Linguistics
Linguistique

HANDBOOK

The Language of Cybercrime

With financial support from the Justice Programme of the European Union
Avec le soutien financier du Programme Justice de l'Union Européenne

Copyright Note

This Handbook has been compiled solely for educational purposes.

All the texts and materials included in this Handbook, except where otherwise stated, are the exclusive Property of the European Judicial Training Network (EJTN).

Absolutely no reproduction of the contents of this Handbook, in whole or in part, may be made without the express written permission of EJTN.

Extracts of the Handbook may be reviewed, reproduced or translated for private study only. This excludes sale or any other use in conjunction with a commercial purpose. Any public legal use or reference to the Handbook should be accompanied by an acknowledgment of EJTN as the source and by a mention of the author of the text referred to.

Disclaimer
The contents and views expressed herein reflect only those of EJTN and the European Commission is not responsible for any use that may be made of these contents and views.

European Judicial Training Network
Réseau européen de formation judiciaire

Linguistics
Linguistique

ejtn

With financial support from the Justice Programme of the European Union
Avec le soutien financier du Programme Justice de l'Union Européenne

ISBN-NUMBER: 9789082810622

EAN: 9789082810622

Foreword of the EJTN's Secretary General

Mastering a foreign language and its legal terminology should form an inevitable part of the training of judges and prosecutors. Knowledge of a foreign legal language is key to participation in cross-border activities and to smooth cross-border judicial proceedings and cooperation.*

The European Judicial Training Network (EJTN) has devoted special attention to designing and implementing linguistic training activities for members of the judiciary of EU Member States, supported by the European Commission.

EJTN courses aim to develop participants' legal and linguistic skills by combining legal knowledge and language exercises in a practical and dynamic way, including highly-acclaimed linguistic training on the vocabulary of judicial cooperation in criminal/civil matters, human rights, family law, competition law and cybercrime.

This Handbook is the 1st edition compiling the most relevant training materials used in EJTN linguistic seminars on the vocabulary of cybercrime. It is addressed not only to participants, but also to all judges and public prosecutors interested in developing their linguistic skills. Definitions, exercises and examinations of real cases make the Handbook an invaluable, hands-on resource for any judge, prosecutor or trainer involved in linguistic endeavours.

On behalf of the EJTN, I would like to express my sincere gratitude to the authors of the texts and exercises in the Handbook for their dedicated work. I wish also to express appreciation to the EJTN Project Coordinator, Ms Carmen Domuta, for her dedication in executing the EJTN linguistic activities, as well as members of the EJTN Linguistic Sub-Working Group, chaired by Ms Renata Vystrčilová from the Czech Judicial Academy, and which supervises all EJTN linguistic activities.

Enjoy using this Handbook.

Wojciech Postulski
EJTN Secretary General

* European Commission – Roadmap, European Judicial Training Strategy 2019-2025, Ref. Ares(2017)5432247 - 08/11/2017

List of authors, editor and coordinator

BOYD, MICHAEL S.
Lecturer in English language and translation, Department of English, University of Rome Three (Università degli Studi Roma Tre). Legal linguistics trainer for the Italian School for the Magistracy and the Italian School of Advocacy (SSA).

CAMPOS PARDILLOS, MIGUEL ANGEL
Lecturer in Legal English and Translation, Department of English. University of Alicante.

PETRÁLIKOVÁ, DENISA
Linguist and methodology consultant with Judicial Academy of the Slovak Republic; legal English lecturer at Czech Constitutional Court.

SAMANIEGO FERNÁNDEZ, EVA
Lecturer in Legal English and Translation, Departamento de Filologías Extranjeras, UNED, Spain. Sworn legal translator. Teacher of Legal English for the Spanish Council of the Judiciary, ERA and EJN/Eurojust.

TROPINA, TATYANA
Senior Researcher, Information Law and Legal Informatics Section, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany.

WALBAUM ROBINSON, ISABEL ALICE
Lecturer in Legal Linguistics, Department of Law, University of Rome Three(Università degli Studi, Roma Tre). Legal linguistics educator for the Italian National School of Magistracy (SSM) and the Italian National School of Advocacy, Rome (SSA).

EDITOR: BOYD, MICHAEL S.

COORDINATOR
DOMUTA, CARMEN, Senior Project Manager, Head of Programmes Unit, European Judicial Training Network.

Table of contents:

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

INTRODUCTION

EJTN and Cybercrime Investigations Capacity Building

Tatyana Tropina

Criminal investigations on the Internet are becoming increasingly important as nowadays almost every crime can leave digital traces. Timely judicial and police cooperation is critical as cyberspace knows no borders. One of the ways of addressing the problem of timely mutual legal assistance is capacity building, which helps to create understanding of legal and technical terminology, phenomena and challenges of cybercrime, digital investigations and electronic evidence. Training of members of law enforcement and the judiciary in order to understand the technical characteristics of cybercrime and "speak the same language" is a critical component of this capacity building.

EJTN takes the concept of "speaking the same language" to an entirely new level by providing courses that combine both legal and linguistic aspects of a particular area of law.

I had the pleasure and honour of participating in two EJTN Linguistic Seminars "Language Training on the Vocabulary of Cybercrime" as a cybercrime legal expert: in Madrid in 2016 and in Lublin in 2017. I have participated in many capacity building programmes on cybercrime and digital investigations in the past decade; however, the EJTN program is absolutely exceptional compared to all other training courses I have been involved in. The combination of legal training and language exercises provides a unique dynamic learning environment. Every presentation related to legal and phenomenological aspects of cybercrime is followed by discussions and language exercises, allowing participants to read, listen and speak using the new vocabulary they just acquired from the presentation. Language experts take care of every aspect, be it listening, grammar, pronunciation or comprehension. The groups are small enough to pay attention to every participant and to involve everyone in a meaningful and interactive way.

While both trainers work before the course to prepare the training manual and to agree on the sequence of presentations and exercises, I was very lucky to be paired with language experts, who were very flexible in following the dynamics of the group. For example in Lublin after the part of the course that provided training on the use of information technologies by both cybercriminals and traditional organized crime, Michael – the language expert – and I decided spontaneously to organise a role play activity. We divided participants into several small groups that were tasked with "walking in the shoes of criminals" and explaining how they could use Internet to enhance their criminal activity. It was incredibly rewarding to see the groups thinking outside of the box and using the new IT and crime terminology they had just learnt.

And we, trainers, learn from the participants, too: at the end of the course everyone was asked to talk about a particular cybercrime case that happened in their jurisdiction or in their practice and about legal problems related to the case. Sometimes these presentations are the stories of successful investigations, but some of them are about cases that couldn't be solved because of the failure of mutual legal assistance in cybercrime cases. The stories always make me reflect and think about what I could do better to improve the situation to make fewer failed cybercrime cases happen, to build capacity and to facilitate and enhance cross-border cooperation. The EJTN course is definitely one of the places to provide my input. More important is that it's a place to appreciate both teaching and learning, social activities and sightseeing, meeting people from different European countries, making new friends.

I would like to thank Carmen Domuta for her dedication and tireless work on the preparation of the EJTN Cybercrime Linguistic Seminars. She managed to create an exceptional environment where everyone could enjoy learning and teaching. I would also like to thank my co-trainers – linguistic experts Michael Boyd and Eva Samaniego Fernández – who really made me look at capacity building from a different perspective, provided me with a unique option to think outside of the box of a "lawyer". It was such a joy working with them! Ultimately, it is also the groups of participants who made every day of the course, asked the questions, challenged my opinions, shared their knowledge with each other and us.

This handbook comprises the training materials used in the seminars. The excellent team of the English language skills trainers I had the pleasure of working with has put the handbook together, so it can be used by those who took part in the training to revise their knowledge or by anyone who wishes to improve their language skills and get acquainted with the vocabulary of cybercrime. Congratulations to the team on this significant step in building capacity among law enforcement officers and the Judiciary to address one of the most significant problems – cybercrime investigations.

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 inpenetrability 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 licence – even for the most basic of services – and examine the long and seemingly unending sentences, technical words and

[1] For those interested in the history of English legal language, see especially Tiersma (1999) and Mattila (2006).

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 Varó & 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.

[2] http://legal-dictionary.thefreedictionary.com/assault

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 multi-word 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 wide-spread 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[3]

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.

[3] Activity by E. Samaniego Fernández.

II LEGAL 'DEFINITIONS' OF CYBERCRIME[4]

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

[4] Reproduced with kind permission for educational purposes from The United Nations. Adapted and abbreviated from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Activity by D. Petriláková

III. WHAT IS CYBERCRIME

a) PART I: Collocations[5]

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

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

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)

[5] Adapted from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en. Activity by M. S. Boyd.

- 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 at the end of the handbook and review.

b) PART II: Verb Review[6]

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.

[6] Adapted from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en. Activity by M. S. Boyd.

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[7]

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.

[7] Adapted from http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI(2014)140775_REV1_EN.pdf Activity by D. Petriláková.

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

- *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*
- *B.* *adjective formed by joining an adverb and an adjective*
- *C.* *verb*
- *D.* *adjective formed by joining a noun and an adjective*
- *E.* *a noun formed by joining an adjective and a noun*

1. *to counteract* ________
2. *ever-increasing* ________
3. *profit-driven* ________
4. *combating* ________
5. *cyber-security* ________

d) PART IV: Prepositions and grammar[8]

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

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

[8] Adapted from http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI(2014)140775_REV1_EN.pdf Activity by D. Petriláková.

IV. EUROPOL ON CYBERCRIME[9]

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 cyber-attacks, 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), cyber-crime (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;

[9] Reproduced with kind permission for educations purposes and adapted from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime. Activity by M. S. Boyd.

[10] European multidisciplinary platform against criminal threats

[11] evil or criminal

- 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[12]

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.

[12] Reproduced with kind permission and adapted from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime. Activity by M. S. Boyd.

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)[13]

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

[13] Reproduced with kind permission and adapted from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime. Activity by M. S. Boyd.

- 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[14]

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.

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 (__________________________)

[14] Activity by E. Samaniego Fernández.

VI. BASIC CRIMINAL LAW VOCABULARY[15]

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. LISTENING: CYBERCRIME – EUROPEAN UNION HOME AFFAIRS

First, look for the video available at one of the two websites provided below[16]. Now read the transcript and try to guess what the missing words might be. Look up any other words that you do not understand. Then listen and complete the gaps with the two missing words.

Every day Thomas works, plays and (A) _________________ _________________ on the internet. And sometimes he even (B)_________________ _________________ his Aunt Clarissa. Today the internet is an (C)_________________ _________________ of Thomas' life. In fact, the internet is a world of virtually (D) _________________ _________________ for all of us, but sadly also for criminals. Every day, they attack our computers, steal our personal and (E) _________________ _________________ or send false messages from banks. That's how Aunt Clarissa lost €600. But cybercriminals also use computers to perpetrate (F)_________________ _________________ such as fraud or theft of (G) _________________

[15] Activity by M.A. Campos Pardillos.

[16] Original video available http://ec.europa.eu/avservices/video/player.cfm?sitelang=en&ref=I093336 and https://www.youtube.com/watch?v=O7SiVssPWBg. Activity by M.S. Boyd.

_________________ details. To plan and execute attacks on a (H) _________________ _________________, cybercriminals often use *botnets*, which are networks of compromised personal computers that have been infected by (I) _________________ _________________. Cybercriminality may affect governments, businesses and even Thomas' computer. Without even knowing it Thomas may have already contributed in a (J) _________________ _________________ towards the billions of euros of annual (K) _________________ _________________. He may also be one of the 1 million (L) _________________ _________________ there are in the world every day. Or his computer may have been infected with one of the 150,000 computer viruses (M) _________________ _________________ daily. To avoid that Thomas and his aunt Clarissa are exposed to these dangers on the net the EU is developing a (N) _________________ _________________ to fight borderless cybercriminality. It includes

- close international cooperation and new (O) _________________ _________________;
- identification and removal of child pornography sites and networks, protection of victims and (P)_________________ _______________ those responsible;
- effective partnerships between governments and other (Q) _________________ _________________, such as law enforcement authorities and private companies;
- criminalizing the creation, use and provision of *botnets* aimed at attacking (R) _________________ _________________.

But policies alone are not enough. Thomas knows he must be (S) _________________ _________________. He never sends out his credit card details by email, or gives (T) _________________ _________________ to anyone, or puts private information free on the internet. And he always remembers to update his (U) _________________ _________________. Thanks to the EU policies and his own efforts, Thomas can now surf more securely. He just needs to keep an eye on aunt Clarissa.

VIII. HACKERS, HACKTIVISTS AND CYBERCRIMINALS[17]

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:

[17] All activities in VII by E. Samaniego Fernández.

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?

b) PART II: Hackers vs. Cybercriminals (Listening)

First find the video on YouTube[18]. Then watch it and fill in the gaps. Darren Kitchen, host of tech show Hak5, says why hacking isn’t the same thing as cybercrime. Jorge Ribas sits down with him to find out the difference.

[18] Video available https://www.youtube.com/watch?v=w0u_7DHuuNg. Activities by E. Samaniego Fernández. Reproduced with kind permission of the authors at https://www.hak5.org/.

Darren Kitchen wants to make one thing crystal-clear:

"Hackers aren't out to steal your credit card information, criminals are."

The systems administrator and host of tech show Hack5 recently sat down with Discovery News to **(1)** ________________ a distinction between hacker culture and cybercrime.

"There's a difference between hacking, computer security and then cybercrime, and I don't know any cyber criminals. I mean, I don't -I wouldn't say that anybody should be **(2)** ________________ for trying that, you know, for putting their -their face on YouTube or Google at an airport. I mean, that's just good fun, but there is, you know, definitely cybercrime going on. I haven't met anyone that's **(3)** ___________________ that."

WhatKitchenandhis**(4)**__________________areintoontheirweeklyvideo**(5)**___________________ is a **(6)** __________________ approach to everything from hacking a digital camera to building a cheap video **(7)** ________________ machine.

"One of the biggest **(8)** ______________ is that hackers are **(9)** __________. I mean, hackers are just those guys that like to take apart **(10)** ___________, maybe put it back together, change it, you know, I want to break my iPhone and make it do different stuff that maybe **(11)** __________ didn't want me to do; and that could be considered, you know, hacking on its most basic level; it's uh- it's not being **(12)** ________________ with what you had, it's a **(13)** _____________ for knowledge and exploration."

A thirst that sometimes does lead Kitchen into a bit of **(14)** _____________. "I have a **(15)** __________________ curiosity and I do things in the lab that might get me arrested if I actually tried them on the streets. But that's not to say that I'm evil I'm just , you know, having fun with–with **(16)** ________________."

Tools like **(17)** _______________ phones, video game **(18)** ________________ and laptops that *you* probably use for their **(19)** _________________ use. Boring!!! For hackers like Kitchen, every new **(20)** ________________ is a new opportunity.

"As long as there is curiosity there will be hackers, as long as there is a **(21)** _____________ that has more potential than, you know, the original manufacturer intended, there will be a hacker. And as long as there's a **(22)** ______________ there'll be a hacker and you remember: hackers are what built the internet so, you know, we will continue to build it with their exploits and we're actually making it more secure by pointing out these **(23)** _____________ and then, you know, developing **(24)** ________________."

Which is why so many hackers often land jobs as computer security professionals, literally **(25)** _______________ the holes they themselves helped to expose. It's kinda like the old **(26)** _________________-or-**(27)** __________ argument.

"Right, what's really interesting about it is that it's the **(28)** _________ and the **(29)** __________, I mean, the industry actually created itself by, you know, in in the eighties and even before, just all these hackers coming out of university is good with computers doing fun, you know, normally not malicious stuff but, you know, **(30)** _____________ in some systems for fun and that there was a need for computer security then, so it's both sides of the **(31)** ________________ because the only difference between a hacker and a computer security professional's a **(32)** ___________________."

For Discovery News, I'm Jorge Rivas.

Now answer the following questions about the video and the text:

1. **Lines 7-9:** Kitchen says that he doesn't think anybody should be arrested for doing things that he thinks are mere fun.

- *Can you give examples of the computing world where something that might be considered fun by some would however be an offence or at least a petty crime/misdemeanour?*
- *Can you now give examples from the real world of things that youngsters may think are harmless fun but which are crimes?*

2. **Line 14:** The presenter mentions that Kitchen and his team show people how to hack a digital camera.

- *Can you think of a reason why anyone would want to hack their own digital cameras?*

3. **Lines 17-19:** Kitchen says that "hackers are just those guys that like to take apart stuff, maybe put it back together (…) break my iPhone and make it do different stuff that maybe Apple didn't want me to do."

- *Would you agree that this is all that hackers do?*

4. **Line 23:** The presenter says that Kitchen's curiosity sometimes leads him into a bit of mischief.

- *What do you think he presenter means by saying that Kitchen gets into mischief if what he does only takes place in his lab?*

5. **Line 34:** Referring to the internet, Kitchen states that hackers are actually making it more secure by pointing out its flaws and then mending them.

- *How do you think they can discover internet's flaws without actually committing any type of offence?*

6. **Lines 39-40:**

- *What is meant by "the chicken-or-egg" argument?*
- *Do you have the same expression in your language, or does it use a different comparison?*

7. **Line 42:**

- *What are the yin and the yang? Why does Kitchen mention them?*

8. **Line 46:**

- *What two sides of the coin does Kitchen refer to?*

9. **Lines 47-48:**

- *Do you agree with Kitchen that "the only difference between a hacker and a computer security professional is a pay check?"*

Now read the following statement:

(…) most laws require that the person committing the crime be present in the state when the crime was committed. Computer hacking is, however, one of those crimes, where the criminal is often in a different state.

- *Is this the case in your country at the national level?*
- *What do you think is the EU's approach to the place where a crime is committed, especially dealing with cybercrime?*
- *Why is judicial cooperation important in order to fight cybercrime?*

c) PART III: Grammar (Subjunctive)

Look at following structure from the text above:

"most laws require that the person committing the crime be present in the state when the crime was committed".

In it you can see the following structure:

Subject + infinitive (without 'to)

(*the person committing the crime*) + (*be*)

This is called a "**subjunctive**" in English. In modern English the use of the subjunctive is almost always limited to formal/academic language and legal contexts.

1. A subjunctive is built in the following way: adjective/noun/verb + (that) + subject + the infinitive (without "to").

   It's essential that *the defendant arrive* in time.

   She demanded that *he give* it back.

   What does your mother suggest *I do*?

2. In colloquial language, however, the subjunctive has been replaced with a verb in the present, in the past, or by "should" (It is essential that the defendant *arrives/should arrive* in time).

The subjunctive is used in the following cases:

A. After adjectives such as "important", "essential", "crucial", "advisable", "urgent", etc.

It is essential that counsel for the defence submit a skeleton argument.

It is crucial that a search order be issued immediately.

B. After verbs such as: "ask", "advise", "command", "demand", "insist", "order", "propose", "recommend", "request", "require", "suggest", "urge", etc.

The judge insisted that the jury be sworn in on Monday morning.

C. After nouns, in expressions like the following:

There is the proposal that both claimant and defendant try Alternative Dispute Resolution before going to court.

There is the obligation that the judgment be recognised.

The use of the subjunctive is even more complicated when it involves a passive, a negation or a continuous tense:

> It is *important that the public stand up* when the judge enters the courtroom.
>
> The Head of Chambers insisted *that Jones not be* lawyer for the claimant in the Smith case.
>
> The judge ordered *that the summons be served* promptly.

Use the subjunctive in the following sentences. After that, build the sentence with the 'colloquial' alternative ('should' or a verb in the correct tense):

1. The President of the Third Chamber has ordered that the case ______________________ (REMOVE) from the register.
2. The court requested that __________________________________ (ALL PARTIES, BE) present at the hearing.
3. Prosecuting counsel suggested that ____ (EXHIBITS FIVE TO SIX, MAKE) available to the jury.
4. The presiding judge ordered that _____________________________ (THE PROCEEDINGS, JOIN).
5. The lawyer recommended that the claimant _________________________________ (CHANGE, HIS ACCOUNT) of the facts.
6. In the event of a withdrawal, an order that a party ________________________ (BEAR) the costs of the other party is only possible if the other party has made an application to that effect.
7. It is essential that witnesses ________________________________ (BE) available in the premises of the court at all times.
8. It was requested that the jury ______________________________ (LEAVE) the courtroom for a few minutes.

d) PART IV: Working definitions

Discuss the following terms, which are used by crackers/hackers. What does each of them mean? You can use the internet to help you.

1. Script kiddy/kiddie:
2. Skid:
3. Script bunny:
4. Packet monkeys:
5. S'kiddiots:
6. Lamers:
7. Warez d00dz:
8. Wannabes:
9. Phreaks:

Now consider the following working definitions. Are there any categories which you think could be merged? If so, how would you re-organise these categories?

Script kiddie/skid/script bunny: an unskilled person who uses scripts or programs developed by others to attack computer systems, networks or websites, often not fully understanding the potentially harmful consequences. The term does not refer to the actual age of the person, although they are mostly young people.

Packet monkey: a person who intentionally fills a website or network with data packets, often created or made available by hackers, which results in a denial-of-service for users of the site or network.

S'kiddiots: colloquially it is a word used to refer to kids who run around in a place like 'idiots' while parents pretend to have no control over them. In this context, the term is used to refer to people who use hacker-style techniques without actually knowing how they really function, which sometimes causes harm.

Lamers: people who distribute and/or offer pirated and usually infected software through the internet for downloading. Crackers also use the term to refer to aspirants who are in the initial stages of computer cracking.

Wannabes: a near-synonym for "lamer"; a term used to refer to people who use hacker techniques without knowing or having the curiosity to learn how they function.

Warez d00dz: people who obtain illegal copies of copyrighted software. and distribute it via several gateways.

Phreaks: early hackers who manipulated tone-based telephone switching systems to carry out unauthorized activity within that system.

Insiders: the term refers to hackers that lurk within an organisation. They want to right a wrong they believe a company has perpetrated toward them and either steal sensitive documents or try to disrupt the organisation.

Answer the following questions:

1. In your opinion, which of these four categories are most dangerous for a company: script kiddies, hacktivists, cybercriminals or insiders? Why?
2. Which of those are not dangerous for individual computer users?
3. Would you say that hacktivists are criminals? Why/why not?
4. In what ways can script kiddies be dangerous? Do they break the law?
5. Script kiddies usually don't know what they are doing, or at least they are not fully aware of the consequences of what they do. Is that a mitigating factor? Why/why not?
6. Recital (12) of Directive 2013/40/EU of the European Parliament and of the council of 12 August 2013 on attacks against information systems provides as follows:

   > This Directive does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts are committed without criminal intent, for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system.

   How does this relate to what script kiddies, lamers or wannabes do? Would you take this into consideration if such a case came before you or if you had to prosecute it?

7. Recital (12) of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems provides as follows:

   > The identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems is a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems. Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities for the legal detection and reporting of security gaps.

   What role could hackers play in this? Does the adjective "legal" in "legal detection" exclude hackers? What "legal detection" mechanisms/tools can you think of? Do they clash with privacy and/or confidentiality rights?

e) PART V: Reflection

Do you know the difference between these three types of hackers?

Black hat hackers

White hat hackers

Grey hat hackers

Read the following definitions in order to discover the differences between the categories above and then discuss if the differences are clear-cut.

Black hat hackers: people who violate computer security for personal gain (such as stealing credit card numbers or collecting personal data for sale to identity thieves) or for pure maliciousness.

White hat hackers: term used for "ethical hackers" who use their abilities for legal purposes rather than for criminal purposes. Many of them are employed by different companies, bodies or organisations to test their computer security systems and report back in order to improve their defences.

Grey hat hackers: people who do not work for their own personal gain or to cause harm, but who may technically commit crimes and do arguably unethical things.

Below you will find some of the roles of cybercriminals. Can you guess what each of them does?

Cybercriminals often work in organized groups. Try to define the following roles *from a purely criminal point of view*:

- Programmers:
- Distributors:
- IT experts:
- Fraudsters:
- System hosts and providers:
- Cashiers:
- Money mules:
- Tellers:
- Leaders:

UNIT 2
CYBERCRIME: REGULATIONS, DIRECTIVES & ORGANIZATIONS

INTRODUCTION

In this Chapter we propose a number of language activities that are based on some of the legislative initiatives introduced by the EU (and other organizations) to combat the spread of cybercrime. The European Commission provides a list[19] of the most important legislative actions including

- Directive 2013/440/EEU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems which replaced Council Framework Decision 2005/2222/JJH;
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA;
- The so-called ePrivacy Directive, Directive 2009/1136/EEC of the European Parliament and of the Council of 25 November 2009;
- The Framework Decision on Combating Fraud and Counterfeiting of non-cash payment from 2001

There are other pieces of legislation that we will be looking at through the language exercises; can you find them? In addition to the legislation some of the activities also deal with the important organizations involved in combating cybercrime.

LANGUAGE EXERCISES

I. THE INTERNET ORGANISED CRIME THREAT ASSESSMENT[20]

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

[19] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

[20] Adapted from https://www.europol.europa.eu/latest_news/iocta-2015-europol-annual-report-cybercrime-threat-landscape-published. Activity by D. Petriláková.

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[21]

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

[21] Activity by I.A. Walbaum Robinson.

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. ARTICLE 3 OF COUNCIL FRAMEWORK DECISION 2004/68/JHA[22]

Read Article 2 of the EU Framework Decision and answer the questions that follow.

> Each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of a computer system or not, when committed without right is punishable:
>
> (a) production of child pornography;
>
> (b) distribution, dissemination or transmission of child pornography;
>
> (c) supplying or making available child pornography;
>
> (d) acquisition or possession of child pornography

1. What is the sentencing option in your country for production of child pornography?
2. How different would a sentence be if imposed on an offender found guilty of possession of child pornography as oppose to supplying or making available child pornography?
3. Would the sentence imposed upon a person convicted of conduct related to child pornography be the one of imprisonment or could a more lenient sentence be imposed?

Now look at Article 2 above again and choose the expressions you think could be used as synonyms for 6 of the words and concepts above (some of words cannot be used):

making, deliberate, done, steps, less strict, incarceration, obtaining, spreading, *convicted, actions, connected to, the accused, prison, terminology, selling, stricter,* *having, sentencing, associated with, minor, baby*

[22] Adapted from Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography available http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004F0068&from=EN. Activities by D. Petriláková.

IV. DIRECTIVE 2013/40 EU: VOCABULARY IN CONTEXT[23]

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.

(6) a. hindering b. bothering c. interfering

(7) a. inserting b. inputting c. implanting

[23] Adapted from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN. Activities by E. Samaniego Fernández.

(8) a. wiping out b. rubbing out c. deleting

(9) a. transforming b. altering c. amending

(10) 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

V. COE CONVENTION ON CYBERCRIME – EXTRADITION: PREPOSITIONS[24]

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.

VI. DIRECTIVE 2009/136/EC: "TO BE" STRUCTURES[25]

a) PART I: Grammar in context

Look at the sentences in bold below, which appear in Directive 2009/136/EC of 25 November 2009 of the European Parliament and of the Council. What grammatical structure is being used. Read the grammar explanation below.

Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances

[24] Adapted from http://www.interlex.it/2testi/ue/conv-cybercrime2001.pdf. Activity by M. A. Campos Pardillos.

[25] Adapted from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=en/ and http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0093&from=EN. Activities by E. Samaniego Fernández.

in which providers are required to notify personal data breaches, the format of such notification and **the manner in which the notification is to be made**.

It is for the national regulatory authority **to decide which information is to be published** by the undertakings providing public communications networks and/or publicly available telephone services.

Any digital television set with an integral screen of visible diagonal greater than 30 cm which is put on the market for sale or rent in the Community **is to be fitted** with at least one open interface socket.

The structure "to be to" in English is used to convey different meanings:

1. Future arrangements / scheduled events/ plans. In this case, it can be replaced by "going to". Frequently used by the press: "The King of Spain is to visit Peru".
2. Orders, instructions, obligation or prohibitions. Frequently used in the third person (impersonal): "Nobody is to leave the examination room before 3". Also used in the second person: "You are to submit the report by Tuesday".
3. In if-clauses for an event that might or might not happen: "If you were to bake muffins, I would have some".
4. If it appears with the perfect infinitive, it refers to a planned event that did not happen: "The Head of the unit was to have addressed a speech to the staff but she missed her train".

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.

Now replace the appropriate structures in the following sentences from Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography with a "to be to" structure.

1. Decision 2004/68/JHA should be replaced by a new instrument providing such comprehensive legal framework to achieve that purpose.
2. The Council conclusions of 24 and 25 April 2002 on the approach to apply regarding approximation of penalties, which indicate four levels of penalties, should be kept in mind in the light of the Lisbon Treaty.
3. Serious forms of sexual abuse and sexual exploitation of children should be subject to effective, proportionate and dissuasive penalties.
4. The definition of child pornography should also be clarified and brought closer to that contained in international instruments.
5. The aggravating circumstances should not be provided for in Member States' law when irrelevant taking into account the nature of the specific offence.
6. This Directive provides for levels of penalties which should apply without prejudice to the specific criminal policies of the Member States concerning child offenders.
7. To ensure successful investigations and prosecutions of the offences referred to in this Directive, their initiation should not depend, in principle, on a report or accusation made by the victim or by his or her representative.

VII. Directive 2011/92/EU: More Practice with the Subjunctive

Before you do this activity review the rules for the formation of the subjunctive in Exercise VIII in Unit 2.

Now look at the sentences below from Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. Use the subjunctive in the gaps using the clue provided. The first one has been done for you.

1. A direct intent requirement that those tools ______________________ (THOSE TOOLS, USE) to commit one or more of the offences laid down in this Directive must be also fulfilled.
2. In such cases, it may be expedient that __________________ (THE REQUEST FOR INFORMATION, ACCOMPANY) by telephone contact in order to ensure that the request is processed swiftly by the requested Member State and that feedback is provided within eight hours.
3. Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that ____________________ (IT, USE) to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence
4. A Party may require that ______________________ (THE OFFENCE, COMMIT) with dishonest intent, or in relation to a computer system that is connected to another computer system.
5. Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that ______________________________ (THE COMMITTEE OF MINISTERS, SUPPORT) the work on cybercrime carried out by the European Committee on Crime Problems (CDPC).

6. A Party may reserve the right to require that ______________________________ (THE CONDUCT DESCRIBED IN PARAGRAPH 1, RESULT) in serious harm.

7. A Party may require by law that ___________________________ (A NUMBER OF SUCH ITEMS, POSSESS) before criminal liability attaches.

8. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to ensure that ___________________________ (SUCH EXPEDITIOUS PRESERVATION OF TRAFFIC DATA, BE) available.

9. Prior to providing such information, the providing Party may request that ___________________________ (IT, KEEP) confidential or only used subject to conditions.

10. Member States shall take the necessary measures to ensure that ________________________________ (AN ATTEMPT TO COMMIT ANY OF THE OFFENCES REFERRED TO IN ARTICLE 3(4) AND (6), BE) punishable.

11. Member States shall take the necessary measures to ensure that in criminal court proceedings relating to any of the offences referred to in Articles 3 to 7, that it may be ordered that ________________________ (THE HEARING, TAKE) place without the presence of the public.

Now try to form these more difficult subjunctives.

12. The prosecutor suggested that ________________________________ (EXHIBITS ONE TO FOUR, NOT MAKE) available to the jury.

13. Counsel recommended that defendant _______________________________ (NOT CHANGE) his account of the facts.

14. It was requested that _____________________________ (THE PARTIES, BE WAITING) at the door of the court.

15. The judge requested that the jury ____________________________ (NOT LEAVE) the courtroom.

16. It is essential that solicitors __________________________ (BE, PREPARING) the case paperwork long before instructing a barrister.

UNIT 3
THE LANGUAGE OF CYBERCRIME: CASES

INTRODUCTION

In this Chapter we will look at a few actual cases in the area of cybercrime, which in recent years have been spreading fast. As stated in one of texts in the exercises that follow "[t]he past 12 months have seen a number of unprecedented cyber-attacks in terms of their global scale, impact and rate of spread." Due to the borderless nature of cybercrime, most such cases involve a number of different countries as coordinated law enforcement efforts that operate employing joint investigation teams, and are often supported by Eurojust, and its IOCTA (Organised Crime Threat Assessment), and Europol[26] as well as non-EU law enforcement agencies such as the FBI. Information about such cases can be found at the institutional websites as well as sites such as that of the US Justice Department (www.justice.gov) and the UK National Crime Agency's Cyber Crime Unit[27]. The cases we deal with in the exercises range from WannaCry ransomware, Darknet, and Darkode (and Operation Shrouded Horizon), to the Love-Bug virus and involved a number of countries including Ukraine, the United States, and the Philippines.

LANGUAGE EXERCISES

I. Joint Investigation Team in Ukraine[28]

a) PART I: Reading comprehension

Read about the case and answer the questions below:

A **joint investigation team** (JIT) consisting of investigators and judicial authorities from six different European countries, supported by Europol and Eurojust, has taken down a major cybercriminal group during a coordinated action in Ukraine. With on-the-spot support from Europol, Austrian and Belgian law enforcement and judicial authorities, the action in Ukraine on 18 and 19 June resulted in the arrest of five suspects, eight house searches in four different cities, and the seizure of computer equipment and other devices for further forensic examination.

The aim of this JIT was to target high-level cybercriminals and their accomplices who are suspected of developing, exploiting and distributing Zeus and SpyEye malware – two well-known banking Trojans –

[26] For Eurojust, see http://www.eurojust.europa.eu and Europol https://www.europol.europa.eu.

[27] For the US Justice Department, see https://www.justice.gov and for UK National Crime Agency's Cyber Crime Unit, see http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

[28] Adapted from https://www.europol.europa.eu/newsroom/news/major-cybercrime-ring-dismantled-joint-investigation-team. Activities by D. Petriláková.

as well as channelling and cashing-out the proceeds of their crimes. The cybercriminals used malware to attack online banking systems in Europe and beyond, adapting their sophisticated banking Trojans over time to defeat the security measures implemented by the banks.

Each cybercriminal had their specialty and the group was involved in creating malware, infecting machines, harvesting bank credentials and laundering the money through so-called money mule networks. On the digital underground forums, they actively traded stolen credentials, compromised bank account information and malware, while selling their hacking 'services' and looking for new cooperation partners in other cybercriminal activities. This was a very active criminal group that worked in countries across all continents, infecting tens of thousands of users' computers with banking Trojans, and subsequently targeted many major banks. The damage produced by the group is estimated to be at least EUR 2 million.

"In one of the most significant operations coordinated by the agency in recent years Europol worked with an international team of investigators to bring down a very destructive cybercriminal group. With our international partners, we are committed to fighting the threats brought about by malware and other forms of cybercrime, to realise safer technology infrastructures and online financial transactions for businesses and people the world over," said Rob Wainwright, Director of Europol.

"This case demonstrates that it is only possible to combat cybercrime in a successful and sustainable way if all actors-that means investigative judges and judicial authorities- coordinate and cooperate across the borders." Ingrid Maschl-Clausen, National Member of Austria to Eurojust, commented at a press conference in Vienna.

The recent action was part of the wider investigation that was launched in 2013 by the JIT members (Austria, Belgium, Finland, the Netherlands, Norway and the United Kingdom), and facilitated by Europol and Eurojust. Last week's results brings the total number of arrests in this operation to 60 – 34 who were captured as part of a 'money mule' operation run by Dutch law enforcement authorities.

Europol has provided crucial support to the investigation since 2013 including handling and analysis of terabytes of data, and thousands of files in the Europol Malware Analysis System; handling of thousands sensitive operational messages; production of intelligence analysis reports; forensic examination of devices; organisation of operational meetings and bi-monthly international conference calls. The enormous amount of data that was collected and processed during the investigation will now be used to trace the cybercriminals still at large. Both Eurojust and Europol provided funding for the joint investigation team.

Eurojust hosted coordination meetings, bringing the judicial authorities and investigative judges together. Moreover, Eurojust provided legal advice, and assisted with the drafting of the Joint Investigation Team Agreement, as well as supported the joint investigation team during the lifetime of the entire process. Eurojust also enabled contacts at judicial level between non-EU Member States, in particular with Ukraine.

1. How many different countries did the JIT (Joint Investigation Team) of investigators and judicial authorities come from?
2. Can you name countries the law enforcement and judicial authorities of which were providing the JIT with on the spot support?
3. What was the focus of the JIT and where was the operation located?
4. How many properties were searched?
5. Were any electronic devices seized? If so for what purpose?

6. Were any suspects or persons of interest arrested?
7. What are Zeus and SpyEye?
8. How did the cybercriminals defeat security measures implemented by the banks?
9. How was the harvested money eventually laundered?
10. How were the stolen bank credentials traded?
11. What kind of services were the suspects offering and to whom?
12. How many competitors were estimated as having been compromised by this particular group of suspects?
13. What was the estimated damage?
14. When was the investigation launched and which organisations facilitated this operation?
15. How many people have been arrested in total in this operation?

b) PART II: Self-reflection

Now consider the following questions. Do you know the answers?

- Have you heard about JITs before?
- Have you met, heard of or do you personally know anyone who has been involved with JITs?¨
- Have you ever had any personal experience with a Trojan?
- Could you explain how a Trojan operates?
- Would you enjoy being involved in your professional capacity in an operation similar to the one describe in the above text?
- If yes, why? if not, why not?
- Would a court order be needed in your country in order to search a house of a suspected criminal?
- When and under what circumstances would the law enforcement agency be able to seize electronic devices from a) residential premises of a suspect b) non-residential premises of a suspect?

c) PART III: Grammar INPUT

Find the sentences containing the following verb structures and forms and underline them:

1. consisting
2. has taken down
3. resulted
4. are suspected
5. to defeat
6. stolen

7. to bring down
8. fighting
9. demonstrates
10. will now be used

Then find the grammatical label below best suited for the structure or the form within the context of the article (NB: not all of those will be used):

A. past simple active

B. past simple passive

C. gerund

D. future simple active voice

E. future simple passive voice

F. phrasal verb

G. present participle

H. past participle

I. present perfect simple active

J. present perfect simple passive

K. present simple third person singular

L. present perfect continuous active voice

M. present perfect continuous passive voice

N. bare infinitive

O. conditional

II. LAW ENFORCEMENT SUCCESSES IN CYBERCRIME[29]

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.

[29] Reproduced by kind permission and adopted from https://www.europol.europa.eu/newsroom/news/2017-year-when-cyber-crime-hit-close-to-home. Activities by I. A. Walbaum Robinson.

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 Organised 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 Organised 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: “Cross-border 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 recognise 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 destabilise 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.

III. Darkode and Shrouded Horizon – Department of Justice[30]

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.

[30] Adapted from https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled. Activity by M. S. Boyd.

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.

b) Listening: Operations Shrouded Horizon[31]

First find the audio file at the URL listed below. Then listen to the file and complete the gaps with the missing words.

Mollie Halpern: In what is the largest coordinated international law enforcement (A) ________________ targeting an online cyber criminal (B) ________________, the FBI and its partners from 20 countries dismantled a forum known as Darkode.

The computer hacking forum was (C) ________________ protected; prospective members had to be invited and were required to prove how they could contribute to the forum's criminal (D)________________.

Scott Smith: This underground online forum was a (E) ________________ ________________ for those criminals interested in buying, selling, and trading (F) ________________, botnets, or stolen personal identifiable information, credit card information, and (G) ________________ that would help facilitate cyber crimes all over the globe.

Halpern: That was Scott Smith, the special agent in charge of the FBI's Pittsburgh Field Office, which led Operation Shrouded Horizon, a two-year long undercover (H) ________________. Investigators infiltrated Darkode, targeting the most egregious cyber (I) ________________ from around the world who believed they were impenetrable. This investigation is ongoing, but so far, a dozen cyber criminals face (J)________________.

Smith: It takes a lot of effort, a lot of (K) ________________, and a lot technical savvy. Our agents exemplify what the FBI's cyber program is all about—to be able to keep up with the current (L)________________ and the most sophisticated cyber criminals.

[31] Adapted from https://www.fbi.gov/audio-repository/news-podcasts-thisweek-operation-shrouded-horizon.mp3/view. Activity by M. S. Boyd.

Halpern: For more information on this operation and the FBI's Cyber Division, visit www.fbi.gov. With FBI, This Week, I'm Mollie Halpern of the Bureau.

IV. CYBERSTALKING AND SEXTORTION[32]

You are going to read an article about cyberstalking and sextorting. Before you read the text, answer the following questions:

Do you know what "sextortion" is?

How do these criminals gain access to the sensitive materials?

Now, read the text about a real case in the US:

Pennsylvania Man Pleads Guilty to Cyberstalking and "Sextorting" Massachusetts College Student

BOSTON – A Pennsylvania man pleaded guilty today in U.S. District Court in Boston to engaging in a "sextortion" campaign against a Boston-area college student. James F. Connor V, 20, of West Chester, Penn., pleaded guilty to one count of cyberstalking and one count of extortion. U.S. District Court Judge William G. Young scheduled sentencing for April 7, 2016.

In 2012, Connor and the victim met through social media and developed an online relationship. In the course of that relationship, the victim sent Connor naked pictures of herself through Snapchat and engaged in sexually explicit video chats with him using FaceTime. Connor preserved many of these images without her consent. After the relationship ended, Connor attempted to continue communications with the victim and initiated a campaign of harassment and intimidation. He threatened to harm her physically and harm her reputation by publicly disseminating the sexually explicit images. Connor also repeatedly threatened to commit suicide if the victim did not take his calls, and sent her pictures of him holding a knife to his throat with blood, which was later determined to be fake, dripping down his neck.

In September 2015, Connor escalated his campaign of harassment when he began blackmailing the victim and threatening to send the sexually explicit images to her parents and Twitter followers if she did not send additional naked pictures and engage in sexually explicit video chats with him. As part of Connor's cyberstalking and sextortion campaign, he sent the victim a detailed list of sexual demands, which included, among other things, that she send him five sexually explicit pictures and have five sexually explicit video chat sessions per week over a five week period. Connor also insisted that she break up with her current boyfriend.

Connor frequently employed a telephone and text message spoofing, or anonymizing, application that allows users to easily change telephone numbers to conceal their identity. In October 2015, Connor was arrested and charged via criminal complaint after the victim reported the threats and prior pattern of harassment to law enforcement authorities.

The charge of cyberstalking carries a sentence of no greater than five years in prison, three years supervised release and a fine of $250,000. The charge of extortion provides for a sentence of no greater than two years in prison, one year supervised release, and a fine of $250,000. Actual sentences for federal crimes are typically less than the maximum penalties. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

[32] Adapted from https://www.justice.gov/usao-ma/pr/pennsylvania-man-pleads-guilty-cyberstalking-and-sextorting-massachusetts-college-student. Activities by M. A. Campos Pardillos.

a) PART I: True or False

Now decide whether the following statements are, according to the text, true (T), false (F), or whether the text neither confirms nor denies the statement (?):

a) Connor sent explicit pictures of himself to the victim. ______

b) Connor persuaded the victim to let him store the naked pictures that she sent him ______

c) Connor said that, if the victim did not accept his sexual demands, he would use the Internet to defame her. ______

d) Connor used technological means to hide his telephone number when making the threats. ______

e) The victim reported Connor's final threats, but not the previous harassment, which was exposed later. ______

f) After pleading guilty, Connor is likely to serve a seven-year prison sentence. ______

b) PART II: Vocabulary

Find words in the text corresponding to the definitions below.

a) _______________: blackmail in which sexual information or images are used to extort sexual favours and/or money from the victim.

b) _______________: crime of using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person.

c) _______________: a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

d) _______________: crime in which one person forces another person to do something against his will, generally to give up money or other property, by threat of violence, property damage, damage to the person's reputation, or extreme financial hardship.

e) _______________: (sometimes also called special or mandatory parole) is a preliminary period of freedom for recently released prisoners.

f) _______________: rules that set out a uniform sentencing policy for individuals and organizations convicted of certain offences.

c) PART III: Synonyms

In the following sentences, extracted from the text, <u>one</u> word has been replaced by a synonym. Find such word, and try to remember what the original word was.

a) Connor kept many of these images without her consent.

b) If she did not send more naked pictures and engage in sexually explicit video chats with him.

c) Real sentences for federal crimes are typically less than the maximum penalties.

d) Connor frequently used a telephone and text message spoofing, or anonymizing, application.

e) The victim reported the threats and previous pattern of harassment to law enforcement authorities.

V. The Love-Bug virus[33]

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.

[33] Reproduced by kind permission of WSWS, https://www.wsws.org/en/articles/2000/05/bug-m10.html. Activities by M. S. Boyd and D. Pertiláková.

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 organisation 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?

VI. U.S. EMPLOYEE SENTENCED FOR HACKING AND CYBERCRIMES[34]

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.

[34] Adapted from https://www.justice.gov/opa/pr/former-us-state-department-employee-sentenced-57-months-extensive-computer-hacking. Activities by I. A. Walbaum Robinson.

"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.

ANSWER KEY

Unit 1

Exercise I

The definitions coming from official bodies/agencies/institutions are letters C (Interpol), E (European Union webpage on home affairs policies) and F (Australian government).

Exercise II

1. F; 2. F; 3. T; 4. F; 5. T.

Exercise III

a) Part I: Collocations
(A) criminal acts; (B) information systems; (C) bank accounts; (D) sexual abuse; (E) terrorist acts; (F) operational cooperation; (G) legislative actions; (H) criminal sanctions; (I) child pornography; (J) communications services; (K) Framework Decision.

b) Part II: Verb Review
1. f 2. a 3. d 4. c 5. b 6. e
(A) has played (B) started (C) acts (D) was launched (E) is involved.

c) Part III: General framework
(1) a; (2) e; (3) f; (4) g; (5) d; (6) c; (7) h; (8) j; (9) b.

Grammatical explanations
1. C; 2. B; 3. D; 4. A; 5. E.

d) Part IV: Prepositions and grammar
defined **by**; access **to**; interception **of**; **In** particular; required **for**; **in** order to; **over** the internet; imposed **on**; **in** case; **from** which they benefit.
Bonus question:
preposition; preposition and particle; pronoun; preposition.

Exercise IV

a) Part I: Verbs
(A) are committed (have been committed); (B) generate (have generated/have been generating); (C) affect; (D) *can* be harnessed; (E) are also getting (have also got [UK]/gotten [US]) (F) are taking (have been taking); (G) is becoming (has become); (H) can be seen; (I) is leading (has led); (J) have sought (are seeking/seek); (K) gain; (L) infiltrates; (M) gains; (N) *can* complement.

b) Part II: Adjectives
(A) innovative; (B) institutional; (C) law; (D) intelligence-led; (E) cross-border; (F) notable; (G) joint; H) large-scale; (I) compromised.

c) Part III: Vocabulary (Definitions)
(A) botnet; (B) distributed denial-of-service; (C) rootkit; (D) privileged access; (E) Trojan; (F) file infector; (G) infected code; (H) remote-access trojan; (I) Ransomware; (J) Scareware; (K) security threats; (L) Spyware; (M) Adware; (N) pop-ups.

Exercise V

1. AS (Access Server); 2. ATM (Automatic Teller Machine); 3. BT (Bluetooth); 4. BW (Bandwidth); 5. CERT (Computer Emergency Response Team); 6. CNP Transaction (Card Not Present Transaction); 7. CPS (Characters per Second); 8. CSP (Cloud Service Provider); 9. CSV (Comma-separated values); 10. DBMS (Database Management System); 11. DL (Download); 12. DNS (Domain Name System); 13. EFS (Encrypting File System); 14. FAQs (Frequently Asked Questions); 15. FxP (File Exchange Protocol); 16. GB (Gigabyte); 17. IP (Internet Protocol); 18. IS (Information Systems); 19. ISP (Internet Service Provider); 20. IT (Information Technology); 21. LCD (Liquid Crystal Display); 22. MB (Megabyte); 23. MS (Memory Stick); 24. NFS (Network File System); 25. ODBC (Open Database Connectivity); 26. OLTP (Online Transaction Processing); 27. OS (Operating System); 28. PDF (Portable Document Format); 29. RAS (Remote Access Service); 30. RAM (Random Access Memory); 31. RAT (Remote Administration Tool); 32. RC (Region Code); 33. ROM (Read Only Memory); 34. SMTP (Single Mail Transfer Protocol); 35. SSD (Software Specification Document); 36. TB (Terabyte) 37. URL (Uniform Resource Locator); 38. VGA (Video Graphics Adapter) 39. VR (Virtual Reality); 40. WAN (Wide Area Network); 41. WAP (Wireless Access Point); 42. WiFi (Wireless Fidelity); 43. WLAN (Wireless Local Area Network); 44. WWW (World Wide Web).

Exercise VI

The sentences are shown with the correct answers and in the right chronological order.
(8) The youth was **arrested** at his home, where computer equipment was **seized** containing evidence of his illegally tampering with websites.
(4) Once at the police station, he was **interrogated** in the presence of counsel, but refused to answer most of the questions.
(2) He was finally **charged** with criminal damage, but at the initial hearing, he **pleaded** not guilty.
(7) The judge who was **trying** the case **admitted** most of the evidence presented by the prosecution.
(6) The judge **found** him guilty, although in most jurisdictions a jury would probably have not **convicted** him.
(5) The conviction was quite surprising to him, since he expected to be **acquitted.**
(1) He was **sentenced** to an eight-month juvenile term.
(3) On appeal, the conviction was **quashed**.

Exercise VII

(A) buys things; (B) speaks with; (C) integral part; (D) unlimited possibilities; (E) confidential information; (F) other misdeeds; (G) credit card; (H) large scale; (I) computer viruses; (J) small way; (K) cybercrime profit; (L) cybercrime victims; (M) in circulation; (N) common policy; (O) stronger laws; (P) pursuit of; (Q) public bodies; (R) information systems; (S) more careful; (T) his passwords; (U) antivirus software.

Exercise VIII

a) Part I: Definitions
(open answers)

b) *Part II: Hackers vs. Cybercriminals (Listening)*
1. draw; 2. arrested; 3. into; 4. cohorts; 5. podcast; 6. DIY; 7. arcade; 8. misconceptions; 9. evil; 10. stuff; 11. apple; 12.satisfied; 13. thirst; 14. mischief; 15. malicious; 16. tools; 17. cell; 18. consoles; 19. intended; 20. gadget; 21. device; 22. flaws; 23. fixes; 25. patching; 26. chicken; 27. egg; 28. yin; 29. yang; 30. breaking; 31. coin; 32. pay check.

Questions 1-9
(open answers)

c) Part III: Grammar
1. Be removed; is removed, should be removed; 2 all parties be present; all parties were present, all parties should be present; 3. exhibits five to six be made available; exhibits five to six were made available, exhibits five to six should be made available; 4. the proceedings be joined; the proceedings were joined, the proceedings should be joined; 5. the claimant change his account; the claimant changed his account, the claimant should change his account; 6. a party bear; a party bears, a party should bear; 7. witnesses be available; are available, should be available; 8. leave; left, should leave.

d) Part IV: Working definitions
(open answers)

e) Part V: Reflection
Programmers: they write code or programs used by cybercriminal organisations*;* **Distributors**: they distribute and sell stolen data and goods from associated cybercriminals; **IT experts**: they maintain a cybercriminal organisation's IT infrastructure (servers, encryption technologies, databases, etc.); **Fraudsters**: they create and implement schemes like spam and phishing; **System hosts and providers**: they host sites and servers that have illegal contents; **Cashiers**: they provide account names to cybercriminals and control accounts; **Money mules**: they manage bank account transfers; **Tellers**: they transfer and launder illegal money through digital and foreign exchange methods; **Leaders**: they assemble and direct cybercriminal teams, and usually lack technical knowledge.

Unit 2

Exercise I

(1) a; (2) c; (3) b; (4) c; (5) a; (6) a; (7) b; (8) b; (9) c; (10) a; (11) b; (12) a; (13) c; (14) a; (15) b; (16) a; (17) c.

Exercise II

a) Part I: IOCTA
1. f; 2. j; 3. l; 4. i; 5. c; 6. e; 7. h; 8. g; 9. d; 10. b; 11. n; 12. a; 13. k; 14. m.

b) Part II: Organizations and authorities
1. e; 2. j; 3. d; 4. a; 5. i; 6. c; 7. h; 8. b; 9. f; 10. g.

c) Part III: Telecommunications
1. b; 2. c; 3. e; 4. a; 5. f; 6. d.

Exercise III

Questions:
(open answers)
Synonyms:
measures (*steps*); intentional (*deliberate*); means (*done*); production (*making*); dissemination (*spreading*); child (*minor*)

Exercise IV

1. c; 2. b; 3. A; 4. b; 5. c; 6. a; 7. b; 8. c; 9. b; 10. a; 11. c; 12. b; 13. a; 14. c; 15. c; 16. a; 17. b; 17bis. b; 18. a; 19. b; 20. a; 21. c; 22. a; 23. c; 24. b; 25. b; 26. a; 27. c; 28. a; 29. a; 30. b; 31. a; 32. c; 33. a; 34. a; 35. b; 36. c; 37. b; 38. A; 39. b; 40. a.

Exercise V

(1) between; (2) with; (3) under; (4) by; (5) by; (6) under; (7) on; (8) under; (9) on; (10) from; (11) for; (12) to; (13) on; (14) over; (15) at; (16) for; (17) in; (18) under

Exercise VI

b) Part II: Grammar practice

1. (FUTURE ARRANGEMENTS) The President WILL make a further visit to New York next week. 2. (ORDER) You MUST carry your ID at all times. 3. (OBLIGATION) All students MUST take a mental maths test at the end of the term. 4. (FUTURE ARRANGEMENT) The Secretary General WAS GOING TO speak to the Committee meeting. 5. (PROHIBITION) You may go to John's birthday party but you MUST not return later than 12pm. 6. (IF-CLAUSE: FUTURE ACTION) If you ARE GOING TO work in Spain for longer than three months, you have to apply for a work permit. 7. (PLANNED EVENT THAT DID NOT HAPPEN) Mr. Jones SHOULD have spoken at the conference, but he didn't make it in time. 8. (SCHEDULED EVENT) An employee of the firm WILL appear in court today to give evidence about the alleged fraud. 9. (IF-CLAUSE) If I were to lend you 80 euros, would you be able to return them by Monday? 10. (INSTRUCTIONS/ ORDERS) No books or notes of any kind MUST be taken into the examination room 11. (PROHIBITION) You CANNOT/ MUST NOT leave the premises without parental permission

from Directive 2011/92/EU

1. Decision 2004/68/JHA IS TO BE replaced by a new instrument providing such comprehensive legal framework to achieve that purpose. 2. The Council conclusions of 24 and 25 April 2002 on the approach to apply regarding approximation of penalties, which indicate four levels of penalties, ARE TO BE kept in mind in the light of the Lisbon Treaty.3. Serious forms of sexual abuse and sexual exploitation of children ARE TO BE subject to effective, proportionate and dissuasive penalties. 4. The definition of child pornography IS also TO BE clarified and brought closer to that contained in international instruments. 5. The aggravating circumstances ARE not TO be provided for in Member States' law when irrelevant taking into account the nature of the specific offence. 6. This Directive provides for levels of penalties which ARE TO APPLY without prejudice to the specific criminal policies of the Member States concerning child offenders. 7. To ensure successful investigations and prosecutions of the offences referred to in this Directive, their initiation IS NOT TO depend, in principle, on a report or accusation made by the victim or by his or her representative.

Exercise VII

1. those tools be used; 2. the request for information be accompanied; 3. it be used; 4. the offence be committed; 5. the committee of ministers support; 6. the conduct described in paragraph 1 result; 7. a number of such items be possessed; 8. such expeditious preservation of traffic data be; 9. it be kept; 10. an attempt to commit any of the offences referred to in Article 3(4) and (6) be punishable; 11. the hearing take place.

More difficult subjunctives

12. exhibits one to four not be made; 13. not change; 14. the parties be waiting; 15. not leave the room; 16. be preparing.

Unit 3

Exercise I

a) Part I: Reading comprehension

1. six; 2. Europol, Austrian and Belgian law enforcement and judicial authorities; 3. to target high-level

cybercriminals and their accomplices…; in four different cities in Ukraine; 4. eight; 5. Yes, computer equipment and other devices for further forensic investigation; 6. Yes, five suspects were arrested; 7. two well-known banking Trojans; 8. by adapting banking Trojans over time; 9. through so-called money mule networks; 10. using digital underground forms; 11. they sold their hacking 'services' to new cooperation partners; 12. tens of thousands of computers; 13. EUR 2 million; 14. it was launched in 2013 by the JIT members (Austria, Belgium, Finland, the Netherlands, Norway and the UK) and facilitated by Europol and Eurojust; 15. 60.

b) Part II: Self-reflection
(Open answers)

c) Part II: Grammar INPUT
A. past simple active – resulted in; B. past simple passive – not used (in the text e.g. were captured); C. gerund – fighting; D. future simple active voice – not used; E. future simple passive voice – will now be used; F. phrasal verb – to bring down, has taken down; G. present participle – consisting; H. past participle – stolen; I. present perfect simple active - has taken down; J. present perfect simple passive – not used; K. present simple third person singular - demonstrates; L. present perfect continuous active voice - not used; M. present perfect continuous passive voice - does not exist; N. bare infinitive - to bring down, to defeat; O. conditional - not used

Exercise II

a) Part I: Reading comprehension
1. To provide suggestions to stakeholders such as policy makers, law enforcement agencies and other interest groups. It also informs decision-makers on ways to fight cybercrime. 2. The cybercrime activities are being carried out not only against government, companies, the military but also against individuals of all walks of life. 3. ENISA is responsible for providing expertise to ensure cyber security in Europe. 4. CERT is a computer emergency response team that provides nationwide volunteer training and organization that professionals responders can rely on in disaster situations. 5. Resilience.

b) Part II: Word formation 1
1/a Professionalism; 2/b Globalism; 3/e Enforcement; 4/d Expert; 5/a Crime; 6/f Equipment; 7/g Width.

c) Part III: Word formation 2
1/a Leading; 2/b Threatening; 3/c Environmental; 4/d Aware; 5/e Coordinated; 6/f Able; 7/g Expansive; 8/h Fraudulent.

d) Part IV: Definitions
1. syndicate; 2. darknet; 3. dedicated legislation; 4. expertise; 5. perpetrator; 6. Internet of Things or IoTs.

Exercise III

a) Part I: Press release
(a) was dismantled; (b) have been filed; (c) use; (d) can accomplish; (e) represented; (f) have dismantled; (g) was believed; (h) should not have; (i) convened; (j) becoming; (k) were allegedly vetted; (l) is taking; (m) announced; (n) comprising.

b) Part II: Listening
(A) effort; (B) forum; (C) password ; (D) agenda; (E) meeting place; (F) malware; (G) software ; (H) operation; (I) criminals; (J) charges; (K) patience; (L) technologies.

Exercise IV

Part I: T/F

a) Connor sent explicit pictures of himself to the victim. **(?; it is said that she sent pictures of herself to him, but the reverse is not mentioned**).

b) Connor persuaded the victim to let him store the naked pictures that she sent him **(F; it was done without her consent)**

c) Connor said that, if the victim did not accept his sexual demands, he would use the Internet to defame her. **(T: he said he would send the photograph to her Twitter followers)**

d) Connor used technological means to hide his telephone number when making the threats. (T; he used spoofing apps)

e) The victim reported Connor's final threats, but not the previous harassment, which was exposed later. (**F: "she reported the threats and prior pattern of harassment to law enforcement authorities")**

f) After pleading guilty, Connor is likely to serve a seven-year prison sentence. **(F: "Actual sentences for federal crimes are typically less than the maximum penalties.")**

Part II: Vocabulary

a) sextortion; b) cyberstalking; c) spoofing; d) extortion; e) supervised release; f) Sentencing Guidelines

Part III: Synonyms

a) Connor <u>kept</u> many of these images without her consent. (*preserved*)

b) if she did not send <u>more</u> naked pictures and engage in sexually explicit video chats with him (*additional*)

c) <u>Real</u> sentences for federal crimes are typically less than the maximum penalties. (*actual*)

d) Connor frequently <u>used</u> a telephone and text message spoofing, or anonymizing, application (*employed*)

e) The victim reported the threats and <u>previous</u> pattern of harassment to law enforcement authorities. (*prior*)

Exercise V

a) Part I: grammar (verbs)

(A) has caused; (B) was originally distributed; (C) is opened; (D) deletes; (E) is directed; (F) managed; (G) has continued; (H) is being charged; (I) has been completely rewritten; (J) warn; (K) be regarded; (L) scrutinised

b) Part II: vocabulary and reading for detail

multiple choice questions

1. A; 2. B; 3. C; 4. C; 5. B; 6. C; 7. A; 8. C; 9. B; 10. C.

short answer questions

1. the name of the password collection software used in the file….; 2. Barok is popular password-stealing software and "spyder" is the name used by the hacker who created it; 3. Because they thought that the clues were so numerous that they could have been left deliberately as false tips, to throw investigators off track; 4. Outside his home in in the Bagong Barangay suburb of Manila; 5. In a bank; 6. Police said they did not have enough evidence to hold him; 7. They examined chat room logs containing incriminating references to hacking and the creation of viruses, which were traced back to an email account said to belong to either Ramones or de Guzman (his girlfriend); 8. eight; 9. to instigate new police powers and more intrusive forms of control over the Internet; by the massive police operation under way in the Philippines and the sensationalised media coverage it is receiving.

Exercise VI

a) Part I: True or False
1) T; 2) T; 3) F; 4) F; 5) T; 6) T; 7) F.

b) Part II: Definitions
1) CLOSURE; 2) TO ENTICE; 3) VOYERISM; 4) TO PREY ON SOMEONE; 5) INDELIBLE DAMAGE; 6) TO ESCALATE

c) Part III: Synonyms
1. An ex; 2. making the person responsible for his/her actions; 3. evil; 4. sending fraudulent e-mails to legitimate accounts to obtain valuable data from account owners' so as to commit criminal offences without their knowledge; 5. person committed to serving others.

GLOSSARY

Here is a list of some of the most important terms in the field of cybercrime. Some of the terms already dealt with in the exercises for each unit have been excluded from this list so as not to duplicate entries.

For each term, the Standard British English pronunciation definition and an example of usage are provided, as well as, where applicable, the sources of such definitions and examples.[35]

0-day (zero-day) attack (ˈzɪərəʊ ˈdeɪ əˈtæk)

an attack which exploits a previously unknown vulnerability in software. (2015 NTT Group Global Threat Intelligence Report)

Example: *DEATH by PowerPoint: Microsoft warns of 0-day attack hidden in slides.* (http://www.theregister.co.uk/2014/10/22/powerpoint_attacks_exploit_ms_0day/)

adware (ˈæd,wɛə)

[type of software that] collects information about an Internet user in order to display advertisements in the user's Web browser based upon information it collects from the user's browsing patterns. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *According to the plea agreement, MAXWELL and two unnamed co-conspirators created the botnet to fraudulently obtain commission income from installing adware on computers without the owners' permission.* (https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/maxwellPlea.htm)

APT (Advanced Persistent Threat) (ædˈvɑːnst pəˈsɪstənt ˈθrɛt)

An attacker with long-term goals who is highly skilled and well-funded, generally by a government or by organized crime. An APT is usually a complex attack using multiple techniques for maximum benefit.
(2015 NTT Group Global Threat Intelligence Report)

Example: *The most challenging part of Advanced Persistent Threat Attacks is to exfiltrate the collected data because; this has to be transported out of the network in to the attacker's server.* (http://resources.infosecinstitute.com/advanced-persistent-threats-attack-and-defense/)

ATM (ˈeɪ ˈtiː ˈem)

Automatic Teller Machine.

Example: *Through the use of specially designed malware, attackers no longer need to use traditional safe cracking methods to empty an ATM's money safe.* (https://www.europol.europa.eu/latest_news/europol-and-trend-micro-release-comprehensive-overview-atm-malware-threat)

back door (ˈbækˈdɔː)

Secret (undocumented), hard-coded access codes or procedures for accessing information. Some back doors exist in commercially-provided software packages; e.g., consistent (canonical) passwords for third-party software accounts. Alternatively, back doors can be inserted into an existing program or system to provide unauthorized access later. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *In some cases, the victim learned that personal and financial information had also been removed from their computer via the back door.* (https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division)

bot (ˈbɒt)

[..] derived from the word "robot", [...] and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots have been created to perform tasks automatically on Internet Relay Chat ("IRC") servers. The term "bot" also refers to computers that have been infected with a program used to control or launch distributed denial of service attacks against other computers. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *On or about August 21, 2004, during a chat in IRC, ANCHETA told an unindicted co-conspirator using the nickname "o_2riginal" that he*

[35] Glossary by M. A. Campos Pardillos.

was hosting “around lOOk bots total,” that in a week and a half 1,000 of his bots scanned and infected another 10,000, and that his botnet would be bigger if he had not used some himself for “ddosing.” (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

botnet (ˈbɒtˌnɛt)
A network of computers infected with bots that are used to control or attack computer systems. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gaining unauthorized access to computers on the Internet, and infecting the computer with a particular bot program. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *Once he received payment, ANCHETA would set up or configure the purchased botnet for the purchaser, test the botnet with the purchaser in order to ensure that DDOS attacks or proxy spamming would be successfully carried out, or advise the purchaser about how to properly maintain, update, and strengthen the purchased botnet.* (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

botherder, bot herder (ˈbɒt ˌhɛrdər)
Individuals who operate SpyEye botnets through SpyEye C&C servers. (http://krebsonsecurity.com/wp-content/uploads/2014/01/Panin-Indictment.pdf

Example: *After confidential personal and financial information is obtained through a SpyEye botnet, it is available to the bot herder) to use or provide to other co-conspirators.* (http://krebsonsecurity.com/wp-content/uploads/2014/01/Panin-Indictment.pdf)

breach (ˈbriːtʃ)
A cyberattack in which an organization’s data has been stolen or made public through compromise of networks or systems. (2015 NTT Group Global Threat Intelligence Report)

Example: *Former home office minister Hazel Blears said the TalkTalk data breach was “a wake-up call”. She said it should prompt a debate about whether further regulation was needed “because this is probably the biggest threat to our* economy”. (http://www.bbc.com/news/uk-34622754)

brute force (attack) (ˈbruːt ˈfɔːs ˈəˈtæk)
Process whereby an attacker tries many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. (https://en.wikipedia.org/wiki/Brute-force_attack

Example: *On Tuesday, we reported that cybercriminals had launched a brute force attack against GitHub accounts. Users reported seeing failed login attempts coming from China, Venezuela, Indonesia, Ecuador and other countries.* (http://news.softpedia.com/news/GitHub-Accounts-with-Weak-Passwords-Hacked-40-000-IPs-Used-in-the-Attack-401823.shtml)

CERT (ˈsiːˈiː ˈɑː ˈti)
Computer Emergency Response Team. Expert groups that handle computer security incidents. Also called computer emergency readiness team and computer security incident response team (CSIRT). (https://en.wikipedia.org/wiki/Computer_emergency_response_team)

Example: *Apart from the national/governmental CERTs, private CERTs who lack a formal governmental mandate could also play a significant role in ensuring the correct functioning of key national communication networks.* (https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport)

clicker (ˈklɪkə)
Malicious code or exploits that redirect victim machines to specified web sites or other Internet resources. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *Clickers can be used for advertising purposes or to lead a victim computer to an infected resource where the machine will be attacked further by other malicious code.* (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

cloud computing (ˈklaʊd kəmˈpjuːtɪŋ)
A kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. (https://en.wikipedia.org/wiki/Cloud_computing

Example: *The main concern arising from the growing reliance on cloud computing is less the possible increase in cyber fraud or crime than the loss of control over individual identity and data.* (http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf)

CNP (transaction) (ˈsiːˈen ˈpiː trænˈzækʃən)

Card not present: payment card transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time that an order is given and payment effected, such as for mail-order transactions by mail or fax, or over the telephone or Internet. (https://en.wikipedia.org/wiki/Card_not_present_transaction)

Example: *In 2012, 60% of the total payment card fraud value occurred when the card was not present (CNP) at the transaction, which occurs predominantly online.* (https://www.europol.europa.eu/iocta/2014/chap-3-4-view1.html)

computer data (kəmˈpjuːtə ˈdeɪtə, also ˈdɑːtə)

Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. (CoE Convention on Cybercrime).

Example: *If only a minuscule fraction of offences involving computer data and systems can be prosecuted, victims have a very limited expectation of justice. This raises questions regarding the rule of law in cyberspace.* (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf)

computer system (kəmˈpjuːtə ˈsɪstəm)

Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. (CoE Conventions on Cybercrime, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

Example: *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.* (CoE Convention on Cybercrime)

cookie (ˈkʊkɪ)

Cookies are small files stored on a user's computer by the user's web browser. Upon a user's connection to a webmail server, the server can read the data in the cookie and obtain information about that specific user. (US v Dokuchaev et al.)

Example: *The cookie itself does not reveal any personal information about you, but it allows the website storing the cookie to link a particular action with a specific user.* (http://cybercrimenews.norton.com/nortonretail/feature/prevention/cookies_friend_or_foe/index.html)

cracking (ˈkrækɪŋ)

Gainingaccesstoasystembycrackingapassword (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Another method of cracking a password include combining letters, symbols or numbers to form the all possible combinations of a password and then trying them one by one to find the correct password.* (http://www.ijcaonline.org/research/volume127/number16/singh-2015-ijca-906706.pdf)

credit card fraud (ˈkrɛdɪt ˈkɑːd frˈɔːd)

Theft of goods or services using false or stolen credit card information. (http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Keyword_Index_and_Glossary_of_Core_Ideas)

Example: *IP addresses are also recorded in e-commerce type transactions to provide a point of reference in situations where credit card fraud has occurred.* (https://www.icewarp.eu/privacy/)

crimeware (ˈkraɪm,wɛə)

Software tools designed to aid criminals in perpetrating online crime. Refers only to programs not generally considered desirable or usable for ordinary tasks. (http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Keyword_Index_and_Glossary_of_Core_Ideas)

Example: *The increasing proportion of these attacks which relate to some form of hacking or malware can be attributed to the increasing availability of crimeware kits and hacking services available on the digital underground.* (https://www.europol.europa.eu/iocta/2014/chap-3-7-view1.html)

cryptocurrency (,krɪptəʊˈkʌrənsɪ)

Medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Bitcoin is one of the most famous ones. (https://en.wikipedia.org/wiki/Cryptocurrency)

Example: *It is difficult to evaluate the EC's plan, since at the moment it is extremely general and vague. However, very likely it will open the door for the introduction of cryptocurrencies to the EU payment services regulations.* (https://www.onelife.eu/zh/news/eu-proposal-cryptocurrencies)

cryptography (krɪpˈtɒgrəfɪ)

A method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. (http://searchsoftwarequality.techtarget.com/definition/cryptography)

Example: *ENISA started its efforts in the area of cryptography by identifying and analysing reference documents from EU member states where the cryptographic protective measures are identified and recommended.* (https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools)

CSRF attack (ʻsiː ʻes ʻɑːr ʻɛf əˈtæk)

Cross-site request forgery (or "sea-surf") attack. Malware from someone who appears to be a trusted user of a site. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.* (http://remote.eptron.eu/etms/docs/general/security.html)

cyberattack, cyber attack (ˈsaɪbərə,tæk)

An attempt by hackers to damage, disrupt or destroy a computer network system (2015 NTT Group Global Threat Intelligence Report)

Example: *During that time period, certain members of Anonymous have waged a deliberate campaign of online destruction, intimidation, and criminality, as part of which they have carried out cyber attacks against businesses and government entities in the United States and throughout the world.* (https://www.wired.com/images_blogs/threatlevel/2012/03/Ackroydet-al.-Indictment.pdf)

cyberbullying (saɪbəˈbʊlɪɪŋ)

Using the Internet, cell phones, video games, or other technology gadgets to send, text, or post images intended to hurt or embarrass another person. (https://nobullying.com/what-is-cyberbullying/)

Example: *If it is simple to read intentionality in the episodes of traditional bullying, in cyberbullying responsibility can be extended and shared to those who "simply" watch a video and decide to send it to others.* (http://www.bullyingandcyber.net/en/definitions/)

cyberstalking (ˈsaɪbəˌstɔːkɪŋ)

Crime of using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person. (http://legaldictionary.net/cyberstalking/)

Example: *A victim of cyberstalking can apply to the courts under the Protection from Harassment Act 1997 (PfHA) to obtain an immediate civil injunction restraining a stalker from continuing the offensive conduct online.* (http://www.stalkinghelpline.org/wpcms/wp-content/uploads/8005352_1-NSH-FAQ-Final-2.pdf)

dark web (ˈdɑːk ˈwɛb)

Private networks not accessible by the general public. These networks are often used for nefarious or illegal purposes. (2015 NTT Group Global Threat Intelligence Report)

Example: *A hacker is reportedly selling on the dark web copies of databases stolen from three unidentified U.S. healthcare organizations and one unnamed health insurer containing data on nearly 10 million individuals for prices ranging from about $96,000 to $490,000 in bitcoin for each database.* (http://www.databreachtoday.com/3-stolen-health-databases-reportedly-for-sale-on-dark-web-a-9227)

data diddling (ˈdeɪtə (ˈdɑ:tə) ˈdɪdlɪŋ)

Modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing book-keeping and audit regulations. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Data diddling […] involves altering raw data just before a computer processes it and then changing it back after the processing is completed.* (http://www.crime-research.org/articles/Dubey/)

data leakage (ˈdeɪtə (ˈdɑ:tə)ˈliːkɪdʒ)

Uncontrolled, unauthorized transmission of classified information from a data centre or computer system to the outside. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *For the first time this European Fraud Update also includes information on Payment Fraud, with nine countries reporting related issues. Three of them reported data leakage from hotel booking sites and one country reported contactless card fraud.* (https://www.european-atm-security.eu/tag/payment-fraud/)

data mining (ˈdeɪtə *also* ˈdɑ:təˈmaɪnɪŋ)

The process of extracting hidden information and correlations from one or more databases or collections of data that would not normally be revealed by a simple database query. (http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Keyword_Index_and_Glossary_of_Core_Ideas)

Example: *One example of data mining techniques used in the financial sector with the aim of detecting potential terrorists is the Investigative Data Warehouse (IDW) of the FBI.* (http://profiling-project.eu/wp-content/uploads/2013/10/PROFILINGproject_WS1_Fundamental_1110.pdf)

deep web (ˈdiːp ˈweb)
Any Internet information or data that is inaccessible by a search engine and includes all Web pages, websites, intranets, networks and online communities that are intentionally and/or unintentionally hidden, invisible or unreachable to search engine crawlers. Also known as hidden Web, Undernet, Deepnet or Invisible Web. (https://www.techopedia.com/definition/15653/deep-web)

Example: *On the deep web, drug sales can take place in a marketplace (such as Silk Road), within a decentralised network or between individuals*. (http://www.era-comm.eu/Drugs_Supply_Reduction/kiosk/pdf/315dt06_docu.pdf)

defacement (dɪˈfeɪsmənt)
A form of vandalism in which a website is marked by hackers or crackers who are trying to make their mark. […]The usual targets for defacement are government organizations and religious websites. (https://www.techopedia.com/definition/4870/defacement)

Example: *Among other things, MARTYN and O'CEARRBHAIL accessed without authorization computer servers in Arizona used by Fine Gael to maintain its website, and uploaded code that defaced the website.* (https://www.wired.com/images_blogs/threatlevel/2012/03/Ackroydet-al.-Indictment.pdf)

denial of service (dɪˈnaɪəl əv ʻsɜːvɪs)
An incident in which a user or organization is deprived of the services of a resource they would normally expect to have. (http://searchsoftwarequality.techtarget.com/definition/denial-of-service)

Example: *But the minister responsible for the census, Michael McCormack, dismissed privacy concerns and insisted the website was not "attacked", despite confirming the site was shut down after repeated denial of service attempts.* (http://www.starwoodnews.cf/census-site-down)

DoS attack (ˈdiːˈəʊ ˈɛs əˈtæk)
Overwhelming or saturating resources on a target system to cause a reduction of availability to legitimate users. On the Internet, it usually involves spoofingpackets or e-mail headers. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *The DoS attacks (Denial of Service) are different than the previous (IP spoofing, ...) as the goal is no longer to gain access to a network, but rather to render a service (www, ftp, email, ...) offered by a car unavailable to users, using different techniques*. (https://macronetwork.eu/knowledgebase.php?action=displayarticle&id=85&language=english)

DDoS attack (ˈdiːˈdiːˈəʊ ˈɛs əˈtæk)
A type of malicious computer activity where an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function and legitimate users are denied the services of the computer.* (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

domain hijacking (dəˈmeɪn ˈhaɪdʒækɪŋ)
Act of changing the registration of a domain name without the permission of its original registrant. (https://en.wikipedia.org/wiki/Domain_hijacking)

Example: *This will help prevent domain hijacking which happens when a domain registrar is hacked and the ip addresses changed to point to another server.* (http://www.ippatrol.eu/blog2011.html)

domain name system (DNS) (dəˈmeɪn ˈneɪm ˈsɪstəm)
System for naming computers and hierarchical system of names, standards, and servers that organizes the internet as an aggregate of domains, and enables the translation of domain names into their unique four-part Internet Protocol (IP) addresses. (http://www.businessdictionary.com/definition/domain-name-system-DNS.html)

Example: *The Infoblox DNS Threat Index is an indicator of malicious infrastructure-building ac-*

tivity worldwide that exploits the Domain Name System (DNS). (https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-whitepaper-dns-threat-index-q1-2016-report_0.pdf)

dox (dɒks)

Publicly disclosing online a victim's personal identifying information, such as the victim's name, address, Social Security number, email account, and telephone number, with the object of, among other things, intimidating the victim and subjecting the victim to harassment. (US v Ackroyd et al, https://freanons.org/wp-content/uploads/court-documents/Ryan-Ackroyd.pdf)

Example: *[The] coconspirators used information gained from those stolen emails to access, without authorization, and steal the contents of an email account belonging to a senior executive of HBGary, Inc. (the "HBGary, Inc. Executive"); […]; and dox the HBGary Federal Executive by, among other things, posting his Social Security number and home address on his Twitter account without his authorization or approval.* (US v Ackroyd et al).

DNS (ˈdiːˈen ˈes)

See **domain name system**.

Example: *Cybercriminals are increasingly using false DNS servers to intercept legitimate Web addresses and redirect users to fake sites in order to capture personal information or install malware.* (http://www.computerweekly.com/tip/DNS-server-security-Finding-and-using-DNSSEC-tutorial-resources)

dumpster diving (ˈdʌmpstə ˈdaɪvɪŋ)

A method of obtaining proprietary, confidential or useful information by searching through trash discarded by a target. (http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas#Keyword_Index_and_Glossary_of_Core_Ideas)

Example: *Dumpster diving may provide them with even more sensitive information such as usernames, passwords, credit card statements, bank statements, ATM slips, social security numbers, telephone numbers, etc.* (http://blog.globalknowledge.com/technology/security/hacking-cybercrime/the-5-phases-every-hacker-must-follow/)

electronic funds transfer fraud (ɪlɛkˈtrɒnɪk ˈfʌndz ˈtrænsfə ˈfrɔːd)

Crime related to the transfer of funds over the Internet, by diverting funds, stealing financial information, etc. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Another sophisticated electronic funds transfer fraud is a "man in the middle" (MITM) attack. […] Posing as a trusted vendor, the cyber-criminals send a request for payment, instructing the company to wire the money to a bank account that appears to be legitimate but is really under the criminals' control.* (https://www.cnb.com/fraud/ach-wire.asp)

encryption (ɪnˈkrɪpʃən)

Scrambling sensitive information so that it becomes unreadable to everyone except the intended recipient. (http://www.businessdictionary.com/definition/encryption.html#ixzz4Gk3nm2sY)

Example: *However, striking the right balance in cyberspace has become particularly challenging due to the ever increasing use of encryption and online anonymity tooling.* (https://www.europol.europa.eu/content/privacy-digital-age-encryption-anonymity-online)

exchangeable image file format (EXIF) (ɪksˈtʃeɪndʒəbl ˈɪmɪdʒ ˈfaɪl ˈfɔːmæt)

A variation of JPEG, used by almost all digital cameras to record extra interchange information to image files as they are taken.(http://graphicssoft.about.com/od/exifinformation/)

Example: *Government expert witnesses testified that they had examined the "metadata" or "EXIF" data, which is information about a picture that is embedded in the picture such as the date and time the photo was taken, from Mr. Gutierrez's electronic devices to determine the dates and times the photographs were taken.* (http://cases.justia.com/federal/appellate-courts/ca10/14-2129/14-2129-2015-09-14.pdf?ts=1442246454)

exploit (ˈɛksplɔɪt)

Computer code written to take advantage of a vulnerability or security weakness in a computer system or software. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *If attackers have control of your Internet connection, they have the ability to insert exploits into any website you visit.* (https://securityevaluators.com/knowledge/case_studies/iphone/)

extension (ɪkˈstɛnʃən)

An identifier specified as a suffix to the name of a computer file. The extension indicates a characteristic of the file contents or its intended use. A file extension is typically delimited from the filename with a full stop (period). (https://en.wikipedia.org/wiki/Filename_extension)

Example: *If child pornographic photographs were taken by the user himself, the exif data of the photographs may shed light on the tools and locations for taking those photographs.* (Information Resources Management Association (2011) *Cyber Crime: Concepts, Methodologies, Tools and Applications*. Gale Virtual Reference Library.)

firewall (ˈfaɪəwɔːl)

Software or hardware designed to control incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed, based on a predetermined rule set. (2015 NTT Group Global Threat Intelligence Report)

Example: *Personal firewalls should be installed on each computer that is connected to the internet and monitors (and blocks, where necessary) internet traffic. They are also sometimes known as 'software firewalls' or 'desktop firewalls'.* (https://www.getsafeonline.org/protecting-your-computer/firewalls/)

flash drive (ˈflæʃ ˈdraɪv)

See **USB stick.**

Example: *Ratigan was charged in May 2011 after police received a flash drive from his computer containing hundreds of images of children, most of them clothed, with the focus on their crotch areas.* (https://www.neweurope.eu/article/us-prosecutors-seek-50-year-sentence-priest-who-pleaded-guilty-child-porn-charges/)

grooming (ˈgruːmɪŋ; *also* ˈgrʊmɪŋ)

Building an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. (https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/)

Example: *The court ruled that the doctor could testify about "grooming," his opinion that Hofus was not a hebophile, and generally about fantasy-based communications.* (US v Hofus, http://cyb3rcrim3.blogspot.com.es/2010/03/fantasy-alone.html)

hacker (ˈhækə(r))

In computing, any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. (https://en.wikipedia.org/wiki/Hacker)

Example: *At certain times relevant to this Indictment, AMIN SHOKOHI, the defendant, was a computer hacker who worked for ITSec Team.* (US v Fathi et al)

hacktivism, hactivism (ˈhæktɪvɪzəm)

Politically- or ideologically-motivated vandalism. Defacing a Web site for no particular reason is vandalism; the same defacement to post political propaganda or to cause harm to an ideological opponent is hacktivism. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *The government sector has been targeted the most by hacktivism in 2016 by a large margin. The data breach of the Philippines Commission on Elections is by far the top trending hacktivism target.* (https://blog.surfwatchlabs.com/2016/05/26/anonymous-ops-trending-government-targeted-where-are-the-other-hacktivists/)

hashing (ˈhæʃɪŋ)

Generating a value or values from a string of text using a mathematical function. It is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. (https://www.techopedia.com/definition/14316/hashing)

Example: *The government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves.* (http://caselaw.findlaw.com/us-9th-circuit/1166919.html)

hoax email (ˈhəʊks ˈiːmeɪl)

Phoney email, usually an alert about a non-existent threat, that is passed throughout a system by a large number of individuals who believe it to be true – and that overwhelms the system as a result. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *A fisherman from Messolonghi, a car worker from Chania, a self-employed from Athens and two other unidentified persons are targeted by the cyber-crime police as the senders of the hoax e-mail claiming the collapse of the Greek economy*. (http://www.keeptalkinggreece.com/2011/03/17/five-targetted-by-cyber-police-on-hoax-e-mail-claiming-collapse-of-economy/)

honeypot (ˈhʌnɪ̡pɒt)

Decoy systems set up to gather information about an attack or attacker and to potentially deflect that attack from a corporate environment. (2015 NTT Group Global Threat Intelligence Report)

Example: *As soon as an attacker sends data to the honeypot, it issues an alert. The attacker will most likely start rummaging around, performing passive scans of hosts on the network. The beauty of a honeypot is, legitimate users know it is fake.* (http://www.americanbanker.com/news/bank-technology/deception-may-be-the-best-way-to-catch-cybercriminals-1076667-1.html)

hosting (ˈhəʊstɪŋ)

Using a remote hosting service provider to host websites, data, applications and/or services. Also also known as Web hosting. (https://www.techopedia.com/definition/9937/virtual-hosting)

Example: *Earlier this year, the FBI busted shady web-hosting company Freedom Hosting – known for turning a blind eye to child porn websites.* (https://www.newscientist.com/article/dn24345-silk-road-bust-hints-at-fbis-new-cybercrime-powers/)

identity theft (aɪˈdɛntɪtɪ ˈθɛft)

Creating a false identity using someone else's identifying information (e.g., name, Social Security Number, birthday) to create new credit cards or establish loans which then go into default and affect the original victim's credit record.
(http://www.mekabay.com/overviews/glossary.pdf)

Example: *Even people who don't use social networks at all can be affected by identity theft. Why? Cybercriminals create user profiles under their victims' names and find their way onto their friends' lists.* (http://newsroom.kaspersky.eu/pt/noticias/detalhe/article/security-guide-social-media-for-children-and-parents-3/?no_cache=1)

injection (ɪnˈdʒɛkʃən)

An attack performed by inserting malicious code or data into what the receiving system sees as a valid query. (2015 NTT Group Global Threat Intelligence Report)

Example: *Beginning on or about October 23, 2007, Company A was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.* (https://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf)

IP (ˈaɪ ˈpiː)

Intellectual property.

Example: *It is essential to deepen the understanding of how the online environment interacts with IP infringements. We noticed IPRs are systematically being misused as a way to disseminate malware, carry out illegal phishing and simple fraud to the detriment of consumers, businesses and the ordinary user of the internet.* (https://www.europol.europa.eu/content/launch-ipc3-europe%E2%80%99s-response-intellectual-property-crime)

IP address (ˈaɪ ˈpiː əˈdrɛs)

Internet Protocol Address. A unique numeric address used by computers on the Internet. An IP address is designated by a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *Interestingly, a pretty impressive 26% [of teenagers] knows how to hide their IP address.* (http://newsroom.kaspersky.eu/en/texts/detail/article/is-your-teenager-a-hacker/?no_cache=1&cHash=101e326a5cdaa60ec6086efd1b08193d)

IRC (Internet Relay Chat) (ˈaɪ ˈɑːˈsiː)

A network of computers connected through the Internet that allows users to communicate with others in real time text (known as "chat"). (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *IRC channels are also used to control botnets) that are used to launch DDOS attacks, send unsolicited commercial email, and generate advertising affiliate income.* (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

ISP (ˈaɪ ˈɛs ˈpiː)

Internet Service Provider.

Example: *If the ISPs exercise editorial control over messages posted on bulletin boards, use Board Leaders to enforce the content guidelines or provide them with an emergency delete function to control content there is great likelihood that they may end up being treated as a primary publisher.* (https://indiancaselaws.files.wordpress.com/2014/04/cyber-defamation-liabilities-of-internet-service-providers-isps-and-intermediary.pdf)

IT (ˈaɪ ˈtiː)

Information technology.

Example: *If members of management are found to be in breach of their duty to ensure appropriate IT security, they are personally at risk of claims for damages being brought against them by their employer.* (http://de.vgd.eu/en/news/in-practice-how-secure-is-you-it-system)

keylogger (kiːˈlɒgə)

A type of malicious software designed to monitor the keystrokes input into an infected computer and to transmit this data back to the hacker. (US v Ulbricht)

Example: *Backdoor Trojans typically come with a built-in keylogger; and the confidential data is relayed to a remote hacker to be used to make money illegally.* (http://newsroom.kaspersky.eu/fileadmin/user_upload/be/Downloads/PDFs/101920_Article_Security_ABC_for_Parents.pdf)

key logging (kiːˈlɒgɪŋ)

Recording the keystrokes made by an authorized user. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Imran Uddin used four key-logging devices on university computers to capture login details from staff members, including one who had access to the system which kept records of his grades*. (https://www.easterneye.eu/news/detail/scamming-student-jailed-for-altering-grades)

latency (ˈleɪtənsɪ)

Period during which a time bomb, logic bomb, virus or worm refrains from overt activity or damage (delivery of the payload). (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Long latency coupled with vigorous reproduction can result in severe consequences for infected or otherwise compromised systems.* (http://www.mekabay.com/overviews/glossary.pdf)

logic bomb (ˈlɒdʒɪk ˈbɒm)

Program in which damage (the payload) is delivered when a particular logical condition occurs; e.g., not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse; time bombs are a type of logic bomb. Most viruses are logic bombs. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Former UBS PaineWebber system administrator, Roger Duronio, has been charged with sabotaging company computer systems in an attempt to manipulate its stock price. Duronio placed logic bombs that deleted files on the computers.* (http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door)

mail-bombing (ˈmeɪl ˌbɒmɪŋ)

Sending large numbers of unwanted e-mail messages to a single recipient or to a group of such recipients. To be distinguished from spamming. Mail-bombing is a form of denial of service. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Spammers could become the victims of mail-bombing, as thousands of irate spam recipients strike back with messages of their own.* (https://www.surveysquare.com/acceptable-use-policy/)

malware (ˈmælˌwɛ(ə))

Computer code with malicious intentions. Malware includes Trojan horses, ransomware, rootkits, scareware, spyware, viruses and worms (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Malware may be created for the purpose of a range of criminal activities, such as: Data theft; obtaining personal information from a victim; disruption or monitoring of a system; to take control of a device for a criminal purpose such as ransomware or creating a botnet*. (http://www.interpol.int/Crime-areas/Cybercrime/The-threats/Malware,-bots,-botnets)

misinformation spread (ˌmɪsɪnʃəˈmeɪʃən ˈspred)

Using the Internet to circulate incorrect information and cause panic (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Misinformation of a different kind occurred in the United States during the December 2012 Newtown shootings and the April 2013 Boston bombings. In the Newtown case, online and mainstream media misidentified a Facebook page as that of the shooter.* (http://www.huffingtonpost.com/farida-vis/the-rapid-spread-of-misinformation-online_b_4665678.html)

moneymule (ˈmʌnɪ ˌmjuːl)

Individual who is used to transport or launder stolen money in furtherance of criminal activity and its related organizations. These individuals can be either wittingly or unwittingly participating in the fraud. (https://www.justice.gov/opa/press-release/file/956511/download)

Example: *A group of "money mules" who helped defraud Wonga of £3.8 million by having cash funnelled into their accounts have been jailed.* (http://www.standard.co.uk/news/crime/jailed-money-mules-who-helped-defraud-wonga-of-38m-a3170751.html)

NFC (ˈen ˈef ˈsi:)
Near Field Communication. A set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within about 4 cm (2 in) of each other. (https://en.wikipedia.org/wiki/Near_field_communication#Commerce)

Example: *One of the most pressing privacy issues with NFC is eavesdropping when a third party 'listens in' to transactions and copies data transmitted between phone and reader.* (http://www.assuringbusiness.com/knowledge_network/NFC_Implications_in_Mobile_Payments.html)

notice and takedown (ˈnəʊtɪs ən ˈteɪkdaʊn)
Process operated by online hosts in response to court orders or allegations that content is illegal. Content is removed by the host following notice. (https://en.wikipedia.org/wiki/Notice_and_take_down)

Example: *Essentially, so long as a service provider follows the DMCA's notice-and-takedown rules, it won't be liable for copyright infringement based on user-generated content.* (https://help.github.com/articles/dmca-takedown-policy/)

P2P (ˈpi: ˈtu: ˈpi:)
Peer to peer, person to person. A computing or networking distributed application architecture that partitions tasks or workloads among peers. (https://en.wikipedia.org/wiki/P2P)

Example: *Of P2P users arrested in 2009, 33 percent had photos of children age three or younger and 42 percent had images of children that showed sexual violence.* (http://www.huffingtonpost.com/mary-l-pulido-phd/child-pornography-basic-f_b_4094430.html)

payload (ˈpeɪ̯ləʊd)
Unauthorized activities of malicious software. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Attachments attempt to install their payload as soon as you open them. Your internal defenses may protect you, but don't count on it.* (https://cybercoyote.org/security/av-top.htm)

penetration (ˌpɛnɪˈtreɪʃən)
Unauthorized access to restricted systems or resources. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *For many computer virus writers and cybercriminals, the objective is to distribute their virus, worm or Trojan virus to as many computers or mobile phones as possible – so that they can maximise malware penetration.* (http://www.kaspersky.co.uk/internet-security-center/threats/malware-system-penetration)

pharming (ˈfɑmɪŋ)
Redirecting users from a legitimate site to a bogus one; information entered on the phoney site is captured for fraudulent purposes. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Pharming attacks target DNS servers or location IP resolution tables via malware to redirect unsuspecting users to a fake website. On the fraudulent site, the customer experience mimics that of the online bank, and users are prompted to enter their online banking credentials.* (https://securityintelligence.com/pharming-attacks-target-small-home-offices/)

phishing (ˈfɪʃɪŋ)
Directing users to a bogus site through an email that appears legitimate; information entered on the phony site is captured for fraudulent purposes. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *We caution consumers to be on the lookout for phishing scams in which various fraudulent emails, claiming to come from the bank, that ask you to click on links to update account or personal information. These are not legitimate emails from the bank; instead, they are fraudulent emails sent as part of a scam in which criminals try to trick people into divulging their confidential information.* (https://www.vistbank.com/security/online-scams/)

piggybacking (ˈpɪgɪ̯bækɪŋ)
Entering secure premises by following an authorized person through the security grid; also unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification). (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Furthermore, a network that is vulnerable to piggybacking for network access is equally vulnerable when the purpose is data theft,* *dissemination of viruses, or some other illicit activity.* (http://whatis.techtarget.com/definition/piggybacking)

POS (ˈpiː ˈəʊ ˈes)

Point of Sale. Time and place where a retail transaction is completed. Acronym for point of sale. (https://en.wikipedia.org/wiki/Point_of_sale)

Example: *POS malware aims to scrape the RAM memory of POS terminals in order to steal credit and debit card data. It is particularly attractive for cybercriminals because rewards can be lucrative and they do not need to be physically present to execute an attack.* (https://securityintelligence.com/pos-malware-and-loyalty-card-fraud-growing-in-popularity/)

proxy server (ˈprɒksɪ ˈsɜːvə)

A server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. (https://en.wikipedia.org/wiki/Proxy_server)

Example: *Using a proxy server anyone can bounce their activity off a system that is either in a far distant country, or keeps no records of where the activity originated, or worse still, both.* (http://www.bbc.com/news/technology-17302656)

ransomware (ˈrænsəm,wɛə)

A type of malicious software designed to block access to a computer system until a sum of money is paid. (http://www.oxforddictionaries.com/definition/english/ransomware)

Example: *The United Kingdom Police Ransomware is a computer infection targeted at people who live in the United Kingdom and does not allow you to access your Windows desktop, applications, or files until you pay a ransom.* (http://www.bleepingcomputer.com/virus-removal/remove-united-kingdom-police-virus)

RAT (ʻɑːr ʻeɪ ʻti)

See **remote administration tool.**

Example: *RATs have been used by nation states and hacktivists for many years, but only recently 12 have we seen this remote access attack vector migrate to online banking fraud, where the main use is to neutralize all device-related defenses such as device recognition, IP geo-location, and proxy detection.* (http://informationsecurity.report/Resources/Whitepapers/bbb3b0fb-9ba1-4602-8cec-17dcb2381892_detecting-remote-access-attacks-on-online-banking-sites-pdf-7-w-1088.pdf)

remote administration tool (RAT) (rɪˈməʊt ədˌmɪnɪˈstreɪʃən ˈtuːl)

A piece of software that allows a remote "operator" to control a system as if he has physical access to that system. While desktop sharing and remote administration have many legal uses, "RAT" software is usually associated with criminal or malicious activity. (https://en.wikipedia.org/wiki/Remote_administration_software)

Example: *The art of hacking has become extremely simple in the last couple of years. In the past 10 years, hundreds of new remote administration tool builders were released to the public.* (http://www.redsocks.nl/blog-2/cybercriminals-use-these-weak-passwords-to-ex-filtrate-stolen-data/)

responsible disclosure (rɪˈspɒnsəbəl dɪsˈkləʊʒə)

A vulnerability disclosure model. It is like full disclosure, with the addition that all stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details (https://en.wikipedia.org/wiki/Responsible_disclosure)

Example: *Implementing a responsible disclosure policy will lead to a higher level of security awareness for your team. Bringing the conversation of "what if" to your team will raise security awareness and help minimize the occurrence of an attack.* (https://bugcrowd.com/resources/what-is-responsible-disclosure)

rogueware (ˈrəʊg,wɛə)

A standalone malware computer program that pretends to be a well-known program or a non-malicious one [antivirus] in order to steal money and/or confidential data (http://www.collinsdictionary.com/submission/13869/Rogueware)

Example: *Rogueware fake antivirus strains are increasing at a stunning rate. Panda Security reports that this cyber crime bilks users out of about $34 million every month.* (http://searchsecurity.techtarget.com/news/1363031/Panda-reports-fast-spreading-rogueware-antivirus-fraud-rakes-in-millions)

rootkit (ˈruːṭkɪt)

A set of programs used to gain unauthorized access to a computer's operating system, esp. in order to destroy or alter files, attack other computers, etc. (http://www.wordreference.com/definition/rootkit)

Example: *Rootkits have been used increasingly as a form of stealth to hide Trojan virus activ-*

ity. When installed on a computer, rootkits are invisible to the user and also take steps to avoid being detected by security software. (http://www.kaspersky.com/internet-security-center/internet-safety/faq)

router (ˈruːtə; *US* ˈraʊtə)

Device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded (http://searchnetworking.techtarget.com/definition/router)

Example: *Maitland explained to them that as an officer who worked in child protection he used such software some time ago but not recently. He also offered the explanation that he had had issues with his broadband router. He was duly arrested on the suspicion of having downloaded indecent images of children.* (http://www.mirror.co.uk/news/uk-news/child-abuse-detective-who-wanted-7964107)

sabotage (ˈsæbəˌtɑʒ)

Deliberate damage to operations or equipment (http://www.mekabay.com/overviews/glossary.pdf)

Example: *In some countries, computer sabotage may be regarded as a breach of civil law rather then criminal law, but there are laws clearly defining cyber-crime as a criminal offense.* (http://definitions.uslegal.com/s/sabotage/)

salami (slicing) attack (səˈlɑmɪ ˈslaɪsɪŋ əˈtæk)

Making small, undetectable changes over an extended period of time; "penny shaving" is a type of salami attack. Also called salami slicing attack (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *A typical salami attack would add a small amount to a debit that the account holder would not check, such as a debit that represented a service charge. This small increase in debit (often a few pence or a few cents) would then be credited to the perpetrator's bank account.* (http://cybercrimeandforensic.blogspot.com.es/2009/11/salami-attacks.html)

scareware (ˈskɛəˌwɛə)

Malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection: (http://www.oxforddictionaries.com/definition/english/scareware)

Example: *A Swedish credit card payment processor was sentenced today to 48 months in prison for his role in an international cyber crime ring that netted $71 million by infecting victims' computers with scareware and selling rogue antivirus software that was supposed to secure victims' computers but was, in fact, useless.* (https://archives.fbi.gov/archives/seattle/press-releases/2012/payment-processor-for-scareware-cyber-crime-ring-sentenced-to-48-months-in-prison)

script kiddy (ˈskrɪpt ˈkɪdɪ)

A derogative term, originated by the more sophisticated crackers of computer security systems, for the more immature, but unfortunately often just as dangerous exploiter of security lapses on the Internet. (http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy)

Example: *Because of the many programs available on the internet that were developed by true hackers or crackers, script kiddies are able to easily create mischief, sometimes by simply entering an IP address and clicking a button.* (http://www.pctools.com/security-news/script-kiddie/)

server (ˈsɜːvə)

A centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *In preparing for a DDoS attack, the malicious actor typically compromises and gains remote control of computers and computer servers by placing malicious software, or malware, on them.* (https://www.justice.gov/opa/file/834996/download)

service provider (ʻsɜːvɪs prəˈvaɪdə)

Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; any other entity that processes or stores computer data on behalf of such communication service or users of such service. (CoE Convention on Cybercrime)

Example: *Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.* (CoE Conventions on Cybercrime, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

sexting (ˈsekstɪŋ)

The sending of sexually explicit photos, images, text messages, or e-mails by using a cell phone or other mobile device. (http://www.dictionary.com/browse/sexting)

Example: *Over the last year in the province of Ontario, five teens caught sexting (three in Norfolk County and three in the Woodstock area) have been charged with possessing and distributing child pornography.* (https://news.vice.com/article/canadas-new-cyberbullying-law-is-targeting-teen-sexting-gone-awry)

sextortion (seksˈtɔːʃən)

Blackmail in which sexual information or images are used to extort sexual favours and/or money from the victim. (http://www.interpol.int/es/Crime-areas/Cybercrime/Online-safety/Sextortion)

Example: *And the sentences meted out in sextortion cases in state courts seem inadequate both in purely punitive terms and, given the high rates of recidivism among sex offenders, in terms of public protection.* (https://www.brookings.edu/research/closing-the-sextortion-gap-a-legislative-proposal/)

shoulder surfing (ˈʃəʊldə ˈsɜːfɪŋ)

Using direct observation techniques, such as looking over someone’s shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data. (https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

Example: *Are you alert to criminals’ shoulder-surfing your PIN at a checkout?* (https://nationaldebtadvisors.co.za/cybercrime-how-secure-are-our-banks/)

skimming (ˈskɪmɪŋ)

Getting private information about somebody else’s credit card used in an otherwise normal transaction. The thief can procure a victim’s card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims’ card numbers. (https://en.wikipedia.org/wiki/Credit_card_fraud#Skimming)

Example: *Credit card skimming incidents can be difficult to detect. Since your credit card is never lost or stolen. The best way to detect a skimmed credit card is to watch your accounts frequently. Monitor your checking and credit card accounts online at least weekly and immediately report any suspicious activity.* (http://credit.about.com/od/privacyconcerns/a/credit-card-skimming.htm)

smishing (ˈsmɪʃɪŋ)

Phishing using text messages rather than emails (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Examples: *With this specific wave of smishing attacks, hackers fool customers into downloading their malware by posing as a legitimate, unrelated app. The malware then takes over a legitimate SMS communication between the customer and their bank to socially engineer the customer into giving away their PII information and access their account.* (http://www.scmagazineuk.com/natwest-online-banking-suffers-sms-smishing-scams/article/481378/)

social engineering (ˈsəʊʃəl ˌendʒɪˈnɪərɪŋ)

Psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional “con” in that it is often one of many steps in a more complex fraud scheme. (https://en.wikipedia.org/wiki/Social_engineering_(security)

Example: *Social engineering is becoming ever more targeted and personal, which is why it’s no surprise that the number of cases is on the rise. What’s worrying, however, is the complex nature of these scams and how they tap perfectly into feelings that make us panic - if we get an email purporting to come from someone we trust (such as our bank) about something that is emotive to us all (money) and then demand that we act urgently, it’s almost like the perfect storm.* (https://www.cityoflondon.police.uk/news-and-appeals/Pages/think-twice-before-act-phishing-scams.aspx)

spam (ˈspæm)

Unsolicited commercial email. “Spamming” refers to the mass or bulk distribution of unsolicited commercial email. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *Often spammers use computers infected with malicious code and made vulnerable to subsequent unauthorized access by routing spam through the victim computer in order to mask their originating email and IP address information. In this way, the infected computer serves as a “proxy” for the true spammer.* (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

spear-phishing (ˈspɪə ˈfɪʃɪŋ)

A highly targeted phishing attack, using knowledge about a specific person or organization. (2015 NTT Group Global Threat Intelligence Report)

Example: *However, in recent years cybercriminals have upped their phishing game with more sophistication. Spear phishing emails are crafted in order to make someone believe they're from a legitimate source. The messages might appear to come from banks or businesses, and could include full names, usernames, and other personal info.* (https://blog.malwarebytes.com/101/2016/01/hacking-your-head-how-cybercriminals-use-social-engineering/)

spoofing (ˈspuːfɪŋ)

A fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. (https://www.techopedia.com/definition/5398/spoofing)

Example: *Phishing is basically tricking someone to give up sensitive information – usually social and bank account credentials and credit card details. Spoofing, on the other hand, refers to how cybercrooks actually trick their target – by posing as a well-known, trustworthy entity. So, more often than not, phishers rely on spoofing in order for their phishing scams to be successful.* (http://www.bullguard.com/bullguard-security-center/internet-security/internet-threats/spoofing-recurring-internet-security-threat.aspx)

spyware (ˈspaɪ̯wɛə)

Except as provided in Subsection 7)(b), "spyware" means software on the computer of a user who resides in this state that: (i) collects information about an Internet website at the time the Internet website is being viewed in this state, unless the Internet website is the Internet website of the person who provides the software; and (ii) uses the information described in Subsection (7)(a)(i) contemporaneously to display pop-up advertising on the computer (https://le.utah.gov/~2005/bills/static/HB0104.html)

Example: *The implementation and enforcement of the provisions of this Directive often require cooperation between the national regulatory authorities of two or more Member States, for example in combating cross-border spam and spyware.* (Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009)

synflood (ˈsɪn,flʌd)

A type of DDOS attack where a computer or network of computers send a large number of "syn" data packets to a targeted computer. Syn packets are sent by a computer that is requesting a connection with a destination computer. A synflood typically involves thousands of compromised computers in a botnet that flood a computer system on the Internet with "syn" packets containing false source information. The flood of syn packets causes the victimized computer to use all of its resources to respond to the requests and renders it unable to handle legitimate traffic. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *On or about July 24, 2004, during a chat in IRC, zxpL again asked ANCHETA to conduct a synflood DDOS attack, this time against an IP address belonging to Sanyo Electric Software Co., Ltd. in Osaka, Japan, which zxpL identified for ANCHETA.* (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

temporary internet file (ˈtɛmpərərɪ ˈɪntəˌnɛt ˈfaɪl)

A file that is located on a computer's hard drive that a browser uses to store Web site data for every Web page or URL address that is visited. (http://www.webopedia.com/DidYouKnow/Internet/Temporary_Internet_Files.asp)

Example: *Under the "Jim" profile, there was a temporary internet file known as the Web "cache," an automatic storage mechanism designed to quickly display previously visited web pages.* (http://www.ediscoverylawalert.com/2010/11/articles/legal-decisions-court-rules/cached-web-files-may-serve-as-evidence-in-child-pornography-case/)

thumbnail (θʌmˌneɪl)

A miniature display of a page to be printed. Thumbnails enable you to see the layout of many pages on the screen at once (http://www.webopedia.com/TERM/T/thumbnail.html)

Example: *Special Agent Blackmore attempted to download these files, but was unsuccessful. (Id.). He did, however, capture of number of thumbnail images that depicted child pornography.* (https://www.gpo.gov/fdsys/pkg/USCOURTS-mnd-0_13-cr-00256/pdf/USCOURTS-mnd-0_13-cr-00256-0.pdf)

time bomb (ˈtaɪm ˌbɒm)

Program or batch file waits for a specific time before causing damage. Often used by disgruntled and dishonest employees who find out they're to be fired or by dishonest consultants who put unauthorized time-outs into their programs without notifying their clients. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Clayton did not pay its bill, and PSC, claiming the need to make program changes, went to Clayton's place of business and secretly installed a "time bomb" that at a pre-set time would lock the system so Clayton could not access its files.* (http://cyber.law.harvard.edu/property00/alternatives/roditti.html)

traffic data (ˈtræfɪk ˈdeɪtə, *also* ˈdɑ:tə)

Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service. (CoE Convention on Cybercrime)

Example: *The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system*.

(Article 33, CoE Conventions on Cybercrime, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

trojan (horse) (ˈtrəʊdʒən ˈhɔːs)

A malicious program that is disguised as a harmless application or is secretly integrated into legitimate software. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *Ukrainian experts in information security are sure that 95% of victims of the hacker group were wiretapped via a trojan on their phones*. (http://belsat.eu/en/news/banda-hakerau-tsikankurenty-kdb/)

unallocated cluster (ʌnˈæləˌkeɪtɪd ˈklʌstə)

Area on a hard drive where the data belonging to deleted files can be found. The data will remain there until it is overwritten by another file. (http://kb.digital-detective.net/display/HstEx3/File+System+Data+Recovery)

Example: *Using my forensic software I was able to locate 73 pictures files in the unallocated clusters which had been deleted and were no longer accessible to the camera user.* (http://www.mccannpjfiles.co.uk/PJ/VIDEO_MEMORY.htm)

URL (ˈju: ˈɑ:r ˈel, *also* ˈɜ:l)

Uniform Resource Locator. Unique address for a file that is accessible on the Internet. (http://searchnetworking.techtarget.com/definition/URL)

Example: *It is no secret that cyber criminals also use URL shorteners to aid them in achieving their objectives. URL shorteners are often used by cyber criminals to obfuscate redirects to malicious destinations*. (https://blog.malwarebytes.com/threat-analysis/2016/01/when-url-shorteners-and-ransomware-collide/)

USB stick (ˈju: ˈes ˈbi: ˈstɪk)

A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a keychain. Also called flash drive. (http://searchstorage.techtarget.com/definition/USB-drive)

Example: *In February 2012 he was arrested and confessed to using his work computer to download pictures of children, share them online, and discuss them with other adults. Officers found a total of 3,699 images and videos stored on his computer, a USB stick and a hard drive, including 295 of children being abused.* (http://www.oxfordmail.co.uk/news/10554932.Ex_Brookes_lecturer_guilty_over_child_abuse_pictures/?ref=nt)

vandalism (ˈvændəˌlɪzəm)

Obvious, unauthorized, malicious modification or destruction of data such as information on web sites. (http://www.mekabay.com/overviews/glossary.pdf)

Example: *Wikipedia bans editing of its pages by Congressional staffers after 'online vandalism. The internet encyclopaedia announces ban in response to "persistent disruptive editing" – such as describing Donald Rumsfeld as a "alien lizard" – by anonymous users in House of Representatives.* (http://www.telegraph.co.uk/technology/wikipedia/10992143/Wikipedia-bans-editing-of-its-pages-by-Congressional-staffers-after-online-vandalism.html)

virus (ˈvaɪrəs)

A program that replicates rapidly within a computer causing damage to the host computer (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Further problems arise with the mass victimization caused by offences such as virus propagation, because the numbers of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the offenders have been caught and punished.* (http://www.unodc.org/pdf/crime/10_commission/4e.pdf)

vishing (ˈvɪʃɪŋ)

(From "voice" + "phishing") tricking a user (through an email or phone call) into entering credit card information into a bogus voice response system; information entered into the phony system is captured for fraudulent purposes.
(http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *The vishing campaign was discovered by researchers from cybercrime intelligence firm PhishLabs while investigating a recent attack against customers of an unnamed midsize bank. The bank's customers had received text messages claiming their debit cards had been deactivated and instructing them to call a phone number.* (http://www.pcworld.com/article/2149840/voice-phishing-campaign-hits-customers-at-dozens-of-banks.html)

VoIP (ˈviː ˈəʊ ˈaɪ ˈpiː)

VoIP is short for Voice over Internet Protocol, a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls (http://www.webopedia.com/TERM/V/VoIP.html)

Example: *VoIP systems are being used to support vishing (telephone-based phishing) schemes, which are now growing in popularity.* (https://en.wikipedia.org/wiki/International_cybercrime)

vulnerability (vʌlnərəˈbɪlɪtɪ)

Weakness or flaw permitting an attack on a computer system or network. (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Cisco says there is no evidence that this vulnerability has been exploited in the wild, but users are advised to update their installations to protect themselves against potential attacks.* (http://www.securityweek.com/hackers-can-exploit-libreoffice-flaw-rtf-files)

watering hole (ˈwɔːtərɪŋ ˌhəʊl)

A computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. (https://en.wikipedia.org/wiki/Watering_Hole)

Example: *A Chinese attack group infected Forbes.com back in November in a watering hole attack targeting visitors working in the financial services and defense industries, according to two security companies.* (http://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms)

worm (wɜːm)

A program that replicates itself over a computer network and usually performs malicious actions, such as exhausting the computer's resources and possibly shutting the system down. Unlike a virus, a worm needs little or no human assistance to spread. (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *In October 2010, a worm based piece of computer malware was discovered across industrial sites in Iran, Indonesia and beyond. The worm targeted industrial control systems, based on legacy versions of Microsoft's Windows operating system.* (http://www.uinfc2.eu/wp/wp-content/uploads/2014/12/UINFC2_D1.1-Cybercrime_Threats_and_Patterns.pdf)

XSRF attack (ˈɛks ˈɛs ˈɑːr ˈɛf əˈtæk)

See **CRSF attack.**

Example: *Forced browsing is an XSRF attack in which a user is forced to browse a content without his/her knowledge.* (https://programmingmastercoding.blogspot.com.es/2011/05/forced-browsing-attack.html)

XXS attack (ˈɛks ˈɛks ˈɛs əˈtæk)

Cross-site scripting attack. Malware injected into a trusted site, presented through a hyperline (http://news.nicsa.org/2013/08/14/the-vocabulary-of-cyber-crime/)

Example: *Three websites of the Mexican chapter of Article 19, an international nonprofit organization focused on freedom of expression, were attacked over the course of three days via a Cross-Site Scripting (XXS) attack.* (https://freedomhouse.org/report/freedom-net/2015/mexico)

zombie (ˈzɒmbɪ)

(Also “drone”) Unsuspecting computers infected or compromised by a botnet, used to launch distributed denial of service attacks.) (http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf)

Example: *Zombie computers have been used extensively to send e-mail spam; as of 2005, an estimated 50–80% of all spam worldwide was sent by zombie computers.[1] This allows spammers to avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth.* (https://en.wikipedia.org/wiki/Zombie_(computer_science))

BIBLIOGRAPHY

Alcaraz, E. & B. Hughes (2002.), *Legal Translation Explained*. Manchester, St. Jerome..

Balteiro, I. and Campos, M.A. (2010), "A comparative study of Latinisms in court opinions in the United States and Spain". *International Journal of Speech, Language and the Law*, 17, 1: 95-118.

Bajčić, M. (2017), *New Insights into the Semantics of Legal Concepts and the Legal Dictionary*. Amsterdam: John Benjamins.

Bhatia, V.K. (1983), *An Applied Discourse Analysis of English Legislative Writing*. Birmingham: The University of Aston Language Study Unit.

---- (1987), *Language of the Law*. *Language Teaching* 20, 227-234.

Bhatia, V.K. et al. (2008, eds.), *Legal Discourse across Cultures and Systems*. Hong Kong University Press.

Brody, S.L. et al. (2003), Legal Drafting. Boston: Little, Brown & Co.

Cao, D. (2007), *Translating law*. Clevedon: Multilingual Matters.

Campos, M.A. (2011), "False Anglicisms in Legal and Business English as a Lingua Franca (ELF): A Process of Back-borrowing", in I. Balteiro, (ed.) *New Approaches to English Lexicology and Lexicography*. Newcastle: Cambridge Scholars Publishing, 83-96. Also available at http://rua.ua.es/dspace/bitstream/10045/43975/1/Campos (2011) - False Anglicisms in Legal and Business ELF.pdf.

Campos, M.A. (2017), "'Liaison magistrates' and 'contact points' as a 'remedy' against 'high levels of mistrust': Metaphorical imagery in scholarly papers on EU judicial cooperation". Iberica, 34: 231-256. Available at http://www.aelfe.org/documents/34_10_IBERICA.pdf.

Crystal, D and D. Davy (1969), *Investigating English Style*. Indiana University Press.

Danet, B. (1980), "Language in the Legal Process". *Law and Society Review*, 14, 3, 445-564.

European Commission Directorate-General for Translation (2017). *English Style Guide. A handbook for authors and translators in the European Commission*. Eighth edition. Site: http://ec.europa.eu/info/sites/info/files/styleguide_english_dgt_en.pdf

Finnegan, E. (2012) "Discourses in the Language of the Law". In: J. P. Gee & M. Handford, (eds.) *The Routledge Handbook of Discourse Analysis*. London: Routledge, pp. 482-493.

Garner, B. (2001), *Legal Writing in Plain English*. University of Chicago Press.

Garner, B. A. & Black, H. C. (2004), *Black's Law Dictionary*. New York: West Group.

Gibbons, J. (1990, ed.), *Language and the Law*, London: Longman.

---- (2002), *Forensic Linguistics: An Introduction to Language in the Justice System*. Massachussetts: Blackwell Publishers.

Goźdź-Roszkowski, S. (2011), *Patterns of Linguistic Variation in American Legal English: A Corpus-Based Study.* Frankfurt am Main: Peter Lang.

Gubby, H. (2004), *English Legal Terminology*. Den Haag.

Gustafsson, M. (1975), *Some Syntactic Properties of English Law Language*. Publication 4, Turku: University of Turku.

Haigh, R. (2004/2009), *Legal English*. Routledge.

Krois-Lindner, A. (2006), *International Legal English*. Cambridge University Press.

Maher, C. (1996), *Language on Trial: The Plain English Guide to Legal Writing*. Robson Books.

Mattila, H.E.S. (2006), *Comparative Legal Linguistics*. Translated by Christopher Goddard. Hampshire: Ashgate.

Mazzi, D. (2007), *The Linguistic Study of Judicial Argumentation: Theoretical Perspectives, Analytical Insights*. Modena: Edizioni Il Fiorino.

Lee McGowan, L. & D. Phinnemore (2004), *A Dictionary of the European Union*. Europa Publications: London and New York.

McKay, W.R. and Charlton, H.E. (2005), *Legal English. How to Understand and Master the Language of the Law*. Pearson Education.

Mellinkoff, D. (1963) *The Language of the Law*. Boston, MA: Little, Brown.

Riley, A. (2005), *English for Law*. Longman Pearson Education.

Robertson, D. (2004), *A Dictionary of Human Rights*. London: Routledge.

Rossini, C. (1998), *English as a Legal Language*. Kluwer Law International.

Russell, F. and C. Locke (1995), *English Law and Language. An Introduction for Students of English*. Hemel Hempstead: Phoenix ELT.

Schauer, F. (2015), "Speaking of Language and Law: On the Relationship Between Legal and Ordinary Language". In: L. Solan, J. Ainsworth & R. W. Shuy, (eds.) *Conversations on the Work of Peter Tiersma*. Oxford: Oxford University Press, pp. 35-38.

Solan, L. M. (1993), *The Language of Judges*. Chicago: University of Chicago Press.

Solan, L. M. and P.M. Tiersma (2005), *Speaking of Crime: The Language of Criminal Justice*. Chicago: University of Chicago Press.

Stubbs, M. (1996), *Text and Corpus Analysis*. Oxford: Blackwell.

Tiersma, P. (1999), *Legal Language*. Chicago: University of Chicago Press.

Trebits, A. & M. Fischer (2010), *EU English. Using English in EU Contexts*. Kleltortlett.

Wagner, A. and S. Cacciaguidi-Fahy (2006, eds.), *Legal Language and the Search for Clarity*. Peter Lang.

Wodak, R. and G. Weiss (2005), "Analyzing European Union discourses: Theories and applications". In R. Wodak and P. Chilton (eds) *A New Agenda in (Critical) Discourse Analysis*. Amsterdam: Benjamins.

Wojcik, M.E. (2001/2009), *Introduction to Legal English: An Introduction to Legal Terminology, Reasoning and Writing in Plain English*. BNI Publications (Book Network International).