information

MDPI

Article

Fake News Incidents through the Lens of the DCAM Disinformation Blueprint

Matina Rapti [1], George Tsakalidis [1,2], Sophia Petridou [1] and Kostas Vergidis [1,*]

[1] Department of Applied Informatics, University of Macedonia, 54636 Thessaloniki, Greece; mrapti@uom.edu.gr (M.R.); giorgos.tsakalidis@uom.edu.gr (G.T.); spetrido@uom.edu.gr (S.P.)
[2] Financial and Economic Crime Unit (S.D.O.E.), Operational Directorate of Macedonia, 57009 Thessaloniki, Greece
* Correspondence: kvergidis@uom.edu.gr; Tel.: +30-2310-891-637

Abstract: The emergence of the Internet and web technologies has magnified the occurrence of disinformation events and the dissemination of online fake news items. Fake news is a phenomenon where fake news stories are created and propagated online. Such events occur with ever increasing frequency, they reach a wide audience, and they can have serious real-life consequences. As a result, disinformation events are raising critical public interest concerns as in many cases online news stories of fake and disturbing events have been perceived as being truthful. However, even at a conceptual level, there is not a comprehensive approach to what constitutes fake news with regard to the further classification of individual occurrences and the detection/mitigation of actions. This work identifies the emergent properties and entities involved in fake news incidents and constructs a disinformation blueprint (DCAM-DB) based on cybercrime incident architecture. To construct the DCAM-DB in an articulate manner, the authors present an overview of the properties and entities involved in fake news and disinformation events based on the relevant literature and identify the most prevalent challenges. This work aspires to enable system implementations towards the detection, classification, assessment, and mitigation of disinformation events and to provide a foundation for further quantitative and longitudinal research on detection strategies.

Keywords: fake news overview; disinformation blueprint; detection strategies

check for updates

Citation: Rapti, M.; Tsakalidis, G.; Petridou, S.; Vergidis, K. Fake News Incidents through the Lens of the DCAM Disinformation Blueprint. *Information* **2022**, *13*, 306. https://doi.org/10.3390/info13070306

Academic Editor: Arkaitz Zubiaga

Received: 31 May 2022
Accepted: 20 June 2022
Published: 22 June 2022

1. Introduction

The Internet provides new ways (e.g., websites, blogs, and social media) of news sharing that reach a wider audience almost instantaneously. For its first few decades, this connected world was idealized as an unfettered civic forum space where disparate views, ideas, and conversations could constructively converge [1]. However, the emergence of the Internet and web technologies, apart from original news dissemination, magnified the intentional spread of disinformation or 'fake news'. Fake news is a phenomenon whereby fake news stories are created and propagated online, often by small-scale digital media platforms that are not subject to effective regulation and do not subscribe to normal standards of professional journalism.

Fake news stories can be hard to spot; they are typically designed to appear plausible, commonly mimic the appearance of articles from reputable sources, and are disseminated through the same channels as original news. The emergence of fake news negatively influences online users through false, slanderous, and misleading information and completely denigrates the reporting of original news items. Disinformation events, fake news stories, and misleading information in general can reach as many readers as a reputable online newspaper [2]. The frequency of disinformation events is increasing exponentially, and this trend is unlikely to be reversed anytime soon [3]. The importance of thoroughly examining fake news lies in the fact that although it mostly occurs online, its implications are far reaching with serious real-life consequences. The dissemination of fake news is argued to have large negative effects on public information and to disrupt political processes, including elections [4,5]. This phenomenon appears to have three important elements: (i) it is intentional and originates mostly from human actors; (ii) it is exploiting and advancing current and emerging networking technologies; and (iii) it largely occurs online, but its implications—both short-term and long-term—can have drastic effects in the real world (e.g., election results, reduction in vaccinations, etc.).

Based on the above, this research intends to propose DCAM-DB, a disinformation blueprint (DB) that Detects, Classifies, Assesses and Mitigates (DCAM) fake news incidents in a systematic and timely manner. The proposed blueprint is based on the cybercrime incident (CI) architecture [6], a framework that serves as a reference for monitoring, assessing, and mitigating cybercrime incident occurrences [7,8], and it has been the foundation for many applied approaches such as the classification of cybercrime offenses using machine learning techniques [9]. Using a similar approach, this work aims to lay the ground for the investigation and mitigation of fake news incident occurrences. The first step towards constructing a blueprint for the effective handling and mitigation of such incidents is to investigate the fake news phenomenon and examine its various properties. The authors conducted an extensive literature research and identified the main issues and challenges of fake news dissemination. Each of the challenges corresponds to a fake news property that is incorporated in DCAM-DB. These challenges are articulated below and detailed in the rest of the paper:

1. What have fake news and disinformation come to encompass? What phenomenon do they describe?
2. What are the types of disinformation, and what are the attributes that distinguish them? Are all types of disinformation malicious?
3. Who are the participating actors in the fabrication and propagation of fake news? What is their motivation and expected gains/benefits, if any?
4. What is the target audience of disinformation, and what is the impact and consequences of fake news exposure?
5. What are the existing detection strategies, and what is expected towards fake news mitigation and handling?

The aim of the paper is to identify the emergent properties and entities involved in fake news incidents and to construct a disinformation blueprint of such events. The rest of the paper is organized around these issues, providing a critical overview of the existing literature. The first two challenges are discussed in Section 2. Section 3 separates the participating actors in content producers and broadcasters and discusses these two groups along with their motivation for fabricating and disseminating intentionally deceiving content. Section 4 examines the target audience of fake news, the factors that affect its susceptibility, and the impact of exposure to disinformation. Section 5 discusses the existing detection and mitigation strategies that include both manual and automated approaches. Finally, in Section 6 the authors lay the ground for DCAM-DB by proposing a thorough examination of the emergent fake news properties and entities through the lens of the cybercrime incident architecture [6].

2. Definitions, Types and Attributes of Fake News

Based on the first two challenges, the aim of this section is to provide a framework for understanding the phenomena of fake news and intentional disinformation. We argue that not having an established common understanding for fake news undermines its effective handling, detection, and mitigation. In this context, the authors examine existing fake news definitions, identify common forms of disinformation, and discuss the importance of two distinguishing content-related attributes: essence and intention.

2.1. Fake News Definitions

The term 'fake news' is not appropriately defined and is often interchangeably used with other Internet or technology-linked misinformation acts such as fabricated news, hoaxes, clickbait, etc. [10]. The Collins English Dictionary [11] selected fake news as the most popular term in 2017 and defined it as "*false, often sensational, information disseminated under the guise of news reporting*". Based on Shu et al. [12], fake news is intentionally and verifiably false and can mislead readers. These authors also suggest that "*fake news is essentially a distortion bias on information manipulated by the publisher*" [12]. Tandoc et al. [13] note that the word 'fake' is often used interchangeably with words such as copy, forgery, counterfeit, and inauthentic. Other authors situate fake news within the context of *misinformation* and *disinformation.* Wardle [14] suggests that precise definitions often deal narrowly with fabricated news reports produced either for profit or for political purposes and that the term 'fake' does not fully describe the complexity of the different types of misinformation and disinformation. Misinformation refers to "*the inadvertent sharing of false information*" [14,15] and disinformation refers to "*the deliberate creation and sharing of information known to be false*" [14]. A European Union (EU) report based on the independent High-Level Expert Group [16] discourages the use of the term fake news as the term is considered inadequate to communicate the magnitude of the consequences it begets. Instead, the report adopts the term *disinformation* described as "*false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for-profit*" [16,17].

There are considerable challenges in finding common ground on what the phenomenon of fake news encompasses as depending on the area of focus, it is identified differently. Based on our research on existing fake news and disinformation definitions, we assert that fake news is an umbrella-term synonymous with disinformation, and it is the deliberate dissemination of distorted events, non-cross-referenced facts, or fabricated information that is spread online with the intent to mislead or deceive its target audience.

2.2. Prevalent Types of Disinformation

Less research exists on the categorization of the disinformation events that occur online. Zannettou et al. [18] conducted relevant research on the types of false information available online and proposes a categorization into six types: fabricated, propaganda, hoaxes, rumors, clickbait, and satire news. Similarly, Tandoc et al. [13] categorize the types of fake news into propaganda, advertising, photo manipulation, fabrication, parody, and satire. Based on extensive research and consulting the above classifications, we assembled the most prevalent forms of disinformation that are encountered online and fall under our fake news umbrella-term definition. For each of the identified types below, the authors provide a short description and an indicative occurrence:

Clickbait—News items with misleading headlines, or captions that intend to incite excitement and curiosity to entice users. Such items exploit linguistic features such as capital and bold letters, exclamation marks, ellipsis, sentimental words and interjections, or unfinished sentences. The content of click bait articles generally contains opinionated and inflammatory language [12,19,20]. An example of clickbait is a news story [21] titled "*Cat DIES after COVID-19: Report*". In this article it is explicitly mentioned that the cat did not die from the SARS-CoV2 infection. This is a typical clickbait example, using capital letters and a strong word to attract the users, whereas the actual content of the article does not reflect the clickbait title.

Computational propaganda—The deployment of algorithms and automated propagation methods to intentionally generate and share distorted information online. Computational propaganda includes learning from and mimicking original online accounts on social media platforms and aims to distort public opinion. It is mainly executed by bots that orchestrate the activity of several online accounts to disperse false information [22]. A recent example of computational bot-produced propaganda is tweets—produced by fake accounts—demeaning climate change an as non-existent [23].

Conspiracy theories—Fictional stories that invoke a conspiracy without proof; such stories revolve around supposedly illegal acts conducted by governments or powerful individuals. These theories put forward unsourced information or jump to conclusions lacking disclosure [18,24]. A popular example of conspiracy theory is the one claiming that the Earth is flat [25]. The conspiracy theorists do not benefit in any particular way from disseminating such theories; they strongly consider them as true and aspire to reach a wider audience.

Fabricated news—News items with no factual basis that appear legitimate by being disguised as original news items. They include no implicit disclosure that the item is fabricated, including the intention of misinforming, and can be published on a website, blog, or social media platform. An example of fabricated news is the Washington Post story of an 8-year-old heroin addict titled "Jimmy's World" that earned a Pulitzer Prize for the journalist Janet Cook. Later research showed that Jimmy did not exist [26].

Hoax articles—News stories that contain facts that are either fabricated or inaccurate but presented as legitimate half-truth or factoid stories (hoax facts or hoax articles, respectively) [10]. These stories are published online in an attempt to convince their reader into believing that something false is valid [14,26,27]. One of the most well-known examples of hoax stories is known as the "Great Moon Hoax", published in 1835 by the New York Sun about the alleged exploration of life on the moon [28].

News parody—This shares many characteristics with satire due to the fact that both rely on humor as a means of drawing an audience; it also uses a presentation format that mimics mainstream news media [13]. news parodies differ from satire in their use of nonfactual information to inject humor [29]. An example of news parody is the Saturday Night Live TV show with spoof and parody performances [30].

News satire—Disguised as real news, it contains humor or exaggeration to present audiences with news updates; they are not meant to be taken seriously and can be found on TV or websites. Nonetheless, a key difference of satire and parody compared to other forms of disinformation is that they provide disclosure to the fact that their primary target is entertainment rather than accurate news delivery [13,18,31]. A typical example of news satire is the content produced by the known website "The Onion" [32]. As an example, a satire report titled "*DNC Concerned Warm, Cozy Beds On Brisk November Morning Could Keep Voters From Going To Polls On Election Day*" addresses the issue of abstinence during the elections in a humorous manner [33].

Photo manipulation—Tampering with original images or videos to create a false narrative; visual news that aims to mislead, which takes advantage of the advent of digital photos, powerful image manipulation software, and knowledge of manipulation techniques [10]. It is common knowledge that an image can be easily used to mislead [13,34] when placed in unrelated context. An example of photo manipulation occurred on January 2020 during the Australia wildfires where photos of animal suffering spread online. However, one illustrating a deer standing amid burned rubble was taken in a previous fire and a totally different location, specifically in California during another fire season [35].

Political propaganda—A type of fake story that aims to inflict damage on a particular political party or nation-state with no implicit disclosure that the story is fabricated and with the intention of deceiving the audience into a particular political/social agenda [17,31,36]. A recent item of political propaganda was produced by Donald Trump, claiming that "*In manufacturing I brought back 700 thousand jobs, (Obama and Biden) brought back nothing*". This statement according to the statistics is false [37,38] as the actual increase is about 450 thousand and during the Obama presidency the increase was about 900 thousand.

(Online) rumors/comments—Narratives whose accuracy is vague or never established, passed along from person to person, usually by word of mouth or online comments/posts, without reliable standards of evidence; however, the information is ever-modified according to the desires of those who pass it on [39,40]. For example, many individuals and groups believe that Barack Obama is a Muslim even after this was exposed to be untrue [41].

2.3. The Importance of Content Essence and Intention

Two underlining features emerging from the identified types of fake news are that (i) its content is presented as original but it is—entirely or partly—fabricated and (ii) it is easily propagated online. Apart from these features, which serve as a common denominator, there are also two attributes that differentiate them:

1. The *essence* of the content; whether the news item is based on actual facts or is entirely fictional, and,
2. The *intention* of the authoring source; whether the news item attempts to intentionally mislead and deceive, or whether it properly discloses the nature of the content.

Table 1 presents a classification of the identified fake news types based on the above attributes. In relation to essence, conspiracy theories, fabricated news, and news parodies present entirely fictional stories with no factual basis. Computational propaganda, clickbait, photo manipulation, and political propaganda and rumors present stories that have a partial factual basis but, in most cases, contain a distorted fact, an exaggerated truth, or a non-cross-referenced event [10]. Finally, hoax articles and news satire can either contain factual or fictional content. Regarding intention, news parody and news satire are the only types that provide disclosure of the nature of their content; they hence alleviate any malignant effect from their factual or fictional—but not genuine—nature. All the remaining types of fake news do not provide any explicit disclosure and thus attempt to intentionally mislead and deceive their audience. Based on the essence and intention criteria, it emerges that the disinformation items that combine a fact-based essence with misleading intentions are the most dangerous as they can deceive their recipients. This conjecture stems from the observation that a semi-true story could be much more easily perceived as true. On the other hand, the pieces of information that are completely fictional are less dangerous since the deception is generally more obvious and thus is easily dismissed. At a later research stage, the severity of fake news types based on the targeted audience and the projected impact can be added to the proposed classification.

Table 1. Classification of fake news types.

Type of Fake News	Essence	Intention
Click bait	fact- based	misleading
Computational propaganda	fact-based	misleading
Conspiracy theories	fictional	misleading
Fabricated news	fictional	misleading
Hoax articles	fact-based/fictional	misleading
News parody	fictional	disclosure
News satire	fact-based/fictional	disclosure
Political propaganda	fact-based/fictional	misleading
Photo manipulation	fact-based	misleading
Rumors	fact-based	misleading

3. Fake News Producers and Broadcasters

The emergence of fake news originates from specific actors that generate, host, support, and disseminate the disinformation material. These entities can be human or non-human, and their aim is to produce and broadcast content that falls into one or more of the categories of the previous section, i.e., to disseminate fake news. Based on further examination, these actors can be broadly separated into the *content producers* or *generators* (human and non-human) and the *content hosts* or *broadcasters*. This section also touches on the motivating factors behind the generation of disinformation material.

3.1. Content Producers (Human)

The web has made content generation easy and accessible to the public within various platforms (e.g., WordPress) and social media sites (e.g., Facebook, Twitter). This means that any individual with Internet access can potentially generate fake news content by writing an article or uploading a post or a tweet [42]. These posts can either be anonymous or eponymous, both with their own advantages and disadvantages. Posting anonymously—or under a nickname—can lead to unrestrained, conspiring, or obscene claims since there is (in the majority of cases) no accountability. A particular group that engages in malicious anonymous posting is trolls. The term "troll" [43] is used increasingly in social media networks and digital news media and applies to users that intend to bother or upset other users [10]. An example of troll-originating offensive practice is posting aggravating or irrelevant messages to derail the flow of discussion on a website and upset its users [44].

Posting eponymously can utilize the weight of the name bearer, especially in the case of an influencer or a professional journalist, thus lending credibility to non-credible sources, claims, and theories. Influencers are digitally famous individuals that assert significant influence over online users and have gained prominence by promoting products and services through specific lifestyle choices. Journalists are responsible for the majority of online news-related generated content. They can employ professional techniques and strategies to increase traffic, i.e., by using an exaggerated headline or a provocative distorted photo that is appealing to the readers [4,17,45].

3.2. Content Generators (Non-Human)

Another category of the disinformation crew is bots. Bots are automated software programs deployed to spread computational propaganda, by performing simple, repetitive, robotic tasks [21,22,46]. These are programs that are, among others, responsible for the online activity of several fake accounts that disseminate false information. Bots are usually attached to fake accounts that are recruited to produce and spread false information on the Web [10]. A bot is usually used for financial gain by organizations [18] or to infiltrate political dialogue, handle the stock market, remove personal information, and spread misinformation in general. This category is severely harmful for the public as bots have the capability to disguise themselves as human users [47] and reproduce content on a very large scale [48]. This can easily mislead users to share the disinformation item after believing it is actually legitimate news. Bots are capable of increasing traffic in a website in a much higher quantity than human content generators [49].

3.3. Content Hosts and Broadcasters

This category refers to the (dis)information broadcaster, which can be a news organization, a political or activist organization, an unlawful acting group or even a government, or a social networking site (SNS). The influential power of a news organization provides them with the capability to skew data and relevant information towards a specific point of view. Additionally, some news organizations can be prone to broadcasting falsehoods by making stories more appealing, to increase their audience and business activity [18,50]. There are also other groups that promote their interests by sharing false information to support a specific narrative. A recent example involves the National Rifle Association, a non-profit organization that defends gun rights, which disseminated false information to manipulate people about guns [51]. Other examples include political parties that share false information, especially near major elections [2]. Another type of fake content broadcasters is entities with unlawful background that employ mischievous tactics to communicate their message. Recent examples include the ISIS terrorist organization, which feeds SNSs with fabricated information [12,20,52], and white supremacist/nationalist groups, which employ the web to recruit new members [53]. Such groups use misleading tactics to draw attention to their causes while presenting themselves as serious and scholarly [54].

National governments have also been exploiting social media to shape public opinion on different topics. Donald Trump, as President of the USA, embraced anti-vaccination conspiracies [54,55]. Another recent example of government-oriented information manipulation took place in early 2020, when a network of Twitter accounts was employing coordinated inauthentic activity that was primarily targeted at domestic audiences within Turkey. This was proved to be a collection of fake and compromised accounts that were being used to amplify political narratives. As a result, Twitter removed 7340 accounts. The same happened with inauthentic Saudi, Russian, and Chinese accounts that were inflating information on geopolitical issues [56,57]. Social networking sites (i.e., Facebook, Twitter, and YouTube) play an important role in hosting and broadcasting disinformation items as they are the main gateways through which information is being sought and shared. They have developed into a fertile ecosystem for the extensive dispersion of unverified stories because they nurture homogeneous and polarized communities (echo chambers) that have similar information consumption patterns [58,59]. It is shown in [60] that users on Facebook tend to follow like-minded people and thus acquire knowledge that supports their existing narratives. We argue that the echo chamber effect facilitates and accelerates the consumption and propagation of fake news.

3.4. Motivation

In relation to the motivation that drives the fake news content producers and broadcasters, it can be financial, political, or to assert influence on their audience. Shu et al. [12] refer to the social and psychological foundations of the fake news ecosystem, while Bakir and McStay [61] report the economic or political gain that motivates the fake news circulation. Many actors in the false information ecosystem seek monetary profit for their organization or website. To accomplish this, they regularly propagate false information that raises the traffic on their website. This leads to grown advertisement income that results in pecuniary profit for the organization or website, at the expense of manipulated users [18]. One of the most recent examples of fake news stories produced for financial profit includes North Macedonian teenagers who created and spread distorted and fictional stories about the 2016 American presidential candidates [62].

A political impulse has also been recognized as a strong motivator in fake news stories recently [22]. The actors of such disinformation intend to manipulate public judgment on special matters and individuals and on their opinions of the society [52]. Political disinformation efforts are typically used to plant mistrust and confusion about what sources of information are authentic, making people confused about what and whom to believe in. Politically driven disinformation requires serious attention due to the hurdles it poses for society and democratic institutions [10]. New advanced technologies produce and share political disinformation and thus make it harder to detect and fight the manipulation, for journalists, fact-checkers, and citizens [17].

4. Target Audience and Projected Impact

On the receiving and consuming side of the digital communities are the content recipients, the platform users, or simply the online audience. The content recipients are the individuals who use the Internet as a portal to receiving the news but also to repost articles, react, comment, “like”, retweet, and share without being the content producers themselves. The content recipients can propagate disinformation by reading, relating to, and sharing a story they encountered on a social media platform or a website, without previously cross-checking the accuracy of the content. It has been noted that the spread of information among users is characterized by homophily, i.e., the tendency for people to seek out or be attracted to those who are similar to themselves [60]. Online users tend to follow online communities of like-minded people and acquire knowledge that reinforces their already-supported existing narratives [60].

The most prevalent audience motives that make it susceptible to disinformation are entertainment, personal enjoyment, online socializing, information seeking, self-expression, and status-seeking [63]. Users may actively generate and distribute disinformation to create online social relations to earn fame and digital friends [64]. They are mobilized by likes, shares, and comments to create content that will resonate with their friends, followers, and groups, and media manipulation might be a way to gain “rank” and express individuality among their peers [54,65].

Two important concepts that explain the behavior of the online audience regarding disinformation are *naive realism* and *confirmation bias* [12]. Naive realism represents users who tend to believe that their opinions and understandings of reality are the only accurate ones, while others who differ are considered uninformed, irrational, or biased. Confirmation bias users prefer to accept information that establishes their existing beliefs. Due to these patterns of thought, fake news can often be regarded as real. The effects of fake news regarding the online audience are also influenced by three main factors.

4.1. Target Group Availability

The availability characteristic focuses on the quality and quantity of time the users spend on using the Internet in the first place. People with more free time, and thus more availability, are characterized as heavy media users [66], and are the ones who have more time to spend searching various media offerings. The heavy media users are aware of most of the information alternatives that are offered by the media ecosystem since they have the time to investigate more. According to a study [67], the heavy media users cover a smaller part of the overall audience but they are also the ones that exploit the popular, as well as the unpopular, news outlets; thus, they are far more prone to propagate fake news content [68]. On the other hand, those with less free time, and thus less availability, are characterized as light media users [69]. Light media users focus their attention on the more established news media platforms and websites since they lack the time to devote to additional sources.

4.2. Target Group Age

Age is a very important factor of fake news distribution by users [70]. Particularly, the older people are more affected and manipulated by fake news stories [10]. The age factor is one of the most reliable signs of how the Internet and especially social media users interact with disinformation, more than factors such as sex, race, income, or education

4.3. Digital Intelligence

Digital literacy is the ability to understand information and to evaluate and integrate information in multiple formats that the computer can deliver. In light of the accelerated and constant evolution of digital technology, people are expected to use a developing variety of technical, cognitive, and sociological skills to perform tasks and solve problems in digital ecosystems [71–74]. The lack of digital intelligence equated to not comprehending the ways that information is produced and distributed, or the motives that drive the disinformation-content producers.

Regarding the impact of fake news, there is also scarce research [75]. Apart from elementary results, knowledge about the effects of disinformation consists of some possible kinds of influence such as increasing cynicism and apathy, and the encouragement of extremism [75,76]. Based on relevant research [77], news stories can lure audiences into developing false beliefs. Moreover, according to Gelfert [78], repetition effects entail that repeated exposure to the same information renders that information more persuasive. On an individual level, regular exposure to a particular message affects a user's perspective, viewpoints, and their behavior in general [79,80].

5. Detection Strategies

Fake news detection is the prompt and accurate identification of a news item being intentionally misleading. Timely detection is essential for the prevention and mitigation of the disinformation phenomenon to minimize its consequences. The volume of scattered information and the speed of its propagation creates a practical impossibility of estimating trustworthiness and authenticity promptly, increasing the need for automatic fake news detection systems [42]. Conroy et al. [81] claim that disinformation may be defined as the prediction of the chances of a particular news article being intentionally deceptive. The authors of the particular study also claim that a text analytical system can improve human skills to recognize falsifications, contribute proof for its doubts, and alert users to further fact-checking. However, it is shown that people are not great in recognizing lies, not much better than speculation, and computers can insignificantly defeat humans on limited tasks [82]. Our assertion is that fake news detection and mitigation can be deployed across two distinct paths:

- *Soft detection and reporting* by educating and training the online audience, and,
- *Hard (automated) detection* by designing and developing algorithms that can trace, detect, and recognize fake news.

In the relevant literature, a series of hard detection approaches are explored. An example is the code developed for hoax detection that samples and classifies posts into hoax and non-hoax [83]. Another instance is developed by Vlachos and Riedel [84] that constructs fake news and fact-checking datasets. Similarly, Ferreira and Vlachos [85] have published the Emergent dataset, which includes 300 labeled rumors. However, limited-size datasets cannot be utilized to yield a model for machine learning algorithms to detect disinformation events. Wang [86] introduced a different method to reveal falsehood. The author utilized empirical techniques to investigate disinformation events based on surface-level linguistic patterns by composing a heterogeneous network to combine metadata with text. Conroy, Rubin, and Chen [81] separate the fake news detection methods in (a) linguistic approaches in which the content of deceptive messages is extracted and analyzed to associate language patterns with deception; and (b) network approaches in which network information, such as message metadata or structured knowledge network queries, can be harnessed to provide aggregate deception measures. Both forms typically incorporate machine learning techniques for training classifiers to suit the analysis. Likewise, Figueira and Oliveira [87] divide these methods into (i) algorithms that are based on the content; (ii) algorithms that are based on the diffusion dynamics of the message; and (iii) hybrid algorithms, which are based on a weighted sum, or a group of features feeding a learning algorithm. Similarly, Rubin et al. [88] discuss that for a fake news detection tool to be developed, news satire needs to be studied as a starting point for the investigation of deliberate deception in news stories.

Some of the most popular social platforms such as Facebook and Twitter are more and more under increasing pressure to control their algorithms [89,90]. As a result, social media platforms are currently warning their members about misleading and dubious content, by developing their policies over falsehoods and adopting automated systems in detecting such content [91,92]. For example, regarding the dealing of the COVID-19 health crisis, Facebook formed a full sub-section informing its members about the new virus and at the same time, along with the Twitter platform, they have introduced a new policy of blocking posts with inaccurate content [93–95].

Apart from the automatic technologies that will be able to assist the users in recognizing falsehood, the digital education of the users is equally important. Digital skills, as a sum of technical, cognitive, post-cognitive, and socioemotional abilities and skills, allow users to cope with digital life's challenges and adjust to its demands [10]. People educated and equipped with digital intelligence are more capable, intelligent, and future-ready to be digital citizens [96]. Recently, on an official level, an intensive effort has been made to identify and reduce incidents of disinformation. Part of the EU Program "Horizon 2020" is the Social Observatory for Disinformation and Social Media Analysis (SOMA) [97], a content verification platform. It includes incident-control tools, methods for assessing the socio-economic impact of misinformation, actions to increase digital literacy, the analysis of legal regulations, and a repository of knowledge on disinformation. Likewise, other EU-funded disinformation-control programs have been formed, such as the PROVENANCE [98], which aims to establish solutions for verifying digital content directly from the source, without intermediaries, providing greater control to social media users and supporting the dynamics of social sharing with values of trust, transparency, and open participation. The European-funded projects "SocialTruth", "EUNOMIA", and "WeVerify" have a similar goal [99].

As for education, the EU Commission [100] suggests that a greater level of digital literacy will benefit European citizens to recognize online disinformation and access the Internet critical content. This would be accomplished by providing educational material to schools and students via the fact-finding teams and civil society organizations [100]. This pathway is also being followed by Canada, the Netherlands, Denmark, and Singapore, which have concentrated on peoples' fake news education with projects, campaigns, and school lessons [101–103]. Several manual, human-operated fact-checking tools and platforms such as PolitiFact [104] and Snopes [105] have emerged to assist the public on this matter. Equally, some automated falsehood predictors have arisen. For example, the Captain Fact tool [106] is trying to bring to the surface the credibility of an item based on users' votes. Likewise, the Claim Buster is using natural language processing methods for live fact-checking, functioning as a search engine for key words and structures that are commonly found in factual statements through fact-checking websites [107]. Nevertheless, the existing fact-checking tools cannot compete with the volume of newly generated and distributed information, particularly on social media. This enhances the necessity for further systematic approaches in fake news mitigation that combine both soft and hard detection methods.

6. Towards a Disinformation Blueprint Based on CI Architecture

What is evident from the above overview is that, even at a conceptual level, a comprehensive blueprint of what constitutes fake news, that features the further classification of occurrences, detection methods, and mitigation actions, does not exist. The authors identify three main challenges that prohibit the effective detection and mitigation of disinformation events: (a) a lack of a commonly accepted reference of what the fake news phenomenon encompasses; (b) a lack of a typology for the various occurrences of fake news incidents; and (c) the absence of longstanding qualitative/quantitative studies of fake news cases that could effectively contribute to the recommendation and adoption of appropriate measures and effective mitigation actions. In previous work [6], we have identified similar challenges for cybercrime incidents (CIs) and constructed the cybercrime incident architecture, a comprehensive blueprint towards effective CI management. This structure has succeeded in generating insights for CIs, monitoring their threat severity, and producing actionable measures and guidelines for individuals, organizations, and law enforcement agencies.

The architecture has been the foundation for a variety of applied approaches such as the classification of cybercrime offenses using machine learning techniques [9]. In a similar manner, this work proposes DCAM (detect, classify, assess, and mitigate)—DB (disinformation blueprint) for fake news mitigation based on the CI architecture. Table 2 shows the architectural components for handling CIs and how they can be accommodated towards disinformation handling and mitigation.

The first component of the CI architecture identifies the main features of cybercrime incidents and results in a feature-based description that facilitates the elaborate understanding of a specific incident. This component could be fine-tuned to the context-specific features of disinformation that are discussed in this paper, namely, *essence*, *intention*, *producer*, *broadcaster*, *motivation*, *audience*, and *impact*. By distinguishing between these features in terms of specific values for particular fake news incidents, we argue that the detection strategies will be facilitated and become more customized and effective based on specific feature combinations. For example, different techniques will need to apply for detecting computational propaganda originating from another country, unlike conspiracy theories on a non-crucial issue. The second component of the CI architecture provides a two-level offense classification system for CIs that can produce association rules that contextualize the CI features. In Section 2, the authors presented an initial classification of fake news types that can be further elaborated on and combined with the component I features in DCAM-DB to help identify how these features associate and interact with each other. This will result in a much better understanding of fake news dynamics. For example, it could emerge that conspiracy theories (*fake news type*) target a specific vulnerable portion of the audience (*fake news feature*); thus, this needs to be prioritized in training and education.

Table 2. CI architecture's components [6] as qualifiers for DCAM-DB.

CI Architectural Component	Component Goal	DCAM Disinformation Blueprint
Component I: CI Features	*Describe* a CI in a systematic manner by identifying its distinctive features	**Detect** a fabricated news story in a systematic manner (manual or automated) based on its distinctive features
Component II: Classification and CI Schema	*Classify* a CI utilizing an offense classification system that enables feature associations	**Classify** a fake news item based on specific attributes employing a taxonomy that enables feature associations
Component III: Threat Severity	*Assess* a CI based on its past occurrences and their perceived severity	**Assess** a fake news incident based on its target audience, motivation, and expected impact
Component IV: Adaptive Response Policy	*Tackle* a CI based on specific response measures	**Mitigate** the incident through specific response measures and action taken from the respective stakeholders

The third component is occupied by monitoring cybercrime offenses and analyzing their individual occurrences. As this paper discussed, there is largely a lack of datasets or assessment methods for fake news incidents, except for mostly manual approaches. This component can be used in DCAM-DB as a qualifier to monitor and gather data from past acknowledged fake news incidents to be able to better assess and take appropriate action towards existing and/or new disinformation events. The first three components essentially help one to distinguish between unique disinformation events and the fourth component attempts to match them with appropriate (a) short-term preventive measures and actions for mitigation, and (b) long-term policy legislation in national or international level. The principal aim of adaptive response policy (ARP) [6] is to produce (i) immediate *actions* for particular CIs, (ii) specific *measures* to prevent similar offenses, and (iii) elaborated *policies* for a specific category of CIs. The same should transfer to disinformation events by allocating specific actions, measures, and policies so that they are tackled with an ammunition that ranges from immediate actions to national policies.

The cybercrime incident architecture—by having four interconnected components, each dealing with a separate aspect of an incident—can be a rounded approach for mitigating disinformation events. The authors intend, as future work, to further adapt and customize DCAM-BD as a solid blueprint for disinformation detection and effective mitigation. Currently, we are working on acclimatizing components I and II with corresponding case studies based on recent disinformation events (e.g., COVID-19 pandemic, USA 2020 presidential elections). We assert that DCAM-DB will facilitate the detection approaches by (a) creating real-life or synthetic structured datasets based on the identified features and their values, and (b) enabling machine learning and natural language processing algorithms to be trained on crawled datasets based on a given structure.

7. Conclusions

The Internet contributed to the democratization of the media as it extended their reach and the capability of content creation to the wider public. However, the digital ecosystem has become a rich soil for disinformation dissemination. This paper presented an overview of challenges surrounding fake news and disinformation events based on the relevant literature under the lens of composing them to a structured disinformation blueprint. It provided a definition of fake news along with examples of the most prevalent types of fake news. These types were discerned based on essence and intention in a classification that can be further elaborated on based on additional distinguishing features. The human and non-human producers of fake news, along with their respective motives, were discussed in an effort to understand the originators of disinformation events. The vulnerability of the target audience was identified based on respective attributes, i.e., availability, age, and digital literacy. Additionally, the most common detection approaches were located in literature and were classified as either soft or hard detection strategies. The paper argued that an effective mitigation course of action should deploy a combination of both strategies.

The overview of these subsequent challenges revealed the importance of addressing them in the context of a concise framework such as DCAM-DB. The authors qualified the CI architectural framework, briefly addressing how it could be further customized to accommodate disinformation events. The benefits of having an established approach towards detection, classification, assessment, and mitigation could provide a solid foundation for the timely resolution of the ubiquitous fake news phenomenon. The main contributions of this work to disinformation are (i) a thorough study of relevant literature, (ii) the compilation of the different properties and entities around disinformation, and (iii) the proposal of DCAM-DB as a systemic investigation approach through the lens of the cybercrime incident architecture. The authors acknowledge the need for further quantitative and longitudinal research to solidify their theoretical findings, the more elaborate classification of fake news incidents, and the effective detection and mitigation of disinformation.

Author Contributions: Conceptualization, K.V.; data curation, M.R.; investigation, M.R. and G.T.; methodology, S.P. and K.V.; resources, S.P.; supervision, S.P. and K.V.; validation, G.T. and S.P.; writing—original draft, M.R.; and writing—review and editing, G.T. and K.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Anderson, J.; Rainie, L. *The Future of Truth and Misinformation Online*; Pew Research Center: Washington, DC, USA, 2017.
2. Allcott, H.; Gentzkow, M. Social Media and Fake News in the 2016 Election. *J. Econ. Perspect.* **2017**, *31*, 211–236. [CrossRef]
3. Peterson, M. A High-Speed World with Fake News: Brand Managers Take Warning. *J. Prod. Brand Manag.* **2019**, *29*, 234–245. [CrossRef]
4. Lee, T. The Global Rise of “Fake News” and the Threat to Democratic Elections in the USA. *Public Adm. Policy* **2019**, *22*, 15–24. [CrossRef]
5. Adamkolo, M.I.; Umaru, A.P. In a Democratized Media Context What a Hoax Can Do, a Misinformation Can Do Even Worse: Influences of Fake News on Democratic Processes in Nigeria. *New Media Mass Commun.* **2019**. [CrossRef]
6. Tsakalidis, G.; Vergidis, K.; Petridou, S.; Vlachopoulou, M. A Cybercrime Incident Architecture with Adaptive Response Policy. *Comput. Secur.* **2019**, *83*, 22–37. [CrossRef]
7. Tsakalidis, G.; Vergidis, K. A Systematic Approach toward Description and Classification of Cybercrime Incidents. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *49*, 710–729. [CrossRef]
8. Tsakalidis, G.; Vergidis, K.; Madas, M. Cybercrime Offences: Identification, Classification and Adaptive Response. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; IEEE: Manhattan, NY, USA, 2018; pp. 470–475.
9. Rupa, C.; Gadekallu, T.; Abidi, M.; Al-Ahmari, A. Computational System to Classify Cyber Crime Offenses Using Machine Learning. *Sustainability* **2020**, *12*, 4087. [CrossRef]
10. Rapti, M. Fake News in the Era of Online Intentional Misinformation; a Review of Existing Approaches. Master Thesis, University of Macedonia, Thessaloniki, Greece, 2019.
11. Alison Flood Fake News Is “very Real” Word of the Year for 2017 | Books | The Guardian. Available online: https://www.theguardian.com/books/2017/nov/02/fake-news-is-very-real-word-of-the-year-for-2017 (accessed on 20 October 2020).
12. Shu, K.; Sliva, A.; Wang, S.; Tang, J.; Liu, H. Fake News Detection on Social Media: A Data Mining Perspective. *ACM SIGKDD Explor. Newsl.* **2017**, *19*, 22–36. [CrossRef]
13. Tandoc, E.C.; Lim, Z.W.; Ling, R. Defining “Fake News”: A Typology of Scholarly Definitions. *Digit. J.* **2018**, *6*, 137–153. [CrossRef]

14. Wardle, C. Fake News. It's Complicated. Available online: https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79 (accessed on 3 August 2019).
15. Tandoc, E.C. The Facts of Fake News: A Research Review. *Sociol. Compass* **2019**, *13*. [CrossRef]
16. HLEG Final Report of the High-Level Expert Group on Fake News and Online Disinformation. Available online: https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (accessed on 29 August 2019).
17. Bente, K. Fake News—Oxford Research Encyclopedia of Communication. Available online: https://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-809 (accessed on 6 August 2019).
18. Zannettou, S.; Sirivianos, M.; Blackburn, J.; Kourtellis, N. The Web of False Information: Rumors, Fake News, Hoaxes, Clickbait, and Various Other Shenanigans. *J. Data Inf. Qual. (JDIQ)* **2019**, *11*, 1–37. [CrossRef]
19. Clickbait | English Definition and Meaning. Lexico Dictionaries English. Available online: https://www.lexico.com/en/definition/clickbait (accessed on 30 May 2022).
20. Chakraborty, A.; Paranjape, B.; Kakarla, S.; Ganguly, N. Stop Clickbait: Detecting and Preventing Clickbaits in Online News Media. In Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Davis, CA, USA, 18–21 August 2016; IEEE: Manhattan, NY, USA, 2016; pp. 9–16.
21. Farber, M. Death of Cat with Coronavirus in Alabama Being Investigated. Available online: https://www.foxnews.com/health/death-cat-coronavirus-alabama-prompts-investigation (accessed on 10 October 2020).
22. Woolley, S.C.; Guilbeault, D.R. Computational Propaganda in the United States of America: Manufacturing Consensus Online. 2017, p. 29. Available online: https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf (accessed on 14 October 2020).
23. Miller, C. What Are "Bots" and How Can They Spread Fake News. Available online: https://www.bbc.co.uk/bitesize/articles/zjhg47h (accessed on 14 October 2020).
24. Sunstein, C.R.; Vermeule, A. Conspiracy Theories: Causes and Cures*. *J. Polit. Philos.* **2009**, *17*, 202–227. [CrossRef]
25. CNN, R.P. The Flat-Earth Conspiracy Is Spreading around the Globe. Does It Hide a Darker Core. Available online: https://www.cnn.com/2019/11/16/us/flat-earth-conference-conspiracy-theories-scli-intl/index.html (accessed on 14 October 2020).
26. Friendly, J. Writer Who Fabricated Story Tells of Pressure "to Be First". *New York Times*, 29 January 1982.
27. Kumar, S.; West, R.; Leskovec, J. Disinformation on the Web: Impact, Characteristics, and Detection of Wikipedia Hoaxes. In Proceedings of the 25th International Conference on World Wide Web, Montreal, QC, Canada, 11–15 April 2016; pp. 591–602.
28. Thornton, B. The Moon Hoax: Debates About Ethics in 1835 New York Newspapers. *J. Mass Media Ethics* **2000**, *15*, 89–100. [CrossRef]
29. Achter, P. Comedy in Unfunny Times: News Parody and Carnival After 9/11. *Crit. Stud. Media Commun.* **2008**, *25*, 274–303. [CrossRef]
30. Saturday Night Live - NBC.Com. Available online: https://www.nbc.com/saturday-night-live (accessed on 14 October 2020).
31. Rashkin, H.; Choi, E.; Jang, J.Y.; Volkova, S.; Choi, Y. Truth of Varying Shades: Analyzing Language in Fake News and Political Fact-Checking. In Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing, Copenhagen, Denmark, 7–11 September 2017; Association for Computational Linguistics: Copenhagen, Denmark, 2017; pp. 2931–2937.
32. The Onion The Onion | America's Finest News Source. Available online: https://www.theonion.com/ (accessed on 9 October 2020).
33. DNC Concerned Warm, Cozy Beds on Brisk November Morning Could Keep Voters From Going To Polls On Election Day. Available online: https://www.theonion.com/dnc-concerned-warm-cozy-beds-on-brisk-november-morning-1845310952 (accessed on 14 October 2020).
34. Carlson, M. The Reality of a Fake Image: News Norms, Photojournalistic Craft, and Brian Walski's Fabricated Photograph. *J. Pract.* **2009**, *3*, 125–139. [CrossRef]
35. Photo of Deer in Burned Rubble Is from California, Not Australia. Available online: https://www.politifact.com/factchecks/2020/jan/07/viral-image/photo-deer-burned-rubble-california-not-australia/ (accessed on 14 October 2020).
36. Nielsen, R.K.; Graves, L. "News You Don't Believe": Audience Perspectives on Fake News. 2017. Available online: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Nielsen%26Graves_factsheet_1710v3_FINAL_download.pdf (accessed on 11 October 2020).
37. Jacobs, L. PolitiFact - During Debate, Donald Trump Overstates Manufacturing Job Gains. Available online: https://www.politifact.com/factchecks/2020/sep/30/donald-trump/during-debate-donald-trump-overstates-manufacturin/ (accessed on 11 October 2020).
38. U.S. Bureau of Labor Statistics All Employees, Manufacturing. Available online: https://fred.stlouisfed.org/series/MANEMP (accessed on 11 October 2020).
39. Levin, J.; Arluke, A. *Gossip: The Inside Scoop*; Plenum Press: New York, NY, USA, 1987; ISBN 978-0-306-42533-2.
40. Houmanfar, R.; Johnson, R. Organizational Implications of Gossip and Rumor. *J. Organ. Behav. Manag.* **2004**, *23*, 117–138. [CrossRef]
41. Hollander Persistence in the Perception of Barack Obama as a Muslim in the 2008 Presidential Campaign: Journal of Media and Religion: Volume 9, No 2. Available online: https://www.tandfonline.com/doi/abs/10.1080/15348421003738769 (accessed on 28 August 2019).

42. Zhang, X.; Ghorbani, A.A. An Overview of Online Fake News: Characterization, Detection, and Discussion. *Inf. Process. Manag.* **2020**, *57*, 102025. [CrossRef]
43. Mendoza, M.; Poblete, B.; Castillo, C. Twitter under Crisis: Can We Trust What We RT. In Proceedings of the First Workshop on Social Media Analytics—SOMA '10; ACM Press: Washington, DC, USA, 2010; pp. 71–79.
44. Hine, G.; Onaolapo, J.; Cristofaro, E.D.; Kourtellis, N.; Leontiadis, I.; Samaras, R.; Stringhini, G.; Blackburn, J. Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web. In Proceedings of the Eleventh International AAAI Conference on Web and Social Media, Montreal, QC, Canada, 15–18 May 2017.
45. Albright, J. Welcome to the Era of Fake News. *Media Commun.* **2017**, *5*, 87–89. [CrossRef]
46. Allport, G.W.; Postman, L. *The Psychology of Rumor*; Henry Holt: New York, NY, USA, 1947.
47. Ferrara, E. Measuring Social Spam and the Effect of Bots on Information Diffusion in Social Media. In *Complex Spreading Phenomena in Social Systems*; Lehmann, S., Ahn, Y.-Y., Eds.; Computational Social Sciences; Springer International Publishing: Cham, Switzerland, 2018; pp. 229–255, ISBN 978-3-319-77331-5.
48. Gilani, Z.; Farahbakhsh, R.; Tyson, G.; Crowcroft, J. A Large-Scale Behavioural Analysis of Bots and Humans on Twitter. *ACM Trans. Web* **2019**, *13*, 7:1–7:23. [CrossRef]
49. Hwang, T.; Pearce, I.; Nanis, M. Socialbots: Voices from the Fronts. *Interactions* **2012**, *19*, 38–45. [CrossRef]
50. McGonagle, T. "Fake News": False Fears or Real Concerns. *Neth. Q. Hum. Rights* **2017**, *35*, 203–209. [CrossRef]
51. Luo, M. How the N.R.A. Manipulates Gun Owners and the Media. *The New Yorker Magazine*, 11 August 2017.
52. Jowett, G.; O'Donnell, V.; Jowett, G. *Propaganda & Persuasion*, 5th ed.; SAGE: Thousand Oaks, CA, USA, 2012; ISBN 978-1-4129-7782-1.
53. Daniels, J. *Cyber Racism: White Supremacy Online and the New Attack on Civil Rights*; Rowman & Littlefield Publishers: Washington, DC, USA, 2009; ISBN 978-0-7425-6525-8.
54. Marwick, A.; Lewis, R. Media Manipulation and Disinformation Online. 2017, p. 106. Available online: https://datasociety.net/library/media-manipulation-and-disinfo-online/ (accessed on 21 October 2020).
55. Cha, A.E. The Origins of Donald Trump's Autism/Vaccine Theory and How It Was Completely Debunked Eons Ago. *The Washington Post*, 17 September 2015.
56. Twitter Disclosing Networks of State-Linked Information Operations We've Removed. Available online: https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html (accessed on 21 October 2020).
57. Paul, K. *Twitter Suspends Accounts Linked to Saudi Spying Case | Reuters*; Thomson Reuters: Ann Arbor, MI, USA, 2019.
58. Garrett, R.K. Echo Chambers Online?: Politically Motivated Selective Exposure among Internet News Users. *J. Comput.-Mediat. Commun.* **2009**, *14*, 265–285. [CrossRef]
59. Flaxman, S.; Goel, S.; Rao, J.M. Filter Bubbles, Echo Chambers, and Online News Consumption. *Public Opin. Q.* **2016**, *80*, 298–320. [CrossRef]
60. Quattrociocchi, W.; Scala, A.; Sunstein, C.R. Echo Chambers on Facebook. *SSRN Electron. J.* **2016**. [CrossRef]
61. Bakir, V.; McStay, A. Fake News and The Economy of Emotions: Problems, Causes, Solutions. *Digit. J.* **2018**, *6*, 154–175. [CrossRef]
62. Subramanian, S. Inside the Macedonian Fake-News Complex. *Wired*, 15 February 2017. Available online: https://www.wired.com/2017/02/veles-macedonia-fake-news/ (accessed on 30 May 2022).
63. Chen, Y.; Conroy, N.J.; Rubin, V.L. News in an Online World: The Need for an "Automatic Crap Detector". Available online: https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/pra2.2015.145052010081 (accessed on 30 August 2019).
64. Wardle, C.; Derakhshan, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Available online: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html (accessed on 29 August 2019).
65. Wardle, C.; Derakhshan, H. How Did the News Go 'Fake'? When the Media Went Social | Claire Wardle and Hossein Derakhshan. *The Guardian*, 10 November 2017.
66. Taneja, H.; Viswanathan, V. Still Glued to the Box? Television Viewing Explained in a Multi-Platform Age Integrating Individual and Situational Predictors. *Int. J. Commun.* **2014**, *8*, 26.
67. Taneja, H.; Webster, J.G.; Malthouse, E.C.; Ksiazek, T.B. Media Consumption across Platforms: Identifying User-Defined Repertoires. *New Media Soc.* **2012**, *14*, 951–968. [CrossRef]
68. Nelson, J.L.; Taneja, H. The Small, Disloyal Fake News Audience: The Role of Audience Availability in Fake News Consumption. *New Media Soc.* **2018**, *20*, 3720–3737. [CrossRef]
69. Anita Elberse Should You Invest in the Long Tail? Available online: https://hbr.org/2008/07/should-you-invest-in-the-long-tail (accessed on 20 October 2020).
70. Guess, A.; Nagler, J.; Tucker, J. Less than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook. *Sci. Adv.* **2019**, *5*, eaau4586. [CrossRef]
71. Pool, C.R. A New Digital Literacy: A Conversation with Paul Gilster. *Educ. Leadersh.* **1997**, *55*, 6–11.
72. Eshet, Y. Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era. *J. Educ. Multimed. Hypermedia* **2004**, *13*, 93–106.
73. Gardner's Multiple Intelligences. Available online: http://www.tecweb.org/styles/gardner.html (accessed on 26 August 2019).
74. Adams, N.B. Digital Intelligence Fostered by Technology. *J. Technol. Stud.* **2004**, *30*, 93–97. [CrossRef]
75. Lazer, D.M.J.; Baum, M.A.; Benkler, Y.; Berinsky, A.J.; Greenhill, K.M.; Menczer, F.; Metzger, M.J.; Nyhan, B.; Pennycook, G.; Rothschild, D.; et al. The Science of Fake News. *Science* **2018**, *359*, 1094–1096. [CrossRef] [PubMed]

76. Kalla, J.L.; Broockman, D.E. The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments. *Am. Polit. Sci. Rev.* **2018**, *112*, 148–166. [CrossRef]
77. Sternisko, A.; Cichocka, A.; Van Bavel, J.J. The Dark Side of Social Movements: Social Identity, Non-Conformity, and the Lure of Conspiracy Theories. *Curr. Opin. Psychol.* **2020**, *35*, 1–6. [CrossRef] [PubMed]
78. Gelfert, A. Fake News: A Definition. *Informal Log.* **2018**, *38*, 84–117. [CrossRef]
79. Pennycook, G.; Cannon, T.D.; Rand, D.G. Prior Exposure Increases Perceived Accuracy of Fake News. *J. Exp. Psychol. Gen.* **2018**, *147*, 1865–1880. [CrossRef]
80. Islam, A.K.M.N.; Laato, S.; Talukder, S.; Sutinen, E. Misinformation Sharing and Social Media Fatigue during COVID-19: An Affordance and Cognitive Load Perspective. *Technol. Forecast. Soc. Chang.* **2020**, *159*, 120201. [CrossRef]
81. Conroy, N.J.; Rubin, V.L.; Chen, Y. Automatic Deception Detection: Methods for Finding Fake News: Automatic Deception Detection: Methods for Finding Fake News. *Proc. Assoc. Inf. Sci. Technol.* **2015**, *52*, 1–4. [CrossRef]
82. Rubin, V.L.; Conroy, N. Discerning Truth from Deception: Human Judgments and Automation Efforts. *First Monday* **2012**, *17*. [CrossRef]
83. Tacchini, E.; Ballarin, G.; Della Vedova, M.L.; Moret, S.; de Alfaro, L. Some Like It Hoax: Automated Fake News Detection in Social Networks 2017. *arXiv* **2017**, arXiv:1704.07506.
84. Vlachos, A.; Riedel, S. Fact Checking: Task Definition and Dataset Construction. In Proceedings of the ACL 2014 Workshop on Language Technologies and Computational Social Science, Baltimore, MD, USA, 26 June 2014; Association for Computational Linguistics: Baltimore, MD, USA, 2014; pp. 18–22.
85. Ferreira, W.; Vlachos, A. Emergent: A Novel Data-Set for Stance Classification. In Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, San Diego, CA, USA, 12–17 June 2016; Association for Computational Linguistics: San Diego, CA, USA, 2016; pp. 1163–1168.
86. Wang, W.Y. "Liar, Liar Pants on Fire": A New Benchmark Dataset for Fake News Detection. *arXiv* **2017**, arXiv:1705.00648.
87. Figueira, Á.; Oliveira, L. The Current State of Fake News: Challenges and Opportunities. *Procedia Comput. Sci.* **2017**, *121*, 817–825. [CrossRef]
88. Rubin, V.; Conroy, N.; Chen, Y.; Cornwell, S. Fake News or Truth? Using Satirical Cues to Detect Potentially Misleading News. In Proceedings of the Second Workshop on Computational Approaches to Deception Detection, San Diego, CA, USA, 17 June 2016; Association for Computational Linguistics: San Diego, CA, USA, 2016; pp. 7–17.
89. Pierson, D. Facebook and Google Pledged to Stop Fake News. So Why Did They Promote Las Vegas-Shooting Hoaxes? Available online: https://www.latimes.com/business/la-fi-tn-vegas-fake-news-20171002-story.html (accessed on 4 October 2019).
90. Atodiresei, C.-S.; Tănăselea, A.; Iftene, A. Identifying Fake News and Fake Users on Twitter. *Procedia Comput. Sci.* **2018**, *126*, 451–461. [CrossRef]
91. Barzic, G.; Kar-Gupta, S. Facebook, Google Join Drive against Fake News in France. *Reuters*, 2017. Available online: http://www.reuters.com/article/us-france-election-facebook-idUSKBN15L0QU (accessed on 30 May 2022).
92. Kosslyn, J.; Yu, K. Fact Check Now Available in Google Search and News around the World. Available online: https://www.blog.google/products/search/fact-check-now-available-google-search-and-news-around-world/ (accessed on 24 September 2019).
93. BBC News QAnon: Twitter Bans Accounts Linked to Conspiracy Theory—BBC News. Available online: https://www.bbc.com/news/world-us-canada-53495316 (accessed on 11 August 2020).
94. BBC News Coronavirus: Twitter Bans "unsafe" Advice about the Outbreak—BBC News. Available online: https://www.bbc.com/news/technology-51961619 (accessed on 11 August 2020).
95. Kelly, H. Facebook, Twitter Penalize Trump for Posts Containing Coronavirus Misinformation. *The Washington Post*, 5 August 2020.
96. Choi, M. A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. *Theory Res. Soc. Educ.* **2016**, *44*, 565–607. [CrossRef]
97. SOMA Social Observatory for Disinformation and Social Media Analysis | SOMA Project H2020. Available online: https://cordis.europa.eu/project/id/825469 (accessed on 27 August 2020).
98. PROVENANCE Providing Verification Assistance for New Content | PROVENANCE Project | H2020. Available online: https://cordis.europa.eu/project/id/825227 (accessed on 27 August 2020).
99. European Commission Financialy Supported Projects against Disinformation. Available online: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_en (accessed on 27 August 2020).
100. European Commission European Commission—Press Release. Available online: https://europa.eu/rapid/press-release_IP-17-4481_el.htm (accessed on 3 September 2019).
101. Pieters, J. Dutch Government to Launch Anti-Fake News Campaign. Available online: https://nltimes.nl/2018/12/13/dutch-government-launch-anti-fake-news-campaign (accessed on 4 October 2019).
102. Baumann, A. Danmark Får Ny Kommandocentral Mod Misinformation. Available online: //www.mm.dk/tjekdet/artikel/danmark-faar-ny-kommandocentral-mod-misinformation (accessed on 4 October 2019).
103. Funke, D.; Flamini, D. A Guide to Anti-Misinformation Actions around the World. Available online: https://www.poynter.org/ifcn/anti-misinformation-actions/ (accessed on 25 September 2019).
104. PolitiFact. Available online: https://www.politifact.com/ (accessed on 26 October 2020).

105. Snopes.Com—The Definitive Fact-Checking Site and Reference Source for Urban Legends, Folklore, Myths, Rumors, and Misinformation. Available online: https://www.snopes.com/ (accessed on 26 October 2020).
106. CaptainFact.Io. Available online: https://captainfact.io/ (accessed on 26 October 2020).
107. Fray, P. Is That a Fact? Checking Politicians' Statements Just Got a Whole Lot Easier | Peter Fray. *The Guardian*, 18 April 2016.