?
- Do you know of any forms of terror other than bombs?
- Have you been a victim of terror?
- Do you think terror is justified?
- How has airline travel been affected by terrorism?
- What do you think of airport security?
- Have you ever been patted down?
- Have you ever had a body scan?

What do you think security personnel think when they see you in a body scanner?

Is violence ever okay?

Where were you during the 9/11 attack on the World Trade Center buildings in New York City?

Are terror tactics ever effective? When?

What is the difference between a 'freedom fighter' and a 'terrorist'? Is there a difference?

Is it possible for governments to cause terror? Ifso, giveexamples.

In your own words define the word "terrorism."

What is terrorism about?

- Race?
- Religion?
- Nationality?

Can you name any terrorist groups?

Can you name any fugitive terrorists?

How do terrorist groups operate?

What methods/tactics do terrorists use?

Why do people commit terrorist acts?

How much do you know about the Catholic/Protestant/Islamic religions?

Is religion to blame for the increase in world terrorism? Ifso, howmuch?

Which countries have been accused of harboring terrorists?

Which countries have been victims of terrorist plots?

What specific terrorist acts can you recall?

Who's winning the war on terrorism?

What do you believe is the best way to deal with terrorism?

What can governments do to eradicate world terrorism?

What kind of power could be given to special terrorist operations task-forces?

Would you ever consider committing suicide for the sake of a cause you believe in?

What cause would you fight for?

Where do terrorists get their money and weapons from?

If the money was right, would you work in a known terrorist-plagued state?

Are governments listening hard enough to extremists? Ifnot, whynot?

How much do you believe extremists are open to dialogue with Governing bodies?

In your opinion will terrorism spread or decline in the future?

Do you know anything about terrorist activities?

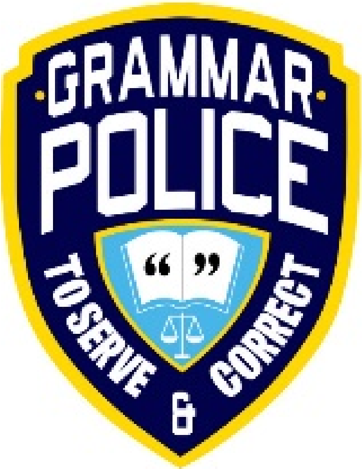
Have you ever seen a terrorist?

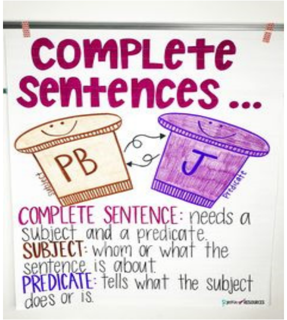
Do you have a friend of terrorist?

What do you know about suicide bombers?

Do you think that abusing a group of people can make them into terrorists?

GRAMMAR IN USE





Complete sentences ...

COMPLETE SENTENCE: needs a subject and a predicate.
SUBJECT: whom or what the sentence is about
PREDICATE: tells what the subject does or is.

1. Complete the sentences in your own words:

1) The militia officer would have gone abroad, if ________________________.

2) I would tell the officer about the accident, if __________________________.

3) We will go to the cinema, if ____.

4) If you have finished the work, ______________________________________.

5) If you lose your favourite umbrella, __________________________________.

6) If I get a lot of money, ____.

7) I would have bought that expensive painting, if ______________________.

8) If he earned a lot, ____.

9) If you spend your holidays abroad, ___________________________________.

10) I will leave the door ajar, if _______________________________________.

11) You will miss your bus, if ____.

12) If it rains tomorrow, ____.

13) They would go boating after a busy working day, if _________________.

14) If you should change your mind, _____________________________________.

15) If it was possible, ____.

2. Put the verb into the correct form (Appendix 4):

1) If she ___ (to go) abroad, she ___ (to be) very happy.

2) I ___ (to visit) him in the hospital, if I ___ (to have) free time.

3) If we ___ (not to like) his suggestion, we ___ (to tell) him about it.

4) If John ___ (to want) the advice, he ___ (to ask) you.

5) If you ___ (to have) better qualification, you ___ (to be able to) applyfor better job.

6) If you ___ (to want) to find necessary information, you ___ (to surf) thenet.

7) If somebody ___ (to steal) your collection of stamps, you ___ (to call)the police.

8) If I ___ (to have) a billion dollars, I ___ (to travel) around the world.

9) You ___ (to feel) better, if you ___ (to go to bed) earlier.

10) You ___ (to have) free time, if you ___ (to do) everything in time atwork.

11) If he ___ (not to lose) his ticket, he ___ (to go) home by train.

12) If you ___ (to ask) a militia officer, he ___ (to help) you to find yourbaggage.

13) Don't be nervous if you ___ (to hear) bad news.

14) Our group ___ (to go) to Paris, if we ___ (to win) the competition.

15) If I ___ (to know) her phone number, I ___ (to phone) her.

	If-clause	Main clause	use	Example
Type 0 Real present	If + any present form	Present Simple	Real - for general truth	If you heat the water, it boils.
Type 1 Real present	If + any present form	Future / Imperative can/ may / might / must/	Real - likely to happen in the present or future	If you work hard, you'll be tired.
Type 2 Unreal present	If + Past Simple / Past Continuous	Would/ could/ might + bare inf.	Unreal-unlikely to happen in the present or future; also used to give	If I were you, I wouldn't judge him.

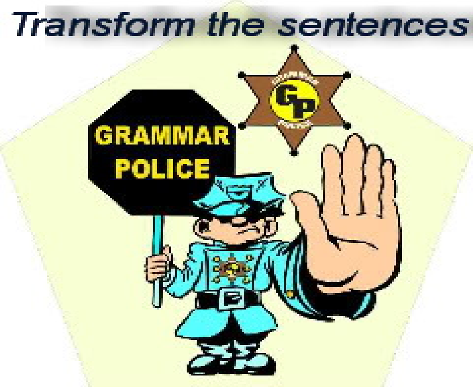
Type 3 Unreal past	If + Past Perfect/ Past Perfect Continuous	Would/ could/ might + have + past participle	Unreal situation in the past; also used to express regrets and criticism	If you had locked the car, it wouldn't have been stolen.

3. Work in pairs. Make a dialogue. Student A is a police officer. StudentB is a tourist. Discuss all unpleasant situations which can happen witha tourist and the preventive methods:

e.g. A: If you go abroad on holiday, you should know the laws of the countryyou are going to.

B: Yes, I know, but I'd like to clarify some points. What should I do if I lose mypassport?

A: If you do it, you should go to a militia station and…



4. Transform the sentences, using "I wish" (Appendix 3):

1) I'd love to know five foreign languages.

2) Why don't we go to the restaurant more often?

3) She hates working on Saturdays.

4) He'd love to investigate this case.

5) I'd like to live in Great Britain.

6) They hate playing board games after dinner.

7) They didn't go to the party.

8) He decided to stop working as a detective.

9) He lost all his money.

10) Unfortunately, I didn't tell you the truth.

5. Imagine that you are a wizard and you can change your life.

Tell your group what you'd like to change. Use "I wish".

6. Put the verb in brackets into the correct form (Appendix 3).

1) I wish I ___ (to hang out with friends) after a busy working day.

2) He fell and broke his leg pursuing the criminal. I wish he ___ (to be)more careful.

3) I wish you ___ (to read) more English books in future, because it isnecessary for working abroad.

4) I can't remember where I've put my binoculars. I wish I ___ (to can).

5) I wish I ___ (not to lend) him my new car. He has broken it.

6) My watch has stopped. I wish I ___ (to have) a better watch.

7) I feel so tired. I wish I ___ (not to stay up) so late last night.

8) I wish I ___ (not to spend) all my money last night.

9) I wish he ___ (to present) me his painting.

10) I wish I ___ (to watch) comedy show after stressful working day.

7. In pairs write a short story on "The ideal working day of a police officer". Use "I wish" constructions. Write 80-100 words.

Choose one correct variant

8.

1. If she is as clever as you say, she ___ rich by now.

a) will be b) would be c) would have been

2. If he had finished his work yesterday, he ___ free now.

a) would be b) would have been c) will be

3. If I were you, I ___ the facts before I accused them.

a) would check b) will check c) would have

checked

4. If she were in your position, she ___ him by now.

a) will help b) would help c) would have helped.

5. They ___ that expedition if they have enough free time.

a) will join b) would join c) would have joined

6. If her neighbours are too noisy, she always ___.

a) complains b) complained c) has complained

7. I wish cadets ___ more fashionable clothes.

a) wear b) wore c) worn

8. I wish she ___ more pleasant to the victims of the robbery.

a) had been b) is c) will be

9. I wish they ___ me more.

a) pay b) paid c) would pay

10. If they liked that souvenir, they ____ it.

a) will buy b) would buy c) would have bought

9. Put the verbs in brackets into the correct tense:

"If you don't call the police, you 1)__________ (never find) your collection ofbadges". I remember my relatives saying me these words when myhouse was robbed. If I 2)_________ (listen) to them, I 3)________ (get) back mybadges. If I 4)_________ (explain) the situation to a police officer, hecertainly 5)________ (help) me. If I 6)__________ (can / change) anything aboutthat situation, I 7)_________ (get) my badges back. But for me, everything8)________ (find) and the thief 9)________ (punish). If only I 10)________(understand) it earlier…

10. Read the dialogue between the interviewer and the policeofficer. Then rewrite it into Reported Speech (Appendix 1):

I:Good afternoon! We are glad to see you!

P:Hello! I'm glad to see you too!

I:You are so brave and strong. How can you connect your job with healthylife style?

P:Actually I do not have enough time for cooking meals and going in forsports, but I try to do my best. I eat fresh fruit and vegetables and drinka lot of milk.

I:What role does sport play in your life?

P:As I have mentioned I do not go in for sports, but I am fond of suchactivities that allow me to keep fit at home. I start with running then Itake exercise programmes.

I:Do your colleagues go in for sports?

P:Yes, of course. Some of them prefer swimming, skiing, playingbadminton, others are keen on football, boxing. Unfortunately, publicsport facilities are not always available to my colleagues and they areengaged into outdoor activities. Most of them prefer running too.

I:What do you know about foreign sport programmes for police?

P:According to the latest figures the most popular sports in Europe andAmerica are walking, cycling and jogging.

I:So, we see that our officers are very strong and healthy.

P:Certainly! Sport is very important in our life. Keep fit. Be in harmony withyour soul and body!

I:Thank you…

11. Read the passage from the policeman's report and rewrite it intoReported speechand translate it:

Policeman: "I visited Sandra Black on Monday (the 6th of November) she was withher two children: a boy, named Peter, and girl, named Betty. Peter is five yearsold and Betty is seven.

The house of Sandra is not appropriate for children living. There is nolightening inside. Also, it is cold in the rooms. The rooms are dirty and there is alot of rubbish. It would be great if Sandra Black cleans her rooms and Betty helpsher about the house. Another good idea is to pay for central heating and hotrunning water or to install a boiler. Also it is necessary for them to cover the floorwith a carpet. If Sandra Black doesn't do these recommendations her childrencan catch a cold, have a headache, sore throat and bad cough. Moreover, SandraBlack should pay attention to her children's way of life. It is forbidden to eat junkfood and drink cola every day. Children need in vitamins and sport activities.

They ought to eat fresh fruit and vegetables, dairy products, drink green tea andjuice. Furthermore, they must not play computer games and watch TV all daylong. It is necessary to walk, to go in for sports and to have a rest and lots ofsleep.

If Sandra Black doesn't follow my advice her children will have lots ofproblems with their health."

13. Choose the correct answer (Appendix 1):

1. He asked me if I would be working late this/that night.
2. Frank asked her where she bought/had bought that oily fish.
3. The doctor told me to keep/kept fit.
4. Alice said she was tired and she is going/was going to liedown.
5. My friend asked me how long I had been eating/ate junk food.
6. She asked us if we would/would we agree to help her.
7. Peter said he learnt/had learned the rule and he was doingthe exercise.
8. George said he doesn't/didn't want to catch cold and stay athome.
9. My aunt said she could hardly stop/stopped from laughing.
10. She asked Tim if his cold is/was any better that day.

14. First read then report what the colonel told the lieutenants:

1. Do not smoke in no-smoking areas.

2. Keep fit and go in for sports.

3. Don’t be drunk!

4. Wear your uniform!

5. Visit a doctor at least two times a year.

6. Be smart!

7. Don’t sleep during your work.

8. Never miss your breakfast.

9. Don’t be nervous.

10. Follow healthy lifestyle.

1. He told them…____

2. ____

3. ____

4. ____

5. ____

6. ____

7. ____

8. ____

9. ____

10. ____

15. Paraphrase using Direct Speech:

1) Steve told me that he had been working sixty hours a week for thelast 2 months.

2) Alison told me she was having dinner.

3) She asked me not to open the window.

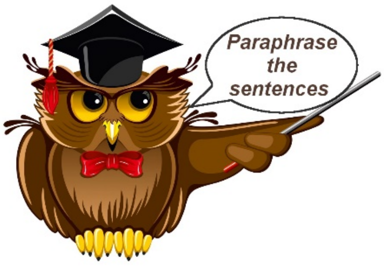
4) said he had had an accident.

5) The boy said he was afraid he had broken his leg.

6) Kate told her mother she would not be out for long.

7) He said that he had gone in for boxing before he entered theuniversity.

8) David said he had broken the bicycle.



16. Paraphrase using Reported speech:

1) "Give me a cup of tea, please", said the captain to a cadet.

2) "Don't drink too much alcohol", said the lieutenant to an old man.

3) "Don't make so much noise at night", said the militia officer to amusician.

4) "Don't smoke in public", said the major.

5) "Get up early and do mourning exercises", advised the doctor.

6) "Don't eat for several days", my doctor told me.

7) Nick's father said to him: "Please, pass me a cigarette".

8) "Stay back!" – ordered the militia.

9) "Don't sell alcohol to children", – the militiaman told the shopassistant

17. The captain asked the suspect some questions. First read,then report the captain's questions:

1. What's your name?
2. Where do you work?
3. Where were you last night?
4. Are you familiar with Mr. Simons?
5. Why did you visit him?
6. What pills did you give him?
7. When did you buy the medicine?
8. Where did you buy it?

9. Why didn't you consult the doctor?

1. The captain asked the suspect… ________________________________

2. ____

3. ____

4. ____

5. ____

6. ____

7. ____

8. ____

9. ____

Choose one correct variant

18.

1) "Please sir, can I have some more food?" _____ Oliver.

a) told b) said c) tell

2) He insisted that I _____ breakfast.

a) had missed b) missed c) miss

3) Alan asked the doctor _____ lose weight.

a) how could he b) how he can c) how he could

4) He offered _____ me some delicious meals.

a) cooked b) to cook c) cook

5) The doctor didn't suggest _____ pizza.

a) ordering b) ordered c) had ordered

6) The officer informed us that all pills _____.

a) were still being

checked

b) is still being

checked

c) still checked

7) The policeman ordered the driver _____ of his car.

a) step out b) to step out c) stepping out

8) The policeman explained that it _____ illegal to sell cigarettes to children.

a) been b) is c) was

9) An old man protested that he _____ junk food.

a) had eaten b) was eaten c) ate

10) Christine complained that she _____ a cold.

a) caught b) catch c) to catch

11) Katy asked _____ they would be able to visit the gym thefollowing year.

a) if b) of c) unless

12) He promised that they _____ the following night.

a) would have a rest b) will have a rest c) had a rest

13) He denied _____ the truth.

a) tell b) said c) telling

14) That man accused me of acting as if _____ guilty.

a) I am b) I were c) I had

15) The militiaman _____ whether I saw a wrongdoer.

a) wondered b) told c) said

16) We _____ how we could avoid stressful situations.

a) wonder b) asked c) ask

APPENDIX

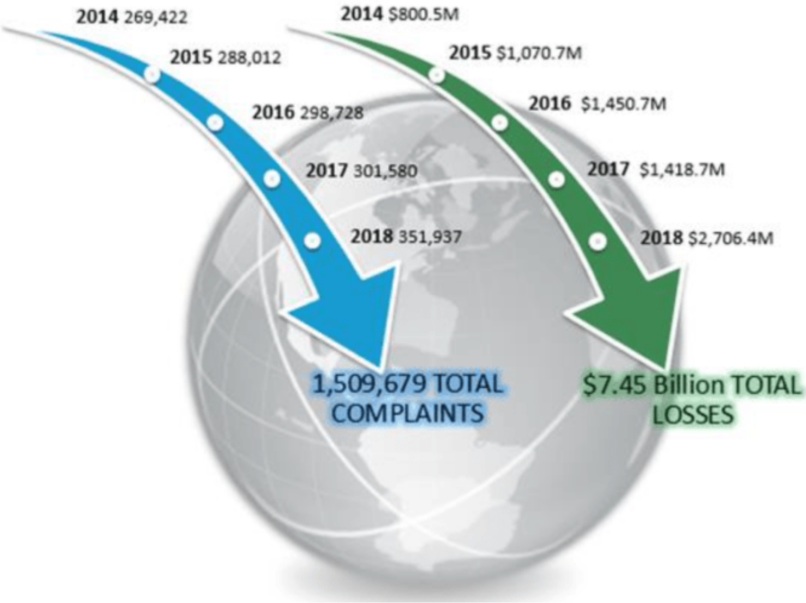
Supplementary Reading

THE FINANCIAL TELEGRAM

FINANCIAL INTELLIGENCE MAGAZINE

MARK CORMICK APRIL 25, 2019 CYBERCRIME

FBI Internet Crime Report – Cybercrime On The Rise



Losses from Internet crime in the U.S. nearly doubled in 2018 to $2.7 billion, with almost half of that from business email schemes that targeted wire transfer payments, according to the FBI's 2019 Internet Crime Report.

The report said that the FBI's *Internet Crime Complaint Center (IC3)* received approximately 352,000 complaints about cybercrime activity last year. The center has averaged about 300,000 complaints in each of several prior years, but the reported losses increased from $800.5 million in 2014 to $1.42 billion in 2017.

- **Business email scams** caused $1.2 billion in losses. This is a sophisticated scam targeting both businesses and individuals performing wire transfer payments. Perpetrators compromise legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- **Investment scams** caused $253 million in losses from 3,583 victims in 2018. Perpetrators induce investors to make investments on the basis of false information. These scams usually offer the victims large returns with minimal risk. Variations of this scam include retirement schemes, Ponzi schemes, and pyramid schemes.
- **Cyber extortion** caused 51,146 complaints and $83 million in losses in 2018, a 242% increase in complaints from the previous year. Extortion is used in various schemes including Denial of Service attacks, hitman schemes, sextortion, government impersonation schemes, loan schemes, and high-profile data breaches (see cybercrime dictionary below).

According to the FBI report, virtual currency is commonly demanded as the payment mechanism in cybercrime schemes because it provides the criminal with an additional layer of anonymity when perpetrating these schemes.

In February 2018, the FBI launched a *Recovery Asset Team (RAT)* to focus on recovering monies lost through business email scams. In 2018, the team recovered $257 million that has been wired by cybercrime victims, a recovery rate of 75%, the report says.

Cybercrime Dictionary

- A *Denial of Service attack* typically uses one computer and one Internet connection to flood a network/system.
- A *hitman scheme* is an email extortion in which a perpetrator sends a disturbing email threatening to kill the recipient and/or their family. The email instructs the recipient to pay a fee to remain safe and avoid having the hit carried out.

- *Sextortion* occurs when a perpetrator threatens to distribute an individual's private and sensitive material unless the individual provides the perpetrator images of a sexual nature, sexual favors, or money.
- *Government impersonation* occurs when a government official is impersonated in an attempt to collect money.
- A *loan scheme* involves perpetrators contacting victims claiming to be debt collectors from a legitimate company and instructing victims to pay fees in order to avoid legal consequences.
- A high profile *data breach* is when sensitive, protected or confidential data belonging to a well-known or established organization is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- A *Distributed Denial of Service (DDoS)* attack uses multiple computers and Internet connections to flood a network/system.

Here are the biggest cybercrime trends of 2019

Cybercriminals are using more advanced and scalable tools to breach user privacy, and they are getting results. Two billion data records were compromised in 2017, and more than 4.5 billion records were breached in the first half of 2018 alone.

Here are the most pressing cybersecurity issues in 2019, as well as rising trends into 2020.

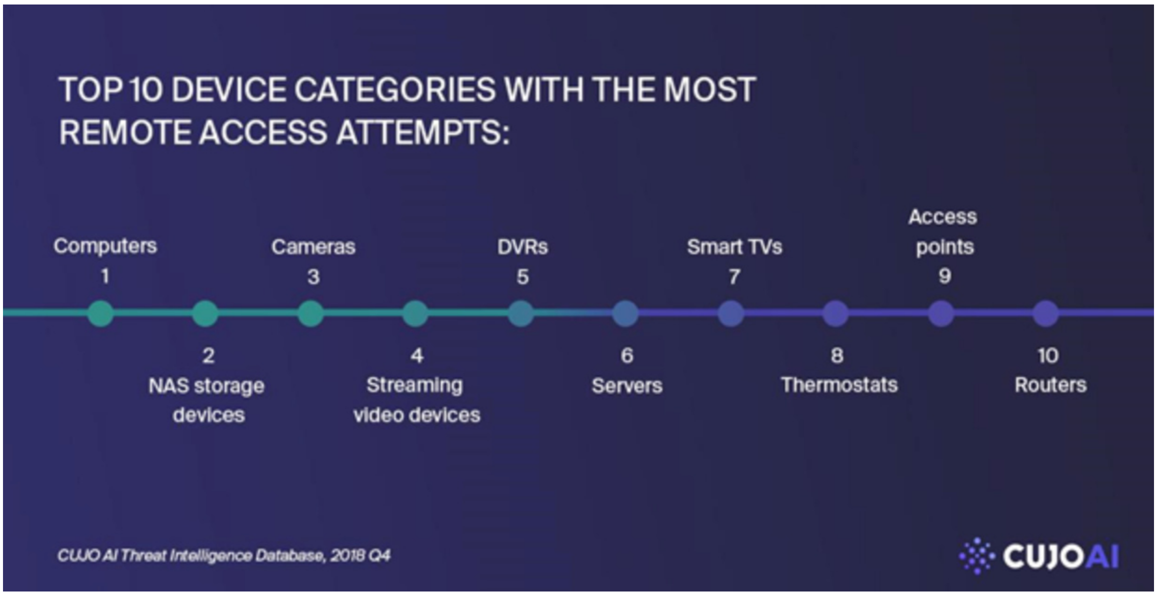
Advanced phishing kits

Four new malware samples are created every second. Phishing remains one of the most successful attack vectors due to its speed, as most phishing sites stay online for just four to five hours. Users only report 17% of phishing attacks, and it is seen as a low-risk type of activity. As a result, today only 65% of all URLs are considered trustworthy. This puts a strain on both the consumer and any enterprise with an online presence.

We predict that 2020 will be known for advanced phishing attacks, due to the number of new phishing kits available on the dark web. These kits enable people with only basic technical knowledge to run their own phishing attacks. With more tools available, phishing will become an even more dangerous attack method.

Remote access attacks

Remote attacks are growing in number, as well as becoming more sophisticated. One of the main types of remote access attack in 2018 was cryptojacking, which targeted cryptocurrency owners. Another popular type of attack threatened perimeter devices.



TOP 10 DEVICE CATEGORIES WITH THE MOST REMOTE ACCESS ATTEMPTS:

Computers
1

2
NAS storage devices

Cameras
3

4
Streaming video devices

DVRs
5

6
Servers

Smart TVs
7

8
Thermostats

Access points
9

10
Routers

CUJO AI Threat Intelligence Database, 2018 Q4

CUJO AI

According to our threat intelligence database, remote access attacks are among the most common attack vectors in a connected home. Hackers target computers, smartphones, internet protocol (IP) cameras and network attached storage (NAS) devices, since these tools usually need to have ports open and forwarded to external networks or the internet.

Attacks via smartphones

One of the most common attack vectors to smartphones are related to unsafe browsing (phishing, spear phishing, malware). More than 60% of fraud online is accomplished through mobile platforms, according to RSA, and 80% of mobile fraud is achieved through mobile apps instead of mobile web browsers.

As most people use their phones to manage financial operations or handle sensitive data outside the security of their home network, this becomes a prominent threat. The fact that users typically hold all their information on their phone, and that smartphones are now used for two-factor authentication - one of the most widely used cybersecurity tools - increases the security risk if the device is lost or stolen.

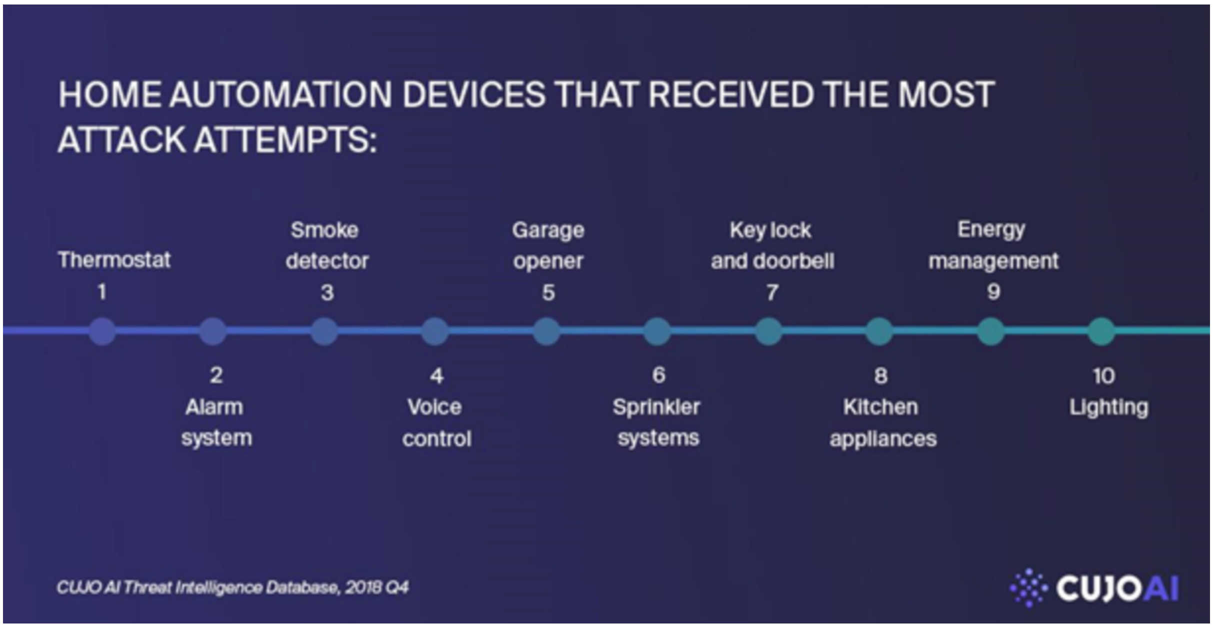
Have you read?

- Releasing trapped value is key to success in the digital world
- To better treat depression, these phone surveys track real-time emotions
- The mobile phone gender gap is a $700 billion opportunity

Vulnerabilities in home automation and the Internet of Things

The consumer Internet of Things (IoT) industry is expected to grow to more than seven billion devices by the end of 2020, according to Gartner. Many consumers do not see IoT devices as a vulnerability, because a significant portion of them do not have a user interface. This could lead to issues understanding what kind of data the device collects or manages.

However, IoT devices are not only collecting valuable user data. They could become an entry point for an attacker or tool to launch a distributed denial-of-service (DDoS) attack. IoT devices are not secure by design, because putting a focus on security would significantly increase manufacturing and maintenance expenses.



HOME AUTOMATION DEVICES THAT RECEIVED THE MOST ATTACK ATTEMPTS:

1 Thermostat

2 Alarm system

3 Smoke detector

4 Voice control

5 Garage opener

6 Sprinkler systems

7 Key lock and doorbell

8 Kitchen appliances

9 Energy management

10 Lighting

CUJO AI Threat Intelligence Database, 2018 Q4

CUJO AI

According to CUJO AI threat intelligence data, 46% of all attack types that these devices experience are remote access attempts and 39% are used for detecting behavioural patterns. With the exponential growth of connected devices at home, these threats are likely to increase.

Utilizing artificial intelligence

Most of the biggest industries already use machine learning (ML) and artificial intelligence (AI) to automate their processes and improve overall performance. Cybersecurity and cybercrime are no exception.

AI is often considered to be a dual-use technology - while more cybersecurity companies are implementing AI-driven algorithms to prevent threats, hackers are also taking the opportunity to become more effective.

The majority of AI qualities serve malicious purposes. AI systems are cheap, scalable, automated, anonymous and they provide physical and psychological distance for the attacker, diminishing the immediate morality around cybercrime.

- **Artificial intelligence for cybersecurity evasion**. Cybercriminals are using various evasion methods to avoid detection, and AI helps to optimize different elements of this process.

- **Artificial intelligence in phishing.** AI could help to create content that can pass through typical cybersecurity filters, such as email messages that are indistinguishable from those written by humans.

- **Artificial intelligence in social engineering**. While social engineering is one of the most popular hacking techniques, it takes a lot of time to implement properly. AI could help in not only collecting information, but also by writing emails or calling potential victims.

With new advances in AI-driven technology, utilizing AI in cyber attacks will become an even more popular and dangerous trend. (8582 печ.зн)

CYBERCRIME

Cybercrime is one of the EMPACT priorities, Europol's priority crime areas, under the 2018–2021 EU Policy Cycle.: the aim is to combat cybercrimes that are committed by organised crime groups and that generate large profits from such activities as online and payment card fraud, cybercrimes that cause serious harm to their victims such as child sexual exploitation, and cyber-attacks, which affect critical infrastructure and information systems in the EU.

Technical innovation can be harnessed for social good, but just as readily for nefarious ends. This is truer of cybercrime than of perhaps any other crime area. And cybercriminals are also getting more aggressive. That's why Europol and its partner organisations are taking the fight to them on all fronts.

According to the most recent Internet Organised Crime Threat Assessment (IOCTA) , cybercrime is becoming more aggressive and confrontational. This can be seen across the various forms of cybercrime, including high-tech crimes, data breaches and sexual extortion.

Cybercrime is a growing problem for countries, such as EU Member States, in most of which internet infrastructure is well developed and payment systems are online.

But it is not just financial data, but data more generally, that is a key target for cybercriminals. The number and frequency of data breaches are on the rise, and this in turn is leading to more cases of fraud and extortion.

The sheer range of opportunities that cybercriminals have sought to exploit is impressive. These crimes include:

- using botnets—networks of devices infected with malware without their users' knowledge—to transmit viruses that gain illicit remote control of the devices, steal passwords and disable antivirus protection;
- creating "back doors" on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets;
- creating online fora to trade hacking expertise;
- bulletproof hosting and creating counter-anti-virus services;
- laundering traditional and virtual currencies;
- committing online fraud, such as through online payment systems, carding and social engineering;
- various forms of online child sexual exploitation, including the distribution online of child sex-abuse materials and the live-streaming of child sexual abuse
- the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services.

High-tech crimes

Malware, or malicious software, infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware, and they can complement each other when performing an attack.

- A **botnet** (short for robot network) is made up of computers communicating with each other over the internet. A command and control centre uses them to send spam, mount distributed denial-of-service (DDoS) attacks (see below) and commit other crimes.

- A **rootkit** is a collection of programmes that enable administrator-level access to a computer or computer network, thus allowing the attacker to gain root or privileged access to the computer and possibly other machines on the same network.
- A **worm** replicates itself over a computer network and performs malicious actions without guidance.
- A **trojan** poses as, or is embedded within, a legitimate programme, but it is designed for malicious purposes, such as spying, stealing data, deleting files, expanding a botnet, and performing DDoS attacks.
- A **file infector** infects executable files (such as .exe) by overwriting them or inserting infected code that disables them.
- A **backdoor/remote-access trojan (RAT)** accesses a computer system or mobile device remotely. It can be installed by another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions, including:
  - monitoring actions
  - executing commands
  - sending files and documents back to the attacker
  - logging keystrokes
  - taking screen shots
- **Ransomware** stops users from accessing their devices and demands that they pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.
- **Scareware** is fake anti-virus software that pretends to scan and find malware/security threats on a user's device so that they will pay to have it removed.
- **Spyware** is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party

- **Adware** displays advertising banners or pop-ups that include code to track the user's behaviour on the internet

Cybercrime https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

(4753 печ.зн.)

COMBATING CYBERCRIME WITH ACTIONABLE INTELLIGENCE: INTERPOL'S ASEAN CYBER CAPABILITY DESK

SINGAPORE – INTERPOL has launched an initiative to provide member countries in Southeast Asia with support in conducting cyber investigations and operations.

With cybercrime a growing threat across the region, the ASEAN Cyber Capability Desk will assist law enforcement in the 10 Association of Southeast Asian Nations (ASEAN) countries to enhance their ability to combat cybercrime through a combination of intelligence development, investigative support and operational coordination.

By turning information gathered from member countries and partners in the private security industry worldwide into actionable intelligence, the project will better position police in Southeast Asia to face the latest cyberthreats.

Through the ASEAN Desk, INTERPOL will also assist police across ASEAN with their cyber investigations by acting as a 'virtual task force' to connect and enhance communications between all relevant countries, both in Asia and beyond. When investigations lead to one-the-ground action against cybercriminals, INTERPOL can provide operational support and develop plans for multi-jurisdictional operations.

"In our globalized digital era, a cyber aspect is interwoven into all facets of our lives, and unfortunately, also into the actions of criminals. Law enforcement faces tremendous challenges to stay ahead of the new breed of cyber-savvy criminals," said Takayuki Oku, Acting Director of INTERPOL's Cybercrime unit.

"The creation of the ASEAN Cyber Capability Desk is a fundamental pillar of our commitment to support the ASEAN region and beyond in the fight against cybercrime," he concluded.

Although training is not a specific component of the project, the ASEAN Desk will liaise with other INTERPOL units which are providing cybercrime-related training in the region to ensure police have the necessary cybercrime skills.

The project, which is supported by the Singapore Ministry of Home Affairs, was presented during the 6th INTERPOL-Europol Cybercrime Conference held in Singapore.

Combating cybercrime with actionable intelligence: INTERPOL's ASEAN Cyber Capability Desk, *24 September 2018* https://www.interpol.int/News-and-Events/News/2018/Combating-cybercrime-with-actionable-intelligence-INTERPOL-s-ASEAN-Cyber-Capability-Desk

(2336 печ.зн.)

CYBERATTACKS KNOW NO BORDERS AND EVOLVE AT A FAST PACE WHILE THE INTERNET ALSO FACILITATES A RANGE OF MORE TRADITIONAL CRIMES.

Hacking. Malware. Botnets. The Darknet. Cybercrime as a service.

Words and phrases that scarcely existed a decade ago are now part of our everyday language, as criminals use new technologies to commit cyberattacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

'Pure cybercrime' refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user.

Traditional forms of crime have also evolved as criminal organizations turn increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. These ‘cyber-enabled’ crimes are not necessarily new – such as theft, fraud, illegal gambling, the sale of fake medicines – but they have taken on a new online dimension.

Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Police must therefore keep pace with new technologies, to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime.

Cyberattacks know no borders and evolve at a fast pace while the Internet also facilitates a range of more traditional crimes. https://www.interpol.int/Crimes/Cybercrime

INTERPOL PROJECT TO COMBAT CYBERCRIME IN THE AMERICAS

RIO DE JANEIRO, Brazil – INTERPOL has launched a training project in the Americas to enhance the capacity of police in the region to investigate and combat cybercrime.

The three-year Cybercrime Capacity Building Project in the Americas is assisting police across Latin America and the Caribbean to build their knowledge and skills to fight cybercrime through needs assessments and mentoring, training courses, operational activity, and public awareness initiatives.

A training course took place in Buenos Aires, Argentina in August which brought together 27 law enforcement officers from police and INTERPOL National Central Bureaus (NCBs) in 17 countries to discuss how INTERPOL’s policing capabilities can be used to tackle cybercrime.

Sessions focused on the role of traditional and digital forensics, information exchange and the support provided by INTERPOL's Regional Bureaus. Participants also visited the Cybercrime Unit of the Argentina Federal Police.

"It is paradoxical that the same technology that aids human development, also opens up the cyberspace as a new terrain for committing crimes without borders nor jurisdictions, and provides the tools for committing common crimes through the use of technology. As such, police and other law enforcement authorities must adapt and evolve, in order to be able to help our fellow citizens and protect them from cybercrime," said Nestor Roncaglia, Chief of Argentinian Federal Police at the opening of the course in Buenos Aires.

In September 2018, some 63 participants from 31 countries and 10 organizations including banks, international and regional organizations, and private cybersecurity companies met in Brazil for the 4th Americas Working Group meeting for Heads of Cybercrime Units. After a briefing on INTERPOL's current activities against cybercrime, the participants reviewed national cases, Internet governance regulations and the importance of information sharing amongst all stakeholders to generate accurate cyber intelligence.

"The opportunity to bring leaders of cybercrime investigations units to Brazil to discuss and exchange lessons learned is the best way to join forces in combating digital crimes. Today, we know that there are no borders in the virtual environment, so the adoption of joint measures is a cornerstone for moving towards a safer world," said the Head of the NCB in Brasilia, Federal Police Commissioner Rodrigo Bartolamei.

The project, funded by the Government of Canada, builds on the success of a pilot project on cybercrime capacity building in Latin America and the Caribbean which ended in 2017. It empowers the 35 beneficiary countries in the region to communicate and collaborate through the provision of specialized training, mentorship, access to a mobile classroom of cyber forensic equipment, a public awareness initiative on 'digital hygiene' or everyday digital security, and through the coordination of cybercrime operational activity.

INTERPOL project to combat cybercrime in the Americas *18 October 2018* https://www.interpol.int/News-and-Events/News/2018/INTERPOL-project-to-combat-cybercrime-in-the-Americas

Scotland Yard looks to set up crack cybercrime unit

Bill Goodwin

Computer Weekly

12 Mar 2003 12:35

Scotland Yard police chiefs are considering plans to create a computer crime unit of up to 25 detectives to investigate hacking and virus attacks against businesses in London and to provide specialist computer forensic services throughout the Metropolitan Police.

The proposed unit, to be formed by merging five existing computer crime operations across the Met, will create a single team of computer crime specialists, second only to the National High-Tech Crime Unit, which focuses on major organised crime.

The plan comes as the Met's existing computer crime unit, which will form the heart of the new operation, faces increasing pressure to provide support for paedophile and anti-terrorist work in addition to investigating a rising tide of hacking complaints.

Detective inspector Clive Blake, acting head of the unit, said his nine-strong team was "stretched" and having to work evenings and weekends to keep up with the volume of work. He believes a single unit could help the Met work more efficiently.

"This is an entirely personal opinion but, looking at what the FBI and the US secret service have been doing, it would make sense to have a large, multitasking team, with an operational cell and an intelligence cell in a self-contained unit."

Well-funded organised crime syndicates are beginning to move into computer crime and are hiring hackers to break into firms' computer systems to gather intelligence on their intended victims, Blake said.

In comparison, the Met's computer crime unit, which lacks its own budget, is considered poorly resourced. It has been forced to ask suppliers to donate sophisticated equipment needed for investigations free of charge under the Met's sponsorship scheme.

Peter Sommer, security expert at the London School of Economics, said, provided the proposals for a combined computer crime unit were not derailed by internal politics in the Met, the move could give police greater flexibility to investigate crime complaints.

"If you have a larger group, you have more flexibility and you can also have people who specialise. The larger the group of people, the more sense it makes to have people specialising in, say, computer networks."

Under the plans, the merged unit would bring together computer crime operations from Special Branch, the paedophile unit, the anti-terrorism division, and clubs and vice.

Scotland Yard looks to set up crack cybercrime unit, *by Bill Goodwin*, 12 Mar 2003 // https://www.computerweekly.com/news/2240049886/Scotland-Yard-looks-to-set-up-crack-cybercrime-unit

Cybercrime Statistics 2019: An In Depth Look at UK Figures and Trends

by Sandra Henshaw - November 9, 2018, Last Updated on June 14, 2019, How To Guides, Statistics https://www.tigermobiles.com/blog/cybercrime-statistics/

Share

In today's increasingly connected world, computers play a vital part in all of our lives. However, computers aren't always as safe as you might think. Whilst rates of cybercrime have been falling in the last twelve months, there's still a shockingly large amount of computer-oriented crime in the UK. What is cybercrime? How bad is the problem? Can you protect yourself? We've got everything you need to know.

What Is Cybercrime?

In very basic terms, cybercrime is any kind of crime that involves a computer. That could be hacking, or it could be identity theft or child pornography. Cybercrime covers a wide range of different offences, all of which are punishable by law in the UK. We can divide cybercrime up into two categories: crimes that affect people, and those that effect businesses.

Personal Cybercrime

The most frequent kind of cybercrime effects individuals or personal accounts. And there are many examples of this:

- **Phishing:** where you receive an email that pretends to be from an authority (perhaps your bank, or maybe your boss) in which you're asked to give out your passwords or personal information such as your address, telephone number, or other data.
- **File Hijacking:** where a hacker enters your computer and accesses your files, locking you out of them. The hacker then demands a ransom (usually money) before he will give you your files back.

- **Webcam Managing:** where hackers take over your webcam. This may be so that they can watch your keyboard and learn your passwords, or it may be to record video of you doing something personal that they can then blackmail you with, or perhaps just to learn personal information about you.
- **Screenshot Managing:** where hackers enter your computer and take screenshots of your display. This can help them get information about you, get passwords, or even blackmail you.
- **Keylogging:** where hackers can record your keystrokes on your computer, thus gaining your passwords or other personal info.
- **Ad Clicking:** where hackers encourage you to click on a link (perhaps by email, or on a webpage) which will then open malware or simply ask for your personal info.

Business Cybercrime

Unless you own your own business, most of us don't need to worry too much about business-oriented cybercrime, although it can affect us. There are generally two kinds of crime in this category:

- **Hacking:** where hackers enter a business's files or servers and gain information from them.
- **DDOS Attacks:** where hackers enter a business's files or servers and change them so that their services or web pages can't be accessed.

Though these kinds of crimes are more the concern of businesses, they can have an effect on you. When a business is hacked and the information is lost, some of that information could be yours. If your bank is hacked, for example, the hackers could gain your online banking password. And if a DDOS attack takes place then you may not be able to access a service that you need, such as that online banking portal.

What Are the Consequences of Cybercrime?

Now that you know what cybercrime is, you may be wondering what the point of it is. And, as with most kinds of crime, the point is money. In some of these crimes (such as file hijacking), it's obvious to see where the money is coming from. But other crimes are sneakier. Any crime that is used to get personal information from you is designed to aid identity theft. This is when someone pretends to be you in order to get money. This could be as simple as getting your banking password and clearing out your bank account. Or as complex as collecting enough personal information about you that the hacker can then open credit cards or apply for loans in your name. To find out more about identity theft, you might want to check out our article on the subject.

How Bad is the Problem?

Each year the UK Office for National Statistics (ONS) releases a Crime Survey for England and Wales. In the most recent survey for the year ending in March 2018, the ONS estimates that around 4.5 million cybercrimes were committed in England and Wales during that twelve month period. Of those, around 3.24 million were fraud offences, and about 1.23 million were related to computer misuse (encompassing child pornography and hacking).

However, the survey does state that though this number is huge, it's a 31% decrease in cybercrime over 2017. This is thought to be due to fewer computer viruses and better anti-virus technology. Don't get complacent, however. You are still far more likely to fall victim to cybercrime than any other kind of crime in the UK. In 2017 around 17 million UK residents were victims of cybercrime, with around £130 billion being stolen.

For the latest year in which figures were available (ending June, 2017), there was a big difference in the kinds of frauds committed under the heading of cybercrimes. Bank and credit card fraud made up around 75% of all offences, with consumer or retail fraud (taking out loans, signing mobile phone contracts, purchasing things in someone else's name) made up around 22% of the total number of crimes. Under the heading of computer misuse, around 67% of cybercrimes were related to malware or viruses whilst 33% were related to unauthorised access of personal information.

When it comes to businesses, the 2018 Cyber Security Breaches Survey estimates that two in five businesses have been subject to some kind of cybercrime within the past twelve months. There is an average cost of around £3000 per business per cybercrime, which adds up to billions of pounds, not to mention the personal costs of consumers losing data or becoming victims of fraud.

What Does All This Mean?

The upshot of all the above statistics is that cybercrime is a problem in the UK. If 17 million people were affected by cybercrime in 2017, that means that 25% of UK residents have been a computer crime victim. That gives you a one in four chance of somehow being affected by cybercrime. And that does NOT include business cyber crimes such as hacking or DDOS, which could have a secondary effect on you. You are ten times more likely to be the victim of cybercrime than you are to be the victim of someone stealing from your person (a pickpocket, perhaps), and thirty-five times more likely to be affected by cybercrime than physical robbery.

Who Is Affected?

According to the Office of National Statistics, there are some factors that make you more likely to be a victim of cybercrime:

Age

Adults aged between 35 and 44 are slightly more likely to be victims of cybercrime (by around 7.4%). This is in comparison to 16 to 24-year-olds (4.9%), 65 to 74-year-olds (5.4%) and over 75 (2.8%).

Income

Households with incomes of more than £50,000 per year have a slightly higher risk than those below that threshold. This could be due to the fact that more affluent households tend to have more internet-connected devices, however.

Occupation

Managers and professionals such as doctors and lawyers have a slightly higher chance of being victims of cybercrimes.

Location

Residents of more affluent areas tend to be more likely to become victims of cybercrimes than those in more deprived areas. Again though, this could be due to the fact that more affluent residents tend to have more internet-connected devices.

However, all the differences found in the ONS cybersecurity reports were very small, far smaller than the differences seen in characteristics of those more likely to be victims of violence, for example. The bottom line is that cybercrime can really happen to anyone.

Cybercrime Laws in the UK

Cybercrime is a crime and it is illegal. The UK has relatively strict laws regarding computer crimes when compared to other countries. Any crime that involves fraud is covered by existing UK fraud laws, most recently the Fraud Act of 2006. However, cybercrime is additionally covered by the Computer Misuse Act of 1990. The unfortunate truth of the matter though is that cybercriminals are seldom caught, and even more seldom prosecuted. In 2017 there were a mere 47 prosecutions of cybercriminals. And the number of fraud prosecutions has fallen by a third since 2011.

How Can I Protect Myself?

Given that so few cybercrimes are actually prosecuted, protecting yourself from cybercrime is key. Whilst there's no way to completely eliminate the threat, there are various things that you can do to defend yourself:

Your Devices

- Ensure that your devices all have solid, up to date anti-virus security.
- Install a firewall on your computer.
- Install anti-spyware software on your computer.
- Ensure that you update your software (including Windows or iOS) when prompted to do so, postponing an update can leave you vulnerable.
- Ensure that your devices are password protected with a strong password. You can find the official governmental advice on creating passwords here.
- Ensure that should any of your devices be stolen that you can quickly change account passwords. This may mean keeping a list of all your accounts so that you know what you need to change.
- Cover your webcam when it's not in use. A small piece of non-transparent tape or a post-it note should be fine.

Your Online Usage

- Be aware of your surroundings, make sure that no one is looking over your shoulder or watching as you type in passwords.

- Do not connect to unfamiliar WiFi networks. If you must do this, do not access any sensitive information whilst on the connection.
- Do not click or anything or download anything unless you are 100% confident in the source.
- Do not reply to emails asking for personal information or passwords. If an authority, perhaps your bank, asks for information over email, call your branch and ask for confirmation that they actually need this data.
- If you're going to enter sensitive information such as a credit card number into a website check the address bar for a padlock symbol and the prefix 'https' rather than just 'http' to indicate that the site is a secure one.
- Do not give out personal information, even something as simple as your address, unless you absolutely know that data is going somewhere trustworthy.

Miscellaneous Tips

- It can be difficult to know if fraud has occurred until it is too late. The best way to know if someone is borrowing money in your name or using your funds is to keep a close eye on your finances. Check bank statements and credit card statements regularly, and check your credit rating at least once a year to be sure that no suspicious transactions are taking place. You can check your credit report with Experian, Equifax, or Transunion (formerly CallCredit) for free.
- Follow news reports of data breaches for major companies, and if you have a connection to a breached company ensure that you change any account passwords related to them.

What Do I Do If I Suspect a Cybercrime?

If you suspect that a cybercrime has occurred then there are a few steps that you can take:

- Report any losses to your local police station
- Report fraud to Action Fraud, the UK's police fraud squad
- In the case of blackmail or ransomware do NOT pay. You can find official government guidance on what to do in these situations here

- Change any passwords that are appropriate and run a full antivirus, malware and spyware check on your devices
- If your credit rating has been affected, contact the credit reporting agency concerned (Experian, Equifax, or Transunion) to file a dispute
- If you suspect someone of misusing a computer, due to things like hacking, possession of child pornography, or something else, report the person concerned to your local police. Do NOT confront them personally

Cybercrime: The Bottom Line

Cybercrime happens every day, and it happens to people just like you. No one is safe, though you can lessen your chances of being affected by following the advice given above. Be alert, be vigilant, and be careful so that you don't become a statistic!

Cybercrime Statistics 2019: An In Depth Look at UK Figures and Trends *by Sandra Henshaw* - November 9, 2018, *Last Updated on June 14, 2019,* How To Guides, Statistics https://www.tigermobiles.com/blog/cybercrime-statistics/

THE BIGGEST CYBERCRIME THREATS OF 2019

BY CBN

ON MARCH 18, 2019

E-HEADLINES

The biggest cybercrime threats of 2019 have already been identified. Despite the fact that this is a new year, most of the threats from last year are still here with us. There is even a possibility of things getting worse than they were in 2018. The reason why cybercrime continues to grow is because it does not get much attention in international law because it is non-violent in nature. Cybercrime is however far from harmless as it poses a major threat to companies. It is estimated that cybercrime will cost $6 trillion per year by 2021 according to a report by Cybersecurity Ventures.

Ransomware

According to Virsec, *the threat of ransomware is steadily growing*. Ransomware can easily lock a user or an organization out of a computer network. This type of cybercrime is not going away anytime soon and targets a large percentage of society's middle classes. It will continue to exist as long as there are still underprotected systems that have data that has not been backed up adequately. The threat is continuously being used. Red herrings distract from other attacks on critical infrastructure. This threat is dangerous because it will block users from accessing data. The internet of things has certainly created a brave new world for hackers to lock users out of. The only precautionary measures that businesses can take is to secure their web applications using the same controls that are being deployed for other markets like user authentication and secure user onboarding.

Cryptocurrency

We can safely conclude that cryptocurrency cybercrime in 2018 did not play as big a role as had been anticipated. As much as the crime rate did not experience a dramatic rise, it was the year that cryptocurrency became a key tool in many of the ransomware schemes, such as the threat of personal data being released online. The only choice the owners are left with is to comply with the hackers. The emergence of digital currencies offer a less traceable way for criminals to make money. Cryptocurrencies are the main exchange medium used by cybercriminals, so there is rampant use of cryptocurrencies for illegal activities. The criminals control computer networks to take on the computer processing. They tie the computer to nefarious threats that direct users to illicit websites which run JavaScript on a webpage. ***This will then turn a user computer into a remote miner.***

Digital Ad Fraud

Very few people are aware of the existence of this type of crime and yet it affects a significantly large number of people each year. This cybercrime makes it difficult for online content publishers to make money. Advertisers lose an estimated $19 billion to fraud every year – that is equivalent to $51 million each day. It is even worse that ad fraud might reach $44 billion by the year 2022. Not only does this crime affect videos, ***it also affects newspaper publishers and every other online content provider***. There are several cases of hijacked advertisements that redirect internet users to phishing pop-ups that enable criminals to steal credit card and identity details. The criminals present themselves as legitimate advertisers using compromised sites to propagate phishing scams.

Phishers

Phishing has existed for many years and it is not going to end anytime soon as long as it works. More organizations are likely to be targeted in 2019. The reason why phishing will still be prevalent is simply because it is cheap and effective as long as people continue to receive and read emails. Internet users should therefore be careful not to download applications from untrusted sources.

Cloud protection

The latest trend in technology is the movement of data to cloud-based storage and services. This has directed cybercriminals to the cloud too. Many companies have the misconception that simply because their data is offsite it is secure, but this remains unwarranted. One should be very careful when choosing a cloud provider and check on their track record and the level of security that they provide. The question is if enough measures have been taken to keep the data in the cloud secure. The fact that traditional security tools are not able to detect cloud attacks should be a matter of great concern to us all. That is it.

The Biggest Cybercrime Threats of 2019 *BY CBN* ON MARCH 18, 2019 *E-HEADLINES* http://cascadebusnews.com/biggest-cybercrime-threats-2019/

FBI PROVIDES REFRESHERS ON CYBERCRIME EFFORTS

By **Janelle Retka**

June 22, 2017

U.S. FBI officials and experts this week provided training on preventing and reacting to cybercrime and cross-border crimes to about 140 participants from 20 Asia-Pacific countries in Cambodia.

This year’s three-day seminar for graduates of the bureau’s academy was held in Siem Reap.

The annual event “brings together graduates from FBI National Academy training programs to network and to share information and best practices,” U.S. Embassy spokesman Jay Raman said this week.

The Cambodian government may nominate two people to attend the FBI academy annually in the future, according to Carl Thayer, a Southeast Asia military expert at the Australian Defence Force Academy.

“Cambodia’s main weaknesses are in human resources and capacity to defend against and counter cyber and transnational crime,” he said.

“Human resources involve not only education and training but updating personnel on latest developments in technology and intelligence on cyber and transnational crimes.”

The seminar and potential studies of future students would bolster these areas, he said.

Interior Ministry spokesman Khieu Sopheak could not be reached for comment.

Clarification: An earlier version of the story incorrectly reported that the Cambodian government has annually nominated two people to attend the FBI academy. In fact, the government intends to do so in the future.

FBI Provides Refreshers on Cybercrime Efforts By **Janelle Retka** - June 22, 2017 https://www.cambodiadaily.com/brief/fbi-provides-refreshers-on-cybercrime-efforts-131619/

Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2019 ***Number of women in the cybersecurity field is recalculated and rising Press Release*** *– Steve Morgan, Editor-in-Chief* Sausalito, Calif. – Mar. 28, 2019 https://cybersecurityventures.com/women-in-cybersecurity/

2019 CYBERSECURITY ALMANAC: 100 FACTS, FIGURES, PREDICTIONS AND STATISTICS (CYBERSECURITY_FBI)

Published by Cisco and Cybersecurity Ventures Press Release

– Steve Morgan, Editor-in-Chief

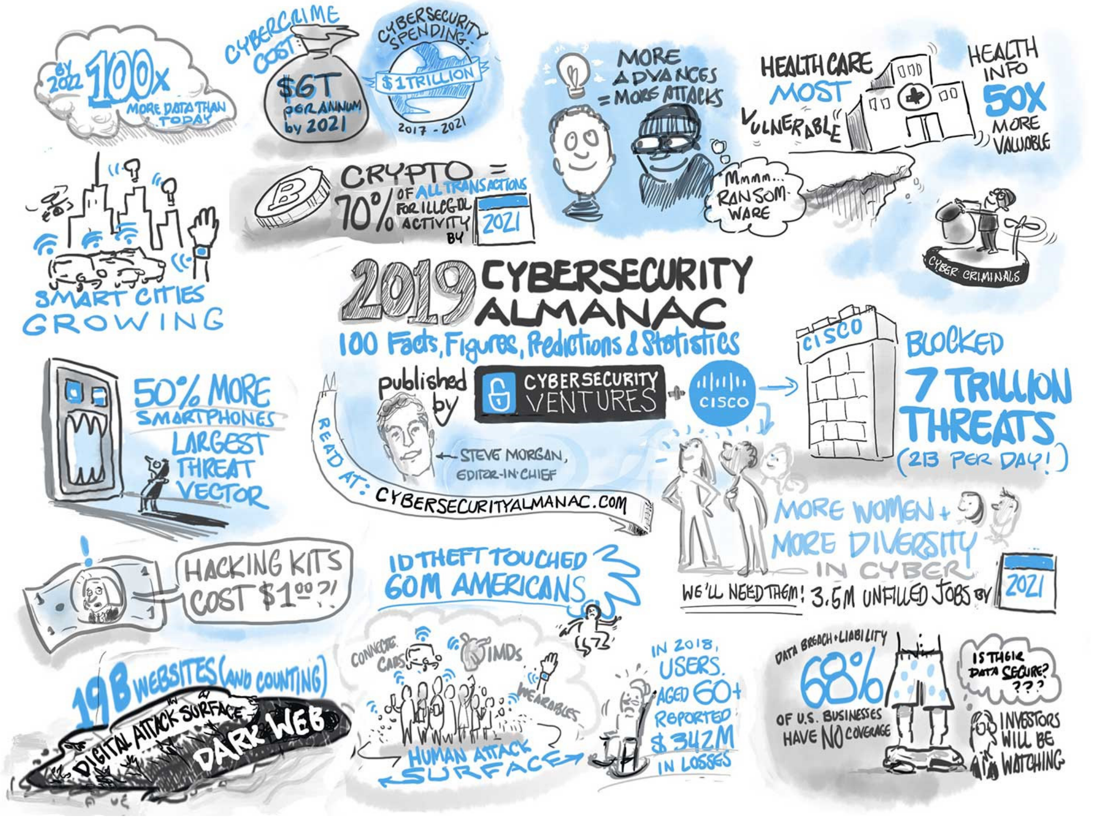
Northport, N.Y. – Feb. 6, 2019

Cybersecurity Ventures is excited to release this special first annual edition of the Cybersecurity Almanac, a handbook containing the most pertinent statistics and information for tracking cybercrime and the cybersecurity market.

Cisco's commitment to security and partnerships starts at the top, and it's one of the reasons why we're collaborating with them. "At Cisco, security is foundational to everything we do," said Chuck Robbins, chairman and CEO. Last year Cisco blocked seven trillion threats, or 20 billion threats a day, on behalf of their customers, according to Robbins.

Cisco and Cybersecurity Ventures have compiled 100 of the most important facts, figures, statistics, and predictions to help frame the global cybercrime landscape, and what the cybersecurity industry is doing to help protect governments, citizens, and organizations globally.

Cybersecurity Ventures formulates our own ground-up research — plus we vet, synthesize and repurpose research from the most credible sources (analysts, researchers, associations, vendors, industry experts, media publishers) — to provide our readers with a bird's-eye view of the most dangerous cyber threats, and the most important solutions.

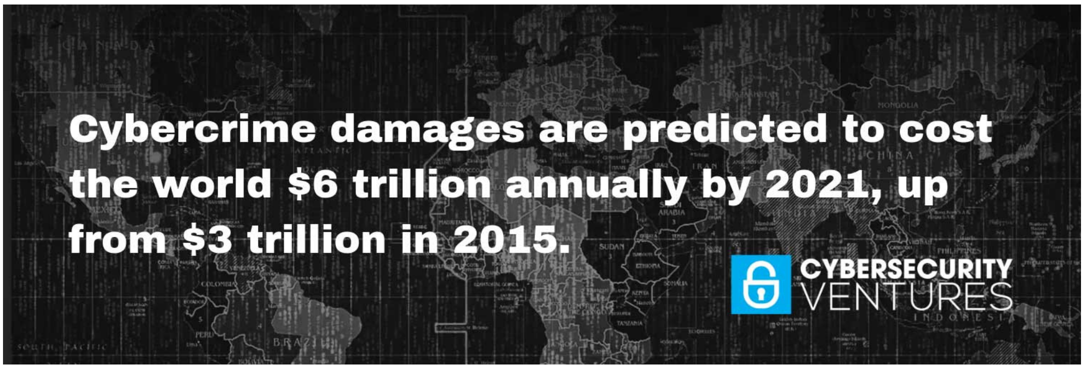

BY 2022 100x MORE DATA THAN TODAY
CYBERCRIME COST
$6T PER ANNUM by 2021
CYBERSECURITY SPENDING
$1 TRILLION
2017 - 2021
MORE ADVANCES = MORE ATTACKS
HEALTH CARE MOST VULNERABLE
HEALTH INFO 50X MORE VALUABLE
Mmmm... RANSOMWARE
CRYPTO = 70% OF ALL TRANSACTIONS FOR ILLEGAL ACTIVITY BY 2021
CYBER CRIMINALS
SMART CITIES GROWING
2019 CYBERSECURITY ALMANAC
100 Facts, Figures, Predictions & Statistics
published by
CYBERSECURITY VENTURES + CISCO
STEVE MORGAN, EDITOR-IN-CHIEF
READ AT: CYBERSECURITYALMANAC.COM
CISCO
BLOCKED 7 TRILLION THREATS (20B PER DAY!)
50% MORE SMARTPHONES LARGEST THREAT VECTOR
MORE WOMEN + MORE DIVERSITY IN CYBER
WE'LL NEED THEM! 3.5M UNFILLED JOBS BY 2021
HACKING KITS COST $1.00?!
ID THEFT TOUCHED 60M AMERICANS
19B WEBSITES (AND COUNTING)
DIGITAL ATTACK SURFACE
DARK WEB
CONNECTED CARS
IMDs
WEARABLES
HUMAN ATTACK SURFACE
IN 2018, USERS AGED 60+ REPORTED $342M IN LOSSES
DATA BREACH + LIABILITY
68% OF U.S. BUSINESSES HAVE NO COVERAGE
IS THEIR DATA SECURE???
INVESTORS WILL BE WATCHING

CYBERCRIME DAMAGE

Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. Cyberattacks are the fastest growing crime globally, and they are increasing in size, sophistication and cost.

- Cybersecurity Ventures predicts that cybercrime damages will cost the world $6 trillion annually by 2021 – exponentially more than the damage inflicted from natural disasters in a year, and more profitable than the global trade of all major illegal drugs combined.
- Cybersecurity Ventures predicts that by 2021 more than 70 percent of all cryptocurrency transactions annually will be for illegal activity, up from current estimates ranging anywhere from 20 percent (of the 5 major cryptocurrencies) to nearly 50 percent (of bitcoin).
- Around $76 billion of illegal activity per year involves bitcoin, which is close to the scale of the U.S. and European markets for illegal drugs, according to a study published by the University of Sydney in Australia, ranked as one of the top 100 universities globally.

- Digital ad fraud is rising sharply. One report found that advertisers lost an estimated $19 billion to fraudulent activities last year, equivalent to $51 million per day. This figure, representing advertising on online and mobile devices, is expected to rise, reaching $44 billion by 2022.
- The “Cyber’s Most Wanted” list on the FBI website features 63 notorious people (up from 19 in 2016) that have conspired to commit the most damaging crimes against the U.S., including computer intrusions, wire fraud, identity theft, money laundering, false registration of domain names, espionage, theft of trade secrets, and other offenses — costing the affected organizations and individuals tens of billions of dollars.
- Cybercrimes are vastly undercounted because they aren’t reported — due to embarrassment, fear of reputational harm, and the notion that law enforcement can’t help (amongst other reasons). The unit chief at the FBI’s Internet Crime Complaint Center (IC3) stated that the number of reported cybercrimes in the agency’s reports only represent 10 to 12 percent of the total number actually committed in the U.S. each year.
- Asia-Pacific companies receive 6 cyber threats every minute, according to Cisco. A Frost & Sullivan study commissioned by Microsoft revealed that the potential economic loss across Asia Pacific due to cybersecurity incidents can hit a staggering $1.745 trillion (USD).



Cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

CYBERSECURITY VENTURES

BREACHES & VULNERABILITIES

Advances in technology are the main driver for economic growth but have also led to a higher incidence of cyberattacks. The leading trends such as e-commerce, mobile payments, cloud computing, Big Data and analytics, IoT, AI, machine learning, and social media, all increase cyber risk for users and businesses.

- The 10 biggest data breaches of all time — with the number of accounts hacked and year occurred — according to Quartz: Yahoo, 3 billion (2013); Marriott, 500 million (2014-2018); Adult FriendFinder, 412 million (2016); MySpace, 360 million (2016); Under Armor, 150 million (2018); Equifax, 145.5 million (2017); eBay, 145 million (2014); Target, 110 million (2013); Heartland Payment Systems, 100+ million (2018); LinkedIn, 100 million (2012); rest of list…

- Cryptocrime is an emerging segment of the cybercrime ecosystem. One report estimates that hacks on cryptocurrency exchanges suffered roughly $1 billion in losses during 2018.

- The 5 biggest bitcoin hacks of all time — with the exchange name, amount stolen, and year occurred — according to CoinSutra: Mt. Gox, 2609 BTC | +750,000 BTC (2011); BitFloor, 24,000 BTC (2012); Poloniex, 12.3 percent of all BTCs – 97 BTC (2014); BitStamp, 19,000 BTC (2015); Bitfinex, 120,000 BTC (2016).

- The cost of the 2018 Coincheck hack, the biggest cryptocurrency heist to date, was $530 million. 523 million NEM coins (known as XEM) had been stolen from a hot wallet (a wallet connected to the Internet) allowing hackers to drain the coins into a separate account. The cost of those stolen coins has since declined dramatically.

- In a keynote at DevNet Create, Susie Wee, SVP and CTO of Cisco DevNet, shared research from Cybersecurity Ventures that estimates there are 111 billion lines of new software code being produced each year — which introduces potential for a massive number of vulnerabilities that can be exploited. Zero-day exploits alone are predicted to reach one per day by 2021, up from one per week in 2015.

- The FBI reported that the Business Email Compromise (BEC), aka Email Account Compromise (EAC) — a sophisticated scam targeting both businesses and individuals performing wire transfer payments — has cost more than $12.5 billion in losses over the past 4.5 years (as of its last tally through May 2018).

- Less than half of companies globally are sufficiently prepared for a cybersecurity attack, according to a PricewaterhouseCoopers report that surveyed 3,000 business leaders from more than 80 countries.
- The 5 most cyber-attacked industries over the past 5 years are healthcare, manufacturing, financial services, government, and transportation. Cybersecurity Ventures predicts that retail, oil and gas / energy and utilities, media and entertainment, legal, and education (K-12 and higher ed), will round out the top 10 industries for 2019 to 2022.
- ATM makers, banks, and law enforcement have been scrambling to defend the 400,000 ATMs in the U.S. against “jackpotting.” When cybercriminals take control of the machine, cash spews out of it like a Las Vegas jackpot. Jackpotting has been rising worldwide, though it’s unclear how much has been stolen because victims and police often do not disclose details.
- Almost 50 percent of Ultra High Net Worth family wealth is being managed through family offices, which can be (cyber) targets due to the potential extortion value attached to reputational threats. 40 percent of family offices lack a cybersecurity policy. 28 percent of these businesses have already been victims of cyberattacks.
- Distributed-Denial-of-Service (DDoS) attacks represent the dominant threat observed by the vast majority of service providers — and they can represent up to 25 percent of a country’s total Internet traffic while they are occurring. Globally the total number of DDoS attacks will double to 14.5 million by 2022 (from 2017), according to the Cisco Visual Networking Index (VNI).
- Hacking tools and kits for cyberattacks, identity theft, malware, ransomware, and other nefarious purposes have been available in online marketplaces for several years — at price points starting as low as $1 — which makes the cost of entry to a life of cybercrime nearly free.

Zero-day exploits are predicted to reach one-per-day by 2021, up from one-per-week in 2015.

RANSOMWARE

Ransomware damage costs are predicted to be 57X more in 2021 than they were in 2015. This makes ransomware the fastest growing type of cybercrime. The U.S. Department of Justice (DOJ) has described ransomware as a new business model for cybercrime, and a global phenomenon.

- Global ransomware damage costs are predicted to hit $20 billion in 2021, up from $11.5 billion in 2019, $5 billion in 2017, and just $325 million in 2015, according to Cybersecurity Ventures.
- Ransomware attacks saw a 350 percent increase in 2018, according to one estimate. Cybersecurity Ventures expects that businesses will fall victim to a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019, and every 40 seconds in 2016.
- Global spending on security awareness training for employees — one of the fastest growing categories in the cybersecurity industry — is predicted to reach $10 billion by 2027, up from around $1 billion in 2014. Much of this training is centered on combating phishing scams and ransomware attacks.
- It’s widely reported that more than 90 percent of successful hacks and data breaches stem from phishing scams, emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn’t. Training users how to detect and react to these threats is a critical ransomware deterrent.
- The No More Ransom online portal is now available in 35 different languages and carries 59 free decryption tools, covering some 91 ransomware

families. So far, the tools provided on No More Ransom have managed to decrypt the infected computers of over 72,000 victims worldwide.

CRYPTOJACKING & SIM-SWAPPING

Cryptojacking is illegally mining cryptocurrencies, and it's gaining ground on ransomware as a favorite revenue stream for cybercriminals. The problem is so severe that Google announced it would ban all extensions that involved cryptocurrency mining from its Chrome browser. SIM swapping is on the rise and poses a major threat to cryptocurrency account holders.

- Cryptojacking was one of the fastest growing cybersecurity threats in 2018, with 25 percent of all businesses already falling victim to it.
- A report from the Cyber Threat Alliance (CTA) indicates a massive 459 percent increase in the rate of cryptojacking, through which hackers hijack computer processing power to mine cryptocurrencies such as bitcoin and Monero.
- Cryptojacking participants can use more sophisticated means to evade detection — and according to one study only around 50 percent of malicious attacks are detected.
- On average, most cryptojackers don't earn much. 1 out of every 500 of the top million Alexa-ranked sites hosts cryptojacking code. The ten most profitable cryptomining sites identified generate between $119 to $340 per day, according to academics at Braunschweig University of Technology in Germany. It remains to be seen how many cryptojackers will revert to ransomware, and data theft and resale on the Dark Web for higher payouts.
- SIM swapping attacks have stolen tens-of-millions of dollars worth of cryptocurrency. The compromise involves tricking a mobile carrier employee into rerouting a subscriber's phone number to a hacker's SIM card. This enables the perpetrator to intercept the victim's messages — including 2FA codes — which helps locate the private keys used to access a cryptocurrency account. The first hacker convicted of SIM swapping was sentenced to 10 years in prison.

Cryptojacking has been the fastest growing but lowest paying job for cybercriminals over the past year.
CYBERSECURITY VENTURES

DIGITAL ATTACK SURFACE

The modern definition of the word “hack” was first coined at MIT in April 1955. The first known mention of computer (phone) hacking occurred in a 1963 issue of The Tech. Over the past fifty-plus years, the world’s attack surface has evolved from phone systems to so many digitally connected “things” that it’s outpacing our ability to properly secure them.

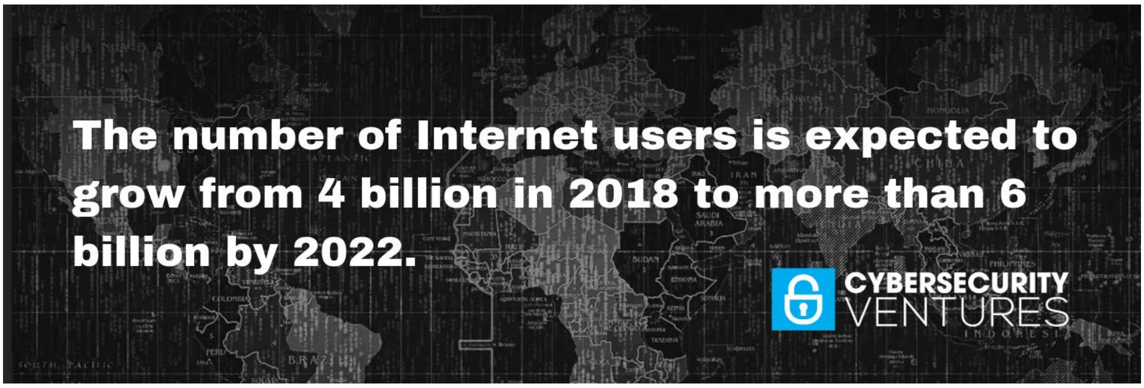
- The World Wide Web was invented in 1989. The first-ever website went live in 1991. Today there are more than 1.9 billion websites.
- The world’s digital content is expected to grow to 96 zettabytes by 2020 (this is how big a zettabyteis), up from 4 billion terabytes (4 zettabytes) just 3 years ago. With this kind of exponential growth the opportunities — for innovation, and for cybercrime — are incalculable because data is the building block of the digitized economy.
- The far corners of the Deep Web — known as the Dark Web — is intentionally hidden and used to conceal and promote heinous criminal activities. Some estimates put the size of the Deep Web (which is not indexed or accessible by search engines) at as much as 5,000 times larger than the surface web, and growing at a rate that defies quantification, according to one report.
- According to the latest Cisco Visual Networking Index (VNI), by 2022, more IP traffic will cross global networks than in all prior “Internet years.” In other words, more traffic will be created in 2022 than in the 32 years since the Internet started. However, increased connectivity brings with it increased security challenges.

- Driven by the rapid increase in the use of cloud apps, cloud data center traffic will represent 95 percent of total data center traffic by 2021, according to Cisco. The growth of Internet of Things (IoT) applications, such as smart cars, smart cities, and connected health devices, will also expand data center demands.
- Cybersecurity Ventures predicts that the total amount of data stored in the cloud — which includes public clouds operated by vendors and social media companies (think AWS, Twitter, Facebook, etc.), government-owned clouds that are accessible to citizens and businesses, and private clouds owned by mid-to-large-sized corporations — will be 100X greater in 2022 than it is today.
- Despite promises from biometrics and facial recognition developers of a future with no more passwords — which may, in fact, come to pass at one point in the far-out future — one report finds that the world will need to cyber protect 300 billion passwords globally by 2020.
- The global smartphone install base is set to grow 50 percent in the next four years to 6 billion devices, up from 4 billion in 2016. Infections for both Android and iPhones continue to increase as they are now the largest threat vector on the planet for technology. 2019 will see this trend continue.
- Research from Cisco and Cybersecurity Ventures indicates that smartphones will account for more than 55 percent of total IP traffic by 2025, and Wi-Fi and mobile devices will account for nearly 80 percent of IP traffic by that time — with BYOD (bring your own device) and mobile apps posing a major security threat to enterprises over the next 6 years.
- The number of connected devices on the Internet will exceed 50 billion by 2020, according to Cisco. To put it another way, the number of IoT devices will be three times as high as the global population by 2021. And by 2022, 1 trillion networked sensors will be embedded in the world around us, with up to 45 trillion in 20 years.

HUMAN ATTACK SURFACE

Like street crime, which historically grew in relation to population growth, we are witnessing a similar evolution of cybercrime. It’s not just about more sophisticated weaponry; it’s as much about the growing number of human targets.

- There were nearly 4 billion Internet users in 2018 (nearly half of the world’s population of 7.7 billion), up from 2 billion in 2015. Cybersecurity Ventures predicts that there will be 6 billion Internet users by 2022 (75 percent of the projected world population of 8 billion) — and more than 7.5 billion Internet users by 2030 (90 percent of the projected world population of 8.5 billion, 6 years of age and older).
- Gartner forecasts that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearables includes smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors.
- Hundreds of thousands — and possibly millions — of people can be hacked now via their wirelessly connected and digitally monitored implantable medical devices (IMDs) — which include cardioverter defibrillators (ICD), pacemakers, deep brain neurostimulators, insulin pumps, ear tubes, and more.
- For the most recent year reported by the FBI, the Internet Crime Complaint Center (IC3) received nearly 50,000 complaints from victims over the age of 60 with adjusted losses in excess of $342 million — which leads all age groups.
- The global market for connected cars is expected to grow by 270 percent by 2022 — and more than 125 million passenger cars with embedded connectivity are forecast to ship worldwide between 2018 and 2022. This means most drivers will be online and susceptible to auto (cyber) intrusions by 2022, regardless of whether they consider themselves to be “online” or not.



The number of Internet users is expected to grow from 4 billion in 2018 to more than 6 billion by 2022.

HEALTHCARE INDUSTRY

Hospitals are more vulnerable than any other type of organization in 2019. Outdated systems, lack of experienced cyber personnel, highly valuable data, and added incentive to pay ransoms in order to regain patient data are magnetizing cybercriminals to the healthcare market.

- Ransomware attacks on healthcare organizations are predicted to quadruple between 2017 and 2020, and will grow to 5X by 2021.
- Cybersecurity Ventures predicts that the healthcare industry will spend more than $65 billion cumulatively on cybersecurity products and services from 2017 to 2021.
- Personal health information is 50 times more valuable on the black market than financial information, and stolen patient health records can fetch upwards of $60 per record (which is 10-20 times more than credit card information).
- Cybersecurity Ventures predicts that healthcare will suffer 2-3X more cyberattacks in 2019 than the average amount for other industries. Woefully inadequate security practices, weak and shared passwords, plus vulnerabilities in code, exposes hospitals to perpetrators intent on hacking treasure troves of patient data.

Healthcare is predicted to suffer 2-3X more cyberattacks in 2019 than the average amount for other industries.

CYBERSECURITY ECONOMY

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 it was worth more than $120 billion. The cybersecurity market grew by roughly 35X during that 13-year period — prior to the latest market sizing by Cybersecurity Ventures, for the 5-year period 2017 to 2021.

- Cybersecurity Ventures predicts that global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five-year period from 2017 to 2021 — and the cybersecurity market will continue growing by 12-15 percent year-over-year through 2021.
- Worldwide spending on information security (a subset of the broader cybersecurity market) products and services exceeded $114 billion in 2018, an increase of 12.4 percent from last year, according to the latest forecast from Gartner, Inc. For 2019, they forecast the market to grow to $124 billion, and $170.4 billion in 2022. (*)
- Cybersecurity Ventures predicts that the global blockchain market will exceed $40 billion by 2025. Results from one survey indicate institutional investors from hedge funds, pension funds, and private equity believe that blockchain technology will have the biggest impact on healthcare, financial services and banking. The study reveals that 39 percent of the investors believe blockchain will do to banking what the Internet did to media.
- In 2019, Cybersecurity Ventures expects that Fortune 500 and Global 2000 chief information security officers (CISOs) will reduce the number of point security products/solutions in use at their corporations by 15-18 percent.

- Total venture capital funding in the cybersecurity space totaled more than $5 billion in 2018, up 20 percent from nearly $4.5 billion in 2017. In 2018, the total amount of funding for Israeli cybersecurity companies grew 22 percent year-over-year to more than $1 billion. According to these figures, Israel, the world's second-largest exporter of cyber technology (behind the U.S.), accounted for roughly 20 percent of all cybersecurity VC funding.
- Based on venture capital dollars invested in cybersecurity, the top 4 countries are (in this order): U.S., Israel, U.K., and Canada.
- Virginia is part of the nation's Cyber Capital, the Washington D.C. region. The state is home to the most cybersecurity companies per capita in the nation.
- 68 percent of U.S. businesses have not purchased any form of cyber liability or data-breach coverage, showing that businesses are not adopting cyber insurance at a rate that matches the risks they face, according to a Cisco paper. However, a majority of the 25 most populous U.S. cities now have cyberinsurance or are looking into buying it, according to a Wall Street Journal survey.
- Legislation such as 2018's EU General Data Protection Regulation (GDPR) is helping drive the demand for cyber insurance as healthcare providers, financial services firms, and companies in all industries are tasked with keeping user data safe — and recovering from data breaches and ransomware attacks. Market forecasts for cyber insurance policies range from $14 billion by 2022 to $20 billion by 2025, up from less than $1.5 billion in 2016.
- Singapore announced the launch of the world's first commercial cyber risk pool, a facility for providing cyber insurance to corporate buyers, as cyberattacks in the Asia Pacific region become more pervasive. The pool will commit up to $1 billion (USD) in risk capacity and will be backed by capital from traditional insurance and insurance-linked securities markets to provide bespoke coverage.

- The $100 million Hull McKnight Georgia Cyber Center (GCC) for Innovation and Training in Augusta, Georgia, marks the single-largest investment in a cybersecurity facility by a state government.
- The 2019 U.S. President's budget includes $15 billion for cybersecurity, a $583.4 million (4.1 percent) increase over 2018. The Department of Defense (DoD) was the largest contributor to the budget. The DoD reported $8.5 billion in cybersecurity funding in 2019, a $340 million (4.2 percent) increase over 2018.
- Driven by the federal government's desire to enhance agency cybersecurity posture at every possible level, Deltek forecasts the demand for vendor-furnished information security products and services by the U.S. federal government will increase from $10.9 billion in FY 2018 to over $14.1 billion in FY 2023at a compound annual growth rate (CAGR) of 5.3 percent.
- Cybersecurity is the single biggest risk organizations throughout Europe are likely to face over the next year, according to the European Confederation of Institutes of Internal Auditing's (ECIIA) annual Risk in Focus 2019 report. The data suggests that spending on cybersecurity in the region will see another uptick in 2019.
- A 2018 report estimates that energy companies, ranging from drillers to pipeline operators to utilities, invest less than 0.2 percent of their revenue in cybersecurity — while the number of hacker groups targeting the energy sector is soaring. Energy networks are vulnerable to cyberattacks — and hackers can cause massive power outages, placing national defense infrastructures at risk, and endangering millions of citizens.
- Estimates placing at least 85 percent of all business assets in digital form, a massive increase of cybercrime, and underinvestment into cyber insurance coverage has led Cybersecurity Ventures to predict that future stock prices of publicly-traded companies — and valuations of most startups and emerging enterprises seeking venture capital — will be influenced by market and investor

perceptions of how secure a business' information systems, data, and employees are.

(*) *The Gartner forecast doesn't cover various cybersecurity categories including IoT (Internet of Things), ICS (Industrial Control Systems) and IIoT (Industrial Internet of Things) security, automotive cybersecurity, and others, which are included in the Cybersecurity Ventures figures.*

Global spending on cybersecurity is predicted to exceed $1 trillion cumulatively from 2017 to 2021.
CYBERSECURITY VENTURES

EMPLOYMENT

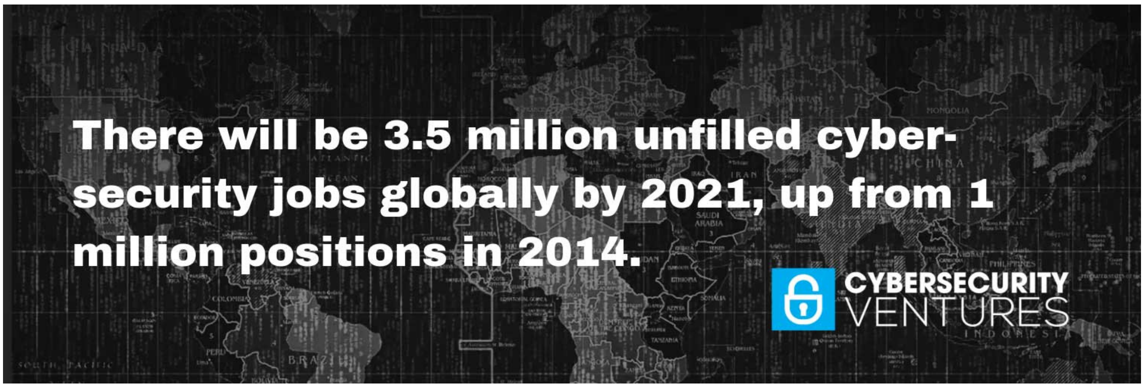
Cisco firmly believes diversity is a mandate in the cyber imperative: diversity of ideas, perspectives, backgrounds, and ways of seeing the world. This diversity creates the opportunity for creative problem solving that the growing security threat requires. Cybersecurity Ventures believes that every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people.

- There will be 3.5 million unfilled cybersecurity jobs by 2021 — enough to fill 50 NFL stadiums — according to Cybersecurity Ventures. This is up from Cisco's previous estimation of 1 million cybersecurity openings in 2014. The cybersecurity unemployment rate is at zero percent in 2019, where it's been since 2011.
- U.S. News and World Report stated that the information security profession is growing at a rate of 36.5 percent through 2022. That bodes well for newbies, much the same as more experienced cyber fighters.

- The population of cyber engineers and analysts throughout the Washington D.C. Beltway is 3.5 times as big as the rest of the U.S. combined.
- With more than 150,000 cyber-related engineering and data science professionals, Maryland has the number one cyber workforce in the world, and leads the U.S. in cyber employment for classified nation-state jobs. Maryland also has the largest concentration of university-trained cyber engineering graduates in the world.
- San Antonio is home to the nation's second-largest concentration of cybersecurity experts.
- The U.S. has a total employed cybersecurity workforce consisting of nearly 715,000 people, and there are currently almost 314,000 unfilled positions, according to Cyber Seek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce.
- Jobs requesting public cloud security skills remain open 79 days on average — longer than almost any other IT skill, according to Cyber Seek.
- The National Association of Software and Services Companies (NASSCOM) estimated that India alone will need 1 million cybersecurity professionals by 2020 to meet the demands of its rapidly growing economy.
- Cybersecurity Ventures predicts that 100 percent of large corporations (Fortune 500, Global 2000) globally will have a CISO or equivalent position by 2021 (up from 70 percent in 2018), although many of them will be unfilled due to a lack of experienced candidates.
- The second-highest paying tech job in 2019 is a CISO, with a salary range of $175,000 to $275,000. Fortune 500 corporations in big cities pay as much as $380,000 to $420,000 annually, and more, to their CISOs, much higher than the average range for the position in mid-sized companies, government agencies, and academia.
- Flaws in software code, which create vulnerabilities, have created a burgeoning bug bounty economy with big payouts to elite freelancer hackers.

Some of them earn more than $500,000 a year. But, that's a far cry from the average take-home pay for most bug bounty hunters that are self-employed part-timers with no guaranteed income.

- For the top coders with leadership and cybersecurity skills — a rare breed — salaries exceed $225,000. In some companies, this position pays more than it does to the CISO. Software plus "soft skills" equals big pay for aspiring programmers with a senior management role in their sights.
- New data indicates that of all IT jobs, cybersecurity engineers — with an average annual salary of $140,000 — are projected to be the highest paying and most recruited heading into 2019.



There will be 3.5 million unfilled cyber-security jobs globally by 2021, up from 1 million positions in 2014.

WOMEN IN CYBERSECURITY

Cisco's John Stewart, senior vice president and chief security and trust officer, said in his keynote at last year's RSA Conference that Women in CyberSecurity and Girls Who Code are examples of groups that are working to close the skills and diversity gap.

- Cybersecurity Ventures predicts that women will represent 20 percent of the global cybersecurity workforce by the end of 2019. This recalculates a 6-year old figure based on a limited survey that concluded women held just 11 percent of cybersecurity positions.
- Research firm Forrester predicts that the number of women CISOs at Fortune 500 companies will rise to 20 percent in 2019, compared with 13 percent in 2017. This is consistent with new research from Boardroom Insiders which

states that 20 percent of Fortune 500 global CIOs are now women — the largest percentage ever.

- Quartz worked with data from private-equity research firm Pitchbook to develop a unique dataset that identifies more than 200 rising stars among the venture-backed companies (across all industries) led by female founders in the U.S. 5 women in cybersecurity showed up in the top 25 — and collectively they raised $300 million. Altogether 9 women in cybersecurity on the index raised nearly half a billion dollars.
- 91 percent of women in cybersecurity have a bachelor's degree, and 20-25 percent of them have an MBA or master's degree. 5 percent have a Ph.D., and 2 percent have no degree.
- Women in the cybersecurity field are trending up in Israel, the world's second-largest country in terms of cybersecurity investment. In 2018, TechCrunch reported that for the most recent year tracked, 15 percent of newly established Israeli cybersecurity startups had a female founder, an increase from 5 percent the previous year.
- RESET, held in London, was the first cybersecurity conference with an all-female speaker lineup. The June 2018 event featured 15 women in cybersecurity speakers with in-depth knowledge of destructive cyberattacks and criminal operations, threat hunting and strategy, and human-centric security. 175 people attended the one-day conference.
- There's a growing number of women in cybersecurity associations, events, lists, media stories, blogs, women-owned companies, and new programs — for instance the 100 Women in 100 Days Cybersecurity Certification — that are creating more momentum than ever for gender equality in our field.

Women will represent 20 percent of the global cybersecurity workforce by the end of 2019.

PERSONAL & DATA PRIVACY

Cybercrime has hit the U.S. so hard that a supervisory special agent with the Federal Bureau of Investigation who investigates cyber intrusions told The Wall Street Journal that every American citizen should expect that all of their data (personally identifiable information) has been stolen and is now on the Dark Web.

- Hackers stole nearly 447 million consumer records containing sensitive personal information last year, according to the Identity Theft Resource Center. That's a jump of 126 percent from the prior year and a new record for the number of compromised files in a single year.
- Over 40 percent of companies have sensitive files that are unprotected and open to every employee, according to TechRepublic.
- Tech Support Fraud is a widespread scam in which criminals claim to provide customer, security, or technical support in an effort to defraud unwitting individuals and gain access to the individuals' devices. In the FBI's most recent Internet Crime Report, they state that there was a 90 percent increase in losses over the prior year — from complaints reported to the Internet Crime Complaint Center (IC3).
- Nearly 60 million Americans were affected by identity theft last year, according to a 2018 online survey by The Harris Poll, an increase from 15 million in 2017.
- 87 percent of companies are experiencing delays in their sales cycle due to customers' or prospects' privacy concerns, up from 66 percent last year, according to those surveyed in the 2019 Cisco Data Privacy Benchmark

Study. This is likely due to the increased privacy awareness brought on by GDPR and the frequent data breaches in the news.

- Those organizations that invested in data privacy to meet GDPR experienced shorter delays due to privacy concerns in selling to existing customers: 3.4 weeks vs. 5.4 weeks for the least GDPR ready organizations. Overall the average sales delay was 3.9 weeks in selling to existing customers, down from 7.8 weeks reported a year ago, according to the 2019 Cisco Data Privacy Benchmark Study.
- Among all respondents in the 2019 Cisco Data Privacy Benchmark Study, 59 percent indicated they are meeting all or most of GDPR's requirements today. Another 29 percent said they expect to be GDPR ready within a year, 9 percent said it would take more than a year to get ready, with the remaining 3 percent stating the requirements did not apply to their organization.

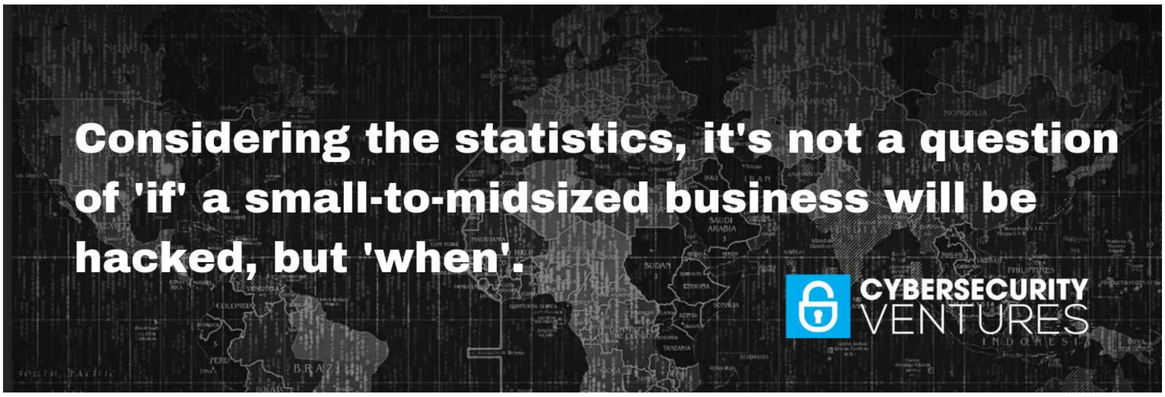
Every Internet user is at serious risk of identity fraud, data theft, and invasion of digital privacy.
CYBERSECURITY VENTURES

SMALL-TO-MIDSIZE BUSINESSES

Adversaries view small/midmarket businesses as soft targets that have less sophisticated security infrastructure and practices and an inadequate number of trained personnel to manage and respond to threats, according to a Cisco Cybersecurity Special Report.

- Nearly half of all cyberattacks are committed against small businesses.
- 60 percent of small companies that suffer a cyberattack are out of business within six months, according to the U.S. National Cyber Security Alliance.

- Cisco’s 2018 SMB Cybersecurity Report found that 53 percent of midmarket companies in 26 countries experienced a breach. For these companies, the top security concerns are targeted phishing attacks against employees, advanced persistent threats, ransomware, denial-of-service attacks and the proliferation of employees allowed to use their own mobile devices.
- A Better Business Bureau survey found that for small businesses — which make up more than 97 percent of total businesses in North America — the primary challenges for more than 55 percent of them in order to develop a cybersecurity plan are a lack of resources or knowledge.
- Cisco security experts explain that small/midmarket businesses are more inclined to pay ransoms to adversaries so that they can quickly resume normal operations after a ransomware attack. They simply can’t afford the downtime and lack of access to critical data — including customer data.


Considering the statistics, it's not a question of 'if' a small-to-midsized business will be hacked, but 'when'.
CYBERSECURITY VENTURES

K-12 & HIGHER EDUCATION

Today, students are learning how to deal with sophisticated cyber threats by becoming hackers themselves — the good kind, according to EdTech Magazine. With the help of experts and educators, many middle and high school students throughout the U.S. are taking ethical hacking courses and setting themselves on the path to becoming cybersecurity experts. Colleges and universities are responding to the labor crunch with diverse programs focused on cybercrime, cybersecurity, and related coursework.

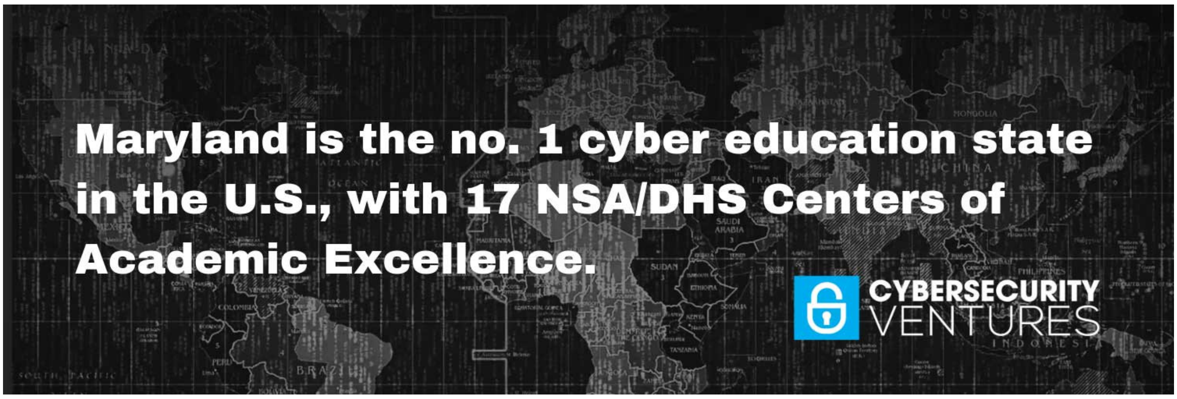
- Since January 2016, there have been more than 410 cyber incidents targeting K–12 schools in the United States, according to EdTech Strategies.

- According to the Center for Cyber Safety and Education’s Children’s Internet Usage Study, over half (53 percent) use the Internet for purposes other than homework or schoolwork seven days a week. Over a quarter (29 percent) of children admit to having used the Internet in a way that their parents would not approve. And alarmingly, four out of 10 (40 percent) say they have “friended” or connected with someone they didn’t know on a site or app.

- Recent data suggests there’s growing interest from students entering college, and IT workers thinking about cybersecurity as an upgrade to their current positions. There are more than 125 colleges and universities in the U.S. alone offering a master’s degree in cybersecurity. Dozens of those programs offer online-only classes and degrees, so even students who can’t attend in person can get a degree.

- Maryland has the largest number of university-trained cyber engineering graduates in the world. Maryland is the number one cyber education state in the country, with 17 NSA/DHS Centers of Academic Excellence. Maryland-based universities have awarded 10,000 bachelor’s degrees in cybersecurity-related programs since 2015.

- With the introduction of 18 new cybersecurity badges in 2018, nearly two million Girls Scouts of all ages (K-12) will be able to explore opportunities in STEM while developing problem-solving and leadership skills, according to Girls Scouts of the USA (GSUSA).


Maryland is the no. 1 cyber education state in the U.S., with 17 NSA/DHS Centers of Academic Excellence.
CYBERSECURITY VENTURES

The 2019 Cybersecurity Almanac will be periodically updated with revised and new facts, figures, predictions and statistics.

– Steve Morgan is founder and Editor-in-Chief at Cybersecurity Ventures.

2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics Published by Cisco and Cybersecurity Ventures Press Release – Steve Morgan, ***Editor-in-Chief*** **Northport, N.Y. – Feb. 6, 2019 https://cybersecurityventures.com/cybersecurity-almanac-2019/**

REFRENCES

1. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics **Published by Cisco and Cybersecurity Ventures** Press Release – Steve Morgan, *Editor-in-Chief* Northport, N.Y. – Feb. 6, 2019 https://cybersecurityventures.com/cybersecurity-almanac-2019/

2. Combating cybercrime with actionable intelligence: INTERPOL's ASEAN Cyber Capability Desk, *24 September 2018* https://www.interpol.int/News-and-Events/News/2018/Combating-cybercrime-with-actionable-intelligence-INTERPOL-s-ASEAN-Cyber-Capability-Desk

3. Cyberattacks know no borders and evolve at a fast pace while the Internet also facilitates a range of more traditional crimes. https://www.interpol.int/Crimes/Cybercrime

4. Cybercrime https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

5. Cybercrime Statistics 2019: An In Depth Look at UK Figures and Trends by Sandra Henshaw - November 9, 2018, Last Updated on June 14, 2019, How To Guides, Statistics https://www.tigermobiles.com/blog/cybercrime-statistics/

6. FBI Provides Refreshers on Cybercrime Efforts By **Janelle Retka** - June 22, 2017 https://www.cambodiadaily.com/brief/fbi-provides-refreshers-on-cybercrime-efforts-131619/

7. FBI Internet Crime Report – Cybercrime On The Rise *by Mark Cormick* // April 25, 2019 // *Financial Telegram* https://fintelegram.news/fbi-internet-crime-report-cybercrime-on-the-rise/

8. Here are the biggest cybercrime trends of 2019 by *Einaras von Gravrock* Chief Executive Officer and Founder, CUJO AI *04 Mar 2019* // https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019

9. https://legaldictionary.net/wp-content/uploads/2015/05/cybercrime.jpg

10. INTERPOL project to combat cybercrime in the Americas *18 October 2018* https://www.interpol.int/News-and-Events/News/2018/INTERPOL-project-to-combat-cybercrime-in-the-Americas

11. *Language of Cybercrime* **handbook** http://www.ejtn.eu/PageFiles/17406/Handbook%20Linguistics%20Cybercrime.pdf

12. Scotland Yard looks to set up crack cybercrime unit, *by Bill Goodwin*, 12 Mar 2003 // https://www.computerweekly.com/news/2240049886/Scotland-Yard-looks-to-set-up-crack-cybercrime-unit

13. The Biggest Cybercrime Threats of 2019 *BY CBN* ON MARCH 18, 2019 *E-HEADLINES* http://cascadebusnews.com/biggest-cybercrime-threats-2019/

14. Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2019 ***Number of women in the cybersecurity field is recalculated and rising Press Release*** – *Steve Morgan*, *Editor-in-Chief* Sausalito, Calif. – Mar. 28, 2019 https://cybersecurityventures.com/women-in-cybersecurity/

15. Терроризм и анти-террористическая деятельность правоохранительных органов Великобритании и США / В.А. Гончарова, С.В. Борисова. – Краснодарский университет МВД России. Краснодар, 2019. – 100 с.

Учебное издание

ЗАРУБЕЖНАЯ ПРАКТИКА ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ КАК ИНСТРУМЕНТОМ СОВРЕМЕННОГО ТЕРРОРИЗМА

Учебное пособие
по английскому языку

Составители:
Гончарова Виктория Аркадьевна
Борисова Светлана Викторовна

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1642-9

9 785926 616429

Подписано в печать 25.03.2020. Формат 60x84 1/16.
Усл. печ. л. 8,4. Тираж 70 экз. Заказ 9.

Краснодарский университет МВД России.
350005, Краснодар, ул. Ярославская, 128.