UNIVERSITEIT GENT

Faculteit Letteren & Wijsbegeerte

Anke De Prijck

The terminology of cybercrime. A contribution to the IATE-CvT project (English-Dutch-Spanish)

Volume I

Masterproef voorgedragen tot het behalen van de graad van

Master in het Vertalen

2015-2016

Promotor Prof. Dr. Joost Buysschaert
Vakgroep Vertalen Tolken Communicatie

ACKNOWLEDGMENTS

First of all, I would like to express my gratitude towards my supervisor Prof. Dr. Joost Buysschaert for his continuous guidance, support and advice.

I would also like to express my gratitude to Jeroen Aspeslagh and everyone at DGT, IATE and CvT for making this project possible.

Finally, I would like to thank my parents and my best friend, Esther Bels, for their constant support.

TABLE OF CONTENTS

Volume I

1 INTRODUCTION

1.1 IATE-CVT PROJECT

This dissertation is a contribution to the IATE-CvT project, which is a cooperation between CvT and the European Commission. As explained on the CvT website, "the aim of the IATE-CvT project is to contribute to specific domains of the EU's multilingual term base IATE on the basis of in-depth research into restricted sets of concepts."[1]

The project was created in 2010 and was originally only available for students of Ghent University. However, since 2015 it has been part of a larger project that involves several other Dutch and Flemish universities, as well as some institutional translation services. It is a possible theme for the dissertation of master students and can optionally be combined with a corresponding internship.

As one of the students who are contributing to the IATE-CvT project this academic year, I have done research on eleven concepts relating to cybercrime. This dissertation describes the justifications for the choices that were made to obtain the final results. It is hoped that those results will be entered in IATE after validation.

1.1.1 IATE

IATE[2] is short for InterActive Terminology for Europe and is the multilingual terminology database for all EU institutions. It was created in 1999, but did not immediately become operative. All former terminology databases of all EU institutions were merged into this one database. The aim of IATE is to share specific terminology in all EU languages to promote standardisation in the EU institutions.

There are two versions of the IATE website: a public and a private one. This means that not all information is available to the general public. However, the public version is still a very useful tool to search for a trustworthy technical translation. The private website has been in use since 2004, while the public interface was only released in 2007.

[1] http://www.cvt.ugent.be/iate-cvt.htm
[2] http://termcoord.eu/iate/about-iate/

IATE does not only suggest possible translations. If all information is available, it can also provide a definition, example contexts in which the term is used, remarks on spelling or usage etc. Each translation also has a rating to indicate the confidence level.

1.1.2 CvT

CvT[3] is the Terminology Centre of Ghent University and was founded within the Department of Translation, Interpreting and Communication. It uses GenTerm as a method to record and store terminographical data. All the data of a concept are gathered in one term record, which is in accordance with the principle of concept orientation (Chan, 2014, p. 654). This principle divides the term record in three different levels: an entry level, an index level and a term level. Concept orientation is part of the ISO standards for terminology and is also implemented in IATE.

The term record used for the IATE-CvT project is partly based on the GenTerm record, and partly on the IATE record. Some of the fields I had to fill in are not used for IATE, but only for GenTerm. Since the final results of the terms will not only be entered into the IATE term base, but also into the GenTerm term base, it was necessary to merge these two records and fill in all fields when possible.

1.2 TERMINOLOGY

Terminology is of paramount importance to the linguistic field. Protopopescu (2013) states that terminology developed out of the need to identify and name things. This is certainly true, and probably remains the main reason for creating new vocabulary. There is a basic need to name each concept that exists in every language.

Eugen Wüster is generally seen as the founder of a theory of terminology. In this context, Cabré (2003) comments that Wüster gave himself three tasks: developing standardised international principles to describe and record terms, formulating general principles of terminology and founding an international terminology centre (Infoterm). The first two goals are still relevant for the development of terminology today. However, creating consistencies and a sort of international standardization will never be fully possible. In certain domains the terminology is

[3] http://www.cvt.ugent.be/index.htm

so country-specific, that translating those terms into another language or even finding an equivalent can lead to serious problems. For example, in the domain of education there exist "inconsistencies in different texts of different levels" (Vandewaetere, 2014, p. 13).

It is also important to note that terminology does not represent general language, but evolves around specific jargon used in specific fields, such as the technical, medical or juridical field. In order to function in a certain type of field, it is necessary to understand the corresponding terminology.

1.3 TOPIC AND CONCEPTS

The concepts discussed in this dissertation are all related to cybercrime, a topic that is very relevant nowadays due to the continuous technological advances. After consulting Prof. Dr. Buysschaert, eleven concepts were chosen and discussed for three languages: English, Dutch and Spanish. The eleven terms are the following:

1. CCIRC
2. command-and-control centre
3. computer crime
4. Computer Security Incident Response Team (CSIRT)
5. hacktivism
6. hashing
7. zombie
8. DDoS attack
9. booter service
10. steganography
11. DKIM

Each of these concepts is thoroughly discussed in section 2. Furthermore, the records of these terms can be found in the appendix. To indicate the changes in the records, different colours were used. If the text is not highlighted, the information was already present in IATE and was not altered. If certain fields are yellow, it means that the information is new. For concepts that are completely new IATE entries, only the IATE number at the beginning of the record was put in yellow. This indication is clear enough to show that all the fields contain new

information. If fields are highlighted in green, the information was replaced, for example by a more recent source.

1.4 MOTIVATION

Storing terminological data is important to gain information and insight into a certain field. It facilitates the communication between specialists of the field and helps to make vocabulary more detailed instead of keeping terms vague.

This sort of research also helps to control the information explosion on the internet. Fields that are rapidly expanding create new terms on a regular basis and do not wait to use them until a valid translation is established. This can result in the co-existence of various terms for one concept, which makes it very hard to maintain a clear overview of the available information.

Cybercrime is a field that is largely and rapidly expanding in recent years due to the continuous technological advances. It is therefore important to keep storing and recording new concepts in order not to get lost in a sea of information. This dissertation's aim is to contribute to this aspect by collecting data for new terms or consolidating information of terms that are already present in IATE.

English is clearly the dominant language in the field of cybercrime. It can be said that all new concepts in this field emerge as English terms and are very often known under the same name in many other languages. In addition, Graddol (2006) claims that English has become a global lingua franca and is often seen as a basic skill instead of a foreign language. Consequently, people are no longer surprised to see an English term appear in the midst of another language. Other languages, including Dutch and Spanish, tend to stay behind. Due to the speed with which new terms occur, most languages simply copy the English term at first, and sometimes create an equivalent in their own language later on. In this context, this thesis will also try to determine whether there is domain loss for Dutch or Spanish in the area of cybercrime. (For the concept of domain loss, see Ferguson, 2007).

1.5 METHODOLOGY

The process implemented to determine the appropriate information for each term was always the same. Firstly, it was checked whether the term was already present in IATE. If this was the

case, then the research was based on the information that was already present. This information could give a clear overview of the number of synonyms or of the validity of the sources. If the term did not yield any results in IATE, I had to begin the research without any information as a starting point.

The next step was to search for an English definition that would fit the concept. Therefore, Google and Google Scholar were used to find appropriate websites that contained a definition. Sometimes, EUR-Lex[4] was also used, but most documents there were only relevant as contexts and did not contain definitions. Once I understood the concept completely, the different sources were compared and it was decided what the best definition was. In some cases different definitions were merged together to be complete, or a piece of information was left out when it was considered redundant.

Thirdly, possible synonyms were considered. Most of the time I had already discovered those while doing the initial research. However, it was always double-checked whether there existed more. This was done by simply typing synonyms "term X" for example, or by consulting additional websites related to the topic.

While the English information was being gathered, the commentary part was written and the IATE-CvT records were filled in. Every decision made was scientifically explained in the commentary part. However, most of the time filling in the records required much more time, since each synonym of a term needs a separate term level record. Finding adequate sources for the context field, where the term was clearly and comprehensively used in a sentence, was not always easy.

Once the English information had been dealt with, Dutch equivalents were considered. If IATE already suggested Dutch synonyms, those were consolidated and checked for validity. If not, EUR-Lex was always the first source to consult. Very often, a text in EUR-Lex is present in various EU languages. When a term was found in an English document, EUR-Lex's multilingual display was used to show the translation of the same text in the other languages, which makes it very easy to check which term is used in another language. Apart from EUR-Lex, traditional translation sources such as Van Dale, Linguee and Glosbe were also considered. When none of the sources mentioned above yielded results, I sometimes had to invent

[4] http://eur-lex.europa.eu/homepage.html

neologisms and try those in Google. As was the case for English, once the required information was gathered for Dutch, the commentary was written and the records were filled in.

Subsequently, the same process was repeated for Spanish. Very often there were clear similarities between the steps I had to take for all three languages.

2 DISCUSSION

2.1 CCIRC (ADP01)

CCIRC Canadian Cyber Incident Response Centre	CCIRC Canadian Cyber Incident Response Centre CCIRC Centro Canadiense de Respuesta a Incidentes Cibernéticos Canadian Cyber Incident Response Centre

The abbreviation *CCIRC* and its full term *Canadian Cyber Incident Response Centre* are not yet present in IATE and also did not render any results in EUR-Lex. This might be because it refers to a Canadian context and EUR-Lex focusses on texts from European contexts.

2.1.1 Definition of the English term

The abbreviation *CCIRC* has various meanings, but by combining *CCIRC* with the additional word “cyber” in a Google search, I found the official website on public safety in Canada, which defines *CCIRC* as follows:

> CCIRC helps ensure that many of the services which Canadians rely on daily are secure. It assists in securing the vital cyber systems of provinces, territories, municipalities and private sector organizations while collaborating closely with partners, including international counterparts and information technology vendors. (Canadian Cyber Incident Response Centre (CCIRC). Public Safety Canada[5].)

Cappa, M. & Donelson, P. (2012, p. 20) thereby add that the *CCIRC* only advises on possible solutions and exercises control of cyber threats. Based on these two sources, the following definition was created: "Canadian government institution that provides advice on cyber security and monitors cyber threats".

2.1.2 Dutch terms

I assumed I would not find many resources in other languages, since this term is very country-specific. There is a Wikipedia page about *CCIRC*, but it only exists in English.

In search of a Dutch translation, the English name was entered in Google and Google Scholar together with site:.be and site:.nl. However, most of the results still appeared in English. Furthermore, the numbers were never higher than 10 and are therefore too low to be considered reliable. Using Google's language filter, "CCIRC" yields 194 results on Dutch sites in Google, but many of those appear to be irrelevant. The full term "Canadian Cyber Incident Response Centre" only yields 45 results.

Accordingly, a Dutch translation for *CCIRC* was not found. I also googled for potential translations of the full term such as "Canadees Cyber Incident Response Centrum" or "Canadees Respons Centrum voor Cyberaanvallen", but all came up with very little to no results. The term is probably too country-specific to appear in a respectable number of Dutch texts and, as a consequence, it has to be concluded that no Dutch translation exists. The best solution, then, will be to keep the English term in Dutch texts. As Maxwell (2006) states, Dutch is a language which easily accepts English words and this is a case where this rule may be applied.

2.1.3 Spanish terms

In search of a Spanish translation I similarly entered the Centre's name in Google and Google Scholar, adding site:.es. Very few to no results were found. One of the (few) resulting hits also

[5] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

mentioned a Spanish equivalent for *CCIRC*, which I used for further research. Various possibilities exist, most of which are not used in governmental or scientific contexts.

	Google, Spanish sites
“Centro de Respuesta a Ciberincidentes de Canadá”	1
"Centro Canadiense de Respuesta a Incidentes Cibernéticos"	2
"Centro Canadiense de Respuesta de Incidentes Cibernéticos"	4
"Centro Canadiense de Respuesta a los Incidentes Cibernéticos"	7
"Centro Canadiense de Respuesta a Ciberincidentes"	77

To decide which one of these possibilities is the best translation, the difference between “Incidentes Cibernéticos” and “Ciberincidentes” was determined. Both are used in governmental contexts, but “Incidentes Cibernéticos” is often found in the phrase “Centro Nacional de Respuesta a Incidentes Cibernéticos”, a Mexican government agency (cf. http://seguridad2012.politicadigital.com.mx/pdf/03.pdf) while “Ciberincidentes” does not yield any results for “Centro Nacional de Respuesta a Ciberincidentes". It appears much more in the combination “Gestión de Ciberincidentes”, but even then, “Gestión de Incidentes Cibernéticos” is more frequent.

	Google, Spanish sites
"Centro Nacional de Respuesta a Incidentes Cibernéticos"	1,960
“Centro Nacional de respuesta a Ciberincidentes"	0
“Gestión de Ciberincidentes”	761
“Gestión de Incidentes Cibernéticos”	1,150

Furthermore, this research also confirmed that the preferred preposition is “a” and not “de” or “a los”, since “de” and “a los” yield very few to no results in combination with “Centro Nacional de Respuesta”. To keep the parallel, I would therefore opt for *Centro Canadiense de Respuesta a Incidentes Cibernéticos*, even though this phrase has the least results in Google.

The Canadian government’s term bank Termium has English, French and Spanish but it lists no Spanish equivalent of *Canadian Cyber Incident Response Centre*. It does list the official French translation: *Centre canadien de réponse aux incidents cybernétiques*, abbreviated as *CCRIC*, which slightly differs from the English abbreviation *CCIRC*[6]. The suggested Spanish translation is close to this French model and bears a strong analogy with the name of an existing Mexican counterpart.

It was also worth checking whether the English terms *CCIRC* and *Canadian Cyber Incident Response Centre* are used in Spanish texts. “CCIRC” yields 2,400 hits on Spanish sites in Google and 23 in Google Scholar. However, all 23 results in Google Scholar do not relate to the context of cybercrime and can therefore not be taken into account. Even so, the abbreviation *CCIRC* can be considered a valid synonym in Spanish. The full English term “Canadian Cyber Incident Response Centre” yields 367 results on Spanish sites in Google and 1 in Google Scholar. This is not much, but since the English abbreviation is also accepted, it can be seen as a valid equivalent. However, the Spanish translation should be promoted over this English term.

2.2 COMMAND-AND-CONTROL CENTRE (ADP02)

command-and-control server	commando- en controleserver
command-and-control centre	commando- en controlecentrum
C&C server	command-and-control server
C&C centre	command-and-control centre
	C&C-server
	centro de comando y control
	centro de mando y control
	servidor de comando y control
	servidor de mando y control
	servidor C&C

[6] http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=Canadian+Cyber+Incident+Response+Centre+&index=alt&codom2nd_wet=1

Command-and-control centre is not yet present in IATE, but it does yield some results in EUR-Lex.

2.2.1 Definition of the English term

In CELEX:52010PC0517 the concept is described as follows:

> The term 'botnet' indicates a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'. (EUR-Lex[7])

In addition, Stephen (2010) states that "the botnet's command-and-control center is used to send instructions to zombie computers, often over http or with more modern methods such as P2P and social networks".

In the latter source, *centre* has changed into *center*, due to American spelling. This spelling predictably yields a higher number of results on the internet, but as the term will be added to a European term base, I chose to keep the British spelling as the preferred one. A new definition was created based on the sources mentioned above: "computer that controls and sends instructions to zombies, for example to attack information systems".

Other collocations with *command-and-control* include *command-and-control server*, *command-and-control channel* and *command-and-control traffic*. Of these, *command-and-control server* may be regarded as a synonym of *command-and-control centre*, as it also refers to the computer that controls the compromised computers. Radware[8] defines *command-and-control servers* as "centralized machines that are able to send commands and receive outputs of machines part of a botnet", which is very similar to the definition of *command-and-control centre*.

To decide which one of the two terms is preferable, I compared their frequency in Google and Google Scholar, adding "malware" to the search entry to avoid results from a military context, although this risk is minimal in the case of the compound with *server*.

---

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1462823522784&uri=CELEX:52010PC0517
[8] https://security.radware.com/ddos-knowledge-center/DDoSPedia/command-and-control-server/

	Google, English sites	Google Scholar, English sites
"command-and-control centre" "malware"	3,060	57
"command-and-control server" "malware"	57,700	979
"command-and-control server"	87,900	1,080

Since *command-and-control server* has significantly more hits than *command-and-control centre*, it can be argued that *command-and-control server* is the preferred term.

Alternative spellings without the hyphens are regularly found on the internet. Since the compound expresses one idea, it is preferable to write it with the hyphens, though nowadays the spelling without the hyphens is not incorrect (cf. rule 1 in http://www.grammarbook.com/punctuation/hyphens.asp). For example, some documents in EUR-Lex write *command-and-control centre* with hyphens, others without. It is important, however, to be consistent within the same text.

Command-and-control is also very often abbreviated to *C&C*. The corresponding compounds *C&C server* and *C&C centre* both yield numerous results in Google. Accordingly, those terms should be considered additional synonyms.

2.2.2 Dutch terms

2.2.2.1 Equivalents for command-and-control centre, command-and-control server

In EUR-Lex, four out of the six available documents in Dutch translated *command-and-control centre* as *commando- en controlecentrum*. The original English term was copied in the other two Dutch sources and put between quotation marks. However, none of the documents that translated the term as *commando- en controlecentrum* are related to computer science, but to military contexts instead. To see whether these translations are also used outside military contexts, I googled them. Again, "malware" was added to the search entry.

Very few hits were found for both Dutch equivalents mentioned above. There are 9 Google results for "commando- en controlecentrum" "malware" (and a further 7 hits with the wrong spelling *commando en controle centrum*). 8 hits are found for "command-and-control centre"

"malware" used in Dutch sites and 125 for "command-and-control center" "malware", again in Dutch sites. To be sure the addition of "malware" was not the problem, I tried the search entries in combination with another noun, "botnet". However, this results in even fewer hits.

Even though *commando- en controlecentrum* is more common in military contexts (cf. 201 Google hits for "commando- en controlecentrum" +militair), it is likely also to be acceptable in computer science. In English, too, *command-and-control centre* is used in both contexts, and there was no need to create another term to distinguish the two meanings. Furthermore, it is a literal translation of the English term and probably easy to understand or look up for speakers of Dutch. Although the use of the English term in Dutch texts is more common, it is clear that a Dutchified version is also in use and should be promoted. Therefore, *commando- en controlecentrum* has been chosen as a valid translation and the preferred term, and *command-and-control centre* as an accepted synonym.

Since *command-and-control server* is a common synonym in English, it was worth checking if *commando- en controleserver* is a possible alternative in Dutch. This appears to be the case. Google gives 8 hits with the correct spelling in Dutch sites and a further 43 in which the spelling deviates from the norm (e.g. *commando en controle server*, *commando en controle-server*; though in 3 of these hits *commando en controle* is an expansion in brackets of C&C). Again, this makes the compound with *server* the more common one in comparison with the variant with *centrum*.

A further alternative is to use the English term *command-and-control server* in Dutch. This solution is found in CELEX:52011DC0225/NL and is also very common on the internet:

	Google, Dutch sites	Google scholar, Dutch sites
"command-and-control server" "malware"	846	7
"command-and-control server"	1,160	23

During the research I also came across *command en controlserver*, which is a mixture of English and Dutch. This yields 123 results in Google. However, it is not advisable to use such a hybrid term.

The conclusion at this point is that *commando- en controleserver* may be regarded as the preferred Dutch equivalent, with *commando- en controlecentrum* and the two English terms as synonyms.

2.2.2.2 The abbreviation C&C

The abbreviation *C&C* is also used in Dutch. According to the Dutch spelling rules, the corresponding compounds should be written with a hyphen: *C&C-centrum* and *C&C-server*. However, there were not enough results in Google to consider *C&C-centrum* an acceptable synonym, and the English *C&C centre* also appears not to be used in Dutch. *C&C-server*, on the other hand, results in 1,250 hits and could be used as a synonym. Considering the findings in the section above, this is a logical consequence. Amongst the results in Google, there are several sources in which *C&C-server* is written without a hyphen, but that is not the correct spelling (cf. rule 6.H in http://woordenlijst.org/leidraad/6/3).

2.2.3 Spanish terms

2.2.3.1 Equivalents for command-and-control centre, command-and-control server

Five documents in EUR-Lex were available in Spanish. Three of them translated *command-and-control centre* as *centro de mando y control*, while the other two used *centro de dirección y control*. Both options were compared in Google and Google Scholar.

	Google, Spanish sites	Google Scholar, Spanish sites
"centro de mando y control"	121,000	56
"centro de dirección y control"	7	13

From these results, it appears that only *centro de mando y control* should be seen as a valid synonym.

However, "mando" has numerous meanings in Spanish and might cause some confusion. *Centro de mando y control* is more common in military and national security contexts, even though it is acceptable to use it in relation to technology. In order to obtain results that are only

related to computer science, I googled “centro de mando y control” in combination with “ordenador” (Spanish for “computer”). This results in 53,400 hits in Google and 14 in Google Scholar.

In search of an alternative, I tried switching *mando* with *comando*, the literal Spanish translation for “command”, which is only used in contexts relating to computer science. Consequently, “centro de comando y control” yields 59,800 results in Google and 54 in Google Scholar, which is slightly more than *centro de mando y control. Centro de comando y control* is therefore the preferred term.

Since in the other two languages synonyms with *server* exist, I searched for a possible Spanish equivalent in CELEX:52011DC0225/ES, which suggests *servidor de mando y control*. This term yields 6,330 results in Google. However, keeping the previous section in mind, I also googled *servidor de comando y control*, which results in 6,420 hits. Both terms clearly appear less than their equivalents with *centro*, but could be considered valid synonyms.

2.2.3.3 The abbreviation C&C

The abbreviation *C&C* is also used in Spanish, but the word order is reversed, which means that the corresponding Spanish compounds are *servidor C&C* and *centro C&C*. *Centro C&C* + “ordenador” yields only 5 results in Google and 0 in Google Scholar, which makes it not an adequate synonym. *Servidor C&C*, on the other hand, did result in an acceptable number of hits: 1,710 in Google and 13 in Google Scholar.

2.3 COMPUTER CRIME (ADP03)

cyber crime	cybercriminaliteit
computer crime	computercriminaliteit
e-crime	digitale criminaliteit
digital crime	e-criminaliteit
high-tech crime	high-tech-criminaliteit
computer-related crime	computergerelateerde criminaliteit
	ciberdelincuencia
	delincuencia informática

	delincuencia de alta tecnología delincuencia digital delincuencia relacionada con los ordenadores
computer crime computer-related crime	computermisdrijf computerdelict computermisdaad computergerelateerd misdrijf computergerelateerd delict
	delito informático ciberdelito delito cibernético

There are two different IATE entries about *computer crime* (IATE895987 and IATE755117), which differ slightly in meaning. One considers *computer crime* in a very broad sense and is an uncountable noun, while the other narrows it down to crimes where the computer is the object of the violation and is thus countable. Both concepts will be discussed separately.

2.3.1 IATE895987

2.3.1.1 Definition of the English term

IATE895987, the broader concept, is defined as "offences against and by means of computers, including computer frauds, cyber-attacks, electronic payment frauds, online child pornography, and others". This definition seems to be correct, but the document on which it is based is no longer available. Therefore, I searched a similar report on the website of the Council of Europe on cybercrime[9] and found one easily. The definition remained the same, but is now based on a different and more recent source.

[9] http://www.coe.int/web/cybercrime/all-reports

A large number of synonyms for computer crime are enumerated in IATE: *e-crime, cybercrime, digital crime, computer crime* and *computer-related crime*. I googled the frequency of all of these terms in English pages.

	Google, English sites	Google Scholar, English sites
"e-crime"	263,000	3,440
"cybercrime"	7,080,000	29,400
"digital crime"	140,000	24,300
"computer crime"	505,000	30,300
"computer-related crime"	42,200	3,630

As can be seen, the synonyms do not appear in the correct order in IATE. *Cybercrime* is undeniably the preferred term, followed by *computer crime, e-crime, digital crime* and *computer-related crime*.

During the research I encountered another alternative, *high-tech crime.* This synonym was found in CELEX:52007DC0267. It yields 187,000 results in Google and 2,280 in Google Scholar. *High-technology crime*, without the abbreviation, results in fewer hits (28,900 in Google and 727 in Google Scholar), which shows that it is preferable to use the spelling with the abbreviation.

2.3.1.2 Dutch terms

The link to the current Dutch definition in IATE does no longer work. Therefore, it was replaced by a new one, based on the English definition: "misdrijf dat gepleegd wordt met behulp van of tegen computers, inclusief computerfraude, cyberaanvallen, kinderpornografie etc.".

IATE suggests three different synonyms: *cybercriminaliteit*, *computercriminaliteit* and *computergerelateerde criminaliteit*. These are correct terms, in accordance with the definition. However, since the English concept has more possible synonyms, I wanted to check whether there are other Dutch equivalents as well. *E-criminaliteit* yields 778 results in Google and 13 in Google Scholar. There are also two sources in EUR-Lex which use the term. Moreover, *digitale criminaliteit* yields one source in EUR-Lex and appears to be used frequently on the internet (cf. 5,050 results in Google and 24 in Google Scholar). Ultimately, *high-tech-criminaliteit* yields 9 hits in EUR-Lex, 613 in Google and 8 in Google Scholar. A further total of 420 results

in Google was found for wrong spellings such as *high-techcriminaliteit, high-tech criminaliteit* and *hightechcriminaliteit*. Given these results, *e-criminaliteit*, *digitale criminaliteit* and *high-tech-criminaliteit* could be considered acceptable synonyms for *cybercriminaliteit, computercriminaliteit* and *computergerelateerde criminaliteit*.

To determine the preferred term, the synonyms were compared in frequency.

	Google, Dutch sites	Google Scholar, Dutch sites
"cybercriminaliteit"	68,600	172
"computercriminaliteit"	42,200	383
"digitale criminaliteit"	5,050	24
"e-criminaliteit"	778	13
"high-tech-criminaliteit"	613	8
"computergerelateerde criminaliteit"	288	7

It is obvious that *cybercriminaliteit* and *computercriminaliteit* are the most common synonyms. The four other terms are correct, but do not nearly appear as much.

2.3.1.3 Spanish terms

The current definition in IATE is

> 1. Actividad delictiva realizada a través de Internet o utilizando medios tecnológicos. Abarca los siguientes tipos delictivos:
> i. Delitos contra la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos.
> ii. Delitos relacionados con la pornografía infantil.
> iii. Delitos de amenazas y contra el honor.
> iv. Defraudaciones en Internet y en el mercado de las telecomunicaciones.
> v. Delitos relativos a la propiedad intelectual e industrial en Internet.
> (computer crime, IATE[10])

In comparison to the definitions in English and Dutch, this one is more detailed and contains more examples. It would be better to only enumerate a few and add "etc.", so as not to exclude

10 http://iate.europa.eu/SearchByQuery.do?method=searchDetail&lilId=895987&langId=&query=computer%20crime&sourceLanguage=en&domain=0&matching=&start=0&next=1&targetLanguages=es&targetLanguages=nl

any possible cases. Furthermore, all this information could not be found in the enclosed reference. Based on the references of the definitions in the other languages, I changed the Spanish definition into “actividad delictiva realizada en contra de o a través de ordenadores, como por ejemplo la pornografía infantil, la defraudación, delitos de amenazas etc.”.

As was the case for the Dutch entry, there are three given translations: *ciberdelincuencia*, *delincuencia informática* and *delincuencia relacionada con los ordenadores*. These are plausible translations, but since there are more equivalents in English and Dutch, I wanted to verify if this was the case for Spanish as well.

E-delincuencia and *high-tech delincuencia* do not yield sufficient results. However, *delincuencia de alta tecnología*, which is the literal Spanish translation of *high-tech delincuencia*, did result in 4,520 hits in Google and 29 in Google Scholar. *Delincuencia digital* also yields enough results (cf. 1720 in Google and 9 in Google Scholar), albeit less than *delincuencia de alta tecnología*.

	Google, Spanish sites	Google Scholar, Spanish sites
“ciberdelincuencia”	245,000	562
“delincuencia informática”	26,300	664
“delincuencia de alta tecnología”	4,520	29
“delincuencia digital”	1,620	9
“delincuencia relacionada con los ordenadores”	455	4

2.3.2 IATE755117

2.3.2.1 Definition of the English term

IATE755117 is defined as an “illegal act in which a computer is the instrument or object of the crime”. It relates to a criminal offence and not the activity in general. This definition is correct and does not need to be altered.

There are two terms for this concept: *computer crime* and *computer-related crime*. Those are the only two that specifically involve using a computer. *Computer crime* is more common and therefore the preferred term.

2.3.2.2 Dutch terms

The Dutch definition for IATE755117 is "misdrijf met een computer als instrument of voorwerp", which is a literal translation of the English definition and therefore also correct. Likewise, there are two suggested terms that fit this definition: *computerdelict* and *computergerelateerd delict.* Interestingly, in Dutch the difference between the two meanings of *computer crime* is clearer, since another noun is used to translate "crime". Therefore, there is less possible confusion about the intended meaning in Dutch.

To achieve a reliable comparison, the terms in this meaning need to be compared as countable nouns to exclude the general meaning of *cybercrime*. Google yields only 263 results for "een computerdelict*"* and 1 result for "een computergerelateerd delict*"*. Due to that low number of results, I tried combining the first part of the compound with two Dutch synonyms of *delict: misdrijf* and *misdaad.* However, there is a difference in the legal vocabulary used in Belgium and the Netherlands, and consequently in when to use *misdrijf* or *misdaad*. More specifically, *misdaad* is not an official legal term in the Netherlands. Even so, Taaladvies[11] states that in non-specific, everyday language both terms can be used in both countries. The difference is that *misdrijf* is more formal than *misdaad.* Accordingly, "een computermisdaad" yields 72 hits in Google, while "een computermisdrijf" yields 214. Moreover, "een computergerelateerde misdaad" results in 0 hits, while "een computergerelateerd misdrijf" results in 8 hits.

Furthermore, Taaladvies states that *delict* is only used in the Netherlands, which might explain the low number of results. To corroborate that statement, I googled "een computerdelict" site:.be, which only yields 2 hits. "Een computerdelict" site:.nl yields 229 results. Therefore, it is probably safe to say that *computerdelict* is a typical term for the Netherlands, but not for Belgium.

At this point, the conclusion is that *computermisdrijf* is the preferred term, acceptable in both Dutch-speaking countries. *Computermisdaad* and *computergerelateerd misdrijf* are acceptable, but less used synonyms, and *computerdelict* and *computergerelateerd delict* are synonyms that are only used in the Netherlands.

[11] http://taaladvies.net/taal/advies/vraag/551/misdaden_misdrijven_tegen_de_mensheid_menselijkheid/

2.3.2.3 Spanish terms

IATE755117 suggests the following definition: “Delito cometido a través de los sistemas de información o contra estos”. However, there seems to be a problem with the use of “sistemas de información”, which means “information system”. In CELEX:32013L0040 the following definition of an information system can be found:

> a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance; (EUR-Lex[12])

This definition shows that *sistema de información* should not be used here. In accordance with the definitions in English and Dutch, it is better to change it to *ordenador* (“computer” in English). Furthermore, “o contra estos” (“or against them”) was left out, since this aspect fits the broader meaning discussed in IATE895987. This definition should only include illegal acts executed through computers. Lastly, I also adapted the capital letter at the beginning of the definition.

IATE provides three equivalents: *ciberdelito*, *delito cibernético* and *delito informático*. These seem to be correct terms for the concept. As in the case of Dutch, the difference between the two meanings of computer crime is clearer in Spanish than in English due to the use of different nouns (*delincuencia* and *delito*).

Since *computer-related crime* and *computergerelateerde misdaad* are both accepted terms, it was worth checking for a similar Spanish equivalent. In line with *delincuencia relacionada con los ordenadores*, which can be used for the broader meaning, I googled *delito relacionado con los ordenadores*. However, this entry only results in 4 hits, which shows that it is not valid as a synonym for *ciberdelito.*

Lastly, I wanted to see which one of the synonyms is used the most. This turned out to be *delito informático*, followed by *ciberdelito* and *delito cibernético*.

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1462823728872&uri=CELEX:32013L0040

	Google, Spanish sites	Google Scholar, Spanish sites
“ciberdelito”	65,700	259
“delito cibernético”	35,600	176
“delito informático”	114,000	1,090

2.4 CSIRT (ADP04)

CSIRT	computercalamiteitenteam
Computer Security Incident Response Team	CSIRT
IRT	Computer Security Incident Response Team
Incident Response Team	IRT
CIRT	Incident Response Team
Computer Incident Response Team	CIRT
IRC	Computer Incident Response Team
Incident Response Center/Capability	SERT
CIRC	Security Emergency Response Team
Computer Incident Response Capability	SIRT
SERT	Security Incident Response Team
Security Emergency Response Team	responsteam voor computernoodgevallen
SIRT	
Security Incident Response Team	

equipo de respuesta a incidentes de seguridad informática
equipo de respuesta ante incidentes de seguridad informática
CSIRT
IRT
equipo de respuesta a incidentes
CIRT
equipo de respuesta a incidentes informáticos
SERT
equipo de respuesta a emergencias de seguridad

CSIRT is already extensively discussed in IATE for English, Dutch and Spanish. Furthermore, the English and Dutch information was updated recently (11.3.2016 and 21.11.2015 respectively) and did not need much adaptation. The Spanish information dates from 11.1.2012 and needed to be consolidated.

2.4.1 Definition of the English term

IATE933803 defines *CSIRT* as a "service organisation that is responsible for receiving, reviewing, and responding to computer security incident reports and activity". This definition seems to be in line with other definitions for *CSIRT* on the internet and does not need to be changed.

CSIRT is the abbreviation for *Computer Security Incident Response Team*. In addition to these terms, IATE933803 lists various other synonyms: *Computer Incident Response Capability (CIRC); Computer Incident Response Team (CIRT); Incident Response Centre or Incident Response Capability (IRC); Incident Response Team (IRT); Security Emergency Response Team (SERT); Security Incident Response Team (SIRT).* Not all of these alternatives are commonly used, but they all refer to the same concept.

However, there is one term, *CERT*®, which cannot be used freely, since this is the trademark name of a Response Team in the U.S. Even so, *CERT* frequently occurs on the internet without the registered trademark symbol, which should be avoided. *CSIRT* is considered the European equivalent of *CERT*, and it can also easily be replaced by one of the synonyms mentioned above.

In addition, *Computer Incident Response Capability (CIRC)* appears almost exclusively as *NCIRC* or *FedCIRC*. The "N" refers to NATO and "Fed" to federal. "Computer Incident Response Capability (CIRC)" only results in 193 hits in Google, while "Computer Incident Response Capability (NCIRC)" results in 2,020 and "Computer Incident Response Capability (FedCIRC)" results in 1,480. This means that those *CIRCs* only fight against cybercrime on websites of the NATO or federal instances of the U.S. Therefore, *CIRC* can be used as a general synonym, but it is probably better to use another term to avoid any confusion.

It is very difficult to establish an order, since most of the acronyms also appear as part of another acronym. However, it is clear that *CSIRT* and *Computer Security Incident Response Team* are the terms that are most common.

2.4.2 Dutch terms

The Dutch definition given in IATE933803 is “team van IT-beveiligingsexperts dat zich vooral bezighoudt met het afhandelen van computerbeveiligingsincidenten - het levert de benodigde diensten voor de afhandeling van de incidenten en biedt ondersteuning aan de constituenten om inbreuken te herstellen”. The reference of the definition was not present, but via Google I found that the source is Enisa[13], which is very trustworthy. There was no need for change, since the content of the definition is correct.

IATE933803 suggests two possible synonyms in Dutch, *Computer Security Incident Response Team* and its abbreviation *CSIRT*, which are the exact same English terms. It is mentioned that Dutch often uses English terms, both the abbreviation and the term in full. Even though this is true, I wanted to check whether there exists a Dutchified version as well. In Linguee, the term *computercalamiteitenteam* was found. It is referred to as a Dutch equivalent of *Computer Emergency Response Team (CERT*) and hence *CSIRT*. *Computercalamiteitenteam* yields 223 results in Google and is already used in EUR-Lex. This valid Dutchified version should therefore be promoted as the preferred term over the English term.

Another possible translation, *responsteam voor computernoodgevallen*, was found in EUR-Lex. It is also referred to as a Dutch equivalent of *CERT*. This term yields 305 results in Google, but all hits are either a link to the document in EUR-Lex, or a translation website that uses the sentence from that document. It is therefore likely that *responsteam voor computernoodgevallen* is a specific EU term or a one-off translation.

As in the case of English, IATE933803 provides a number of different acronyms and their full terms that have the same meaning as *CSIRT*: *CERT* or *CERT/CC, IRT, CIRT* and *SERT*. Likewise, *CERT* or *CERT/CC* cannot be used without mentioning that it is a trademark. It is also noticeable that fewer acronyms are suggested for Dutch than for English, so it was worth checking if the other acronyms that are used in English (*CIRC, IRC* and *SIRT*) are also used in Dutch.

“Computer Incident Response Capability (CIRC)” yields 3 hits in Google and is automatically corrected to “Computer Incident Response Team Capability (NCIRC)”. In English, this term

[13] https://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide-in-dutch/at_download/fullReport

also appeared in a general meaning, but this does not seem to be the case in Dutch, which means that *CIRC* cannot be used as a plausible general synonym.

"Incident Response Center (IRC)" and "Incident Response Capability (IRC)" both result in 0 hits in Google. "Security Incident Response Team (SIRT)" yields 44 results and is the only one out of the three that can be seen as an extra acceptable synonym.

Accordingly, *computercalamiteitenteam* is the preferred term in Dutch, followed by the English abbreviations *CSIRT, IRT, CIRT, SERT, SIRT* and their full terms. *Responsteam voor computernoodgevallen* is exclusively used in EU contexts.

2.4.3 Spanish terms

IATE933803 provides the following Spanish definition: "Organización dedicada a la implantación y gestión de medidas tecnológicas destinadas a mitigar el riesgo de ataques contra los sistemas informáticos de la comunidad a la que se proporciona el servicio." This definition was found in a reliable source and seems to be correct. However, the capital letter and full stop were adapted.

As in the case of English and Dutch, two synonyms are suggested: *equipo de respuesta a incidentes de seguridad informática* and *CSIRT*. The original abbreviation has not changed, but the full term has been literally translated to Spanish. Both terms appear to be correct, but during my research in EUR-Lex I found that *equipo de respuesta a incidentes de seguridad informática* also frequently occurs with a different preposition: *equipo de respuesta ante incidentes de seguridad informática.* The term with "a" yields 5,030 results in Google, while the one with "ante" only yields 1,340. Nevertheless, they should be considered accepted synonyms, since they both appear in authoritative sources. A Spanish translation should be promoted over an English loanword, so *equipo de respuesta a incidentes de seguridad informática* is the preferred term here.

In EUR-Lex I also encountered *equipos de intervención ante incidentes de seguridad informática* as a further alternative, but this term only yields 8 results in Google. Therefore, it is not accepted as a valid synonym.

Unlike in English and Dutch, other possible acronyms are not mentioned here. However, it is likely that some also appear in Spanish. Enisa[14] corroborates that *IRT*, *CIRT* and *SERT* are also used, together with their full forms *equipo de respuesta a incidentes*, *equipo de respuesta a incidentes informáticos* and *equipo de respuesta a emergencias de seguridad*. "Capacidad de respuesta ante incidentes informáticos*"* -OTAN (Spanish for "NATO") only yields 4 results and shows that this term cannot be used generally in Spanish. "Capacidad de respuesta a incidentes (IRC)" and "centro de respuesta a incidentes (IRC)" both yield no results. Lastly, "equipo de respuesta a incidentes de seguridad (SIRT)" also only yields 4 hits and cannot be considered a valid synonym.

It should also be noted that Spanish does not capitalize the full terms of the abbreviations, since they are translated and the first letters of the words do no longer correspond with the acronym. Furthermore, Spanish is a language that, in general, capitalizes significantly less than English.

Hence, for Spanish the preferred translation is *equipo de respuesta a incidentes de seguridad informática*, followed by *equipo de respuesta ante incidentes de seguridad informática, CSIRT, IRT, equipo de respuesta a incidentes, CIRT, equipo de respuesta a incidentes informáticos, SERT* and *equipo de respuesta a emergencias de seguridad.*

2.5 HACKTIVISM (ADP05)

hacktivism	hacktivisme hacktivismo hackactivismo

The concept *hacktivism* was already present in IATE924123 for English and Spanish, but not yet for Dutch. The information about the English and Spanish terms needed to be consolidated, while new information needed to be added for Dutch.

[14] https://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide-in-spanish/at_download/fullReport

2.5.1 Definition of the English term

The current definition in IATE924123 dates from 2005 and defines *hacktivism* as "the practice of promoting a political agenda by hacking, especially by defacing or disabling websites". Most definitions that I found are more extensive. For example, Hampson (2012, p. 515) states that *hacktivism* is not only done for political reasons, but also for social ones. The definition on Techopedia[15] has the same addition: "In contrast to a malicious hacker who hacks a computer with the intent to steal private information or cause other harm, hacktivists engage in similar forms of disruptive activities to highlight political or social causes."

A large number of other websites such as Webopedia[16] and Dictionary.com[17] also consider this social aspect. Therefore, it might be stated that there are enough resources to support the addition of this social element to the already existing definition in IATE.

2.5.2 Dutch term

CELEX:52015IE1058 suggests *hacktivisme* as a possible Dutch translation. To verify whether this term is also used in non-EU contexts, the dictionary Van Dale was consulted, which confirmed the use of this translation. "Hacktivisme" yields 2,170 hits in Google, but only 20 hits in Google Scholar. Nevertheless, this number of results may be considered high enough to accept *hacktivisme* as a plausible translation for *hacktivism*. Linguee and Glosbe were also consulted, but no other translations were found.

2.5.3 Spanish term

IATE924123 provides the following definition: "Utilización no violenta de herramientas digitales ilegales o ambiguas desde el punto de vista legal (como el robo de información o sabotajes y parodias de sitios web) para perseguir fines políticos."

First of all, there should be no capital letter at the beginning of the sentence nor a full stop at the end of the definition. More importantly, however, this definition also does not mention the social aspect of the term. As was the case for English, this element was added to the Spanish definition as well. Moreover, "no violenta" ("not violent" in English) was left out of the

[15] https://www.techopedia.com/definition/2410/hacktivism
[16] http://www.webopedia.com/TERM/H/hacktivism.html
[17] http://www.dictionary.com/browse/hacktivism?s=t

definition, since it is obvious that computers cannot use physical violence to harm people. However, I did insert it as a note.

As a Spanish translation, IATE924123 recommends *hacktivismo*. However, in EUR-Lex there is only one document that translated *hacktivism* into Spanish, and the suggested translation there is *hackactivismo* (CELEX:52015IE1058). I googled both terms to see which one yields the most results.

	Google, Spanish sites	Google Scholar, Spanish sites
"hacktivismo"	146,000	824
"hackactivismo"	1,740	15

Even though this research corroborates that *hacktivismo* is the preferred term, *hackactivismo* seems to be an acceptable synonym.

Ultimately, it is also worth mentioning that neither Van Dale (NL-ES/ES-NL) nor the RAE yield any results for *hacktivismo* or *hackactivismo*. This might imply that the term has not yet been officially introduced into the Spanish vocabulary. If this term keeps occurring in Spanish texts on a regular basis, it will probably be included in dictionaries in the near future.

2.6 HASHING (ADP06)

hashing	hashing hashing

Hashing was not yet present in IATE, so this term is a completely new entry. However, there are some sources available in EUR-Lex.

2.6.1 Definition of the English term

Hashing originally seems to be a mathematical concept involving algorithms. In relation to computer science, Rouse (2005) defines *hashing* as "the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string". Furthermore,

according to Rouse (2005) and Computer Hope[18], *hashing* has two different functions. Firstly, it is used to sort and index items in a database, so as to find the items faster with the hashed key. Secondly, it is used to encrypt data and thus protect the safety of passwords or digital messages. The latter is the intended meaning in the context of cybercrime. Techopedia[19] thereby adds that the "hashing process ensures that the message is not intercepted or viewed by an unauthorized end user".

I did not take the first function into account to form a new definition, since it does not relate to the subject of cybercrime. Based on the other sources mentioned above, the following definition was created: "process that encrypts data by transforming strings of characters into a fixed-length value in order to protect the safety of for example passwords".

During the research, no synonyms were found for *hashing*. It seems to be the only term for the concept.

2.6.2 Dutch term

Since Dutch has a tendency to easily accept English loanwords, it was suspected that the translation for *hashing* would simply be *hashing*. This assumption was confirmed. "Hashing" yields 14,300 hits in Dutch pages in Google, and 131 hits in Google Scholar, also in Dutch pages. Furthermore, the available documents in EUR-Lex all kept *hashing* in the Dutch versions of the texts. In an attempt to restrict the search entry only to the field of cybercrime, I also googled the term in combination with "computercriminaliteit". "Hashing" "computercriminaliteit" results in only 317 hits in Google and 1 in Google Scholar. These numbers are way lower and show that *hashing* might not be used for computer crime that often.

In search of an alternative translation, I tried several translation sites such as Linguee and Context Reverso, but no other synonym was found.

2.6.3 Spanish terms

As in the case of Dutch, Spanish also copies the term *hashing* and does not provide a Spanish alternative. In EUR-Lex, two documents can be found that use *hashing* in the Spanish version. Upon googling the term, however, it was discovered that many hits were related to a sport called *hashing* (running and drinking alcohol at the same time). Logically, this sport has the same

[18] http://www.computerhope.com/jargon/h/hashing.htm
[19] https://www.techopedia.com/definition/14316/hashing

name in English and Dutch, but in those languages it did not yield that many results for the sport on the first pages. “Hashing” yields 50,600 hits on Spanish sites in Google, while “hashing” –deporte (Spanish for “sport”) yields 49,100. Nevertheless, the number of hits is still high enough to consider it a valid Spanish equivalent.

To check whether hashing is frequently used in the context of cybercrime in Spanish, a restricted search entry was also googled. “Hashing” “ciberdelincuencia” yields 156 results in Google and 4 in Google Scholar. In comparison to the number of results without the restriction, this is very low.

2.7 ZOMBIE (ADP07)

zombie	zombie
bot	bot
zombie computer	zombiecomputer
zombie machine	
	zombi
	bot
	ordenador zombi

This term is already present in IATE for English and Spanish, but not for Dutch.

2.7.1 Definition of the English term

IATE3503693 defines *zombie* as “a computer that a remote attacker has accessed and set up to forward transmissions (including spam and viruses) to other computers on the Internet; attackers typically exploit multiple computers to create a botnet, also known as a zombie army”. This definition seems to be correct, although I would remove the second part (“attackers typically exploit multiple computers to create a botnet, also known as a zombie army”) and insert it as a note, since it relates to multiple *zombies* and is not really part of the definition of a single *zombie*.

Three possible synonyms are suggested: *bot*, *zombie* and *zombie computer*. These are valid terms. *Zombie* is short for *zombie computer*, and *bot* is a plausible synonym. Originally, *bot* referred to the malware itself and not the computer, but now the term can be used for both the

malware and the bot infected computer. During the research, a further alternative was found: *zombie machine*. *Compromised computer* is also suggested in certain sources, but this concept is much broader then a *bot.*

To determine which one of the terms mentioned above is the preferred term, their frequency on the internet was determined. For *zombie*, *bot* and *zombie machine* an additional search term ("computer") was added to avoid irrelevant results.

	Google, English sites	Google Scholar, English sites
"bot" "computer"	50,100,000	598,000
"zombie" "computer"	15,300,000	23,900
"zombie computer"	39,100	345
"zombie machine" "computer"	4,930	203

Bot clearly has the most hits, but this result reflects both meanings of the term. I did not find a way to exclude one from the other, since adding additional search terms to avoid results relating to the actual malware (e.g. "-malware" or "-virus") could possible also exclude hits where *bot* is used to refer to an infected computer. Both meanings are too closely related.

For this reason, *zombie* should be the preferred term, since this term cannot result in possible confusion. *Bot* could then be considered a valid synonym. *Zombie computer* and *zombie machine* are also accepted synonyms, but the difference in frequency between those terms and *bot* and *zombie* is very high.

2.7.2 Dutch terms

The documents that contained *zombie* in EUR-Lex were not available in Dutch, but one document that uses *zombie network* did translate that term as *zombienetwerk*. This is already a clear indication that *zombie* is translated as *zombie* in Dutch. Furthermore, *zombie* is a well-known Dutch translation for the English *zombie* in the context of a mythical creature. It would be a logical step to keep that translation for the context relating to computer science as well. These assumptions are confirmed by Google: "zombie" "computer" in Dutch sites yields 193,000 results.

While consulting the sources mentioned above, it soon became clear that *bot* and *zombiecomputer* are other synonyms for Dutch. *Zombiecomputer* needs to be spelled in one word in Dutch (cf. http://woordenlijst.org/leidraad/6/3), but it also frequently occurs with a hyphen between "zombie" and "computer", which is incorrect.

Since an additional alternative was discovered for English, it was worth checking whether *zombiemachine* is also used in Dutch. This appears not to be the case. "Zombiemachine" yields 821 results on Dutch sites in Google, but almost all hits use the term in a different context. I tried narrowing it down, but "zombiemachine" "computer" only yields 277 results and the documents are still not used in the appropriate context.

2.7.3 Spanish terms

The Spanish definition in IATE3503693 is

> Ordenador que ha sido infectado de manera remota por un usuario malicioso con algún tipo de software que, al infiltrarse dentro del propio ordenador manipulado y sin consentimiento del propio usuario, un tercero puede hacer uso del mismo ejecutando actividades ilícitas a través de la Red. (zombi, IATE[20])

This definition is correct, but should not have a capital letter at the beginning, nor a full stop at the end. Moreover, the page that is linked as reference no longer exists. On the website of the Spanish National Cybersecurity Institute[21] an alternative definition was found: "aquel que tras haber sido infectado por un virus es usado por delincuentes para realizar actividades maliciosas sin el conocimiento de su dueño".

Two synonyms are given: *zombi* and *ordenador zombi*. Both terms are correct. Interestingly, Spanish has once again converted the English term to a Spanish equivalent. According to Van Dale (NL-ES) *zombi* can be written both with "i" and with "ie", but the Diccionario panhispánico de dudas of the RAE states that the English spelling with "ie" should be avoided in Spanish[22].

---

20 http://iate.europa.eu/SearchByQuery.do?method=searchDetail&lilId=3503693&langId=&query=zombie&sourceLanguage=en&domain=0&matching=&start=0&next=1&targetLanguages=es&targetLanguages=nl

21 https://www.osi.es/es/actualidad/blog/2012/03/21/es-mi-ordenador-un-zombi.html

22 http://lema.rae.es/dpd/?key=zombie

Since *bot* is a valid synonym for English and Dutch, I wanted to find out whether this term could also be used in Spanish. “Bot” “zombi” yields 45,400 results on Spanish sites in Google, and 36 in Google Scholar. The number of hits is certainly high enough to consider *bot* an accepted alternative.

2.8 DDOS ATTACK (ADP08)

DDoS attack distributed denial-of-service attack	gedistribueerde verstikkingsaanval DDoS-aanval distributed denial of service-aanval ataque DDoS ataque distribuido de denegación de servicio ataque de denegación de servicio distribuido

DDoS attack is already present in IATE918800 for English and Dutch, but not yet for Spanish.

2.8.1 Definition of the English term

IATE918800 defines the concept as follows: “attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system, *denial of service* [IATE:899307]”. This definition is correct, but I find it remarkable that the reference to the IATE entry of *denial of service* is simply added after a comma. It looks as if it is a subordinate clause of the definition. Therefore, this reference was shifted to the field for notes on the definition.

Furthermore, “a multitude of compromised systems” can be replaced by “botnet”, which is shorter and has the same meaning. A reference to the IATE entry for *botnet* (IATE2242284) was also added as a note to assure that the definition of *DDoS attack* remains comprehensible.

Lastly, I also added “or a group of people” after “botnet”, since the attack could also originate from different persons who coordinate their attacks, e.g. the activists of Anonymous. Accordingly, the new definition is “attack in which a botnet or a group of people attacks a single target, thereby causing denial of service for users of the targeted system”.

Two synonyms are suggested: *DDoS attack* and *distributed denial-of-service attack*. "DDoS attack" yields 463,000 hits on English sites in Google and 15,400 in Google Scholar. The full term, "distributed denial-of-service attack" results in 241,000 hits in Google and 5,360 in Google Scholar. Since *DDoS attack* has almost double the amount of hits, it should be regarded as the preferred term.

Alternative spellings of *distributed denial-of-service attack* were frequently found on the internet. Sometimes the term is written without hyphens or the first letters of the different parts of the compound are capitalized. However, the spelling as suggested in IATE918800 is preferred. As was the case for *command-and-control centre*, the compound here expresses one idea. Consequently, the spelling with the hyphens is preferable. Even so, nowadays the spelling without the hyphens is not incorrect. The important thing is to remain consistent within the same text. Furthermore, it is desirable not to capitalize the spelled-out word. According to Mudrak (2012), that is only necessary if the abbreviation represents an official name of an organization or if it is a proper noun.

2.8.2 Dutch terms

The Dutch definition for DDoS attack is "het uitvoeren van een zgn. verstikkingsaanval met behulp van andermans computer(s)". This definition does not seem complete. *Verstikkingsaanval* is a Dutch equivalent, so this term cannot appear in the definition. It also does not explain what the attack actually does. Furthermore, "computer(s)" is wrong, since it should always be plural. A characteristic of a *DDoS attack* is that it is executed by multiple computers and not just one. Therefore, an improved definition was looked for. Based on CSBN (2015)[23], I created the following new definition: "aanval door verschillende computers die een bepaalde dienst (bijvoorbeeld een website) onbereikbaar maakt voor de gebruikelijke afnemers".

Gedistribueerde verstikkingsaanval, *distributed denial of service-aanval* and *DDoS-aanval* are the three suggested terms for the concept in IATE918800. These are all valid synonyms. "Gedistribueerde verstikkingsaanval" only yields 30 results on Dutch sites in Google and 0 in Google Scholar. "Distributed denial of service-aanval" results in 1,250 hits in Google and 7 in Google Scholar, and "DDoS-aanval" yields 48,300 and 49 hits respectively. No other alternatives were found.

[23] https://www.rijksoverheid.nl/documenten/rapporten/2015/10/14/cybersecuritybeeld-nederland-csbn-2015

Even though *gedistribueerde verstikkingsaanval* clearly has the least results, it should still be considered to be the preferred term since a Dutchified version should be promoted. *DDoS-aanval* and *distributed denial of service-aanval* are plausible synonyms.

2.8.3 Spanish terms

EUR-Lex does not contain any document that uses the term *DDoS*. Consequently, a Spanish equivalent could not be found there. However, IATE1484647 does already have a Spanish entry for *DoS attack* and suggests *ataque DoS* and *ataque de denegación de servicio.* Logically, the equivalents for *DDoS attack* should then be *ataque DDoS* and *ataque distribuido de denegación de servicio.*

A quick internet search confirmed these assumptions. “Ataque DDoS” yields 91,400 hits on Spanish sites in Google, and 115 in Google Scholar. “Ataque distribuido de denegación de servicio” yields 5,290 and 42 hits respectively. However, there seems to be some disagreement on where to place the adjective “distribuido”. “Ataque de denegación de servicio distribuido” yields 4,470 hits in Google and 26 in Google Scholar. Both appear to be possible judging by the similar number of results. Spanish is a language that accepts that the noun (“ataque”) and the adjective (“distribuido”) that modifies it are not directly next to each other. Nevertheless, the phrase is easier to comprehend if “ataque” and “distribuido” are placed next to each other, which avoids the misinterpretation that “distribuido” might be an adjective to “servicio”.

The English term *distributed denial-of-service attack* is sometimes used in an explanatory way, but does not appear on its own in a Spanish text and can therefore not be considered a plausible synonym.

It can be concluded that *ataque DDoS* is the preferred term, followed by *ataque distribuido de denegación de servicio* and then *ataque de denegación de servicio distribuido*.

2.9 BOOTER SERVICE (ADP09)

booter	booter
stresser	stresser
IP stresser	booterdienst
IP booter	

DDoSer	stresser
DDoS-as-a-service	booter
DDoS-for-hire service	alquiler de ataques DDoS
booter service	

Booter service is not yet present in IATE for any language, nor does it yield any results in EUR-Lex.

2.9.1 Definition of the English term

Webopedia[24] is one of the only sources that clearly defines *booter service*: "service offered by cyber criminals that provides paying customers with distributed denial of service (DDoS) attack capabilities on demand". It also refers to an article by Kerner (2013) on eWeek[25], which adds that a *booter service* does not cost much and that it is hard to shut down. No other definitions were found.

An alternative for *booter service* was found in the sources mentioned above: *booter*. This shortened term is a valid equivalent for *booter service*. However, while googling *booter*, several other synonyms were found: *IP booter, stresser, IP stresser, DDoSer, DDoS-for-hire service* and *DDoS-as-a-service.* Interestingly, most of these terms do not specifically require the addition of "service", but they all represent computer services that execute a DDoS attack for payment.

Whether *booter* or *stresser* is used is a matter of preference. Cloudbooter[26] states that a "real" *stresser* is a legitimate business service to test how much websites can handle. Therefore, people who use *booters* to perform DDoS attacks sometimes call those *stressers* in an attempt to make their action seem more legal.

To determine the preferred term, the synonyms were compared in frequency on the internet. Some terms needed to be constricted by the addition "DDoS" to avoid irrelevant results.

[24] http://www.webopedia.com/TERM/B/booter_services.html
[25] http://www.eweek.com/security/how-do-booters-work-inside-a-ddos-for-hire-attack
[26] https://cloudbooter.com/

	Google, English sites	Google Scholar, English sites
“booter service”	1,040	6
“booter” “DDoS”	75,500	34
“IP booter”	17,400	0
“stresser” “DDoS”	46,000	16
“IP stresser”	31,100	0
“DDoSer” “booter”	13,600	6
“DDoS-for-hire service”	1,430	6
“DDoS-as-a-service”	3,480	60

These results show that *booter* is the preferred term, followed by *stresser, IP stresser, IP booter, DDoSer, DDoS-as-a-service, DDoS-for-hire service* and lastly *booter service.*

2.9.2 Dutch terms

Translation sources such as Van Dale, Linguee or Glosbe did not contain a possible Dutch translation for *booter* or *booter service*. Therefore, I entered the English term in Google using the Dutch language filter. “Booter service” yields 4 results in Google and 0 in Google Scholar. This is not enough to be considered a valid Dutch term. I also tried “booter dienst”, but that entry results in only 1 hit. “Booter” “DDoS”, on the other hand, yields 2,310 hits in Google and 1 in Google Scholar, which means that it could be accepted as a Dutch equivalent.

Since the English term has so many synonyms, it was worth checking whether those are also used in Dutch. “Stresser” “DDoS” yields 1,170 results in Google and 1 in Google Scholar, which makes it a valid synonym. “IP stresser” yields 263 hits in Google, but the language filter does not seem to work here, since many results are still in English. There were 0 hits in Google Scholar. Similarly, “IP booter” results in 162 hits in Google, but many are in English. Google Scholar also did not yield any results. Therefore, *IP stresser* and *IP booter* cannot be considered plausible alternatives.

For the remaining English synonyms, the outcome was also unsuccessful. “DDoSer” yields 639 results in Google, but seems to be used for persons in Dutch instead of for the service itself. “DDoS-as-a-service” yields 200 hits, most of which are in English or not relevant, and “DDoS-for-hire service” only yields 2 results. Accordingly, those three terms are also not valid as Dutch equivalents.

During the research, however, a few other possibilities were discovered in different sources. *Huur een DDoS-aanval* was found on six different websites, but all published the same article. Therefore, the term cannot be considered an accepted synonym. "DDoS-aanbieder" has 40 hits, but once again, most results publish the same article, which does not make the results varied enough. Lastly, I also encountered *DDoS huren*. This entry only yields 1 result and is unacceptable.

The conclusion so far is that only *booter* and *stresser* can be used in Dutch, and that no Dutchified version of the term seems to be in use yet. Due to the relatively low number of results for the terms in English sites, these results were to be expected for Dutch. The concept is probably fairly new and still needs to be incorporated into the languages. There are several articles in Dutch on the internet that consider this topic, but all describe the concept (e.g. "dienst die DDoS-aanvallen uitvoert" or "DDoS-aanval kopen") instead of naming it with a specific term.

Therefore, I would like to propose a Dutchified neologism for the concept: *booterdienst*. This is a literal translation of *booter service.* Since *booter* is already accepted in Dutch, I found it logical to use that term, and "service" was simply translated to "dienst".

2.9.3 Spanish terms

As was the case for Dutch, no Spanish translation was found for *booter*. Since there was nothing to base my research upon, it was decided to see whether one of the English terms is used in Spanish. As could be expected, most English entries did not yield many results.

Booter and *stresser* are the only two terms worth mentioning for Spanish. "Booter "DDoS" yields 2,770 hits on Spanish sites in Google, but 0 in Google Scholar. "Stresser" "DDoS", however, yields 16,800 hits in Google and 0 in Google Scholar. Surprisingly, in Spanish *stresser* seems to be the preferred term, since it appears much more frequently on the internet than *booter*.

During the research, some further possibilities were found: *alquiler de ataques DDoS* (literally "the rent of DDoS attacks" in Spanish) and *ataques DDoS-como-servicio*. "Alquiler de ataques DDoS" yields 1,110 hits in Google and can be considered a valid synonym. On the other hand, "ataques DDoS-como-servicio" only results in 7 Google hits and should not be regarded as an accepted alternative.

The conclusion here is that *stresser* and *booter* can both be used in Spanish texts and that *stresser* is the preferred term. *Alquiler de ataques DDoS* is a valid Spanish equivalent, so there is no need to propose a Spanish neologism here. However, the same tendency as in Dutch can also be seen in Spanish: most websites discuss the subject and describe what happens instead of specifically naming the concept.

2.10 STEGANOGRAPHY (ADP10)

steganography	steganografie
stego	
	esteganografia
	cifra encubierta

IATE891546 suggests two possible English synonyms for this concept, but both only have reliability 1. There is no information available for Dutch. For Spanish, there is only a definition and one valid term.

2.10.1 Definition of the English term

EUR-Lex contains one document that uses *steganography* and a possible definition was found there: “the ability to hide messages in the "noise" of image or sound files” (CELEX:52001AE1474). To check whether other definitions of s*teganography* describe the concept in a similar way, other sources were also consulted. Rouse (2007) defines it as “hiding of a secret message within an ordinary message and the extraction of it at its destination”. Furthermore, Techopedia[27] adds that it is “an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data”. To be complete, I created a new definition based on the resources previously mentioned: “encryption technique to hide secret messages within ordinary messages”. Some extra information from the Techopedia website was added in a note on the definition.

IATE891546 suggests two terms: *stego* and *steganography*. Both do not have a reference or a context field and their reliability is not verified. From the information gathered above, it is

[27] https://www.techopedia.com/definition/4131/steganography

already clear that *steganography* is a valid term for this concept. Furthermore, "steganography" yields 488,000 hits on English sites in Google and 41,000 hits in Google Scholar. To check whether *stego* is also used for *steganography*, the search entry had to be specified to avoid irrelevant results. "Stego" "hiding" yields 70,400 results in Google and 10,800 in Google Scholar, which is enough to consider it a plausible alternative. The abbreviation *stego* is often used in combination with another noun, e.g. *stego-image* or *stego-text*.

Some sources suggest *cryptography* or *encoding* as other synonyms, but those concepts slightly differ in meaning from *steganography*. As a consequence, no other alternatives were found.

2.10.2 Dutch terms

The Dutch version of CELEX:52001AE1474 translated *steganography* as *steganografie*. Van Dale (NL-EN) confirms this translation, but the term is not present in the other direction (EN-NL). An internet search corroborates that it is a valid term, with 6,710 hits on Dutch sites in Google and 24 in Google Scholar.

It was worth checking whether the abbreviation that is used in English also occurs in Dutch. This appears not to be the case. Several search entries such as "stego" "geheim", "stego" "steganografie" or "stego" "boodschap" were googled, but all yield few and mostly irrelevant results. Very sparsely, a source was found in those results that uses *stego* as a synonym for *steganografie*, but certainly not often enough to make it acceptable in Dutch.

During the research I also came across *stegografie*, which is an incorrect term for the concept. It only has 60 hits in Google and 0 in Google Scholar, which means that it is probably a misspelling of *steganografie*.

2.10.3 Spanish terms

IATE891546 provides the following Spanish definition:

> Complemento de la criptografía que se ocupa de los métodos para ocultar la información cifrada, generalmente dentro de ficheros convencionales (texto, imágenes, sonido...). La criptografía modifica los datos para que no sean legibles, mientras que la esteganografía los toma y los oculta entre otros datos. (esteganografía, IATE[28])

[28] http://iate.europa.eu/FindTermsByLilId.do?lilId=891546&langId=es

This definition is correct content wise, but some other observations are worth a note. First of all, there is no reference of this definition. I tried searching the source by entering the definition in Google, but there were 0 results. This might imply that the definition was created by someone from the DGT department itself. Secondly, the second sentence of the definition should be inserted as a note and not be part of the actual definition. Lastly, the definition should not start with a capital letter, nor end with a full stop.

Due to the remarks mentioned above, the definition was replaced by a new one: "ocultación de información en un canal encubierto (por ejemplo imágenes, textos o sonidos) con el propósito de prevenir la detección de un mensaje oculto". This definition was based on a source from INTECO (Instituto Nacional de Tecnologías de la Comunicación)[29], the National Institute of Communication Technologies of Spain (which is now called INCIBE), but was slightly adapted.

There is also a note on the definition that says "SYN/ANT: Sin.: cifra encubierta; mensaje disimulado". Instead of adding this information in a note, the synonyms should (after consolidation) also be listed as a term for the concept.

The suggested term in IATE891546 is *esteganografía*. This term is the valid equivalent for *steganography*. It yields 53,700 results on Spanish sites in Google and 374 in Google Scholar. However, the reference in IATE is "CESID, Glosario de Términos de Criptología, 1991". No link to this reference could be found, and since the source dates from 1991, it was better to replace it with a more recent source: CELEX:52001AE1474/ES. This document also uses *esteganografía* and dates from 2001.

It was also checked whether the synonyms mentioned above (*cifra encubierta* and *mensaje disimulado*) can be used to refer to *steganography*. "Cifra encubierta" yields 142 hits in Google and 3 in Google Scholar. In several of these sources it is mentioned that CESID mentioned this term as a synonym of *steganography*. The literal English translation is "hidden number", which is more specific than the actual meaning, since *steganography* covers all sorts of messages and not just numbers. Even so, it can be said that it is an accepted synonym due to the importance of CESID as a source, but it should be considered obsolete.

---

29 https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwjtnfyS1ZrMAhUMBcAKHZT7ClkQFgg8MAQ&url=https%3A%2F%2Fwww.incibe.es

"Mensaje disimulado" yields 815 results in Google and 6 in Google Scholar, but almost all hits are not related to *steganography*. The literal translation in English is "hidden message", which has a more general meaning than *steganography*. Therefore, *mensaje disimulado* appears in different, irrelevant contexts that, for example, refer to a wink. As a consequence, this term cannot be considered a valid synonym.

2.11 DKIM (ADP11)

DKIM	DKIM
DomainKeys Identified Mail	DomainKeys Identified Mail
	DKIM
	DomainKeys Identified Mail

DKIM or *DomainKeys Identified Mail* is not yet present in IATE for any language, but it does yield 1 result in EUR-Lex.

2.11.1 Definition of the English term

CELEX:32014D0188 is the only document in EUR-Lex that contains the term *DKIM* and defines the concept as "an ICT technical specification developed by internet Engineering Task Force (IETF) that permits a person, role or organisation that owns the signing domain to claim some responsibility for a message by associating the domain with the message". Furthermore, DKIM.org[30] provides the following definition:

> DomainKeys Identified Mail (DKIM) lets an organization take responsibility for a message that is in transit. The organization is a handler of the message, either as its originator or as an intermediary. Their reputation is the basis for evaluating whether to trust the message for further handling, such as delivery. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication.

Based on these two definitions, I created a new definition: "method that allows a person, role or organisation to validate a domain name identity associated with a message". Additional

[30] http://dkim.org/

information could be found on Techopedia[31]. In a note on the definition, I added that *DKIM* was originally created to fight spam.

Both the abbreviation *DKIM* and the full term *DomainKeys Identified Mail* can be used for the concept. "DKIM" yields 431,000 hits on English sites in Google and 2,210 in Google Scholar, while "DomainKeys Identified Mail" only yields 41,900 hits in Google, and 514 in Google Scholar. Since the abbreviation clearly results in more hits, it should be considered the preferred term.

Interestingly, the full term *DomainKeys Identified Mail* has to be written with "DomainKeys" in one word. "Domain Keys Identified Mail" results in 9,020 hits in Google and 2 in Google Scholar, but both search entries try to correct the entry by suggesting "Domainkeys Identified Mail". Even though the suggestion shows that the correct spelling is in one word, it fails to suggest a fully correct spelling by decapitalizing the 'k' of "Keys".

No other alternatives for *DKIM* were found during the research.

2.11.2 Dutch terms

CELEX:32014D0188 also has a Dutch version, which copies the English terms *DKIM* and *DomainKeys Identified Mail*. To verify these Dutch equivalents, various translation sources were consulted. Van Dale (EN-NL) did not have an entry for *DKIM* or *DomainKeys Identified Mail*. Linguee and Context Reverso, on the other hand, both also kept the English terms in their Dutch translations.

In Dutch sites, "DKIM" yields 7,710 results in Google and 5 in Google Scholar. "DomainKeys Identified Mail" results in 754 hits in Google and 1 hit in Google Scholar. Overall, the results are not very impressive, but the numbers are high enough to consider the terms valid synonyms. As was the case for English, the abbreviation is the preferred term here.

There seems to be no Dutchified equivalent for the concept. Not once did I find a possible Dutch equivalent during the research, nor did my own attempts (e.g. "domeinsleutels geïdentificeerde mail") yield any results.

[31] https://www.techopedia.com/definition/15545/domainkeys-identified-mail-dkim

2.11.3 Spanish terms

As was the case for Dutch, the Spanish version of CELEX:32014D0188 also uses *DKIM* and *DomainKeys Identified Mail*. "DKIM" yields 312,000 results on Spanish sites in Google and 242 results in Google Scholar. However, the results in Google Scholar often seem not related to the context of cybercrime. Therefore, a restriction was added to the search entry in Google Scholar: "DKIM" "correo" (Spanish for "e-mail") results in 101 hits and has more relevant results. The full term, "DomainKeys Identified Mail" yields 5,420 results in Google and 5 in Google Scholar. These results show that in Spanish, too, the abbreviation is the preferred term.

Linguee suggests *correo identificado por clave de dominio* as a Spanish translation. However, this phrase only results in 9 hits on Spanish sites in Google, all of which are directed to Linguee. When I tried to go directly to the sources mentioned in Linguee, the website was either removed or did not contain the example sentence. Therefore, *correo identificao por clave dominio* cannot be considered an equivalent.

No other valid Spanish equivalent was found. In comparison with the previous terms discussed, this is rather unusual.

3 CONCLUSION

3.1 TENDENCIES

During the research on the concepts discussed in section 2, a few tendencies were noticed that are certainly worth mentioning. Firstly, if a concept was already present in IATE, very often more synonyms were discovered than there had been suggested. This was the case for all three languages. Most of the time, the most frequent terms were already present, but possible alternatives that occur less frequently had not yet been included. This might imply that IATE's primary concern is to provide their users with the basic information of as many concepts as possible, by suggesting only one or two valid terms for each concept. Only if more time is available later on, are the concepts researched more in depth.

Another remarkable phenomenon is that Dutch tends to easily copy the English term, only adapting it to its own language later on or sometimes not at all. If a Dutch equivalent exists, it is also very often much less common than the English term. This is a clear indication of domain

loss for Dutch in the field of cybercrime. A possible explanation could be that all the new concepts in cybercrime originate as English terms. Furthermore, as previously explained in section 1.4, language users have become used to seeing English terms appear in their own native language and, due to the almost expected basic English knowledge, there is no immediate need for a Dutch equivalent. However, this dissertation promotes the use of a Dutchified term over the English term, in order to avoid domain loss as much as possible.

For Spanish, a different tendency was noticed. Spanish does not accept an English term as easily as Dutch does, and will often try to immediately adapt it to a Spanish equivalent. That also explains why more already existing Spanish equivalents were found in comparison to already existing Dutch equivalents. For this reason, it can be argued that there is no or very little domain loss in the field of cybercrime for Spanish. Even so, in recent years Spanish has been more open to loanwords from other languages, and is starting to accept them more easily. Almost all of the concepts discussed in section 2 had a Spanish equivalent, but the English term was used as well. Often, the Spanish language will use a Spanish equivalent and put the English term in brackets.

It was also observed that a Dutchified version of an English term is very often misspelled. Even though the rules for spelling compounds in Dutch are different from those in English, many language users copy the English spelling without adjusting the term to the Dutch spelling rules, or they add unnecessary hyphens. For Spanish, on the other hand, there sometimes seems to be doubt regarding which preposition needs to be used in full terms of abbreviations. It is not unusual that two different versions of the same term, each one using a different preposition, are used on the internet, even though most of the time only one of those is acceptable.

3.2 DIFFICULTIES

Terminological research has proved to be very time-consuming. If the term is not yet fully incorporated into a language, it is very difficult to find relevant and authoritative sources to base the research upon. Out of the eleven concepts discussed in section 2, six were not present in my original choice of concepts. This means that six terms were dropped because of a lack of appropriate information or because they occurred as a synonym of another (already discussed) term. I did not expect that more than half of the terms would need to be changed. This resulted in some lost time and frustration during the process.

Furthermore, EUR-Lex did not always turn out to be a useful source. If the term was relatively new, it could not be found in the EUR-Lex database, which means that possible translations or equivalents in other languages were also not present. Moreover, the search engine of EUR-Lex does not always seem to work as it should. Terms that are put between quotation marks sometimes yield results that only contain one of the words between the quotation marks. This is an issue that had better be resolved, as it also resulted in some time loss.

On the other hand, I really learned to appreciate Google Scholar. When EUR-Lex did not provide an authoritative source, Google Scholar was the first website that was consulted as an alternative. It contains many published research articles as well as master dissertations from students all over the world. I found it very interesting to see many different types of sources appear, and consequently Google Scholar was very often used to fill in the context field of the records. Moreover, the Techopedia, TechTarget and Webopedia websites proved very useful to find English definitions in the field of cybercrime. These sources were consulted systematically for most concepts, if only to corroborate a previously found definition.

3.3 GENERAL CONCLUSION

This dissertation's goal was to participate in the continuous process of terminological research on new concepts. The research on the eleven concepts in section 2 was a small contribution to the field of cybercrime. There is without a doubt room for additional research in this field, since it continues to develop every day. However, there should not only be research on new concepts. Concepts that are already present in IATE might also need some consolidation or amplification.

Moreover, for Dutch, domain loss regarding cybercrime clearly poses a challenge. That is why this dissertation promotes the use of Dutchified terms over English terms in Dutch. On the other hand, Spanish might need to be careful not to go down the same road as Dutch, and should continue to create Spanish equivalents instead of following the recent tendency of copying the English terms.

4 BIBLIOGRAPHY

Abrams, R. (2008). Understanding and teaching bots and botnets. In *Virus Bulletin Conference*, pp. 1-4. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.631.865&rep=rep1&type

Acosta, R.E. & Isaza, G.A. (2012). Hacia un arquitectura de buenas prácticas de seguridad para sistemas ERP. En *Vector*, *5*, pp. 53-60. http://vip.ucaldas.edu.co/vector/downloads/Vector5_6.pdf

Advies van het Economisch en Sociaal Comité over de "Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's — Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak", CELEX:52001AE1474/NL

Advies van het Europees Economisch en Sociaal Comité over cyberactivisme en de maatschappelijke organisaties (initiatiefadvies) CELEX:52015IE1058/NL

Advies van het Europees Economisch en Sociaal Comité over de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur „Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht" (COM(2009) 149 definitief), CELEX:52009AE1948/NL

Aeilts, T. (2005). Defending against cybercrime and terrorism. A new role for universities. In *FBI Law Enforcement Bulletin*, pp. 14-20. http://www.au.af.mil/au/awc/awcgate/fbi/universities_fight_terrorism.pdf

Aguilar, M.M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. En *Revista Criminalidad*, *57*(1), pp. 121-135. http://www.policia.gov.co/imagenes_ponal/dijin/revista_criminalidad/vol57_1/v57n1a08.html

Ahmad, A., Hadgkiss, J. & Ruighaver, A.B. (2012). Incident response teams – Challenges in supporting the organisational security function. In *Computers & Security*, *31*(5), pp. 643-652. http://ac.els-cdn.com/S0167404812000624/1-s2.0-S0167404812000624-main.pdf?_tid=fe283532-fb11-11e5-8916-00000aab0f01&acdnat=1459849220_cb183b0392ca6491e31f9df370fb0aec

Aitor (06.02.2015). *Peligro en la red: Troyanos, malware y botnets*. Timos.info. http://www.timos.info/peligro-en-la-red-troyanos-malware-y-botnets/

Albors, J. (2013). *El malware Zeus resurge con fuerza durante este 2013*. Zona Virus. http://www.zonavirus.com/noticias/2013/el-malware-zeus-resurge-con-fuerza-durante-este-2013.asp

Alderweireldt, A. & Thaens, T. (2007). *Steganografische systemen gebaseerd op levende talen, met menselijke interactie*. Masterproef. http://www.aalex.be/khlim/thesis/thesis_E07-ELO-02.pdf

Algemene voorwaarden. Heffiq, slim intern transport. Utilev. http://www.utilev.nl/about-this-site/terms-of-use/

Allman, E. (2006). E-mail authentication: what, why, how? In *ACM QUEUE*, *4*(9), pp. 30-34. http://dl.acm.org/citation.cfm?id=1180191

AlphaStress (February 8, 2016). *All about IP stressers/booters – Network, Security & Performance Blog*. https://alphastress.com/blog/what-is-ip-stresser-booter/

Alruhaily, N., Bordbar, B. & Chothia, T. (2015). Analysis of mobility algorithms for forensic virtual machine based malware detection. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, (1), pp. 766-773. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7345353

Andrade, R. & Fuertes, W. (s.d.). *Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: ESPE.* http://ciencia.espe.edu.ec/wp-content/uploads/2013/05/COM61.pdf

Antonakakis, M., et al. (2012). From throw-away traffic to bots: detecting the rise of DGA-based malware. Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), pp. 491-506. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final127.pdf

Artiles, N.G. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. En *cuadernos de estrategia*, (149), pp. 165-214. http://dialnet.unirioja.es/descarga/articulo/3837337.pdf

Aucsmith, D. (2003). *Information hiding*. Springer, p. 274. https://books.google.be/books?id=1XKqCAAAQBAJ&pg=PA275&lpg=PA275&dq

Avilés, A.S.A. & Matamoros, R.F.E. (2014). *Modelo de análisis forense digital para una entidad bancaria.* Doctoral dissertation. Escuela Politécnica Nacional. http://bibdigital.epn.edu.ec/handle/15000/8702

Aycock, J. & Friess, N. (2006). *Spam Zombies from Outer Space*. University of Calgary. http://prism.ucalgary.ca/bitstream/1880/45374/2/2006-808-01.pdf

Backman, S. (2015). Organizing national cybersecurity centres. In *Information & Security: An International Journal*, *32*. http://procon.bg/system/files/3206_ncscs_backman.pdf

Bada, M., et al. (2014). *Computer Security Incident Response Teams (CSIRTs). An Overview.* Global Cyber Security Capacity Centre. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIRTs.pdf

Baigorri, L. (2003). *Recapitulando: modelos de artivismo (1994-2003).* Artnodes. UOC. https://www.uoc.edu/artnodes/espai/esp/art/baigorri0803/baigorri0803.html

Banday, M.T., Qadri, J.A. & Shah, N.A. (2009). Study of Botnets and Their Threats to Internet Security. In *Sprouts: Working Papers on Information Systems*, *9*(24). http://www.123seminarsonly.com/Seminar-Reports/038/71169818-Botnet-Sprotus.pdf

Bastenier, M.Á.: «Hacktivismo», El País, 30.11.2010 http://internacional.elpais.com/internacional/2010/11/30/actualidad/1291071624_850215.html

Bautista, C.L.V., et al. (2007). Esteganografía en una imagen digital en el dominio DCT. En *Científica*, *11*(4), pp. 169-176. http://www.redalyc.org/articulo.oa?id=61411403

Bechtholt, N. (2014). *De Luuuk bankfraude-campagne: in één week een half miljoen euro gestolen*. Kaspersky Lab Newsroom Europe. http://newsroom.kaspersky.eu/nl/nieuws/detail/article/de-luuuk-bankfraude-campagne-in-een-week-een-half-miljoen-euro-gestolen/?no_cache=1

Bennett, K. (2004). *Linguistic steganography: survey, analysis, and robustness concerns for hiding information in text*. CERIAS Tech Report. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=DD06D8156CD9EB604DD65557B12F501E?doi=10.1.1.158.8602&rep=rep1&type=pdf

Berger-Sabbatel, G. & Duda, A. (2011). Analysis of Malware Network Activity. In *Multimedia Communications, Services and Security, Communication in Computer and Information Science*, pp. 207-215.

http://download.springer.com/static/pdf/918/bok%253A978-3-642-21512-4.pdf?originUrl

Besluit 2009/316/JBZ van de Raad van 6 april 2009 betreffende de oprichting van het Europees Strafregister Informatiesysteem (ECRIS) overeenkomstig artikel 11 van Kaderbesluit 2009/315/JBZ, CELEX:32009D0316/NL

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. In *Communications of the ACM*, *49*(2), pp. 81-83. http://delivery.acm.org/10.1145/1120000/1113075/p81bhaskar.pdf?ip=157.193.5.27&id

Blackwell, A. (2015). *Enfoques situacionales de la delincuencia y la violencia: el caso de américa latina*. Wilson Center. http://www.pensamientopenal.com.ar/system/files/2015/06/doctrina41372.pdf

Blanco, H.M. (2013). *Plataforma de correo electrónico con sincronización de elementos pim mediante servidor funambol*. Proyecto fin de carrera, Universidad Autónoma de Madrid. http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20131202HectorMorenoBlanco.pdf

Boletin de Seguridad UNAM-CERT-2014-011 Crypto Ransomware (2014). Coordinación de Seguridad de la Información. http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=6521

Bolivia CSIRT. (s.d.). *Que es el CSIRT-BO.* Estado Plurinacional de Bolivia. http://www.csirt.gob.bo/csirt.php

Booter top 10 list – the best booter of 2016 (s.d.). The Booter Ranking Site. http://top10booters.com/

Borghello, C. (2007). Botnets, redes organizadas para el crimen. Eset. http://www.eset-la.com/pdf/prensa/informe/botnets_redes_organizadas_para_el_crimen.pdf

Bose, R. (2008). *Information theory, coding and cryptography*. Tata McGraw-Hill Education, p.297. https://books.google.be/books?hl=nl&lr=lang_en&id=SQeUwB0ApY0C&oi=fnd&pg=PR2&dq=%22hashing%22+or+encryption&ots=7gBQEx1Qa-&sig=V7JFOd7C845XtNCCEtHW8Nh6u-4#v=onepage&q=%22hashing%22%20&f=false

Bot/Botnet, begrippenlijst Henst & Lunsen. http://www.datariskverzekeringen.nl/begrippenlijst/betekenis-van-bot-botnet.html

Brito, J.M. (2013). *El ciclo de protesta actual: La acción colectiva después de la indignación*. Pensamiento crítico. http://www.pensamientocritico.org/juabri1212.htm

Bruggen, M. van der, (2015). Een beschouwing van de ontwikkeling van het internet en cybercriminaliteit en de gevolgen hiervan voor de internationale bestrijding van digitale kinderporno. In *Tijdschrift voor Criminologie*, *57*(2), pp. 242-259. http://search.proquest.com/docview/1715691585?pq-origsite=gscholar

Bukac, V., et al. (2015). Service in denial–Clouds going with the winds. In Network and System Security, pp. 130-143. http://download.springer.com/static/pdf/870/bok%253A978-3-319-25645-0.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-3-319-25645-0&token2=exp=1460821017~acl=%2Fstatic%2Fpdf

Butler, J.M. (2013). Encontrando amenazas ocultas al desencriptar SSL. *Un Libro Blanco de Analista de SANS*. Blue Coat Systems.

https://www.bluecoat.com/es/documents/download/ee951b81-7ab8-4cb4-ae90-c5d27506656a/dc6754b1-cd80-4be3-a7fa-158c3e101425

Caballero, J., et al. (2011). Measuring Pay-per-Install: The commoditization of malware distribution. In *Usenix security symposium*. https://www.usenix.org/legacy/events/sec11/tech/full_papers/Caballero.pdf

Cabré Castellvi, M.T. (2003). Theories of terminology: their description, prescription and explanation. In *terminology*, 9(2), pp. 163-199. https://benjamins.com/#catalog/journals/term.9.2.03cab/details

Callewaert, C. (2014). *Anonymous doet parlement panikeren*. De wereld morgen. http://www.dewereldmorgen.be/artikel/2014/11/05/anonymous-doet-parlement-panikeren

Canadian Cyber Incident Response Centre (CCIRC). Public Safety Canada. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

Canadian Cyber Incident Response Centre. TERMIUM Plus, Government of Canada. http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=Canadian+Cyber+Incident+Response+Centre+&index=alt&codom2nd_wet=1

Cappa, M. & Donelson, P. (2012). National Security. In *Public Policy and Governance Review*, *3*(1), pp. 8-46. https://ppgr.files.wordpress.com/2012/01/ppgr-full-text-vol3iss12.pdf

Cárceles, M.M.A. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. En *Revista Criminalidad*, *57*(1), pp. 121-135. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082015000100009

Castillo, C. (s.d.). *Sexy view: el inicio de las botnets para dispositivos móviles*. Pontifica Universidad Javeriana. http://www.eset-la.com/pdf/prensa/concurso/universitario/sexy_view_inicio_botnets_dispositivos_moviles.pdf

Castillo, T. (2014). *¿Tienes un PC zombi? Señales para detectarlo y consejos para revivirlo.* Malavida. http://www.malavida.com/guias-trucos/tienes-un-pc-zombi-senales-para-detectarlo-y-consejos-para-revivirlo

Castrillón, E.P. (2009). Sistemas de información inteligentes para la sociedad de Internet. En *Revista Digital Lámpsakos*, (2) pp. 91-95. http://www.funlam.edu.co/revistas/index.php/lampsakos/article/view/776/745

Catá, A. del Palacio (2014). *Ciberdelincuencia. Desarrollo y persecución tecnológica.* Proyecto fin de carrera. Universidad Politécnica de Madrid. http://oa.upm.es/34795/1/PFC_arturo_cata_palacio.pdf

CBP richtsnoeren: beveiliging van persoonsgegevens. (s.d.). Overheid.nl http://wetten.overheid.nl/BWBR0033572/2013-03-01

Centrum voor Terminologie – GenTerm – Terminology Centre. Universiteit Gent. http://www.cvt.ugent.be/index.htm 23/02/2016

CERT in de organisatie. (2006). Genootschap van Informatie Beveiligers (GvIB), GvIB Expertbrief, *2*(1). https://www.pvib.nl/download/?id=6259871

Cervera, E.R. (2015). *Detección y bloqueo de botnets mediante la combinación de técnicas basadas en el tráfico de red*. Trabajo Fin de Master, Universidad Nacional de Educación a Distancia.

http://www.issi.uned.es/Master_ISSI/WebMISSI/RepositorioTFM/2015/15S_MemoriaTFdM_ISW_TipoB_Juan_Enrique_Ripoll_Cervera.pdf

Chandran, S., Hrudya, P. & Poornachandran, P. (2015). An efficient classification model for detecting advanced persistent threat. In *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI*), pp. 2001-2009. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7275911

Chang, C., Hsiao, J. & Chan, C. (2003). Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. In *Pattern Recognition*, *36*(7), pp. 1583-1595. http://ac.els-cdn.com/S0031320302002893/1-s2.0-S0031320302002893-main.pdf?_tid=57eaba9e-060d-11e6-ad2f-00000aab0f6c&acdnat=1461056686_c3b6ad7e9566977a6bf012bab1e118ba

Chan, S. (2014). *Routledge Encyclopedia of Translation Technology*. Routledge, p. 654. https://books.google.be/books?hl=nl&lr=lang_en&id=S0FWBQAAQBAJ&oi=fnd&pg=PP1&dq=Routledge+Encyclopedia+of+Translation+Technology&ots=fkBv1-xJfO&sig=Qd85zwnOe6zdg9O_wGbCHQ5iv24#v=onepage&q=concept%20orientation&f=false

Cheddad, A., et al. (2010). Digital image steganography: Survey and analysis of current methods. In *Signal processing*, *90*(3), pp. 727-752. http://ac.els-cdn.com/S0165168409003648/1-s2.0-S0165168409003648-main.pdf?_tid=71ae5e54-0608-11e6-8782-00000aacb35e&acdnat=1461054581_ed50aa34ba9d2d854777e07b0ac6dbd7

Chicaiza, N.M.A. & Salazar, M.S.P. (2010). *Investigación, análisis y pruebas de los Procesos de Esteganografía.* Proyecto de tesis, Universidad Técnica de Cotopaxi. http://181.112.224.103/bitstream/27000/1240/1/T-UTC-0865.pdf

Choi, K.S. (2008). Computer crime victimization and integrated theory: An empirical assessment. In *International Journal of Cyber Criminology*, *2*(1), pp. 308-333. http://search.proquest.com/docview/89216682?pq-origsite=gscholar

Choo, K.R. (2007). Zombies and botnets. In *Trends & Issues in crime and criminal justice*. Australian Institute of Criminology. http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi333.pdf

Cifra encubierta. (s.d.). Guía de seguridad (CCN-STIC-401). Glosario y abreviaturas. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=201.html

Claerhout, P. (2013). *Slechts 5 procent kmo's verzekerd tegen e-criminaliteit*. In Trends, Knack. http://trends.knack.be/economie/ondernemen/slechts-5-procent-kmo-s-verzekerd-tegen-e-criminaliteit/article-normal-253059.html

Clavero, J. (2015). *Detección de intrusos con snort*. Proyecto del postgrado. Universitat Oberta de Catalunya. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43087/4/jmclaveroTFM0715memoria.pdf

Clerix, K. (2012) *Inlichtingendienst zkt. hackers*. http://www.mo.be/artikel/inlichtingendienst-zkt-hackers

Cloud Booter. https://cloudbooter.com/

Cobb, S. (2014). Cómo combater una botnet y entender su impacto real. In we live security. http://www.welivesecurity.com/la-es/2014/10/27/botnets-como-combatirlas/

Coll, F.J.M. (2005). El papel de un IRT dentro de la Organización. Red.es, http://www.rediris.es/cert/doc/pres/barcelona.pdf

Collantes de Luca, J.J. (2015). Implementación de una nube de servidores de dns autoritativos con direccionamiento anycast de un proveedor de servicio de internet que mantendrá la integridad y la disponibilidad del servicio de resolución de nombres de dominios antes los ataques de denegación de servicios o fallos de hardware. Escuela Superior Politécnica del Litoral (ESPOL). http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/31480/D-103012.pdf?sequence=-1&isAllowed=y

Comando. In *Diccionario de la lengua española*. Real Academia Española, http://dle.rae.es/?id=9sxsYE6

Comisión Europea (2012). *Un Centro Europeo contra la Delincuencia Informática para luchar contra las delincuentes en línea y proteger a los consumidores que utilizan Internet.* Comunicado de prensa. http://europa.eu/rapid/press-release_IP-12-317_es.htm

Command and control server. In *Radware*. DDoS Attack Definitions – DDoSPedia. https://security.radware.com/ddos-knowledge-center/DDoSPedia/command-and-control-server/

Commission communication: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, CELEX:52000DC0890

Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative, CELEX:32011R1179

Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, CELEX:32013R0611

Commission Staff Working Document Impact Assessment Accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA) {COM(2010) 521 final} {SEC(2010) 1127}, CELEX:52010SC1126

Commission Staff Working Document Montenegro 2013 Progress Report Accompanying the document Communication from the Commission to the European Parliament and the Council Enlargement Strategy and Main Challenges 2013-2014, CELEX:52013SC0411

Commission Staff Working Document Summary of the Impact Assessment Accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA) {COM(2010) 521 final} {SEC(2010) 1126}, CELEX:52010SC1127/NL

Commission staff working document - Annex to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" {COM(2006) 251 final} - Impact assessment, CELEX:52006SC0656

Commission Staff Working Document accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Progress Report on the single

European Electronic Communications Market (15th report) {com(2010) 253}, CELEX:52010SC0630R(01)

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642}, CELEX:52007DC0267

Computercriminaliteit brengt bijna 280 miljard euro per jaar op (17 augustus 2011). Knack. http://www.knack.be/nieuws/technologie/computercriminaliteit-brengt-bijna-280-miljard-euro-per-jaar-op/article-normal-24772.html

Comunicación de la Comisión titulada "Hacia una política general de lucha contra la ciberdelincuencia", p. 2, COM(2007) 267 final, CELEX:52007DC0267/ES

Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, CELEX:52013JC0001/ES

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información - «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia» {SEC(2009) 399} {SEC(2009) 400}, CELEX:52009DC0149/ES

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global», CELEX:52011DC0163/ES

Conclusies van de Raad van 27 november 2008 over een gemeenschappelijke werkstrategie en concrete maatregelen tegen cybercriminaliteit, CELEX:52009XG0317(01)/NL

Conclusiones del Consejo (...) relativas a una estrategia de trabajo concertada y a medidas concretas contra la delincuencia informática (DO C 62/2009, p. 16), CELEX:52009XG0317(01)/ES

Consejo-ES a partir del sitio web del Grupo de Delitos Telemáticos de la Guardia Civil, https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

Convenio sobre la Ciberdelincuencia del Consejo de Europa (BOE n.º 226 de 17-9-2010, p. 78847) http://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

Council Decision 2010/576/CFSP of 23 September 2010 on the European Union police mission undertaken in the framework of reform of the security sector (SSR) and its interface with the system of justice in the Democratic Republic of the Congo (EUPOL RD Congo), CELEX:32010D0576

Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime, CELEX:32001H0703(01)

Cox, I., et al. (2007). *Digital watermarking and steganography*. Morgan Kaufmann. https://books.google.be/books?hl=nl&lr=lang_en&id=JZQLpzihtecC&oi=fnd&pg=PP2&dq=%22steganography%22+&ots=VTJh3VhKBa&sig=xcY1mcMczk6c5DfaoSB7169axDs#v=onepage&q=%22steganography%22&f=false

CSIRT Frequently Asked Questions (FAQ), CERT Software Engineering Institute, Carnegie Mellon University. http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm#1

CSIRT: Productos y servicios. (s.d.) Ministerio del Interior y Seguridad Pública, Gobierno de Chile. http://www.csirt.gob.cl/productos_servicios_2.html

Cyber Security Technical Advice and Guidance. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-eng.aspx%2013/03/2016

Cybersecuritybeeld Nederland, CSBN 2015. (2015). Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie. https://www.rijksoverheid.nl/documenten/rapporten/2015/10/14/cybersecuritybeeld-nederland-csbn-2015

Cyberveiligheid. Gids voor incidentbeheer. (s.d.). Centre for Cyber Security Belgium. http://static1.squarespace.com/static/55d339cfe4b05cbbf5e4a24e/

De Blas, D. (2015). El Número de ataques DDoS se duplica en un año. Globb Security. http://globbsecurity.com/akamai-estudio-q42014-28787/

De Morgen, 08.04.2014, "XPocalypse now: wordt uw computer vandaag een zombie?", http://www.demorgen.be/technologie/xpocalypse-now-wordt-uw-computer-vandaag-een-zombie-b2fd5a13/

De nieuwe bedreigingen (14 maart 2001), "ZDNet", http://www.zdnet.be/article/6169/de-nieuwe-bedreigingen/

De Rooij, J. (2010). Botnet is als de veelkoppige slang Hydra. In *computable.* https://www.computable.nl/artikel/achtergrond/security/3622380/1444691/botnet-is-als-de-veelkoppige-slang-hydra.html

Dhillon, G. & Moores, S. (2001). Computer crimes : theorizing about the enemy within. In *Computers & Security*, *20*(8), pp. 715-723. http://ac.els-cdn.com/S0167404801008136/1-s2.0-S0167404801008136-main.pdf?_tid=01cd35fe-fc96-11e5-9ad8-00000aacb362&acdnat=1460015871_3d68bd8ecca488ba1408051f2e5ff9a0

Diaroti (2 febrero 2015). Aumenta el alquiler de ataques DDoS basados en técnicas de reflexión y multivectores. http://diarioti.com/aumenta-el-alquiler-de-ataques-ddos-basados-en-tecnicas-de-reflexion-y-multivectores/85500

Díaz, L.H. (2009). El delito informático. En *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, (23), pp. 227-243. http://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Dictamen del Comité Económico y Social Europeo sobre «El ciberactivismo y las organizaciones de la sociedad civil» (Dictamen de iniciativa), CELEX:52015IE1058/ES

Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)» [COM(2010) 521 final], CELEX:52011AE0363/ES

Dictamen del Comité Económico y Social sobre la "Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — Seguridad de las redes y de la información: Propuesta para un enfoque político europeo", CELEX:52001AE1474/ES

Dictamen del Comité Económico y Social Europeo sobre el tema Fomentar la alfabetización, la capacitación y la inclusión digitales (Dictamen exploratorio), CELEX:52011AE1182/ES

Dietrich, S., Long, N. & Dittrich, D. (2000). Analyzing Distributed Denial of Service Tools: The Shaft Case. In LISA, pp. 329-339. https://www.usenix.org/legacy/event/lisa2000/full_papers/dietrich/dietrich_html/

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 , relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, CELEX:32013L0040/ES

DomainKeys Identified Mail (DKIM). http://dkim.org/

DomainKeys Identified Mail (DKIM). (s.d.). In *Techopdia.* https://www.techopedia.com/definition/15545/domainkeys-identified-mail-dkim

Dogrul, M., Aslan, A. & Celik, E. (2011). Developing an international cooperation on cyber defense and deterrence against Cyber terrorism. In *3rd international conference on Cyber conflict (ICCC)*, pp. 1-15. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5954698

E-CRIME Project. (2015). The Economic Impact of Cyber Crime. Examination of Regulatory and Enforcement Framework. European Commission. http://ecrime-project.eu/wp-content/uploads/2014/06/E-CRIME-Press-release-3-June-2015.pdf

EcuRed. (s.d.). Ataque de denegación de servicio. http://www.ecured.cu/Ataque_de_denegaci%C3%B3n_de_servicio

Elhacker.net (2 enero 2015). Lizard Squad ofrece su servicio de ataque DDoS pagando. http://blog.elhacker.net/2015/01/lizard-squad-ofrecen-ahora-su-servicio-ataque-ddos.html

Eliasson, J. (2015). *Delito cibernético*. Las Naciones Unidas. http://www.un.org/es/events/crimecongress2015/cibercrime.shtml

El Mundo: «Una red de 'ordenadores zombis'», 14.4.2015 http://www.elmundo.es/espana/2015/04/14/552c00e7268e3e11278b456c.html

Enisa (2006). *Een stapsgewijze aanpak voor het samenstellen van een CSIRT*, blz. 6,7 en 24. https://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide-in-dutch/at_download/fullReport

Enisa (2006). *Cómo crear un CSIRT paso a paso*, pp. 6 & 7. https://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide-in-spanish/at_download/fullReport

Erbschloe, M. (2004). *Trojans, worms, and spyware: a computer security professional's guide to malicious code.* Butterworth-Heinemann, p.17. https://books.google.be/books?hl=nl&lr=lang_en&id=-BsTixXQp08C&oi=fnd&pg=PP2&dq=%22Computer+incident+response+team%22&ots=GghP6wQyuj&sig=GrKqCVc4ui8Ds6EItOgoHpU87Fs#v=onepage&q=%22Computer%20incident%20response%20team%22&f=false

Erp, J.G. van, Stol, D.W. & Wilsem, J. van (2013). Criminaliteit en criminologie in een gedigitaliseerde wereld. In *Tijdschrift voor Criminologie*, 5(4), pp. 327–341. http://hdl.handle.net/1765/50759

Erquiaga, M.J. (2011). Botnets: mecanismos de control y de propagación. En *XVII Congreso Argentino de Ciencias de la Computación*, pp. 1076-1085. http://sedici.unlp.edu.ar/bitstream/handle/10915/18764/Documento_completo.pdf?sequence=1

¿Es mi ordenador un zombi? (23.03.2012). Oficina de Seguridad del Internauta, Instituto Nacional de Ciberseguridad de España (INCIBE). https://www.osi.es/es/actualidad/blog/2012/03/21/es-mi-ordenador-un-zombi.html

Europa nu, "Bestrijding computercriminaliteit - Mededeling van de Commissie over het scheppen van een veiliger informatiemaatschappij door verbetering van de veiligheid

van informatie-infrastructuren en bestrijding van computergerelateerde criminaliteit" http://www.europa-nu.nl/id/vh8rh4ls4vzt/bestrijding_computercriminaliteit

Europese Commissie (7 februari 2013). EU oppert plan voor cyberbeveiliging: bescherming van vrij en open internet en kansen in digitale wereld. Persbericht. http://europa.eu/rapid/press-release_IP-13-94_nl.htm

Evaluatierapport van de zevende wederzijdse evaluatie "De praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit". (Brussel, 26 juni 2015). Raad van de Europese Unie. https://www.tweedekamer.nl/kamerstukken/detail?id=2015D29764

Farrell, S. (2006). Domainkeys identified mail demonstrates good reasons to re-invent the wheel. In *Public Key Infrastructure*, pp. 145-153. http://download.springer.com/static/pdf/232/bok%253A978-3-540-35152-8.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F11774716&token2=exp=1461511018~acl=%2Fstatic%2Fpdf%2F232%2Fbok%25253A978-3-540-35152-8.pdf

Federal Communications Commission. (2012). Computer Incident Response Team. FCC Computer Security. Desk Reference. http://m.iwar.org.uk/comsec/resources/fasp/CIRT-Desk-Reference.pdf

Ferguson, G. (2007). The global spread of English, scientific communication and ESP: Questions of equity, access and domain loss. In *Ibérica*, (13), pp. 7-38. http://www.aelfe.org/documents/02%20ferguson.pdf

Fernández, T.S. (2015). *Selección, instalación y configuración del software de servidor de mensajería electrónica. IFCT0509*. IC Editorial. https://books.google.be/books?hl=nl&lr=lang_es&id=17bbCgAAQBAJ&oi=fnd&pg=PT4&dq=%22DKIM%22+%22DomainKeys+Identified+mail%22&ots=GiPNvMIA5W&sig=4Pf06I1KRI2H8NXLvljZJNTrV-s#v=onepage&q=%22DKIM%22%20&f=false

Fitri, N. (2011). Democracy discourses through the Internet communication: Understanding the hacktivism for the global changing. In *Online Journal of Communication and Media Technologies*, *1*(2), pp. 1-20. http://www.ojcmt.net/articles/12/121.pdf

Focus op security. (s.d.). Basefarm. https://www.basefarm.com/nl/wikitech/onze-focus-op-security

Foro español de equipos de seguridad y atención a incidentes (Foro CSIRT.es), https://www.csirt.es/index.php?option=com_content&view=article&id=45&Itemid=72#1

Freiling, F.C., Holz, T. & Wicherski, G. (2005). *Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks*. Springer Berlin Heidelberg, pp. 319-335. http://download.springer.com/static/pdf/256/bok%253A978-3-540-31981-8.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F11555827&token2=exp=1460716788~acl=%2Fstatic%2Fpdf%2F256%2Fbok%25253A978-3-540-31981-8.pdf

Gallagher, H., McMahon, W. & Morrow, R. (2014). Cyber-Security: Protecting the resilience of Canada's financial system. In *Bank of Canada: Financial System Review*, pp. 47-53. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.1809&rep=rep1&type=pdf

García, E.E. (2012). *Centro Nacional de Respuesta a Incidentes Cibernéticos CERT-MX*. Policía federal. http://seguridad2012.politicadigital.com.mx/pdf/03.pdf

García-Cervigón, J.G. (2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. En *Icade, revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (74), pp. 289-308. https://revistas.upcomillas.es/index.php/revistaicade/article/view/357/283

Garg, V., Husted, N. & Camp, J. (2011). The smuggling theory approach to organized digital crime. In *eCrime Researchers Summit (eCrime)*, pp. 1-7. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6151980

Geiregat, J. (2008). Diversificatie van software door instructiesetlimitatie. Scriptie Universiteit Gent. http://lib.ugent.be/fulltxt/RUG01/001/312/432/RUG01-001312432_2010_0001_AC.pdf

Gezamenlijke Mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace, CELEX:52013JC0001/NL

Gijsbrechts, K. (2016). BNP Paribas Fortis offline na DDoS-aanval. ZDNet. http://www.zdnet.be/nieuws/179137/bnp-paribas-fortis-offline-na-ddos-aanval/

Global Conference on CyberSpace 2015 (Den Haag), "CSIRT Maturity", https://www.gccs2015.com/nl/csirt-maturity

Gogolin, G. (2010). The digital crime tsunami. In *Digital investigation*, *7*(1), pp. 3-8. http://ac.els-cdn.com/S1742287610000526/1-s2.0-S1742287610000526-main.pdf?_tid=cef73cce-f5a6-11e5-825e-00000aacb35e&acdnat=1459253429_59453eb19967e24f131d66ccba248c70

Gómez, A.D. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. En *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR*, (8), pp. 169-203. http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf

Gómez, E.C.F. & Espinosa, H.A.C (2014). Cómo responder a un Delito Informático. En *Revista Ciencia UNEMI*, *11*, pp. 43-50. http://www.unemi.edu.ec/ojs/index.php/cienciaunemi/article/viewFile/111/112

Gónzalez, R.M. (2005). *Un modelo efectivo para la administración de incidentes de Seguridad de Información*. CACS. http://isacamty.org.mx/archivo/133-Mejores_Practicas_la_Admin_de_Incidentes.pdf

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. In *Journal in Computer Virology*, *2*(1), pp. 13-20. http://link.springer.com/article/10.1007/s11416-006-0015-z

Grabosky, P. (2000). *Computer crime: A criminological overview*. Australian Institute of Criminology. http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/Grabosky2000_UNCongress_ComputerCrimeCategories.pdf

Graddol, D. (2006). *English Next*. The British Council. Latimer Trend & Company Ltd, Plymouth. http://englishagenda.britishcouncil.org/sites/ec/files/books-english-next.pdf

Grobauer, B. & Schreck, T. (2010). Towards incident handling in the cloud: challenges and approaches. In *Proceeding*, pp. 77-86. http://delivery.acm.org/10.1145/1870000/1866850/

Grobler, M. & Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. In *Information Security for South Africa (ISSA),* pp. 1-6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588307

Grupo de Trabajo de Seguridad de la Información y Protección de la Privacidad. Software malicioso (malware) una amenaza de seguridad para la economía de internet (28 de abril 2008). OCDE. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/ocde_malware.pdf

Gu, G., et al. (2007). BotHunter: Detecting malware infection through IDS-driven dialog correlation. In *Usenix Security Symposium, 7*, pp. 167-182. http://static.usenix.org/legacy/events/sec07/tech/full_papers/gu/gu_html/

Gualdrón, J.C.A. (2006). *Jóvenes, hacktivismo y sociedad de la información*. Universitat Autònoma de Barcelona. http://www.sindominio.net/metabolik/alephandria/txt/Aceros_-_Juventud_hacktivismo_y_sociedad_de_la_informacion.pdf

Gualpa, E.G.C. & Rubio, D.A.R. (2011). *Análisis y estudio de los virus y antivirus informáticos del mercado local. Caso práctico elaboración de un virus que recopile la mayor cantidad de procesos que pueden causar daños en los computadores*. Tesis de Grado, Universidad Técnica de Cotopaxi. http://181.112.224.103/bitstream/27000/1113/1/T-UTC-0774.pdf

Guidance DomainKeys Identified Mail (DKIM), (February 19, 2016). Government Digital Service. https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim

Gupta, B.B., Joshi, R.C. & Misra, M. (2012). Distributed Denial of Service prevention techniques. In International Journal of Computer and Electrical Engineering (IJCEE), *2*(2), pp. 268-276. https://arxiv.org/ftp/arxiv/papers/1208/1208.3557.pdf

Gutierrez del Moral, L. (2014). *Curso de Ciberseguridad y Hacking Ético 2013*. Punto Rojo Libros, p. 472. https://books.google.be/books?id=sua0BAAAQBAJ&pg=PA472&lpg=PA472&dq=%22ataque+de+denegaci%C3%B3n+de+servicio+distribuido%22&source=bl&ots=XChn20ISOA&sig=g5_ITqE37y3qDS9WU8tYvblCcnI&hl=nl&sa=X&ved

Gutiérrez, A. (2016). *Los ataques DDoS y WAF, tendencias dentro del mundo de la seguridad online.* Ecommercenews. http://ecommerce-news.es/servicios/los-ataques-ddos-y-waf-tendencias-dentro-del-mundo-de-la-seguridad-online-37904.html

G.F., M. (s.d.). *Botnets.* Manpreseg. http://www.manpreseg.es/es/seguridad/codigo-malicioso/41-botnets.html

Guardia Civil http://www.guardiacivil.es/es/institucional/especialidades/gdt/index.html

Hacktivism. (s.d.). In Dictionary.com http://www.dictionary.com/browse/hacktivism?s=t

Hacktivism. (s.d.). In *Van Dale Online*. http://vandale.ugent.be/

Hacktivism. (s.d.). In *Techopedia*. https://www.techopedia.com/definition/2410/hacktivism

Hacktivism. (s.d.). In *Webopedia*. http://www.webopedia.com/TERM/H/hacktivism.html

Hampson, N. (2012). Hacktivism: A new breed of protest in a networked world. *In Boston College International and Comparative Law Review, 35*(2), pp. 511-542. http://poseidon01.ssrn.com/delivery.php?ID=017096020116088011011031002024088098015051021063079059125001021095123121109008070127006055125 0

Hash de contraseñas seguro. (s.d.). PHP. http://php.net/manual/es/faq.passwords.php

Hashing. (s.d.). Computer Hope. http://www.computerhope.com/jargon/h/hashing.htm

Hashing. (s.d.). Techopedia. https://www.techopedia.com/definition/14316/hashing

Heras, J.S. de la. (2006). Estado y perspectiva del servicio de correo electrónico en RedIRIS. En *Boletín de RedIRIS*, (76), pp. 13-20. http://www.rediris.es/difusion/publicaciones/boletin/76/informe.pdf

Het Laatste Nieuws, 20.09.2011, "Cybercriminaliteit maakt drie slachtoffers per minuut", http://www.hln.be/hln/nl/4125/Internet/article/detail/1321582/2011/09/20/Cybercriminaliteit-maakt-drie-slachtoffers-per-minuut.dhtml

Het Nieuwsblad, 01.06.2010, "Schooldirecteur betrapt met kinderporno", http://m.nieuwsblad.be/cnt/gti2qu1mf

Het Laatste Nieuws, 11.04.2012, "Apple werkt aan neerhalen van botnet", http://www.hln.be/hln/nl/4125/Internet/article/detail/1421785/2012/04/11/Apple-werkt-aan-neerhalen-van-botnet.dhtml

Hoefnagel, F.J.P.M. (2007). *ICT en Internet. Casestudie ten behoeve van het project veiligheid.* Wetenschappelijke Raad voor het Regeringsbeleid (WRR). http://www.oapen.org/search?identifier=439942

Hoffmann, P.R. (2015). Vulnerabilidades de "alto" riesgo – top 30. http://www.pentest.cl/2015/05/vulnerabilidades-de-alto-riesgo-top-30/

Hong, J. (2012). The state of phishing attacks. In *Communication of the ACM*, *55*(1), pp. 74-81. http://delivery.acm.org/10.1145/2070000/2063197/p74-hong.pdf?ip=157.193.8.1&id=2063197&acc=OPEN&key=D7FC43CABE88BEAA%2EF15FE2ACB4878E3D%2E4D4702B0C3E38B35%2E6D218144511F3437&CFID=775608324&CFTOKEN=27082300&__acm__=1461510329_53169abdd916c4cff96a763cac73a265

Huerta, A.V. (2002). *Esteganografía.* http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node320.html

Imperva. (s.d.). *Booters, Stressers and DDoSers*. DDoS Protection Center. https://www.incapsula.com/ddos/booters-stressers-ddosers.html

Incident Response (s.d.). Digital Investigation. https://digital-investigation.eu/incident-response/

Information resource management directive 5000.12, USAP information security incident management. (2004). The National Science Foundation, Polar Programs, United States Antarctic Program. https://www.usap.gov/technology/documents/5000_12%20Incident%20Response%205-15-2013.pdf

Informe de la Comisión al Consejo y al Parlamento Europeo Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), CELEX:52011DC0225/ES

INTECO. (s.d.). *Esteganografía, el arte de ocultar información*. Observatorio de la Seguridad de la Información. https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwjtnfyS1ZrMAhUMBcAKHZT7CIkQFgg8MAQ&url=https%3A%2F%2Fwww.incibe.es%2Ffile%2FcMACs_tFRyI_Q1i88xyWtA&usg=AFQjCNFr8K77Nfw5yzMRczkDCxHEK3K5sA&sig2=CvxoLLcQIyHOqQ-gON_bAg

Interinstitutionele organen, (2015). Europese Unie. http://europa.eu/about-eu/institutions-bodies/interinstitutional-bodies/index_nl.htm

Janus, M. (2011). *Heads of the hydra. Malware for network devices*. Secure list. https://securelist.com/analysis/publications/36396/heads-of-the-hydra-malware-for-network-devices/

Johnson, L. (2013). *Computer incident response and forensics team management: conducting a successful incident response*. Newnes, p. 18 and 47. https://books.google.be/books?hl=nl&lr=lang_en&id=6lJxGXfLWkYC&oi=fnd&pg=PP1&dq=%22Security+Incident+response+team+SIRT%22&ots=pjPvZUGfxF&sig=LBIxqiZ3gFyIiEWwsLBK9HPiBsE#v=onepage&q=%22Security%20Incident%20response%20team%20SIRT%22&f=false

Jong, B. de (2013). Russische spionagepraktijken in de 21ste eeuw: de zaak-Raymond P. In *Internationale Spectator*, *67*(10), pp. 47-51. http://dare.uva.nl/document/2/129976

Juist management oorzaak van malware op computers (8 november 2013). Informatiebeveiliging Nederland. https://informatiebeveiliging.nl/nieuws/juist-management-oorzaak-van-malware-op-computers/

Junger, M. et al. (2013). *Modus operandi onderzoek naar door informatie en communicatie technologie (ICT) gefaciliteerde criminaliteit*. Universiteit Twente. http://doc.utwente.nl/85337/1/0_MOIT_DEF_Rapport_def_2013.pdf

Jurisprudentie-bulletin RSJ 2012/1, Zaaknummer 11/2109/GA, www.rsj.nl/Images/bulletin-2012-1-a4_tcm60-404464.pdf

Karami, M. & McCoy, D. (2013). *Understanding the emerging threat of DDoS-As-a-Service*. George Mason University. http://mason.gmu.edu/~mkarami/papers/booter-leet13.pdf

Karami, M., Park, Y. & McCoy, D. (2015). *Stress testing the booters: understanding and undermining the business of DDoS services*. http://arxiv.org/pdf/1508.03410v1.pdf

Kerner, S.M. (2013). *How do booters work? Inside a DDoS for hire attack.* eWeek. http://www.eweek.com/security/how-do-booters-work-inside-a-ddos-for-hire-attack

Kessler, G.C. (2001). *Steganography: hiding data within data.* http://www.garykessler.net/library/steganography.html

Kolbitsch, C., et al. (2010). Inspector gadget: Automated extraction of proprietary gadgets from malware binaries. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pp. 29-44. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5504785

Koops, B.J. & Prins, J.E.J. (2004). Misbruik van technische hulpmiddelen: een beschouwing over de te ver gaande regelingen in het Cybercrime-verdrag en de Auteursrechtenrichtlijn. In *Computerrecht*, (2), pp. 59-67. https://pure.uvt.nl/portal/files/613494/technischehulpmiddelen-cr.pdf

Koops, B.J. (2010). Tijd voor computercriminaliteit III. In *Nederlands Juristenblad*, *85*(38), pp. 2461-2466. https://pure.uvt.nl/portal/files/1300685/Koops_Tijd_voor_Computercriminaliteit_110121_postprint_immediately.pdf

Koops, B.J. (2013). *Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: strafrechtelijke aspecten*. Universiteit van Tilburg. https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/expert_opinion_botnets_koops_mei_2013.pdf

Korteweg, D. (2013). *Nieuwe Europese richtlijn moet cybersecurity beter waarborgen*. Recht in de zorg. http://rechtindezorg.nl/2013/02/15/nieuwe-europese-richtlijn-moet-risico-cybersecurity-beperken/

Krapp, Peter. (2005). *Terror and play, or what was hacktivism?* Grey Room, 21, pp. 70-93. http://www.academia.edu/307639/Terror_and_Play_or_What_Was_Hacktivism

Kristoff, J. & Joffee, R. (2007). Botnets and Packet Flooding DDoS Attacks on the Domain Name System. In *The International Journal of Forensic Computer Science*, *1*(2), pp. 9-18. http://www.ijofcs.org/V02N1-FULL.pdf#page=21

KU Leuven. (s.d.). Virussen, wormen, trojaanse paarden en hoaxen. https://admin.kuleuven.be/icts/e-mune/Virussen

Kufandirimbwa, O. & Gotora, R. (2012). Spam Detection using Artificial Neural Networks (Perceptron Learning Rule). In *Online Journal of Physical and Environmental Science Research*, *1*(2), pp. 22-29. http://onlineresearchjournals.org/JPESR/pdf/2012/june/Kufandirimbwa%20and%20Gotora.pdf

Lee, K., et al. (2008). DDoS attack detection method using cluster analysis. In Expert Systems with Applications, *34*(3), pp. 1659-1665. http://ac.els-cdn.com/S0957417407000395/1-s2.0-S0957417407000395-main.pdf?_tid=6463d3b6-02f0-11e6-8033-00000aacb35d&acdnat=1460714398_7407c215004550062eb6a2c19a34ff7f

Leiba, B. & Fenton, J. (2007). DomainKeys Identified Mail (DKIM): Using digital signatures for domain verification. In *CEAS*. http://internetmessagingtechnology.org/pubs/CEAS-2007-078-DKIM.pdf

Li, L. & Lee, G. (2005). DDoS attack detection and wavelets. In *Telecommunication Systems*, *28*(3-4), pp. 435-451. http://download.springer.com/static/pdf/868/art%253A10.1007%252Fs11235-004-5581-0.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs11235-004-5581-0&token2=exp

Lorinc, J. (2014) *Riesgos de seguridad; la guerra cibernética*. CPA Magazine. Traducción para Veritas. http://veritasonline.com.mx/riesgos-de-seguridad-la-guerra-cibernetica/

Lucas, J. & Moeller, B. (2004). *The effective incident response team*. Addison-Wesley Professional, p.1 and 154. https://books.google.be/books?hl=nl&lr=lang_en&id=hMIxjthVsmsC&oi=fnd&pg=PR13&dq=%22Computer+incident+response+team%22&ots=nSxMo61MjG&sig=Qw5j9H3f90Ry2hDyBIS8cwW3gh0#v=onepage&q=%22Computer%20incident%20response%20team%22&f=false

Luo, Y. (2010). Workload characterization of spam email filtering systems. In *International Journal of Network Security & Its Application (IJNSA)*, *2*(1), pp. 22-41. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.192.2270&rep=rep1&type=pdf

Lyden, J. (2015). *Nice SECURITY, 'Lizard Squad'. Your DDoS-for-hire service LEAKS.* The Register. http://www.theregister.co.uk/2015/01/19/lizard_squad_ddos_for_hire_site_insecure_says_krebs/

Maak jouw wachtwoorden onleesbaar met hashing (20 mei 2015). Thuiswinkel waarborg. https://www.thuiswinkel.org/nieuws/2774/maak-jouw-wachtwoorden-onleesbaar-met-hashing

Mando. In *Diccionario de la lengua española*. Real Academia Española, http://dle.rae.es/?id=OA3ulOZ

Mansfield-Devine, S. (2015). The growth and evolution of DDoS. In *Network Security*, pp. 13-20. http://ac.els-cdn.com/S1353485815300921/1-s2.0-S1353485815300921-

main.pdf?_tid=9570ced2-0485-11e6-b9f3-00000aacb35f&acdnat=1460888426_55be907a9076b73d60008ec16c379eee

Martinez, S. (2003). *Federal Government Incident Response Team (IRC).* Windows Security. http://www.windowsecurity.com/whitepapers/misc/Federal_Government_Incident_Response_Team_IRT.html

Martínez, A. (2014). *La resiliencia de las botnets: "redes duras de pelar"*. Instituto Nacional de Ciberseguridad de España. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/La_resiliencia_de_las_botnets_redes_duras_de_pelar

Mata Barranco, N. J. de la & Díaz, L.H. (2009). El delito de daños informáticos: una tipificación defectuosa. En Estudios Penales y Criminológicos, *29*, pp. 311-362. http://dspace.usc.es/bitstream/10347/4149/1/07.Mata.pdf

Maxwell, K. (2006). *From metrosexual to metrosessuale: the global influence of English in the creation of neologisms*. MED Magazine. MacMillan Publishers Limited. http://www.macmillandictionaries.com/MED-Magazine/March2006/36-New-Word-Neologisms.htm

Mcnamee, K. (2014). *Luchar contra Googost, el malware que roba ancho de banda*. Techzine. https://techzine.alcatel-lucent.com/es/luchar-contra-googost-el-malware-que-roba-ancho-de-banda

Mededeling van de Commissie aan de Raad en het Europees Parlement. De aanpak van criminaliteit in het digitale tijdperk – Oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit, CELEX:52012DC0140/NL

Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's - Naar een algemeen beleid voor de bestrijding van cybercriminaliteit {SEC(2007) 641} {SEC(2007) 642}, CELEX:52007DC0267/NL

Mendez-Garcia, V., et al. (2014). Comparative analysis of banking malware. In *2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV)*, pp. 1-5. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7000412

Mezquida, D.A., et al. (2003). Ocultación de imagenes mediante Esteganografía. En *Novática: Revista de la Asociación de Técnicos de Informática*, (163), pp. 52-57. http://www.ati.es/novatica/2003/163/163-52.pdf

Mirkovic, J. & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. In ACM SIGCOMM Computer Communication Review, *34*(2), pp. 39-53. http://delivery.acm.org/10.1145/1000000/997156/p39-mirkovic.pdf?ip=157.193.5.169&id=997156&acc=ACTIVE%20SERVICE&key=D7FC43CABE88BEAA%2EF15FE2ACB4878E3D%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=770743955&CFTOKEN=27712426&__acm__=1460714716_165012be70709e5fa6dbeb21a17d0498

Misdaden / misdrijven tegen de mensheid / menselijkheid (s.d.). In Taaladvies, taaluniversum. http://taaladvies.net/taal/advies/vraag/551/misdaden_misdrijven_tegen_de_mensheid_menselijkheid/

Mok, S.C. (2008). Alcance de la legislación costarricense en materia de delitos informáticos: Un análisis preliminar. En *Inter Sedes*, (3), pp. 49-64. http://www.intersedes.ucr.ac.cr/ojs/index.php/intersedes/article/view/170/169

Molina, A. (2016). *Claves para entender el concepto del DKIM (DomainKeys Identified Mail).* Mittum. http://www.mittum.com/mx/blog/claves-dkim/

Mooi, R. & Botha, R.A. (2015). Prerequisites for building a Computer Security Incident Response capability. In *Information Security for South Africa (ISSA)*, pp. 1-8. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7335057

Moore, R. (2010). *Cybercrime: investigating high-technology computer crime*. Routledge, p. 3. https://books.google.be/books?hl=nl&lr=lang_en&id=PjQlwXN7CO8C&oi=fnd&pg=PP2&dq=%22a+computer+crime%22&ots=BJgwObm44t&sig=6wXVItDH_Avd3eTT6WyG0kmxC7E#v=onepage&q=%22a%20computer%20crime%22&f=false

Mudrak, B. (2012). *Editing Tip: Capitalization When Defining Abbreviations.* American Journal Experts. https://www.aje.com/zh/author-resources/articles/editing-tip-capitalization-when-defining-abbreviations

Muñoz, A., Alvarez, I.A. & Carracedo, J. (2009). Modificaciones sintácticas en lengua española con utilidad en esteganografía lingüística. En *Revista Electrónica de Lingüística Aplicada (RAEL)*, (8), pp. 229-247. http://dialnet.unirioja.es/descarga/articulo/3143010.pdf

Muñoz, M. & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. En *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, pp. 1-15. http://www.scielo.mec.pt/scielo.php?pid=S1646-98952015000100002&script=sci_arttext&tlng=en

Naedele, M. (2007). Addressing IT security for critical control systems. In *Proceedings of the 40th Hawaii International Conference on System Sciences*, pp. 1-9. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4076600

National Instruction On Classified Information Spillage. (2008). Committee on National Security System (CNSS). https://www.fas.org/sgp/library/cnssi-1001.pdf

Navarro, S.F. (2011). *Detección de malware a partir del comportamiento del navegador*. http://upcommons.upc.edu/bitstream/handle/2099.1/12474/71847.pdf?sequence=1&isAllowed=y

Oerlemans, J.J. (2010). Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien. In *Tijdschrift voor Internetrecht*, *5*, pp. 148-152. http://oerlemansblog.weblog.leidenuniv.nl/files/2010/11/J.J._Oerlemans_-_Tijdschrift_voor_Internet_recht_-_conceptwetsvoorstel_nader_bezien.pdf

Oerlemans, J.J. & Koops, B.J. (2011). De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets. In *Nederlands Juristenblad*, *86*(18), pp. 1181-1185. https://pure.uvt.nl/ws/files/1328649/Koops_HogeRaad_botnets_110509_postprint_immediately.pdf

Olmedo, C.A. (2010). La delincuencia organizada: un asunto interior de la Unión Europea. Concepto, características e instrumentos para su neutralización. En *Revista Española de Relaciones Internacionales*, (2), pp. 152-172. http://reri.difusionjuridica.es/index.php/RERI/article/view/25/26

Opgepakte Mastercard DDoS'ser geïdentificeerd (10 december 2010). Secury. http://www.secury.nl/nieuws/34/opgepakte_mastercard_ddos'ser_ge%EFdentificeerd#.VxDk6fmLTIU

Opinion of the Committee of the Regions on 'Cyber-security Strategy', CELEX:52013IR1646

Opinion of the Economic and Social Committee on the "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on network and information security: proposal for a European policy approach", CELEX:52001AE1474

Opinion of the European Economic and Social Committee on Enhancing digital literacy, e-skills and e-inclusion (exploratory opinion), CELEX:52011AE1182

Opinion of the European Economic and Social Committee on 'Cyberactivism and civil society organisations' (own-initiative opinion), CELEX:52015IE1058

Opinion of the European Economic and Social Committee on 'Cyber attacks in the EU' — (own-initiative opinion), CELEX:52014IE1488

Overill, R.E. & Silomon, J.A. (2011). A complexity based forensic analysis of the Trojan horse defence. In *2011 Sixth International Conference on Availability, Reliability and Security (ARES)*, pp. 764-768. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6046034

Pacek, B. (2012). Cyber security directed activities. In *Internal Security*, pp. 119-137. http://search.proquest.com/docview/1323526044/fulltext/FA02E0094D7B4231PQ/1?accountid=11077

Paget, F. (2012). *Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas*, McAfee Labs™ http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf?view=legacy

Paredes Valdivieso, H.R. (2010). *Implementación de un sistema de gestión central y unificada sobre seguridad en ambientes Microsoft en el Laboratorio de Tecnologías de Información y Comunicación (LTIC) de la Facultad de Ingeniería.* http://repositorio.puce.edu.ec/handle/22000/3424

Perdisci, R., Lee, W. & Feamster, N. (2010). Behavioral clustering of HTTP-based malware and signature generation using malicious network traces. In *NSDI.* http://static.usenix.org/event/nsdi10/tech/full_papers/perdisci.pdf

Pieterse, H. & Olivier, M.S. (2012). Android botnets on the rise: Trends and characteristics. In *Information Security for South Africa (ISSA)*, pp. 1-5. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6320432

Pijpker, J. (2015). *De rol van Internet Service Providers bij de bestrijding van botnets*. Open Universiteit Nederlands. http://dspace.ou.nl/bitstream/1820/6209/1/INF_20151119_Pijpker.pdf

Pilling, R. (2013). Global threats, cybersecurity nightmares and how to protect against them. In *Computer Fraud & Security*, (9), pp. 14-18. http://ac.els-cdn.com/S1361372313700812/1-s2.0-S1361372313700812-main.pdf?_tid=0fb636ac-048e-11e6-afe8-00000aab0f27&acdnat=1460892067_435c1615b72c4fc4481c49ec6e3ea65c

Pirela, M.A. & Wilhelm, S.L. (2011). Tres tipos penales informáticos. En *Cuestiones Jurídicas*, *5*(1), pp. 31-49. http://www.uru.edu/fondoeditorial/revista/pdf/rcj/v5.n1/tres%20tipos%20penales.pdf

Poiters, E. (2015). Implementing a Remote Acces Trojan Infrastructure. Bachelorscriptie Artesis Plantijn Hogeschool Antwerpen. https://www.ap.be/sites/default/files/attachments/wetenschap-en-techniek/poiterselvira_scriptie_20151.compressed.pdf

Prada, I.F. (2015). Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. En *Revista Electrónica de Ciencia Penal y Criminología*, *17*(21). http://criminet.ugr.es/recpc/17/recpc17-21.pdf

Pras, A. (2014) *Alle dagen internet - beheersen door beheren.* Twente University Press, Enschede. http://eprints.eemcs.utwente.nl/25275/01/oratie.pdf

Pras, A. & Meent, R. van de (2004). Meten van internetverkeer voorkomt veel virusleed. Automatisering Gids, *37*(1). http://eprints.eemcs.utwente.nl/7785/01/2004-09-AutoGids.pdf

Previder (15 maart 2016). Cloud-security event voor ISV's. https://www.previder.com/nl/over-previder/actueel/nieuws/art/2121/cloud-security-event-voor-isv%E2%80%99s

Prins, J.E.J. (2002). Wapenwedloop in cyberspace. Gegevensmunitie ten koste van privacy? In *Ars Aequi*, *51*(5), pp. 315-323. https://pure.uvt.nl/ws/files/474072/wapenwedloop_om_cyberspace.pdf

Privacybeleid GGS, Gentsche Geokasjing Sosseteit vzw. https://www.gentsche-geokasjing-sosseteit.be/wp/historiek/privacybeleid/

Programma betreffende politiële en justitiële samenwerking in strafzaken (AGIS-programma) — Jaarlijks werkprogramma en oproep tot het indienen van aanvragen voor 2003, CELEX:C2003/005/06/NL

Proposal for a Directive Of The European Parliament And Of The Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, CELEX:52010PC0517

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - Political agreement, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1459841084798&uri=CONSIL:ST_5894_2016_INIT

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), CELEX:52010PC0521/ES

Protopopescu, D. (2013). Theories of terminology – past and present. In *Studii şi cercetări de onomastică şi lexicologie SCOL,* 6(1-2), pp. 195-201. http://cis01.central.ucv.ro/revista_scol/site_ro/2013/LEXICOLIGIE/PROTOPOPESCU.pdf

Putten, F.P. van der, Meijnders, M. & Rood, J. (2015). *Afschrikking als veiligheidsconcept tegen niet-traditionele dreigingen.* Netherlands Institute of International Relations Clingendael. http://www.clingendael.nl/sites/default/files/Clingendael_monitor_2015_deel_2.pdf

Qué es el CERTuy, (18 de febrero 2013). Centro de Respuesta a Incidentes de Seguridad Informática del Uruguay. https://www.cert.uy/inicio/institucional/que_es_el_cert/

Qinetiq. (2014). *Command & Control: Understanding, denying, detecting.* http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-cc_qinetiq_report.pdf

Radio 1, 01.12.2010, "Wie is Yuliya? De ontknoping", http://www.radio1.be/programmas/peeters-pichal/wie-yuliya-ontknoping

Ramírez, Y.A. (2013). Extracción de datos para clasificación y filtrado de IPS falsas en ataques ddos. Universidad Nacional Abierta y a Distancia (UNAD). http://hdl.handle.net/10596/1610

Ramteke, A.S. (2008). Decision support systems – Risk assessment & asset valuation. In *Proceedings of the 2nd National Conference, INDIACom*. http://www.bvicam.ac.in/news/INDIACom%202008%20Proceedings/pdfs/papers/201.pdf

Rangan, A. (2015). *Perspectivas del director de innovación y tecnologías de información (CIIO): Protocolo de respuesta a incidentes de la ICANN.* https://www.icann.org/news/blog/perspectivas-del-director-de-innovacion-y-tecnologias-de-informacion-ciio-protocolo-de-respuesta-a-incidentes-de-la-icann

Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología, CELEX:32001H0703(01)/ES

REDCEDIA, Red Nacional de Investigación y Educación del Ecuador (6 de abril 2016). Quiénes somos. https://csirt.cedia.org.ec/quienes-somos/

Reglamento (UE) n ° 513/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014 , por el que se establece, como parte del Fondo de Seguridad Interior, el instrumento de apoyo financiero a la cooperación policial, la prevención y la lucha contra la delincuencia, y la gestión de crisis y por el que se deroga la Decisión 2007/125/JAI del Consejo, CELEX:32014R0513/ES

Reglamento (UE) n ° 230/2014 del Parlamento Europeo y del Consejo, de 11 de marzo de 2014 , por el que se establece un instrumento en pro de la estabilidad y la paz, CELEX:32014R0230/ES

Reglamento (UE) n o 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013 , relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n o 460/2004 Texto pertinente a efectos del EEE, CELEX:32013R0526/ES

Reglamento de Ejecución (UE) n o 1179/2011 de la Comisión, de 17 de noviembre de 2011 , por el que se establecen especificaciones técnicas para sistemas de recogida a través de páginas web, de conformidad con el Reglamento (UE) n o 211/2011 del Parlamento Europeo y del Consejo sobre la iniciativa ciudadana, CELEX:32011R1179/ES

Reglamento (UE) n ° 611/2013 de la Comisión, de 24 de junio de 2013 , relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, CELEX:32013R0611/ES

Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA, CELEX:32014R0513

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, CELEX:32014R0910

Reijerman, D. (2007). IETF schaart zich achter DomainKeys. In Tweakers. http://tweakers.net/nieuws/47661/ietf-schaart-zich-achter-domainkeys.html

Reijnders, M. (2001). Ondertekening omstreden cybercrimeverdrag. In *Webwereld*. http://webwereld.nl/overheid/6309-ondertekening-omstreden-cybercrimeverdrag

Reijnders, M. (2003). Voor de rechter? Geef je pc de schuld. In *Webwereld.* http://webwereld.nl/overheid/13121-voor-de-rechter-geef-je-pc-de-schuld

Report From The Commission To The Council And The European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC), CELEX:52011DC0225

Richardson, R. (2008). *CSI Computer Crime & Security Survey*. CSI. http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf

Riemeijer, M. (2013). R.S.P., répondre… In SyntheHis, *2*(12). http://download.springer.com/static/pdf/726/art%253A10.1007%252Fs12494-013-0033-4.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs12494-013-0033-4&token2=exp=1460727872~acl=%2Fstatic%2Fpdf%2F726%2

Rijksoverheid NL, Actueel, Hogere straffen voor computerdelicten, 10.02.2014, https://www.rijksoverheid.nl/actueel/nieuws/2014/02/10/hogere-straffen-voor-computerdelicten

Rochford, O. (2004). Hacken voor dummies. Pearson Eduction, p. 230. https://books.google.be/books?id=mlu5cWlXRggC&pg=PA230&lpg=PA230&dq=%22distributed+denial+of+service-aanval%22&source=bl&ots=Jldz6O-Ikv&sig=nBBjlXeF8rzOiH1kl8BwxfmTeho&hl=nl&sa=X&ved=0ahUKEwi28Izn3pDMAhVtb5oKHZZgC-QQ6AEILTAD#v=onepage&q=%22distributed%20denial%20of%20service-aanval%22&f=false

Rodríguez, N. (2016). *Anonymous hackea información personal de Trump*. Baquia. http://www.baquia.com/seguridad/anonymous-hackea-donald-trump

Rodríguez Leal, D. (2016). *Se identifica una nueva versión del troyano bancario Tinba: Tinbapore*. Globb Security. http://globbsecurity.com/se-identifica-nueva-version-troyano-tinba-llamada-tinbapore-37547/

Rojas, J.A. & Manta, H.C. (2011). Sistemas detectores de intrusos y análisis de funcionamiento del proyecto de código abierto snort. En Redes de Ingeniería, *2*(1), pp. 100-112. http://revistas.udistrital.edu.co/ojs/index.php/REDES/article/view/7187

Rollason-Reese, R.L. (2003). Incident handling: an orderly response to unexpected events. In *SIGUCCS '03 Proceedings of the 31st annual ACM SIGUCCS fall conference*, pp. 97-102. http://delivery.acm.org/10.1145/950000/947496/p97-rollason-reese.pdf?ip=157.193.5.27&id=947496&acc=ACTIVE%20SERVICE&key=D7FC43CABE88BEAA%2EF15FE2ACB4878E3D%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=597597845&CFTOKEN=85578271&__acm__=1459861371_d9a373b2e62b1d4be4a40197c266af86

Ross, B., et al. (2005). Stronger password authentication using browser extensions. In *Unisex Security*. https://www.usenix.org/legacy/events/sec05/tech/full_papers/ross/ross_html/

Rouse, M. (2005). *Hashing.* TechTarget. http://searchsqlserver.techtarget.com/definition/hashing

Rouse, M. (2007). *Steganography.* TechTarget. SearchSecurity. http://searchsecurity.techtarget.com/definition/steganography

Rouse, M. (2008). *Zombie (bot).* TechTarget. Search Midmarket security. http://searchmidmarketsecurity.techtarget.com/definition/zombie

Rouse, M. (2012). Ataque de denegación de servicio (DDoS). TechTarget. SearchDataCenter en Español. http://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

Rouse, M. (2013). *distributed denial-of-service attack (DDoS).* TechTarget. SearchSecurity. http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

Ruiz de Gopegui, C.B. (2015). *Aparecen aplicaciones infectadas por XcodeGhost en la App Store.* Faq-Maq. http://www.faq-mac.com/2015/09/aparecen-aplicaciones-infectadas-por-xcodeghost-en-la-app-store/

Rustici, R.M. (2012). *Armas Cibernéticas: La igualdad de condiciones a nivel internacional.* Military review. http://usacac.army.mil/CAC2/MilitaryReview/Archives/Spanish/MilitaryReview_20120831_art006SPA.pdf

Samenstellingen – bijzondere gevallen met een koppelteken. In *Woordenlijst.org*, http://woordenlijst.org/leidraad/6/3

Samuel, A.W. (2004). *Hacktivism and the future of political participation*. Harvard University. http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

Sanchez, F., Duan, Z. & Dong, Y. (2012). Blocking spam by separating end-user machines from legitimate mail server machines. In *Security and Communications Networks*, *9*(4), pp. 316-326. http://onlinelibrary.wiley.com/doi/10.1002/sec.587/epdf

Sánchez, D. (2016). Ciberseguridad judicial y sellado de tiempo. En *Red seguridad*, (72), pp. 52-53. http://didacsanchez.com/docs/ciberseguridad.pdf

SANS institute. (2001). *Computer Incident Response Team*. https://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641

Santanna, J.J. & Sperotto, A. (2014). Characterizing and mitigating the DDoS-as-a-Service phenomenon. In *Monitoring and Securing Virtualized Networks and Services*, pp. 74-78. http://download.springer.com/static/pdf/392/bok%253A978-3-662-43862-6.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-3-662-43862-6&token2=exp=1460892656~acl=%2Fstatic%2Fpdf

Santanna, J. J., et al. (2015). Booters—An analysis of DDoS-as-a-service attacks. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 243-251. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7140298

San Juan, C., Vozmediano, L. & Vergara, A. (2009). Miedo al delito en contextos digitales: un estudio con población urbana. En *Eguzkilore*, *23*, pp. 175-190. https://www.researchgate.net/profile/Laura_Vozmediano/publication/236333869_Miedo_al_delito_en_contextos_digitales_Un_estudio_con_poblacin_urbana/links/0a85e530c52771b6e9000000.pdf

Schaap, R. & Bak, E. den (2013). CSIRT vanuit een IT-audit perspectief. De IT-auditor. https://www.deitauditor.nl/wp-content/uploads/2014/09/0000027044_CSIRTperspectief.pdf

Scheepers, J. (2007). *Veelbelovende antispantechniek wordt standaard.* ZDNet. http://www.zdnet.be/article/68558/veelbelovende-antispamtechniek-wordt-standaard/

Schless, T. (2013). De organisatie van botnetbestrijding in Nederland. http://dspace.ou.nl/bitstream/1820/5052/1/INF_20130910_Schless.pdf

Schoofs, P. (2014). *Phishing bij de overheid in België*. Masterscriptie, Open Universiteit Nederland. http://dspace.learningnetworks.org/bitstream/1820/5691/1/INF_20141209_Schoofs.pdf

Schriftelijke vraag E-2319/04 van Konstantinos Hatzidakis (PPE-DE) aan de Commissie. Bestrijding van e-criminaliteit in de EU, CELEX:92004E002319/NL

Schriftelijke vragen met antwoord. Lijst van schriftelijke vragen van leden van het Europees Parlement met aanduiding van vraagnummer, originele taal, auteur, fractie, aangeschreven instelling, datum van indiening en onderwerp, CELEX:C2006/125/01/NL

Schriftelijke vraag nr. 2667/98 van Gerhard HAGER aan dee Raad. High-tech-criminaliteit, CELEX:91998E002667/NL

Schriftelijke vraag P-2822/00 van W.G. van Velzen (PPE-DE) aan de Raad. Cerditcardfraude op het internet, CELEX:92000E002822/NL

Securemx (9 julio 2014). DDoser's, Booters y Stressers… https://securemx.wordpress.com/category/ddos/

Security Geek, (31 juli 2009). Top 5 tips bij worm uitbraken. https://securitygeeknl.wordpress.com/2009/07/31/top-5-tips-bij-worm-uitbraken/

Seminario ciberseguridad y delitos informáticos. (2014). Escuela Europea de Ciencias de la Seguridad. http://www.eecs.es/cursos-con-la-universidad-rey-juan-carlos/seminario-sobre-crimen-organizado/

Seo, S. et al. (2014). Detecting mobile malware threats to homeland security through static analysis. In *Journal of Network and Computer Applications*, *38*, pp. 43-53. http://ac.els-cdn.com/S1084804513001227/1-s2.0-S1084804513001227-main.pdf?_tid=31d33016-f366-11e5-9b0d-00000aab0f02&acdnat=1459005775_408cba6e1f212f23a5ba59748b00b8b4

Shapira, I. & Warrick, J. (2010). *WikiLeaks' advocates are wreaking 'hacktivism'*. The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121102897.html?wprss=rss_metro

Silva, D. (2014). *Gevallen engel.* Meulenhoff Boekerij B.V. https://books.google.be/books?id=BBMPAwAAQBAJ&pg=PT191&lpg=PT191&dq=%22steganografie%22&source=bl&ots=yGDIMmBLXx&sig=yI9BW-2JF04ukboF5gah-zgNtlg&hl=nl&sa=X&ved=0ahUKEwjK94aYv5rMAhWDWhoKHbeiCMk4PBDoAQgbMAA#v=onepage&q=%22steganografie%22&f=false

Skoudis, E. (2003). Hiding data in executables: stego and polymorphism. In *Malware: Fighting Malicious Code.* http://www.informit.com/articles/article.aspx?p=102181&seqNum=6

Smith, D. (1994). *Forming an incident response team*. University of Queensland, Brisbane. http://stir.citex.eb.mil.br/Documentacao/Forming%20an%20Incident%20Response%20Team.PDF

Smith, R.G. (2004). Impediments to the successful investigation of transnational high tech crime. In *Trends & Issues in crime and criminal justice, 285*. Australian Institute of Criminology. http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi285.pdf

Sophos. (2013). *Diccionario de amenazas. Amenazas informáticas y para la seguridad de los datos de la A a la Z.* https://www.sophos.com/es-es/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=es-ES.pdf

Sorell, T. (2015). Human rights and hacktivism: The cases of Wikileaks and Anonymous. In *Journal of Human Rights Practice*, *7*(3), pp. 391-410. https://jhrp.oxfordjournals.org/content/early/2015/09/22/jhuman.huv012.full.pdf+html

Steganografie. In Dikke Van Dale Online. http://vandale.ugent.be/

Steganography (s.d.). In *Techopedia.* https://www.techopedia.com/definition/4131/steganography

Stephens, K. (2010). *Malware Command and Control overview*. National Security Cyberspace Institute. http://www.nsci-va.org/WhitePapers/2010-12-30-Malware%20C2%20Overview-Stephens.pdf

Stone-Gross, B., et al. (2011). *The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns*. LEET. http://static.usenix.org/events/leet11/tech/full_papers/Stone-Gross.pdf

Straat, R. (2015). *Digitaal verbonden: een onderzoek naar het idee van verbondenheid binnen het online activisme en hacktivisme.* Universiteit Utrecht. http://dspace.library.uu.nl/handle/1874/324441

Straus, J. (s.d.) Hyphens. http://www.grammarbook.com/punctuation/hyphens.asp

Stroud, F. (s.d.). *Booter service.* Webopedia. http://www.webopedia.com/TERM/B/booter_services.html

Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft (11 December 2012). European Commission. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf

Sucuri. (s.d.). Comprenda un ataque de denegación de servicio (DoS / DDoS). https://sucuri.net/es/firewall-de-sitios-web/proteccion-ddos

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. In *Network security*, pp. 16-19. http://ac.els-cdn.com/S1353485811700861/1-s2.0-S1353485811700861-main.pdf?_tid=1865d6b4-f367-11e5-96b3-00000aab0f6b&acdnat=1459006162_1a75d40c546c50d333b0d371a8981e2c

Tejada, E.C. (2015). *Gestión de incidentes de seguridad informática*. IC Editorial. https://books.google.be/books?id=y63KCQAAQBAJ&pg=PT142&lpg=PT142&dq=%22equipo+de+respuesta+a+incidentes+de+seguridad+inform%C3%A1tica%22&source=bl&ots=zmDDvaGbgQ&sig=8Jcl43MfhrfAImreissm8d1kthQ&hl=nl&sa=X&ved=0ahUKEwio5ry8qfrLAhXBlg8KHd3qCjIQ6AEIVDAH#v=onepage&q=%22equipo%20de%20respuesta%20a%20incidentes%20de%20seguridad%20inform%C3%A1tica%22&f=false

Terminology coordination. *About IATE*. (s.d.). European Parliament. http://termcoord.eu/iate/about-iate/

The cybercrime legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law (Contribution to the Commonwealth Working Group on Cybercrime), Council of Europe/Data Protection and Cybercrime Division, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e4

Thilagavathi, M.S. & Saradha, A.A.(2014). Survey of protection against DoS & DDoS Attacks. In *International Journal Of Computational Engineering Research*, *4*(1). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.588.108&rep=rep1&type=pdf#page=85

Thomas, K. & Nicol, D.M. (2010). The Koobface botnet and the rise of social malware. In *5th International Conference on Malicious and Unwanted Software (MALWARE)*, pp. 63-70. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5665793

Thomas, V. & Jyoti, N. (2007). *Defeating IRC Bots on the internal network*. Virus Bulletin. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.2058&rep=rep1&type=pdf

Top 10 Stressers-Booters-DDoSers (2014). http://top10stressers.com/

Tyugu, E. (2012). Command and control of cyber weapons. In *4th International Conference on Cyber Conflict (CYCON)*, pp. 1-11. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6243984

Uitvoeringsverordening (EU) nr. 1179/2011 van de Commissie van 17 november 2011 tot vaststelling van technische specificaties voor systemen voor het online verzamelen van steunbetuigingen overeenkomstig Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad over het burgerinitiatief, CELEX:32011R1179/NL

Unión Internacional de Telecomunicaciones: El ciberdelito - Guía para los países en desarrollo, http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

United Nations (2005). Computer-related crime. The Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, Thailand. http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf

Vallabhaneni, S.R. (2008). Corporate management, governance, and ethics best practices. John Wiley & Sons, p. 332. https://books.google.be/books?id=BvYbQr9MV_sC&pg=PA332&lpg=PA332&dq=%22Computer+incident+response+capability%22+-nato+-federal&source=bl&ots=7g9bBPL-4k&sig=DSiSbCycypTOHUSwe2iQcvQ-dXc&hl=nl&sa=X&ved=0ahUKEwio_YekyPzLAhWB-w4KHRogD3IQ6AEIOTAE#v=onepage&q=%22Computer%20incident%20response%20capability%22%20-nato%20-federal&f=false

Valls-Prieto, J. (2014). Chapter 10: Fighting Cybercrime and Protecting Privacy: DDoS, Spy Software, and Online Attacks. Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance. IGI Global, p. 147. https://books.google.be/books?hl=nl&lr=lang_en&id=uxqXBQAAQBAJ&oi=fnd&pg=PA146&dq=%22zombies%22+%22cybercrime%22&ots=p5dsXYa5Ng&sig=amqaPoV_SICOFMoBIBj3Imh0iCM#v=onepage&q=%22zombies%22%20&f=false

Vandewaetere, S. (2014). EU-terminology: languages united in diversity? A case-study of Dutch EU texts on education. In *MODERNE SPRACHEN*, 57(1), pp. 7-21. https://biblio.ugent.be/publication/4265658/file/5872113.pdf

Van den Eynde, S. (2001). Wat archiveren en hoe? Op zoek naar de rol van PKI voor digitale archieven. DAVID. http://www.law.kuleuven.be/citip/en/docs/deliverables/156oaismodel-v2-02f90.pdf

Van Eijk, N.A.N.M., et al. (2010). Op weg naar evenwicht: een onderzoek naar zorgplichten op het internet. Universiteit van Amsterdam. http://dare.uva.nl/document/2/95925

Vanlouwe, K. (2012). *Voorstel van resolutie ter beveiliging van elektronische informatie en bescherming tegen cyberaanvallen.* Belgische Senaat. S-1855/1. https://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=83893361&LANG=nl

Van Poucke, K. (2002). *"Cybercrime": analyse en evaluatie van Belgische regelgeving.* Master's thesis, Universiteit Gent. http://www.ethesis.net/cybercrime/cybercrime.pdf

Venosa, P. & Díaz, F.J. (2014). Detección de botnets utilizando herramientas open source. En *XVI Workshop de Investigadores en Ciencias de la Computación*, pp. 832-836. http://sedici.unlp.edu.ar/bitstream/handle/10915/43275/Documento_completo.pdf?sequence=1

Verhaeghe, K. (2012). *Opsporing en vervolging in cyberspace.* Masterproef, Universiteit Gent. http://www.scriptiebank.be/sites/default/files/webform/scriptie/Masterproef%20Kevin%20Verhaeghe_0.pdf

Vermeulen, G. (2002). *Aspecten van Europees materieel strafrecht*. Antwerpen-Apeldoorn: Maklu, pp. 381-382, 393 en 412. https://books.google.be/books?id=jxL-

yHxX3AgC&printsec=frontcover&hl=nl&source=gbs_ge_summary_r&cad=0#v=onepage&q=definitie&f=false

Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, CELEX:32014R0910/NL

Verordening (EU) nr. 513/2014 van het Europees Parlement en de Raad van 16 april 2014 tot vaststelling, als onderdeel van het Fonds voor interne veiligheid, van het instrument voor financiële steun voor politiële samenwerking, voorkoming en bestrijding van criminaliteit, en crisisbeheer en tot intrekking van Besluit nr. 2007/125/JBZ van de Raad, CELEX:32014R0513/NL

Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie, CELEX:32013R0611/NL

Verslag Van De Commissie Aan De Raad En Het Europees Parlement Evaluatie van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG), CELEX:52011DC0225/NL

Verspoor, D.A. (2014). *Cybersecurity in Nederland*. Masterscriptie, Universiteit van Amsterdam. http://dare.uva.nl/document/556946

Vicente, L. (2004). *¿Movimientos sociales en la Red? Los hacktivistas*. El cotidiano, 20(126). http://www.elcotidianoenlinea.com.mx/pdf/12615.pdf

Villacrés, E.J.F., Molina, M.I.A & Miguez, M.B. (2014). *Ciberdelincuencia un mal que afecta a la sociedad actual.* Eumed. http://www.eumed.net/rev/cccss/29/ciberdelincuencia.pdf

Virtual Security. (2016). *Bestrijd ATP's*. http://www.virtualsecurity.nl/oplossingen/bestrijd-atp-s

Virumbrales de Rojas, A. (2015). *Regulación penal de la delincuencia informática. Especial referencia a la reforma del Código Penal en materia de ciberdelincuencia tras la Ley Orgánica 1/2015, de 30 de marzo.* Universidad de Valladolid. https://uvadoc.uva.es/handle/10324/13740

Voorstel voor een Richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad SEC(2010) 1122 final} SEC(2010) 1123 final}, CELEX:52010PC0517/NL

Voorstel voor een Verordening van het Europees Parlement en de Raad Inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), CELEX:52010PC0521/NL

Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende het Agentschap van de Europese Unie voor samenwerking en opleiding op het gebied van rechtshandhaving (Europol) en tot intrekking van Besluiten 2009/371/JBZ en 2005/681/JBZ, CELEX:52013PC0173/NL

VS waarschuwt voor 30 meest aangevallen lekken op internet, (29.04.2015). Security.nl. https://www.security.nl/posting/426683/VS+waarschuwt+voor+30+meest+aangevallen+lekken+op+internet

Walden, I. (2003). Computer crime. In *computer law.* http://kavehh.com/my%20Document/KCL/Internet%20Law/Internet%20Material/Computer%2520Crime%2520%25286th%2520ed.%2529.pdf

Wang, S. & Kao, D. (2006). Internet forensics on the basis of evidence gathering with Peep attacks. In *Computer Standards & Interfaces*, *29*(4), pp. 423-429. http://ac.els-cdn.com/S0920548906000791/1-s2.0-S0920548906000791-main.pdf?_tid=c5c3b58a-0099-11e6-b0f2-00000aab0f02&acdnat=1460457293_a36cc9dd9ca50be5a23c44ace8d19d60

Wat is anti-DDoS protectie? (s.d.). OVH. https://www.ovh.nl/anti-ddos/anti-ddos-principe.xml

Weeteling, D. (2012). *Adaptiviteit & botnets*. Universiteit Utrecht. http://dspace.library.uu.nl/handle/1874/288926

Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II) https://www.eerstekamer.nl/wetsvoorstel/26671_computercriminaliteit_ii

West-Brown, M.J., et al. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs).* Carnegie Mellon Software Engineering Institute. http://www.sei.cmu.edu/reports/03hb002.pdf

What is a CSIRT? (s.d.). Enisa. https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

Wikipedia, onder "Informatiebeveiliging", https://nl.wikipedia.org/wiki/Informatiebeveiliging

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. In *Information and organization, 16*(4), pp. 304-324. http://ac.els-cdn.com/S1471772706000224/1-s2.0-S1471772706000224-main.pdf?_tid=8bb681fc-f68e-11e5-b30b-00000aacb361&acdnat=1459352959_90f09f7466b82359b80d4624308fb861

Wilsem, J. van, (2010). Digitale en traditionele bedreiging vergeleken: Een studie naar risicofactoren van slachtofferschap. In *Tijdschrift voor Criminologie*, *52*(1), pp. 73-87. http://search.proquest.com/docview/883050102?pq-origsite=gscholar

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress.* Library of congress Washington DC congressional research service. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA477642

Wood, P., Gutierrez, C. & Bagchi, S. (2015). Denial of Service Elusion (DoSE): Keeping clients connected for less. In 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), pp. 94-103. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7371572

Written question E-002494/14 Sergio Paolo Francesco Silvestris (PPE) to the Commission. New software to deter digital crime, CELEX:92014E002494

Yong, W., Tefera, S.H. & Beshah, Y.K. (2012). Understanding botnet: From mathematical modelling to integrated detection and mitigation framework. In *Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD)*, pp. 63-70. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6299259

Zhao, D., et al. (2013). Botnet detection based on traffic behavior analysis and flow intervals. In *Computers & Security*, *39*, pp. 2-16. http://ac.els-cdn.com/S0167404813000837/1-s2.0-S0167404813000837-main.pdf?_tid=343668fe-f2b8-11e5-8236-00000aab0f27&acdnat=1458931047_38a91de0dc76952f33ea78325f834fe0

Zombi. Diccionario panhispánico de dudas. Real Academia Española (RAE). http://lema.rae.es/dpd/?key=zombie

Zuñiga, A.R.R & Jatuun, M.G. (2015). Passing the buck: outsourcing incident response management. In *IEEE 7th International Conference on Cloud Computing Technology and Science,* pp. 503-508. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7396204

Zunzunegui, I.J.S. (2008). El Ciberterrorismo: una perspectiva legal y judicial. En *Eguzkilore,* (22), pp. 169-187. http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

(2014/188/EU): Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement (notified under document C(2014) 2120), CELEX:32014D0188

(2014/188/EU): Uitvoeringsbesluit van de Commissie van 3 april 2014 betreffende de identificatie van technische ICT-specificaties die in aanmerking kunnen komen om te dienen als referentie in openbare aanbestedingen (Kennisgeving geschied onder nummer C(2014) 2120), CELEX:32014D0188/NL

(2014/188/UE): Decisión de Ejecución de la Comisión, de 3 de abril de 2014 , sobre la identificación de especificaciones técnicas TIC que se puedan usar como referencia en la contratación pública [notificada con el número C(2014) 2120], CELEX:32014D0188/ES