Computing For Cybercrime Threat Intelligence: a Systematic Multi-Vocal Literature Review

GIUSEPPE CASCAVILLA*, Jheronimus Academy of Data Science, Netherlands
DAMIAN A. TAMBURRI, Jheronimus Academy of Data Science, Netherlands
WILLEM-JAN VAN DEN HEUVEL, Jheronimus Academy of Data Science, Netherlands

Major cybersecurity and threat intelligence analysts agree that Online criminal activity is increasing exponentially. To offer an overview of the techniques and indicators to perform cybercrime detection and threat intelligence over multiple analysis levels (i.e., surface, deep, and darkwebs) we systematically analyse the state of the art in such techniques. We provide (1) a taxonomy of existing methods mapped to (2) an overview of detectable criminal activities as well as (3) an overview of the indicators and risk parameters that can be used for such detection. We conclude that both practitioners and academicians should effectively cooperate to address the emerging field, potentially harnessing a combination of the surveyed techniques.

ACM Reference Format:
Giuseppe Cascavilla, Damian A. Tamburri, and Willem-Jan Van Den Heuvel. 2019. Computing For Cybercrime Threat Intelligence: a Systematic Multi-Vocal Literature Review. *ACM Comput. Surv.* 9, 4, Article 39 (March 2019), 23 pages. https://doi.org/0000001.0000001

1 INTRODUCTION

1.1 Vision and Scope

Techopedia[1] defines Cybercrime as "[...] a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers". As a large-scale phenomenon, Cybercrime hit the headlines in 2017, with the likes of *WannaCry* crippling the National Health Service in May that year, or the Petya/NotPetya ransomware attack infecting global companies shortly thereafter, with a whole host of data breaches from big companies like Equifax. The year 2018 suffered no better fate, indeed [54]. In total, the figures around the phenomenon [2] are staggering: (a) The global cost of Cyber Crime is estimated to reach $2 trillion by 2019, a threefold increase from the 2015 estimate of $500 billion; (2) The cost per record stolen averages $158; (3) in 2018 there were 38% more cyber-incidents

*This is the corresponding author
[1] https://www.techopedia.com/definition/2387/cybercrime
[2] as reported by the InformationAge online media conglomerate.

Authors' addresses: Giuseppe Cascavilla, Jheronimus Academy of Data Science, 's-Hertogenbosch, Netherlands, g.cascavilla@tue.nl; Damian A. Tamburri, Jheronimus Academy of Data Science, Sint Janssingel 92, 's-Hertogenbosch, 5211 DA, Netherlands, d.a.tamburri@tue.nl; Willem-Jan Van Den Heuvel, Jheronimus Academy of Data Science, Sint Janssingel 92, 's-Hertogenbosch, 5211 DA, Netherlands, w.j.a.m.v.d.heuvel@jads.nl.

Manuscript submitted to ACM

than the previous year; (4) 48% of crimes are caused with malicious intent — human error or system failure account for the rest.

At the same time, *threat intelligence* is the discipline whose intent is that of providing organized, analyzed, and refined information about potential or current attacks that threaten an organization, including governments, non-governmental organizations, and more [59].

In this paper we aim at providing a synthesis of the state of the art in *cybercrime* threat intelligence, accounting for both grey and white literature on the matter with a systematic *multi-vocal* literature review [23, 37].

Our results provide a clear overview of most if not all the topics, approaches, indicators, risks, fallacies, and pitfalls around the phenomenon. Our end goal is offering such an overview to encourage analysis, synthesis, and avoidance of the risks connected to cybercrime, starting from techniques existing in the state of the art. The impact of these results is considerable for both practitioners and academicians. On one hand, practitioners may benefit from our results in that they offer indicators, techniques, and tools that help avoiding the damage connected to the phenomenon; on the other hand, the synthesis offered in the following pages offers a starting basis to study the cybercrime phenomenon in deeper detail.

1.2 Approach and Major Contributions

- overview of research questions with one line of methods to address each one
- major contributions outline, with one line to explain the contribution, the intended user and practical impact

1.3 Structure of The Paper

The rest of this paper is organized as follows. First, Sec. 2 outlines the background terms and definitions as well as outlining related work. Further on, Sec. 3 elaborates on the research design behind this study. Subsequently, Sec. 4 outlines the results while Sec. 5 discusses them in context. Finally, Sec. 6 concludes the paper.

to finish with the paragraphs

2 BACKGROUND AND RELATED WORK

To the best of our knowledge, this is the first systematic literature review providing a taxonomy about the different type of cybercrime and threat intelligence solutions. However, in the following paragraph, we are discussing some papers that provide a partial overview of threat intelligence rather than cybercrime risks or guidance note in order to assist to address the problem posed by cybercrime. In the online literature there are no surveys trying to create a general overview of the cybersecurity risks and the proposed solutions in order to contain the risks. Our systematic literature review analyses the state of the art of the upcoming cybersecurity risks and the proposed countermeasures today available. Due to the novelty of the cybersecurity threats and the lack of technologies available to fight the cyber attacks, we will examine also sources from the web like blogs and news, in order to have a broader point of view on the new cybercrime trends.

2.1 Terms and Definitions

we need to add references to each of the elements in the table 1 and also link the table somewhere in the text... else it is dangling! Furthermore, why these terms? we should explain the selection

Table 1 lists all the terms and the related definitions used in this study. The table provides on the first column ***Terms*** the list of those terms considered more technical and more cybersecurity related. On the second column ***Definitions*** we provide a short explanation of the terms related to the cybersecurity environment. We provide this table in order to help the reader to better understand the whole work, indeed, some of the listed technical words are used in our

study, meanwhile other terms could be useful in order to have a better background of the cybersecurity problem we are discussing.

2.2 Related Surveys

In a deeply connected world, like the one we are facing nowadays, hackers are constantly finding new targets and refining the tools they use to break through cyberdefenses. Moreover, the lack of privacy and security of the new upcoming technologies and the lack of awareness of the users poses a real threat to our personal life. In the following, we present some works that face the problem of cybersecurity and try to discuss the countermeasures today available.

Tounsi et al. in [59] provide an overview of the open source/free threat intelligence tools and compare their features with those from AlliaCERT TI[3]. Through their analysis, they found that the fast sharing of threat intelligence, as encouraged by any organization in order to cooperate, is not enough to avoid targeted attacks. Moreover, trust is extremely important for companies that are sharing personal information. Another problem is how much data is important to share in order to prevent attacks and cooperate and in which format in order to avoid to lose information. In order to understand which standard is better Tounsi et al. propose their own analysis. Lastly, the work presents a comparison among the best threat intelligence tools dividing them in tools which privilege standardization and automatic analytics and others that focus on high speed requirements.

Furthermore, If Tounsi et al. focus on what is the best way to keep the trust among organizations and at the same time share information about cyber threats, in Toch et al. [58] the authors pose the accent on the type of data required from those cybersecurity systems that are supposed to protect our privacy from prying eyes. The taxonomy suggested in the article shows that almost all cyber-security technological categories require some access to personal sensitive information. This result can offer guidance not only in choosing one technique over another but, more importantly, in designing more privacy-aware cyber-security technologies with little or no compromise with regard to their effectiveness in protecting from cyber attacks.

The studies from above tried to analyze systems and good practices to mitigate the cyber threats, in Chang et al. [11] we have a study regarding the state-of-the-art of web-based malware attacks and how to defense against. The paper starts with a study of the attack model and the vulnerabilities that enable these attacks, then analyzes the current state of the malware problem, lastly investigates the defense mechanisms. As result, the paper gives three categories of approaches in order to analyze, identify, and defend against the web-based malware problem. Each category with advantages and disadvantages and how these approaches complement each other and how they can work together.

An altogether different approach from the previous ones is presented in Xu et al. [63] where the authors analyze network-layer traffic and application-layer websites contents simultaneously in order to detect the malicious web applications at run-time. The currently available approach to detect malicious websites can be classified into two categories: *static approach* and *dynamic approach*. The first approach analyzes URLs and contents the latter uses clients honeypots to analyze run-time behaviours. The results of this approach showed that cross-layer detection can achieve the same detection effectiveness of the dynamic approach, however it resulted to be much more faster than the dynamic one.

In order to understand the rising concern around the cybersecurity problem another important reference is also the *Guidance Note*[4] of the United Nations Office on Drugs and Crime (UNODC) that is a global leader in the fight against illicit drugs and international crime. The guidance note aims at giving an overview about the most common

[3]Managed Security Services Division, AlliaCERT Team, Alliacom, France
[4]Link: https://bit.ly/2BIy0tP

Terms	Definition
Cyber Crime	Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes) [57].
Surface Web	Surface web is the normal web which is visible for all users using internet. The websites in the surface web is indexed by search engines. Google is the great example of search engine.
Deep Web	Deep web is the secret web which is not visible for normal user. The deep web consist of a website or any page on the website which are not indexed by search engines.
Dark Web	Dark Web is illegal to used. The all criminal activities are act upon on dark web. The criminal activities like drugs dealing, killing humans etc. The user can only access it if the user has Tor Browser.
Threat Intelligence	Is an organized, analyzed and refined information about potential or current attacks that threaten an organization. The primary purpose of threat intelligence is helping organizations understand the risks of the most common and severe external threats.
Open Source Intelligence (OSINT)	Is the insight gained from processing and analyzing public data sources such as broadcast TV and radio, social media, and websites. These sources provide data in text, video, image, and audio formats.
Crawler	A crawler is a program that visits Web sites and reads their pages and other information in order to create entries or retrieve data.
Malware	Or "malicious software", is an umbrella term that describes any malicious program or code that is harmful to systems. Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Like the human flu, it interferes with normal functioning.
Distributed Denial of Service (DDoS)	A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.
Watering Hole Attack	A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.
Spoofing	Is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.
Honeypot	A honeypot is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.
Insider Threat	Insider threat is a generic term for a threat to an organization's security or data that comes from within. Such threats are usually attributed to employees or former employees, but may also arise from third parties, including contractors, temporary workers or customers.
Man-in-the-Middle Attack (MITM)	A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party.
Hacktivism	Hacktivism is the act of hacking a website or computer network in an effort to convey a social or political message. The person who carries out the act of hacktivism is known as a hacktivist.
A	B
A	B

Table 1. Definition of the terms from the survey paper.

cyber security threats today's available. Cybercrimes activities like the online radicalization, or the illicit sales of

pharmaceutical solutions rather then frauds and identity theft are presented and explained in order to outline how UNODC can deliver technical assistance in order to address the problems posed by cybercrime at both regional and national levels. If from scientific literature side we are seeing a huge growing of interest around cybersecurity threats, on the web side we have a lot of blogs and web-pages warning about the new upcoming cybersecurity threats.

Furtheremore, we refer to reports of one of the major companies working in cybersecurity: Kaspersky[5]. On the Kaspersky Threats blog page[6] where the company offers an updated list of the new upcoming cyber threats. More specifically, for example, on the top five worst cybersecurity attacks we have WannaCry and NotPetya/ExPetr two famous ransomware encryptor that use to encrypt the data of the victim user. Stuxnet a worm that targets the types of industrial control systems (ICS) that are commonly used in infrastructure supporting facilities (i.e. power plants, water treatment facilities, gas lines, etc). DarkHotel a spyware in order to conduct targeted phishing attacks using the hotel's Wi-Fi networks. In addition, Mirai is a botnet used to flood the DNS service provider Dyn with requests. The Kaspersky company gives guidelines [17] on how address incident response in order to contain a cybersecurity attack. Kaspersky listed some key-points necessarily for a company to avoid and contain attacks: *(i)* the speed a rapid remediation is key to limiting the costs, *(ii)* proactive protection, *(iii)* presence Of internal specialists. However, in order to have an world wide overview about real time cyber attacks, Kaspersky provided the Cyberthreat Real-Time Map available here https://cybermap.kaspersky.com/ where is possible to see the current cyber attacks around the globe.

Althogether, however, although plenty of white/grey literature exists on the topic, a holistic view over what software, indicators, methods, tools, and approaches to cyber-crime fighting that practitioners and law-enforces can use is still nowhere to be seen. We offer an initial attempt at such a review in the coming pages, for the benefit of practitioners and academicians alike.

Another major company working in cybersecurity is Norton[7]. In [19] a Symanthec employee gives a pictures of cybersecurity threats and the impact they have on the American population. Mobile malware and Third-party app stores seem to be the new concern. Spyware, ransomware, and viruses used to focus on laptop or desktop computer, however since 2017 the malware variants for mobile increased 54 percent. As well, Symantec, found third-party app stores hosted 99.9 percent of discovered mobile malware. From the Symantec report we can read that in 2023 cybercriminals will steal an estimated 33 billion records that might include your name, address, credit card information, or Social Security number. The impact of this identity theft will impact 60 million Americans and the average costs have been estimated in $3.86 million (U.S. dollars) for the companies worldwide and $7.91 million (U.S. dollars) for the U.S. company. Our survey study try to create an overview among cyberthreats providing a taxonomy of the current criminal activities and complementary we provide on overview of indicators and risks parameters in order to detect cyber crime activities. To the best of our knowledge this is the first systematic literature review on cybersecurity and threat intelligence.

3 RESEARCH MATERIALS AND METHODS

This systematic literature review seeks to address the research problem of providing a clear and detailed overview of the methods and indicators that can be used for cybercrime threat intelligence. Because much work has been conducted and disseminated in non-scientific venues and by non-governmental organisations, we opt for a systematic *multivocal* literature review [25], meaning that both grey and white literature are considered as equal sources of valuable data. In the rest of the section we flesh out the research questions and methods that we employed to attain our results.

[5]Link: https://www.kaspersky.com
[6]Link: https://bit.ly/2AijYiF
[7]Link: https://us.norton.com/

3.1 Research Questions and Approach

To address the aforementioned topic we formulate the following master research question:

MRQ. *what guidelines, methods, and principles exist to establish cyberthreat level of online sources?*

Furthermore, to make the MRQ manageable from a scientific and empirical inquiry perspective, we elaborate further on the master question using the following sub-research questions (SRQs), specifically:

SRQ1. what online depth levels are assessed and to what extent?
SRQ2. what degrees of anonymity exist for web-crawling?
SRQ3. what policies exist to vary the degrees of anonymity?
SRQ4. what website features are most indicative of cyberthreats?
SRQ5. what risk assessment techniques exist?

The SRQs were designed to exhaustively cover the conceptual space reflected by our master research question. More specifically, in terms of SRQ1, we aim at figuring out which analysis techniques exist that cover which level of depth. Furthermore, in the scope of SRQ2 and SRQ3, we aim at understanding the techniques and approaches that would allow a law-enforcer to crawl online sources anonymously and to what extent this phenomenon is understood and addressed in the literature. Beyond that, with SRQ4 and SRQ5, we aim at figuring out which detection and analysis techniques exist and how they can be used, that is, upon which data features [64].

A major intrinsic difficulty of our study is our necessary reliance over what is called *grey* literature [24], intended as materials and research produced by organizations outside of the traditional commercial or academic publishing and distribution channels. Common grey literature publication types include reports (annual, research, technical, project, etc.), working papers, government documents, white papers and evaluations. On the one hand, the use of grey literature is risky since there is often little or no scientific factual representation of data or analyses presented in grey literature itself [20]. On the other hand, a growing interest around using grey literature for computing practitioners' benefit as well as combining it to determine the state of the art and practice around a topic is gaining a considerable interest in many fields [20, 55], including software-related fields [24].

For the scope of this study, and in an effort to maximize its validity, we followed a systematic approach based on the guidelines provided by Petersen et al. [48] for conducting systematic literature reviews in software engineering. We hereby outline such a systematic approach, starting from problem definition and describing the triangulation as well as other inter-rater reliability assessment trials we ran to enforce the validity of our findings.

Grey literature studies can typically be identified by exploiting search strings on search engines, with Google being the most prominent example. Following the guidelines provided by Petersen et al. [48], we identified the search string by structuring them guided by our research questions. More precisely, we defined the search strings based on the PICO terms of our question [36], by exploiting only the terms *Population* and *Intervention*. The keywords were taken from each aspect of a research question. More specifically, the following search query was used:

$$(\texttt{cyber*} \vee \texttt{online*}) \wedge (\texttt{threat*} \vee \texttt{attack*} \vee \texttt{activity*} \vee \texttt{crime*}) \wedge (\texttt{Surface*} \vee \texttt{D*})$$

In the above, the "*" symbol is the star wildcard which matches lexically-related terms (e.g., plurals, verb conjugations).

We exploited the above indicated search strings to look for industrial, government, and non-governmental studies (e.g., blog posts, whitepapers, industry-oriented magazines) that were published since the beginning of the internet until the mid of 2018. The search engines we employed are Google (primary), Bing, Duck Duck Go, Yahoo! and Webopedia. Since engines look for the above indicated search strings over the whole pages they index, our search resulted in a high

Case	Criteria
Inclusion	i_1) The study discusses cybercrime or an application of analysis to the topic. i_2) The study discusses the ramifications and challenges around the topics close to our RQs. i_3) The study reports on direct experiences, opinions or practices on said topics by educated practitioners. i_4) The study refers to a practical case-study of design, development or operation of cybercrime threat intelligence approaches.
Exclusion	e_1) The study does not offer details on design or implementation of practices, methods, tools or indicators for cybercrime threat intelligence. e_2) The study is not referred to industrial cases or other factual evidence. e_3) The benefits or pitfalls of discussed topics are not justified/quantified by the study. e_4) The study does not offer scope and limitations of proposed solutions, frameworks, patterns, tools. e_5)The study does not offer evidence of a practitioner perspective.

Table 2. Inclusion and exclusion criteria for sample selection.

number of irrelevant studies, which were further refined with a secondary search and manual screening, based on the inclusion/exclusion criteria and control factors discussed in the following section.

Similarly, to cover for white literature appropriately, we run the aforementioned query in typical and most common computing literature liberaries, namely: (1) ACM Digital Library; (2) IEEEXplore; (3) Wiley Interscience; (3) Elsevier Scopus; (4) Bibsonomy.

3.2 Sample Selection & Control Factors

Table 2 outlines the inclusion and exclusion criteria adopted in our sample selection. The inclusion criteria ($i_1 - i_4$) were designed to focus explicitly on the kind of practical grey literature that identifies the targets of our study. At the same time, the exclusion criteria permit disqualifying studies that do not offer the necessary design/implementation details (e_1), that refer to nonfactual or unquantifiable evidence (e_2 and e_3), and that do not discuss the limitations and practical impact for the proposed solutions or outlined issues (e_4 and e_5). A study is to be selected if it satisfies *all* the inclusion criteria, while it is to be excluded if it satisfies at lease one of the exclusion criteria.

In addition to the inclusion/exclusion criteria in Table 2, to ensure the quality of the selected grey literature, we selected only those industrial studies that were satisfying the following control factors:

(1) **Practical Experience.** A study is to be selected only if it is written by practitioners with 5+ experience in the topic in object, or if it refers to established threat intelligence solutions with 2+ years of operation.
(2) **Industrial Case-Study.** A study is to be selected only if it refers to at least 1 industrial case-study where a quantifiable number of threat intelligence tools are operated.
(3) **Heterogeneity.** The selected studies reflect at least 5 top industrial domains and markets where threat intelligence tools were successfully applied.
(4) **Implementation Quantity.** The selected studies refer to/show implementation details for the benefits and pitfall they discuss, so that other researchers and practitioners can use them in action.

At the end of our screening, 374 studies were selected based on the inclusion/exclusion criteria and on the additional control factors. The complete list of selected studies is provided online [8].

3.3 Analysis Approach & Inter-Rater Reliability Assessment

To attain the findings we adopted a mixed-methods analysis approach [33].

[8] https://tinyurl.com/ANITAstudysourcesMSLR

3.3.1 Thematic Coding. To address SRQs 1-3 and 5-6, we adopted thematic coding [9] to elicit a baseline understanding of the state of the art. More specifically, The selected sample of articles were subject to annotation and labeling with the goal of identifying themes emerging from the analyzed text. This process of analysis was executed in parallel over two 50% splits of the entire dataset, to ensure avoidance of observer bias. The coders of the two splits (viz., the first two authors of this study) were then inverted and an inter-rater evaluation was enacted between the two emerging lists of themes. To evaluate inter-rater reliability, we adopted the widely known and adopted Krippendorff α coefficient (or Kα), which measures the agreement between two ordered lists of codes applied as part of content analysis [38]. As part of our evaluation, Kα was applied twice.

- We applied the evaluation coefficient to measure the agreement between the two emerging lists of codes by the two independent observers who individually coded 100% of the dataset in 2 rounds. The result of applying Kα to measure the agreement between these two lists amounted to 0.71, slightly lower than the typical reference score of 0.80 (i.e., 80% agreement). A discussion and analysis of disagreement points revealed misalignment between the depth of the coding strategy, which was subsequently addressed; this modification brought the agreement between the emerging lists of codes to Kα = 0.83.
- Kα was them applied again to triangulate the 0.83 score for the final list of themes with its identical counterpart, coded by the third author of this paper, who re-coded the entire dataset with the final coding strategy. The agreement between the final list A (obtained by the first 2 authors) and a final list B (obtained by the third author) was evaluated to Kα = 0.93.

3.3.2 Topic Modelling. To address SRQ4, we operated a machine-assisted topic modelling and analysis exercise supported with a thematic coding. More specifically, we used Latent Dirichlet Allocation (LDA) to provide emerging themes in our textual data, subsequently labelling the emerging themes which are visible and observable characteristics of potential online sources for criminal activity (e.g., darknet websites). The application of LDA was carried out after standard text-mining pre-processing aimed at improving results by removing unnecessary information. Specifically: (1) all terms and definitions for the factors were standardised in terms of structure (i.e., definition + sample text extracted from reference papers); (2) punctuation marks and numbers were removed; (3) all letters were converted to lower case; (4) all common stop words for English grammar and syntax were removed.

For the afore-mentioned topic modelling exercise, we selected log-likelihood as our measure of clustering quality, following typical approaches from the state of the art [2]. In our case, however, the number of clusters started from typically used numbers adopted in the state of the art (k = 10 clusters) but the number was increased until at least one of the newly-emerging clusters contained less than half of the mean population of factors in the previous round. This approach was aimed at allowing the extraction of cybercrime activities and indicators that were meaningful, i.e., they reflected semantic commonalities among factors. In addition, We used the genetic algorithm Differential Evolution to tune LDA hyperparameters alpha and beta as suggested by Agrawal et al. [2]. To conduct all the above pre-processing and analyses we exploited the NetCulator bibliometric analytics tool[9] which supports LDA and a number of similar natural-language analyses and clustering techniques and tools of our own design, featuring Python and the python LDA package.

[9] https://www.netculator.com/

Fig. 1. types of organizations involved in the grey-literature, a majority of public organizations are involved.

4 RESULTS

This section elaborates on our results starting from an overview of a randomly-selected, statistically-relevant subset (i.e., 20% of the total of 374 papers) of the attained data-sources and their statistical distribution over a number of control factors. Subsequently, the section elaborates on findings from the study matching our sub-research questions from the Surface-, Deep- and dark-web perspectives, respectively.

4.1 Dataset Descriptive Statistics

The primary sources we reported offer a diverse statistical distribution over the last 20+ years. Figures from 1 to 3 outline statistical descriptors for the elicited grey literature while Figures 4 to 6 offer a similar insight into white literature. More specifically, Fig. 1 outlines the types of organisations who conducted the research reported in our primary studies, ranging from private corporations (e.g., Kaspersky labs) to public institutions (e.g., non-governmental organizations and boards), who cover for the majority of our sample. Further on, Fig. 2 provides a timeline reflecting a linear increase in interest over the phenomenon between the oldest (2006) and newest (2018) article we analysed while Fig. 3 provides a deeeper insight into the types of evaluations conducted in the grey-literature in question, with a striking majority of experience reports being used as basis for argument.

On the white-literature front, Fig. 4 offers an overview of the types of studies reported in literature, with a majority of case-studies being targeted for further research.

Beyond the types of studies, Figures 5 to 6 offer an overview of the topic interest — which reflects some mixed trends — and the typical venues, with a striking preference for conferences — which are typically more divulgative in nature.

Overall, the statistics offer a not-so-comforting picture. The field seems in an emerging phase, with mixed-feelings or forming interest, typically disseminated in conferences but discussed over case-studies (in white) and/or from experience reports (in grey literature).

Finally, as an overview of the thematic coding that we adopted to elicit answers for our research questions, Fig. 7 offers a quantitative overview of the core concepts discovered as part of our analysis (Definition of codes is provided). The figure highlights that most of the literature we analysed focuses on discussing specific detection *methods* for *criminal activity types*, as opposed to providing holistic methods for the discovery of cybercrime. Moreover, from a quantitative

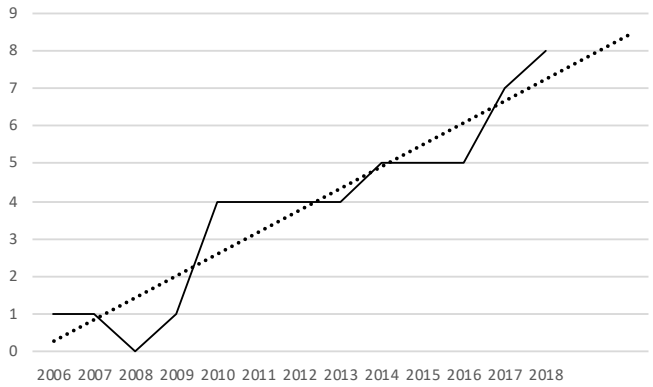


Fig. 2. increase of interest over the topic; a linear increase is reported.

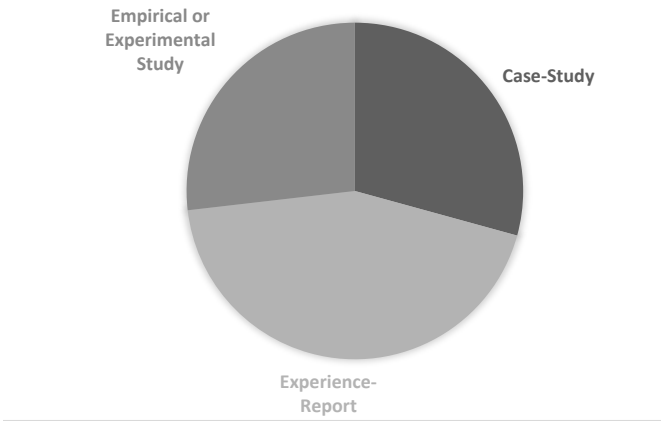


Fig. 3. types of evaluation involved in the grey-literature; experience reports are the striking majority.

perspective, we highlight that *website appearance* and their degree of (software) *security* are major indicators for risk assessment. The next sections offer more detail on the results of our study.

4.2 Cybercrime Threat Intelligence: A Surface-Web Taxonomy

Figure 8 outlines the result of our thematic coding as applied to literature discussing or targeting analyses on the *surface* web only.

The results are articulated using a simple UML-like model structured using the core-concepts (inner-most, white boxes on Fig. 8) emerging from our thematic coding, namely: (a) *assessment methods* — these are the methods, techniques or tools discussed in the state of the art to address cybercrime threat intelligence; (b) *countermeasures* — these are the methods and measures that can limit the damage connected to cybercrime, as discussed in literature; (c) *anonymous crawling policy* — these are the techniques and policies that can limit the detection risk of conducting cybercrime threat intelligence in the open; (d) *risk-level parameters* — these are indicators for increased risk of specific cybercrimes; (e)

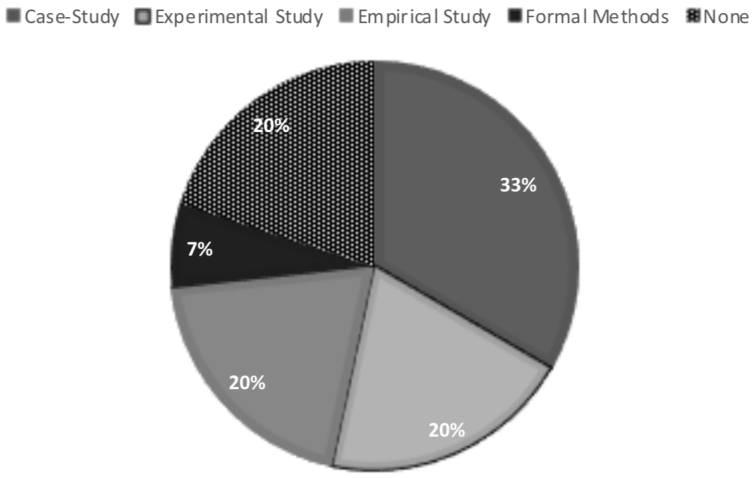


Fig. 4. types of studies conducted in white-literature; case-studies are targeted the most.

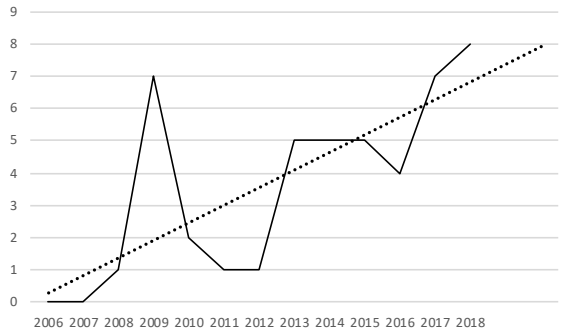


Fig. 5. a linear trend is present in white-literature as well; however, mixed but rising interest is reported over the years.

web-site appearance parameters — these are “hints" that previous research identifies as a certain factor indicating that a web source is hosting a specific criminal activity; (f) *software-quality parameter* — these are software-related quality metrics (e.g., increased throughput or reduced responsiveness) that indicate or are connected to a specific criminal activity being perpetrated; (g) *criminal activity type* — these are the actual criminal activities being carried out.

The outer-most, grey-colored boxes on Fig. 8 outline what we reported from literature, with a frequency cut-off of 3 recurrences over 3 primary studies from *both* grey and white literature, meaning that concepts, techniques, tools and methods discussed less than 3 times and published or discussed before 2018 were not reported for the sake of space.

In the following, we flesh-out the results from Fig. 8 in the same order as the core-concepts were outlined in the text above; resulting concepts appear in *italics* in the descriptive sections. It should be noted that, from this point forward, no distinction is made between grey or white literature to avoid any bias in the exposition of the results.

4.2.1 Assessment Methods. From a policy perspective, literature remarks that the use of *standards and laws* is the single most-used risk assessment method against cybercrime activity; for example, several articles in both grey and white

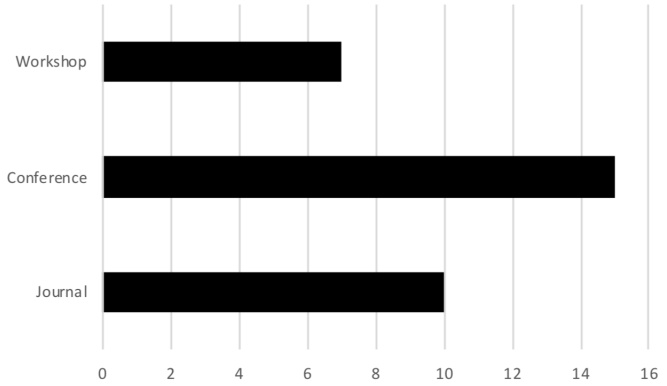


Fig. 6. venues selected for publication; the strong preference for conferences or workshops as opposed to journals reflect an emerging discipline.

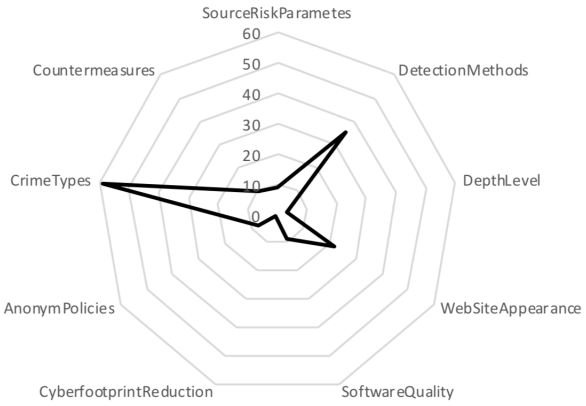


Fig. 7. Count of occurrences for core-concepts across our dataset, normalized on a percentile scale.

literature remark that the Gramm-Leach-Bliley Act (GLBA) [13] or the Fair Credit Reporting Act (FCRA) [32] offer the technical and legal basis to establish the perpetration of online financial crimes of multiple types. In over 30% of our sample, similar legislations (including GDPR in more modern instances) are suggested as tools in their own right to be used against cybercrime of a more shallow and evident nature in the surface web. Furthermore, several experience reports and case-studies elaborate on the use of *limitation of access* or access-control blacklists as a method to establish and limit the involvement with cybercrime. More specifically, tools and approaches such as SquidGuard [10] offer a basis to share and adopt lists of sites hosting criminal activities to be avoided.

From a more technical perspective, *log monitoring* is highlighted as the most obvious cybercrime risk detection and avoidance method. For example, Mataracioglu et al. [43] report on a cybercrime and cybersecurity framework which harnesses log monitoring to detect and avoid social engineering tactics often employed as part of cybercrime. A similar argument is made for the use of log monitoring in several articles from the proceedings of the federated conference

[10] http://squidguard.mesd.k12.or.us/

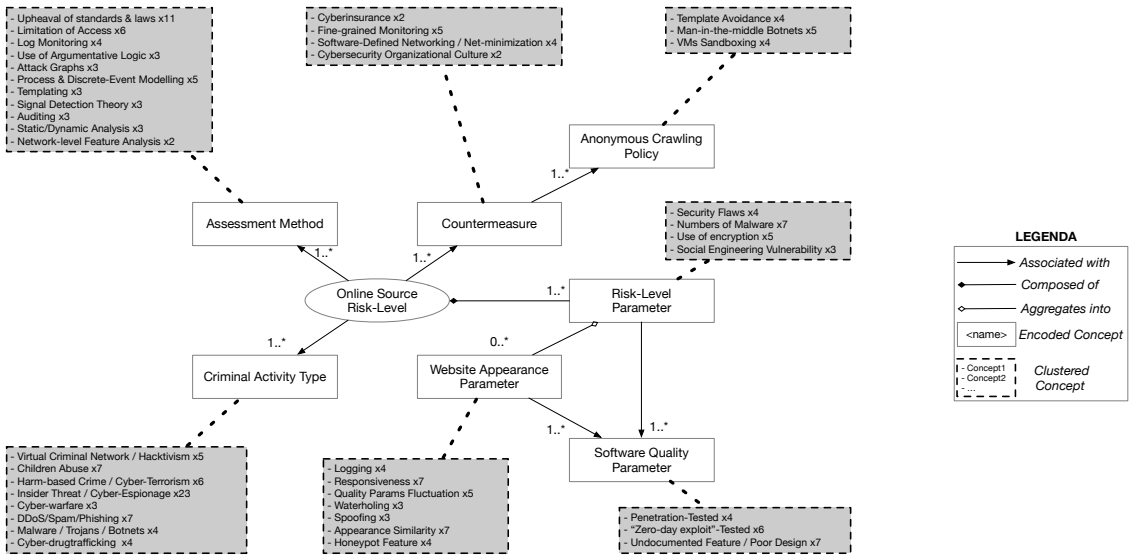


Fig. 8. A taxonomy of cybercrime threat intelligence for the surface web.

on Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance [1]. In these venues, log monitoring is combined with *attack graphs*, a formalism built on top of log monitoring techniques that can elicit social engineering attacks by dissecting the connected social engineering threats and vulnerabilities [5]. Similarly to attack graphs, log monitoring and similar runtime threat detection and avoidance activities combine *process modelling/mining* and *argumentative logic*. For example, Bouyahia et al. [8] introduce a metrics-based technique to assist the detection and avoidance of security threats using reasoning systems which incrementally figure out ongoing attacks — while ontology-based approaches are highlighted in the paper, the authors also remark on the potential to combine a more data-driven machine-intelligence approach.

From a process mining and modelling perspective, the techniques of *discrete event modelling* dating back to '97 and to Harel and Gery seminal work on object state charts [31], to signals-detection theory [28] and signals intelligence [42] applied to *static/dynamic networks traffic analysis*, and ending up with a recent work focusing on terrorist attacks by Gabriels et al. [22].

Overall, on the one hand, the state of the art results as *very* domain-specific (e.g., terrorist attacks [22], insider threats [7]) mostly based on *templating* of crimes — that is, offering a standardized format for the perpetrated crime and matching that format onto available data — and with little generalizable approaches.

On the other hand, the last two approaches we reported as recurrent, namely, *auditing* and *network-level feature analysis* offer theoretical bases for generalisability. More specifically, cybercrime auditing entails providing for strategic checking of organisational and technical infrastructures by randomly selecting a cybercrime type, instrumenting the type and purposefully targeting the organisational and technical infrastructures with it to evaluate the target infrastructures' vulnerability to it [11]. With respect to the auditing technicque highlighted above, Chang et al. [11] offer an in-depth overview of malware-based crimes which is offered as a basis for targeted auditing.

[11] http://m.isaca.org/knowledge-center/research/researchdeliverables/pages/cybercrime-audit-assurance-program.aspx

Finally, with respect to network traffic analysis, several approaches reported in literature offer feature-based (social) network analysis [46] as well as feature engineering and analysis techniques aimed at establishing precursors of social engineering, most notably from our dataset the works by Vidal et al. [61] or Garibi et al. [26].

4.2.2 Countermeasures. As previously specified, with the term *countermeasure* we identify the ability to foresee and enact preemptive or corrective action against a specific cybercriminal activity. On one hand, most of the grey literature highlights the need to conduct business-level impact assessment and incident management, for example, the report of the Australian Government [50] remarks that businesses need to be arrange, quoting from the original document, specific *"actions taken as soon as an attack or breach has occurred to determine the (1) depth of its effect on the business, (2) your ability to recover, and (3) affect the likelihood of future breaches"*. Several proactive actions have been introduced. For example, Baer et al. discuss several approaches to Cyberinsurance [4] and similarly, earlier works by Meland et al. [44] establish the ways in which cyberinsurance actions can be planned as part of corporate governance and towards the reduction of cyberthreats risks.

From a more analytical perspective, several technical countermeasures were proposed, mostly along the lines of fine-grained monitoring of IT assets and business processing; more specifically Ma et al [41], as early as 2012, offer a ightweight framework for monitoring public clouds which is outlined as a potential solution for mitigating cyberthreats, as long as an appropriate incident response organisational structure and culture [12, 56] is also in place whereupon a threat does manifest. Later works offer prototypical solutions where cloud and IT infrastructures monitoring is combined with real-time applications security [15]. Still on a technical perspective, acting as a countermeasure for cybercrime is the use of software-defined networks (SDNs) as well as virtual-networks functions (VNFs), that is, harnesssing with programmable/controllable software the responsibility of handling specific network functions that run on one or more virtual machines. In this specific domain, the survey by Hayward et al. [52] offers an overview of the practices in SDNs which can be used to attain software-controlled granular cybersecurity and safety.

4.2.3 Anonymous Crawling Policies. In terms of maintaining anonymity while performing cybercrime detection or avoidance tasks across an organizational structure, much research has devoted to the use and refinement of Bots and botnets dedicated to detect social engineering attacks or perform anonymous analysis. For example, the works by Lauinger et al. [39] and subsequent trials by the US Chamber of commerce contained in their whitepaper[12] remark that *"an acceptable-use policy for the use of information resources and IT systems [needs] for example, confidential or sensitive business information not to be posted by employees on social networking sites such as Facebook or MySpace [...]"*; the aforementioned actions were experimented upon with the usage of policy-driven bots to perform counterinsurgency of amended actions. Likewise the survey by Chang et al. [11] offers an overview of several approaches along the lines defined above wherefore web-based malware is detected, risk-assessed, avoided using on-purpose, policy-driven botnets.

Finally, in terms of anonymity during detection phases for cybercriminal activity, the use of Virtual-Machine sandboxes is often referred to as the only viable mechanism [11] but several recent works show the endurance of specific attacks or other masqueraded cybecriminal activity such as the S$A and similar shared-cache attacks [3] against a sandboxing approach.

4.2.4 Risk-Level Parameters. This section showcases the few parameters reported in literature which are commonly known to increase the risks of cybercriminal activity being perpetrated in targeted online sources. An outstanding

[12] https://www.uschamber.com/CybersecurityEssentials

number of whitepapers and governmental reports highlight the presence and proliferation of several risk-related parameters; most notably, as noted in the US Chamber of commerce whitepaper about cybercrime[13], "[actions need to be taken to] root out security flaws in computer programs and to counter cyberattacks by "bad" hackers, or cybercriminals", hence indicating the presence and extent of security flaws (of which, the number of Malware is an established minimum, as noted by Rahul et al. [49] and several others [10]) in the code of online sites as a probable factor of risk in establishing high-threat sources. Finally, the haphazard use (or lack thereof) of encryption across online source functions has been established to lead to cybercriminal activity, most notably in the roadmap defined by Kieseberg et al. [35]. More specifically, the lack of encryption is often connected to the use of specific social engineering activities being perpetrated in online sources, which themselves are functional to cybercrime [27]. On this latter front, that of social engineering vulnerabilities specifically designed to accomodate for cybercriminal activity, several authors such as Vidal et al. [61] remark on the necessity to conduct scenario-based situational crime prevention, e.g., using evolutionary computing and social predictive analytics — the work along these lines has mostly concentrated on elaborating more or less complete cyberforensics ontologies for the purpose of knowledge representation and reasoning about cybercriminal investigation in a scenario-based fashion [47].

4.2.5 Software Quality Parameters. The necessity to establish security as a software quality parameter to decide whether an online source bears risk of cybercriminal activity finds agreement in 90% of both grey and white literature alike. More specifically, the quality of software security is established around three axes: (1) whether the online source bear signatures and certificates of successful penetration-testing [21]; (2) whether the online source has been certified against morphisms [29, 40] of known zero-day exploits [6, 18]; (3) finally, whether the online source bears undocumented software features and/or the indications of poor design (e.g., technical debt, etc.) [45].

4.2.6 Website-Appearance Parameters. In terms of website appearance, the literature we analysed identifies seven features as indicative pre-conditions to cybercriminal activity: (1) the lack of logging as well as software features for forward error correction and site responsiveness []; (2) variable responsiveness rates from the online source [] (3) a heavy fluctuation of the overall software quality parameters (e.g., language clarity, documentation, feature stability, etc.) for the online source []; (4) the existence of waterholing features, defined by Trendmico[14] as areas of the site which are uncontrolled, uncontrollable, or never improved overtime by site maintainers [34]; (5) the presence of spoofed information mismatches detectable through online fact-checking []; (6) a high degree of appearance similarity with respect to other known online sources []; (7) finally, honeypot features most predominantly the length and target of the redirection chain upon any navigation request from the source, since almost 68% of our sources from white and grey literature studies observe that malicious landing sites almost always have unusually long redirection chains toward malware distribution sites [11].

4.2.7 Criminal Activity Types. Lastly, the risk assessment of online sources can be supported by focusing the identification of the risk using combined measures of likelihood for reported criminal activity types. This section outlines and discusses all criminal activity types we reported in literature. As previously remarked, we report in this section the crime types reported at least 3 times in at least 3 papers from both grey and white literature (i.e., at least 6 papers in total), later in Sec. 5 we discuss emerging crime activity types reported in more recent literature. Overall, the literature on cyberthreat intelligence focuses around 7 criminal activity types, namely: (1) Virtual Criminal Network / Hacktivism

[13] https://www.uschamber.com/CybersecurityEssentials
[14] https://www.trendmicro.com/vinfo/in/threat-encyclopedia/web-attack/137/watering-hole-101

Groups — these reflect, on the one hand, crime networks dedicated to regular crime activity (e.g., drug trafficking) exploiting online means [] and, on the other hand, forms of cyber-activism (i.e., Hacktivism), where cyber attacks are ideologically motivated and have primarily a demonstrative intent, like damaging the image of the target and/or causing a temporary malfunctioning of the attacked ICT systems []; (2) Children Abuse — these reflect sites exploiting minors for malicious intents and purposes, including and not limited to humans trafficking []; (3) Harm-based Crime / Cyber-Terrorism — these activities are usually ideologically motivated [] exploitations of systems? vulnerabilities with the intent of influencing a state or an international organization []; (4) Insider Threat / Cyber-Espionage — these activities focus on the exploitation of organizational insiders [] for the purpose of information trafficking and intelligence []; oftentimes cyber-espionage is functional to (5) Cyber-warfare — these activities focus on operations carried out in the cyber domain with the purpose of achieving an operational advantage of military significance []; (6) DDoS/Spam/Phishing — similarly to cyber-espionage Distributed Denial of Service, Spam or Phishing criminal activities are connected to crimes against critical infrastructures - for example attacks affecting the integrity of data or information systems used in Supervisory Control and Data Acquisition Systems (SCADA) could be used to overload power grids, block communications and financial transfers, etc; (7) cyber drug-trafficking — these activities focus on the stockade, movement, production, and reselling of illegal substances []

Overall for the above crimes all have been reported in connection to software-based electronic threats, vulnerabilities, and attacks where Malware (including ransomware and similar malware aiming explicitly at financial gains), Trojans, or Botnets play an instrumental knowledge-gathering and insurgency role [].

4.3 Cybercrime Threat Intelligence: A Taxonomy for Deep- and Dark-Web

4.4 Cybercrime Threat Indicators: Topic Modelling Results

In this paragraph we are now going to discuss the results of our Topic Modelling Analysis on our set of papers. We used Latent Dirichlet Allocation (LDA) to highlight the most relevant themes in our textual data, however before applying LDA we pre-processed our text. The pre-processing phase aims at improve our final results and consist of: *i* removal of unwanted chars, numbers and symbols (like words smaller than two chars), *ii* removal of stop-wars, *iii* lemmatization in order to reduce any given word to its root form thereby reducing multiple forms of a word to a single word. After the pre-processing phase we apply LDA method for visualizing and interpreting topics, the method we used is the one described in [53] called **LDAvis** and based on the work of Chuang et. al in [14]. The paper, moreover, gives the instructions to read the diagrams we plotted, however, below continue with a small recap about how to interpret our diagrams. On the left side of our figures we have a recap of our topics, each of the circle represent a topic and how prevalent it is, moreover if the circles are overlapping each other means that those topics have common terms. Into each of this circle are sorted our terms in a decreasing order of prevalence. The right panel of our results depicts a horizontal barchart whose bars represent the individual terms that are the most useful for interpreting the currently selected topic on the left. The overlaid bars represent both the corpus-wide frequency of a given term as well as the topic-specific frequency of the term [14, 53]. The λ slider allows to rank the terms according to term relevance. Moving the slider allows to adjust the rank of terms based on much discriminatory (or "relevant") are for the specific topic, we fixed the λ at 0.8.

suggested value is 0.6, however nothing change with the results

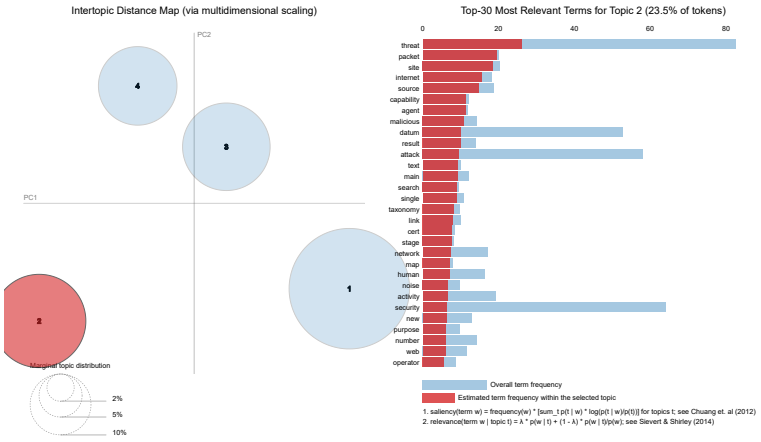
Here below we are now going to discuss our results of our topic modelling analysis. For each analysis in Fig. **??**, Fig. 9 and Fig. 10 we build a table where we summarize and discuss the most relevant terms related to the cybersecurity field.

missed dark and deep web analysis

4.4.1 Topic modelling results for Surface Web. In Table **??** we have the list of words from *Topic 1.*

Terms	Score	
System	26	The system can receive different type of attacks. The operating system of a PC, if not properly maintained, can easily be the target of virus, worm, malware, spyware and other cyberthreat attacks. In order to protect the system of a private user is important to have an antivirus and keep the system updated. In a private company is important to educate the employee to do not use distrusted applications and to use strong passwords in order to protect personal information. An attack to the system can involve a loss of personal data, a destabilization of the running processes of the system and the forward of private information to third parties.
Software	8	Malicious software (MALWARE) is one of the most common cyber threat attack. A MALWARE is any software that does harm to the system, such as a virus or spyware. There are a lot of different versions of MALWARE: virus, trojan, rootkit, worm, spyware and adware, all of them with different characteristics but with the same purpose. The aim of all this malicious software is to steal private information from the victim's PC, profile the habits of the victim user, use the attacked machine as a zombie for network attacks.
Url	8	Url is a unique identifier used to locate a resource on the internet. However, often Url's are used to carry unaware users on distrust websites built in order to steal personal information and banking coordinates and passwords. Url's are spread through emails, gaming platforms from OSN (Online Social Networks), SMS and instant messaging platforms.

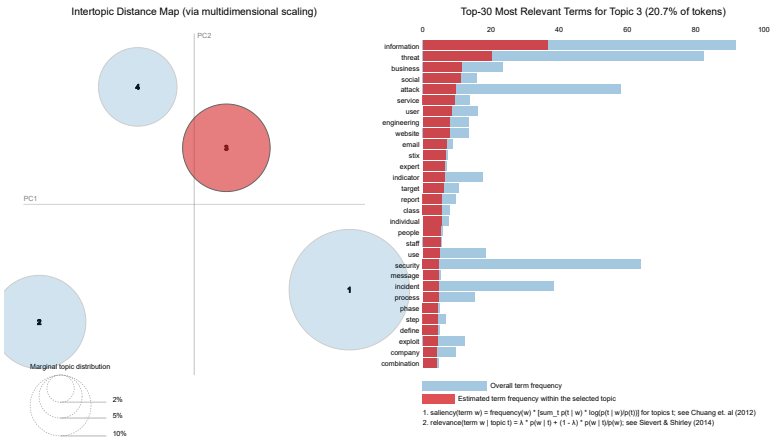
Table 3. Topic analysis results of the second topic for Surface Web.



4.4.2 Topic modelling results for Dark and Deep Web.

Terms	Score	
Process	7	Processes are all the related activities (parts) inside the system that work together to make it function. A compromised process can lead to a unstable system. In order to compromise a process we have different type of attacks, virus, worm, malware, spyware, trojans. All this attacks have as a target the processes of the system in order to change the main functionalities and make them working for the attacker. In order to avoid this type of attacks is extremely important to have an updated system, a proper antivirus installed and a firewall in order to defend the system environment.
Bitcoin	4	Bitcoin is either virtual currency or reference to the technology. You can make transactions by check, wiring, or cash. In the last years we witnessed a huge growth of this king of currency and transactions. As a virtual currency, Bitcoins, can also ensure an high level of anonimity and for that reason is widely used for illegal transactions. In the last year we saw bitcoins used for ask ransom after a cyberattack, their extensively use in Dark and Deep web for illegal trafficking and the adoption of this virtual currency in all those activities that need an high level of anonimity.

Table 4. Topic analysis results of the third topic for Surface Web.



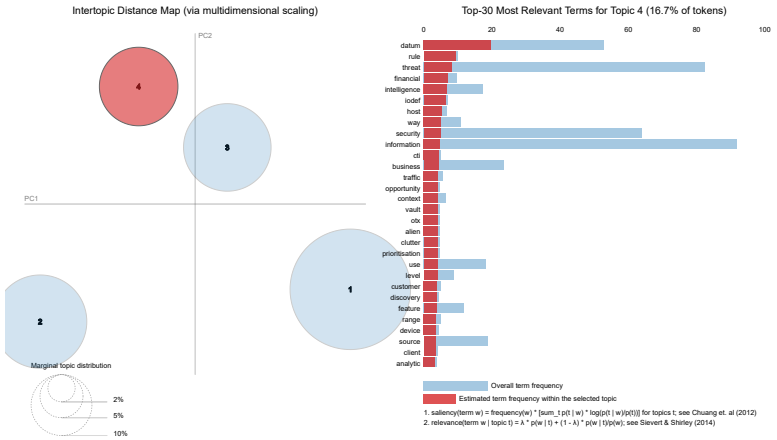
5 DISCUSSION

5.1 Answering our Research Questions

- address each RQ individually (e.g., in a subsubsection?) by stating the RQ and then provide a summary of a response inside a framed box. with a practical impact discussion and target practitioner from academia and elsewhere
- offer an example use of the results in the context of each RQ

5.2 Observations and Lessons Learned

- propose a risk-assessment metric?
- discuss the criminal activity types which were reported in more recent literature?
- elaborate on crime-specific prediction as well as the emerging criminality types from above?



- discuss the sparse community working on the topics and the missed convergence between grey and white literature — offer a descriptive statistic over the community types emerging in the sample and where each result was published to discuss it further.

5.3 Limitations and Threats to Validity

Based on the taxonomy in [62], there are four potential validity threat areas, namely: external, construct, internal, and conclusion validity.

"External Validity" concerns the applicability of the results in a more general context. Since our primary studies are obtained from a large extent of disciplines, our results and observations might be only partially applicable to cyber threat intelligence disciplines, this may threaten external validity. To strengthen external-validity, we organized feedback sessions. We analyzed follow-up discussions and used this qualitative data to fine-tune our research methods, and applicability of our results. In addition, we prepared a bundle of all the raw data, all models drawn, all tables, and everything that we used to compose this paper so as to make it available to all who might want to further their understanding on our data (for links see the Appendix). We hope that this can help in making the results and our observations more explicit and applicable in practice.

"Construct Validity" and *"Internal Validity"* concern the generalizability of the constructs under study, as well as the methods used to study and analyze data (e.g. the types of bias involved). To mitigate these threats, we adopted a mixed-methods research approach. On one hand, a formal grounded-theory method was conceived to avoid bias by construction[16, 30, 60]. On the other hand, we adopted machine-learning and topic modelling techniques which were appropriately fine-tuned using state of the art approaches to the purpose of elaborating the expected results. As previously explained, to ensure internal and construct validity even further, the initial set of codes for grounded-theory was developed by an external researcher and checked against another external reviewer which is not among the authors and not belonging to the software engineering field. In addition we applied grounded-theory in two rounds: (a) first the primary studies were split across a group of students, to apply grounded theory; (b) in the second round one of the authors re-executed a blind grounded-theory on the full primary studies set. When both rounds were finished, both grounded-theories were analyzed evenly to construct a unique theory. When disagreement between the two samples

was found, a session was organized with students researchers and supervisors to examine the samples and check them against literature.

"Conclusion Validity" concerns the degree to which our conclusions are reasonable based on our data. The logical reasoning behind our conclusions are dictated by sound analysis of the data through grounded theory and other analysis methods which try and construct theory from data rather than confirming initial hypotheses, as explained in [30, 51]. Moreover, all the conclusions in this paper were drawn by three researchers and double-checked against data, primary papers or related studies.

6 CONCLUSIONS

This paper provides a Systematic Multi-Vocal Literature Review on the methods, indicators, approaches and techniques previously explored for the purpose of cybercrime threat intelligence, namely, the act of gathering information over, predicting, avoiding, or prosecuting cyber-criminal activities in the surface-, deep-, and dark-webs. More specifically, the attained results provide an overview of the state of the art over (a) what online depth levels are assessed and to what extent; (b) what degrees of anonymity exist for web-crawling; (c) what policies exist to vary the degrees of anonymity; (d) what website features are most indicative of cyberthreats; (e) what risk assessment techniques exist.

Overall, our data, results, and discussions support three conclusions.

First, there is a distinct gap between the grey literature — which mainly discusses reported vulnerabilities as well as organisational/economical/financial consequences of being targeted by cybercriminal activity — and the white research literature — which mainly focuses on offering scattered non-definitive attempts at predicting, avoiding, or protecting against specific criminal-activity types. To address this gap, we discussed our results and the limitations therein, also offering a preliminary formulation of a holistic metric to assess the risk-level that any given online source may be theatre to online criminal activity.

Second, no single community encapsulates cybercrime-fighting software, tools, approaches and techniques, rather, these techniques or their relevant related work is scattered across as many as 30+ domain-specific communities (e.g., software security, data privacy, software engineering, distributed computing, artificial intelligence, and more). In discussing this observation we offered descriptive statistics over our sample in the hope of pointing community leaders in the right direction while fostering cross-fertilisation or community-building.

Third, finally, there is no one definitive solution towards assisting law-enforcement agencies in their cybercrime-fighting activity. A holistic integration effort is advised.

In the future we plan to address the above shortcomings even further, to the extent that, (1) we aim at providing a holistic tool to aid law-enforcers in combatting and prosecuting online criminal activity, (2) we aim at fostering a data-driven, cybercrime-fighting practitioners community and (3) most immediately, we aim at building a tool for large-scale online datasource risk-assessment of criminal activity. We plan to conduct and refine the above activities in the scope of the EU ANITA H2020 project in direct synergy with the law-enforcement practitioners within the ANITA consortium.

ACKNOWLEDGMENTS

The work is supported by the EU H2020 framework programme, grant "ANITA" under Grant No.: and grant "PRoTECT" under Grant No.: .

REFERENCES

[1] 2015. *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance - 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014. Revised Selected Papers.* Lecture Notes in Computer Science, Vol. 8872. Springer.

[2] Amritanshu Agrawal, Wei Fu, and Tim Menzies. 2016. What is Wrong with Topic Modeling? (and How to Fix it Using Search-based SE). *CoRR* abs/1608.08176 (2016). http://dblp.uni-trier.de/db/journals/corr/corr1608.html#AgrawalFM16

[3] Gorka Irazoqui Apecechea, Thomas Eisenbarth, and Berk Sunar. 2015. S$A: A Shared Cache Attack That Works across Cores and Defies VM Sandboxing - and Its Application to AES.. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 591–604.

[4] Walter S. Baer and Andrew Parkinson. 2007. Cyberinsurance in IT Security Management. *IEEE Security & Privacy* 5, 3 (2007), 50–56. http://dblp.uni-trier.de/db/journals/ieeesp/ieeesp5.html#BaerP07

[5] Kristian Beckers, Leanid Krautsevich, and Artsiom Yautsiukhin. 2014. Analysis of Social Engineering Threats with Attack Graphs.. In *DPM/SETOP/QASA (Lecture Notes in Computer Science)*, Joaquín García-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli, and Neeraj Suri (Eds.), Vol. 8872. Springer, 216–232. http://dblp.uni-trier.de/db/conf/esorics/lncs8872.html#BeckersKY14

[6] Leyla Bilge and Tudor Dumitras. 2013. Investigating Zero-Day Attacks. *;login:* 38, 4 (2013). http://dblp.uni-trier.de/db/journals/usenix-login/usenix-login38.html#BilgeD13

[7] Clive Blackwell. 2009. A security architecture to protect against the insider threat from damage, fraud and theft. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW '09)*. ACM, New York, NY, USA, Article 45, 4 pages. https://doi.org/10.1145/1558607.1558659

[8] Tarek Bouyahia, Muhammad Sabir Idrees, Nora Cuppens-Boulahia, Frédéric Cuppens, and Fabien Autrel. 2014. Metric for Security Activities Assisted by Argumentative Logic.. In *DPM/SETOP/QASA (Lecture Notes in Computer Science)*, Joaquín García-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli, and Neeraj Suri (Eds.), Vol. 8872. Springer, 183–197. http://dblp.uni-trier.de/db/conf/esorics/lncs8872.html#BouyahiaICCA14

[9] Jurgen Buder and Ulrike Creß. 2003. Manual or electronic? The role of coding in qualitative data analysis. *Educational Research* 45, 2 (2003), 143–154.

[10] Juan Caballero. 2012. Understanding the Role of Malware in Cybercrime. *ERCIM News* 2012, 90 (2012). http://dblp.uni-trier.de/db/journals/ercim/ercim2012.html#Caballero12

[11] Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West, and Insup Lee. 2013. Analyzing and defending against web-based malware. *ACM Comput. Surv.* 45, 4 (2013), 49:1–49:35. http://dblp.uni-trier.de/db/journals/csur/csur45.html#ChangVWL13

[12] Shuchih Ernest Chang and Chin-Shien Lin. 2007. Exploring organizational culture for information security management. *Industrial Management and Data Systems* 107, 3 (2007), 438–458. http://dblp.uni-trier.de/db/journals/imds/imds107.html#ChangL07

[13] Andrew H. Chen, Kenneth J. Robinson, and Thomas F. Siems. 2004. The wealth effects from a subordinated debt policy: evidence from passage of the Gramm-Leach-Bliley Act. *Review of Financial Economics* 13, 1-2 (2004), 103–119. http://www.sciencedirect.com/science/article/B6W61-48JK7PV-1/1/56667127df9ac7083de3292e49401983

[14] Jason Chuang, Christopher D. Manning, and Jeffrey Heer. 2012. Termite: Visualization Techniques for Assessing Textual Topic Models. In *Proceedings of the International Working Conference on Advanced Visual Interfaces (AVI '12)*. ACM, New York, NY, USA, 74–77. https://doi.org/10.1145/2254556.2254572

[15] Luigi Coppolino, Salvatore D'Antonio, Valerio Formicola, and Luigi Romano. 2014. Real-time Security & Dependability monitoring: Make it a bundle.. In *ICCST*. IEEE, 1–6.

[16] Juliet Corbin and Anselm Strauss. 1990. Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology* 13, 1 (1990), 3–21.

[17] Kaspersky Lab daily. 2018. How to Address Incident Response Challenges. https://bit.ly/2Vd2xca

[18] Melissa Danforth. 2011. WCIS: A Prototype for Detecting Zero-Day Attacks in Web Server Requests.. In *LISA*, Thomas A. Limoncelli and Doug Hughes (Eds.). USENIX Association. http://dblp.uni-trier.de/db/conf/lisa/lisa2011.html#Danforth11

[19] Symantec employee. 2018. 10 cyber security facts and statistics for 2018. https://nr.tn/2pHuWs5

[20] Dominic Farace and Joachim Schöpfel (Eds.). 2010. *Grey literature in library and information studies.* K.G. Saur.

[21] Nilesh Bhingardeve Seeza Franklin. 2018. A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development* 2, 4 (June 2018), 2595–2597. http://www.ijtsrd.com/computer-science/computer-security/15662/a-comparison-study-of-open-source-penetration-testing-tools/nilesh-bhingardeve

[22] Alexander Gabriel, Simon Schleiner, Florian Brauner, Florian Steyer, Verena Gellenbeck, and Ompe AimÃĪ Mudimu. 2017. Process modelling of physical and cyber terrorist attacks on networks of public transportation infrastructure.. In *ISCRAM*, Tina Comes, FrÃĪdÃĪrick BÃĪnaben, Chihab Hanachi, Matthieu Lauras, and AurÃĪlie Montarnal (Eds.). ISCRAM Association. http://dblp.uni-trier.de/db/conf/iscram/iscram2017.html#GabrielSBSGM17

[23] G. Garousi, V. Garousi, M. Moussavi, G. Ruhe, and B. Smith. 2013. Evaluating usage and quality of technical software documentation: an empirical study. In *17th International Conference on Evaluation and Assessment in Software Engineering*. Porto de Galinh, Brazil. http://dl.acm.org/citation.cfm?id=2461003

[24] Vahid Garousi, Michael Felderer, and Mika V. MÃďntylä. 2016. The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature.. In *EASE*, Sarah Beecham, Barbara Kitchenham, and Stephen G. MacDonell (Eds.). ACM, 26:1–26:6.

[25] Vahid Garousi, Michael Felderer, and Mika V. MÃďntylÃď. 2017. Guidelines for including the grey literature and conducting multivocal literature reviews in software engineering. *CoRR* abs/1707.02553. http://dblp.uni-trier.de/db/journals/corr/corr1707.html#GarousiFM17

[26] Wajeb Gharibi. 2012. Some Recommended Protection Technologies for Cyber Crime Based on Social Engineering Techniques – Phishing. *CoRR* abs/1201.0949 (2012). http://dblp.uni-trier.de/db/journals/corr/corr1201.html#abs-1201-0949

[27] Wajeb Gharibi. 2012. Some Recommended Protection Technologies for Cyber Crime Based on Social Engineering Techniques – Phishing. *CoRR* abs/1201.0949 (2012). http://dblp.uni-trier.de/db/journals/corr/corr1201.html#abs-1201-0949

[28] David Marvin Green and John A. Swets. 1989. *Signal Detection Theory and Psychophysics* (reprint ed.). Peninsula Publishers, Los Altos, CA. 521 pages. http://www.amazon.com/Signal-Detection-Theory-Psychophysics-Marvin/dp/0932146236

[29] Deepak Gupta and Rinkle Rani. 2018. Big Data Framework for Zero-Day Malware Detection. *Cybernetics and Systems* 49, 2 (2018), 103–121. http://dblp.uni-trier.de/db/journals/cas/cas49.html#GuptaR18

[30] B.D. Haig. 1995. *Grounded theory as scientific method. Philosophy of education (on-line).* Retrieved on March 2011.

[31] David Harel and Eran Gery. 1997. Executable Object Modeling with Statecharts. *IEEE Computer* 30, 7 (July 1997), 31–42.

[32] Chris Jay Hoofnagle. 2013. How the Fair Credit Reporting Act Regulates Big Data. In *Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet.*

[33] R. Burke Johnson and Anthony J. Onwuegbuzie. 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher* 33, 7 (2004), 14–26. https://doi.org/10.3102/0013189X033007014 arXiv:http://edr.sagepub.com/content/33/7/14.full.pdf+html

[34] Asifullah Khan. 2006. A novel approach to decoding: Exploiting anticipated attack information using genetic programming. *International Journal of Knowledge-Based and Intelligent Engineering Systems* 10, 5 (2006), 337–346. http://iospress.metapress.com/openurl.asp?genre=article&issn=1327-2314&volume=10&issue=5&spage=337

[35] Peter Kieseberg, Olga E. Segou, and Fabio Roli. 2015. CyberROAD: Developing a Roadmap for Research in Cybercrime and Cyberterrorism. *ERCIM News* 2015, 102 (2015). http://dblp.uni-trier.de/db/journals/ercim/ercim2015.html#KiesebergSR15

[36] Barbara Kitchenham and Stuart Charters. 2007. Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01, School of Computer Science and Mathematics, Keele University.

[37] B. Kitchenham, O. Pearlbrereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. 2008. Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology* (November 2008). https://doi.org/10.1016/j.infsof.2008.09.009

[38] Klaus Krippendorff. 2004. *Content Analysis: An Introduction to Its Methodology (second edition).* Sage Publications.

[39] Tobias Lauinger, Veikko Pankakoski, Davide Balzarotti, and Engin Kirda. 2010. Honeybot, Your Man in the Middle for Automated Social Engineering.. In *LEET*, Michael Bailey (Ed.). USENIX Association. http://dblp.uni-trier.de/db/conf/leet/leet2010.html#LauingerPBK10

[40] Zhichun Li, Manan Sanghi, Brian Chavez, Yan Chen, and Ming-Yang Kao. 2006. Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience. In *IEEE06.*

[41] Kun Ma, Runyuan Sun, and Ajith Abraham. 2012. Toward a lightweight framework for monitoring public clouds. In *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on.* IEEE, 361–365.

[42] Meng Ma, Weilan Lin, Disheng Pan, Yangxin Lin, Ping Wang, Yuchen Zhou, and Xiaoxing Liang. 2018. Data and Decision Intelligence for Human-in-the-Loop Cyber-Physical Systems: Reference Model, Recent Progresses and Challenges. *Signal Processing Systems* 90, 8-9 (2018), 1167–1178. http://dblp.uni-trier.de/db/journals/vlsisp/vlsisp90.html#MaLPLWZL18

[43] Tolga Mataracioglu, Sevgi ÃŰzkan, and Ray Hackney. 2015. Towards a Security Lifecycle Model against Social Engineering Attacks: SLM-SEA. *CoRR* abs/1507.02458 (2015). http://dblp.uni-trier.de/db/journals/corr/corr1507.html#MataracioguOH15

[44] Per Håkon Meland, Inger Anne T ønde l, and Bj ørnar Solhaug. 2015. Mitigating Risk with Cyberinsurance. *IEEE Security & Privacy* 13, 6 (2015), 38–43. http://dblp.uni-trier.de/db/journals/ieeesp/ieeesp13.html#MelandTS15

[45] Robert L. Nord, Ipek Ozkaya, Edward J. Schwartz, Forrest Shull, and Rick Kazman. 2016. Can Knowledge of Technical Debt Help Identify Software Vulnerabilities?. In *CSET @ USENIX Security Symposium*, Eric Eide and Mathias Payer (Eds.). USENIX Association. http://dblp.uni-trier.de/db/conf/uss/cset2016.html#NordOSSK16

[46] Sheila O'Riordan, Joseph Feller, and Tadhg Nagle. 2016. A categorisation framework for a feature-level analysis of social network sites. *Journal of Decision Systems* 25, 3 (2016), 244–262. http://dblp.uni-trier.de/db/journals/jds/jds25.html#ORiordanFN16

[47] Heum Park, SunHo Cho, and Hyuk-Chul Kwon. 2009. Cyber Forensics Ontology for Cyber Criminal Investigation.. In *e-Forensics (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering)*, Matthew Sorell (Ed.), Vol. 8. Springer, 160–165. http://dblp.uni-trier.de/db/conf/eforensics/eforensics2009.html#ParkCK09

[48] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. 2008. Systematic Mapping Studies in Software Engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering.* BCS Learning & Development Ltd., 68–77.

[49] Rahul and Sujata. 2018. HOST PROTECTION USING PROCESS WHITE-LISTING,DECEPTION AND REPUTATION SERVICES. *IJIRIS:: International Journal of Innovative Research in Information Security* Volume V, Issue II (February 18 2018), 01–12. https://doi.org/://10.26562/IJIRIS.2018.FBIS10080

[50] Markus Ring, Sarah Wunderlich, Dominik GrÃijdl, Dieter Landes, and Andreas Hotho. 2017. Flow-based benchmark data sets for intrusion detection. In *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS).* ACPI, 361–369.

[51] Craig Schreiber and Kathleen M. Carley. 2004. Going Beyond the Data: Empirical Validation Leading to Grounded Theory. *Computational & Mathematical Organization Theory* 10, 2 (2004), 155–164. http://dblp.uni-trier.de/db/journals/cmot/cmot10.html#SchreiberC04

[52] S. Scott-Hayward, G. O'Callaghan, and S. Sezer. 2013. SDN Security: A Survey. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*. 1–7. https://doi.org/10.1109/SDN4FNS.2013.6702553

[53] Carson Sievert and Kenneth Shirley. 2014. LDAvis: A method for visualizing and interpreting topics. In *Proceedings of the Workshop on Interactive Language Learning, Visualization, and Interfaces*. Association for Computational Linguistics, 63–70. https://doi.org/10.3115/v1/W14-3110

[54] Pablo Casais Solano and Antonio Jose Reinoso Peinado. 2017. Socio-economic factors in cybercrime: Statistical study of the relation between socio-economic factors and cybercrime.. In *CyberSA*. IEEE, 1–4. http://dblp.uni-trier.de/db/conf/cybersa/cybersa2017.html#SolanoP17

[55] Maximilian Stempfhuber, Philipp Schaer, and Wei Shen. 2008. Enhancing Visibility: Integrating Grey Literature in the SOWIPORT Information Cycle. In *Ninth International Conference on Grey Literature: Grey Foundations in Information Landscape (GL-conference series)*.

[56] Mincong Tang, Menggang Li, and Tao Zhang. 2016. The impacts of organizational culture on information security culture: a case study. *Information Technology and Management* 17, 2 (2016), 179–186. http://dblp.uni-trier.de/db/journals/itm/itm17.html#TangLZ16

[57] Techopedia. 2019. Technology Dictionary. https://bit.ly/2w5CXfJ

[58] Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri. 2018. The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Comput. Surv.* 51, 2, Article 36 (Feb. 2018), 27 pages. https://doi.org/10.1145/3172869

[59] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security* 72 (2018), 212–233. http://dblp.uni-trier.de/db/journals/compsec/compsec72.html#TounsiR18

[60] Johanna C. van Niekerk and J. D. Roode. 2009. Glaserian and Straussian grounded theory: similar or completely different?. In *SAICSIT Conf.* (2009-11-17) *(ACM International Conference Proceeding Series)*, Barry Dwolatzky, Jason Cohen, and Scott Hazelhurst (Eds.). ACM, 96–103. http://dblp.uni-trier.de/db/conf/saicsit/saicsit2009.html#NiekerkR09

[61] Chaz Vidal and Kim-Kwang Raymond Choo. 2017. Situational Crime Prevention and the Mitigation of Cloud Computing Threats.. In *ATCS/SePrIoT@SecureComm (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering)*, Xiaodong Lin, Ali Ghorbani, Kui Ren, Sencun Zhu, and Aiqing Zhang (Eds.), Vol. 239. Springer, 218–233. http://dblp.uni-trier.de/db/conf/securecomm/securecomm2017w.html#VidalC17

[62] Claes Wohlin, Per Runeson, Martin Höst, Magnus C. Ohlsson, Björn Regnell, and Anders Wesslén. 2000. *Experimentation in software engineering: an introduction*. Kluwer Academic Publishers, Norwell, MA, USA.

[63] Li Xu, Zhenxin Zhan, Shouhuai Xu, and Keying Ye. 2013. Cross-layer Detection of Malicious Websites. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13)*. ACM, New York, NY, USA, 141–152. https://doi.org/10.1145/2435349.2435366

[64] Pamela Zave. 2003. An experiment in feature engineering. In *Programming methodology*. Springer, imported.

Received February 2019; revised March 2019; accepted June 2019