data

Communication

The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats

Kevin Matthe Caramancion *, Yueqi Li, Elisabeth Dubois and Ellie Seoe Jung

College of Emergency Preparedness, Homeland Security, and Cybersecurity, University at Albany, State University of New York, Albany, NY 12222, USA; yli69@albany.edu (Y.L.); evdubois@albany.edu (E.D.); sjung@albany.edu (E.S.J.)
* Correspondence: kcaramancion@albany.edu

Abstract: This study examines the phenomenon of disinformation as a threat in the realm of cybersecurity. We have analyzed multiple authoritative cybersecurity standards, manuals, handbooks, and literary works. We present the unanimous meaning and construct of the term cyber threat. Our results reveal that although their definitions are mostly consistent, most of them lack the inclusion of disinformation in their list/glossary of cyber threats. We then proceeded to dissect the phenomenon of disinformation through the lens of cyber threat epistemology; it displays the presence of the necessary elements required (i.e., threat agent, attack vector, target, impact, defense) for its appropriate classification. To conjunct this, we have also included an in-depth comparative analysis of disinformation and its similar nature and characteristics with the prevailing and existing cyber threats. We, therefore, argue for its recommendation as an official and actual cyber threat. The significance of this paper, beyond the taxonomical correction it recommends, rests in the hope that it influences future policies and regulations in combatting disinformation and its propaganda.

Keywords: disinformation; infodemic; information disorder; cyber threat; cybersecurity; vulnerability

Citation: Caramancion, K.M.; Li, Y.; Dubois, E.; Jung, E.S. The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data* **2022**, *7*, 49. https://doi.org/10.3390/data7040049

Academic Editors: Riccardo Ortale and Gianni Costa

Received: 13 December 2021
Accepted: 8 April 2022
Published: 12 April 2022

1. Introduction

According to a report by the Institute for Public Relations, 63% of Americans view disinformation as a major problem in society, yet there are limited avenues to combat it outside of media literacy and news spaces [1]. similarly, a report by Neustar International Security Council (NISC) found that 48% of cybersecurity professionals think of disinformation as a threat, of which 49% say the threat is very significant. The study also found that 91% of cybersecurity professionals thought that stricter measures should be implemented on the Internet [2]. The gravity of the impact of disinformation on the confidentiality, integrity, and availability of information makes it necessary to view disinformation not simply as an error of information but as a form of cyberattack.

Cybersecurity relates to the protection and defense of personal information, computer systems, and critical infrastructure. Cyber threats tend to compromise the confidentiality, integrity, and availability of technology systems. Disinformation, the sharing of deliberately misleading or biased information, has been formally classified as an information disorder by the Council of Europe (2017) [3]. The goal of disinformation is to change an individual's thoughts and behaviors, consequently influencing public opinion by altering one's view of reality or accentuating one's prior held beliefs to disrupt truth-seeking. Deceptive information can leave people confused about basic facts and current events, creating a dangerous situation affecting public safety, organizational reputations, or governmental functions. In many ways, disinformation is thus similar to a cyberattack, where instead of compromising a computer system, it compromises our cognitive abilities. Such disruptions have been coined cognitive hacking—where such practices can result in a greater threat than a cyberattack on critical infrastructure [4]. The damage caused by disinformation can be challenging to repair, as people form opinions based on cognitive and confirmation biases. The deceptive nature of disinformation is further accentuated by economic pressures and advertisement-centric models that incentivize disinformation to overload information channels, often drowning the truth. Just as technology and social media expansion increase cybersecurity risks, they exacerbate the impact of disinformation.

Disinformation is plentiful, especially in the current global climate, where much of the deceptive information has been bred or derived from conspiracy theories or political or group ideologies. Here are a few examples of disinformation:

During the 2016 Presidential Campaign, Donald Trump tweeted U.S. crime statistics that stated that the proportion of whites killed by whites was 16% and of whites killed by Blacks was 81%, while in reality, the numbers were reversed, seeing that only about 16% of whites were killed by Blacks [5].

Jayda Fransen, Deputy Leader of Britain First, an ultranationalist hate group, tweeted a video with the caption: "Muslim migrant beats up Dutch boy on crutches!" Then-President Trump retweeted the video, yet soon after, the Netherlands Embassy retweeted with "Facts do matter. The perpetrator of the violent act in this video was born and raised in the Netherlands…" [5].

Natural News, a site commonly dealing in conspiracy theories, headlined that "Vaccines containing mercury are "medical genocide" that target black communities to damage their babies." By mirroring truthful news articles via seemingly realistic external hyperlinks, they seek to sway public opinion [5].

The Seattle Tribune, a fake news site machining a legitimate news site, shared a fake story about an "Idaho mother sentenced to prison for breastfeeding." This story continues to be shared on social media and sways the discussion around breastfeeding in public [5].

Disinformation campaigns have promoted false narratives that 5G technology suppresses immune systems and that 5G spectrum bands spread COVID-19 [6].

During the early days of the pandemic, false claims were being raised that the National Guard Bureau, of which there is no such entity, would be supporting nationwide quarantines [6].

False information about COVID-19 treatments are still being circulated on social media, many of which present harmful suggestions such as drinking bleach or that "illicit drug activity can "cure" the virus." [6].

The questions one must ask are: Does disinformation compromise cognitive reasoning? If so, is it similar to other cybersecurity threats that may cause harm to an organization or harm public health, specific groups, or public order?

Disinformation and similar information disorders are seldom included in the list of recognized cybersecurity threats in the manuals and appendices of standardizing organizations [7] (National Academies of Sciences, Engineering, and Medicine, 2015). Stemming from Caramancion (2020) [8], such exclusion coupled with the increasing use of disinformation campaigns warrant the classification of disinformation as a cybersecurity threat. To properly counteract disinformation, we must treat it as a cybersecurity issue—where experts have successfully understood, mitigated, and defended against malicious threats caused by phishing, viruses, advanced persistent threats, and other issues. Only recently, in the latest report by ENISA, have disinformation and misinformation been identified as one of the 8 cybersecurity threat categories [9].

The literary contribution of this paper is through its investigation of whether disinformation should be included as part of the international cybersecurity risk continuum. This study critically analyzes cybersecurity industry standards and conducts a comparative assessment of common cybersecurity risks. In doing so, we argue that disinformation is not only a critical threat missing from industry standards; in many ways, entities face greater risks along the risk continuum by not understanding the role of disinformation in risk management. This argument places disinformation as a cybersecurity risk, where deceptive information exploits psychological vulnerability, builds off biases, and comprises logical reasoning leading to cognitive discrepancies, much like current cybersecurity threats.

The practical contribution of this paper rests in the discussion that it provides to integrate disinformation into industry standards and the cybersecurity risk continuum to ensure both a technical and human approach to cybersecurity to respond to the increased reliance on technology. This paper aims to better inform academics and practitioners by establishing a novel approach to studying and conducting risk management of cybersecurity threats in the information era.

2. Literary Background

2.1. Disinformation vs. Other Information Disorders

Fake news, as a phenomenon, has been widely misrepresented. The very definition of fake news has been disputed due to the varying nature of its account [10]. The Council of Europe (2017) has promulgated the concept of information disorders with regards to the phenomenon of fake news. Information disorders are defined as polluters of the information environment. These include but are not exhaustively limited to information presenting itself as deceptive content and hate speech usually fueled by radicalism in beliefs and political positions [3].

Information disorders are further divided into three types, (1) misinformation, (2) disinformation, and (3) malinformation. The common end result of the first two types is deception. The only distinguishing characteristic between them is the prong of intent in the act itself [11]. The former lacks the intent of the creators and spreaders [12] and often occurs by accident due to outdated information, mistranslations, and misapplications, whereas the latter is usually grounded in computational propaganda carefully engineered to explicitly deceive in a broader, more public scope [13]. Malinformation, on the other hand, lacks the resulting deception from the two types of information disorders but is characterized by similarity with disinformation, in that they both mean harm. Forms of malinformation include hate speech, the promotion of violence, and leaks. Malinformation, however, lacks the particular effect of deception since it typically has no associated legitimacy in its forms.

From these underpinnings, it can be inferred that the two distinguishing elements of disinformation from the other types of information disorders are its (1) intentional deception and (2) the harm it intends to produce [8]. With regard to the context of being a threat in digital spaces, disinformation's uniqueness is its very form of falsehood, its disguise as legitimate news headlines and information [8]. This phenomenon as a threat is further amplified by increasing its reach through sophisticated technologies, making it appear as highly believable content through the careful engineering of its components, such as words in headlines and exceptional alterations in the supporting media (photos or videos) that come with them [11].

2.2. An Overview of Cyber Threats

Cyber threats were categorized as I.T. issues in the past. As cyberattacks have evolved rapidly and caused increasing damage to organizations and society in recent decades, business leaders have started to recognize cyber threats as an enterprise-wide risk management issue [14]. Today, organizations are expected to take a progressive approach to respond to cyber threats, where C-suite has a deep involvement in the designing and managing of security measures, advanced technologies are employed, and ongoing reviews of cyber risks are conducted by the I.T. team using third-party expertise [15].

There have been multiple attempts to define cyber threats in the literature. The National Institute of Standards and Technology (NIST) defined cyber threats as “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service” [16]. NIST also released a later version of the definition of the cyber threat in NIST SP 800-160 Vol. 1 and emphasizes that the basis of asset loss constitutes all forms of cybersecurity events and their associated conditions [17]. In addition to asset loss, the term “negative impact” was used by Brauch (2011) [18] to cover both tangible losses like financial loss and intangible losses like reputation damage [19,20]. A threat action can be allocated with a sophisticated level of expertise and significant resources using multiple attack vectors; NIST refers to this advanced type of cyber threat as advanced persistent threat (A.P.T.). Other than A.P.T., researchers have also recognized a variety of new generation threats, such as polymorphic threats, zero-day threats, composite threats, and others [21].

Cyber threats can cause huge losses to the market and to individual organizations. So far, a cybersecurity breach can result in a 21,659 USD recovery expense to an organization, on average [22], and a drop in its stock price [23–25]. Among all the security breaches reported in Verizon’s 2021 Data Breach Investigations Report (DBIR) [22], 85% involved a human element, while 61% involved credentials. External attackers consist of mainly state-sponsored groups of geopolitical interest, hacktivists aiming to denounce the activities of target organizations, cybercriminals motivated by financial gains, and some cyberterrorists [26]. Consistent with findings from previous years, the threat actors are mainly external individuals and organizations, while financial gains motivate most of the cyberattacks [27,28].

Phishing, social engineering, web application attacks, denial of service (DoS), malware, and ransomware are the most prevalent threat actions in recent years [22,29,30]. Phishing occurs when an attacker attempts to fraudulently obtain sensitive information from a user by disguising as a trustworthy entity [31]. Social engineering is a threat that relies on human interaction, in which a social engineer manipulates the victim into giving sensitive information [32]. Malware is a file or a program that is intended to damage the computer system; examples include computer worms, viruses, Trojan horses, and spyware [30]. Ransomware is also an example of malware, in which the attacker locks the victim’s computer system files and demands a payment to unlock the file [30]. Web application attacks usually refer to attacks with a small number of actions after the initial web application compromise [22]. DoS is an attack that compromises the availability of networks and systems, forbidding legitimate users to access the system [22]. All these threats have raised broad concerns among industries and society as a whole. Beyond the most prevalent threats, ENISA distinguished itself by detailing eight threat groups including ransomware, malware, cyptojacking, email-related threats, threats against data, threats against availability and integrity, disinformation, and non-malicious threats [9]. ENISA’s report is one of the few that cite misinformation or disinformation at the core of cybercrime activities, which continue to increase exponentially in the wake of COVID-19.

2.3. The Importance and Implications of Classifying Cyber Threats

Previous work has attempted to classify cyber threats in different ways. However, few of them have systematically highlighted the importance and the implications of cyber threat classification. The use of taxonomy is generally to gain a greater understanding of a subject; a useful taxonomy should be precise, logical, intuitive, and can be adapted to different application needs [33]. To manage the threats, one should first understand the threat sources and specific areas of the system that may be impacted [34,35]. Therefore, threat classification is necessary because it helps individuals understand threat causes and impacts.

Despite various steps towards cybersecurity, the ultimate goal is to protect digital assets from attackers. Ref. [36] argued that a completely secure solution considers more than one aspect. Classification efforts on cyber threats contribute to cybersecurity by providing key commonalities of the threats as well as variances among them, covering broad aspects including, for example, attack vectors, operational impacts, defense, informational impacts, and targets [37]. As suggested by Al Hwaitat (2020) [38], classifying cyber threats is the major step in designing and implementing effective mitigation measures, which help entities and individuals to understand the nature of the threat and the corresponding security procedures. Threat classification helps identify and organize cyber threats into categories so that security experts can evaluate the impact category by category and develop appropriate measures to target each categorized threat group [39][40]. While the classification scheme assists the organizational defense in protecting the network, for example, by publicizing critical threat information that guides the design of defense strategies, the classification of security threats also benefits cybersecurity awareness in organizations [37]. Classifying different aspects of the malicious uses of a specific technology, such as artificial intelligence (A.I.), also lays a foundation for the detection of and help in predicting future threats [41].

2.4. Classification Criteria

Cyber threats can be observed and classified in different ways by considering different criteria such as sources, agents, and motivations [33]. In fact, there have been exhaustive attempts to classify cyber threats based on different criteria. In this study, we systematically list the criteria that previous studies use in order to define a set of criteria that we are going to use for the analysis of disinformation.

In the existing literature, a majority of cyber threat classification work tends to use threat agent [22,42], attack vector [37,43], target [37], impact [22,37,41–43], and defense [37,41]. When an individual or group uses several vectors to exploit cybersecurity vulnerabilities and conducts activities harmful to an entity, the attacking individual or group is referred to as a threat agent or threat actor, and the paths the threat agent used to exploit the target's system vulnerabilities are called attack vectors, sometimes referred to as threat actions [22].

The ***threat agent*** is a major element of a successful cyberattack. Previous work has classified cyber threats according to different characteristics of the agent. Most research tends to classify cyber threats into human threats and technological threats (e.g., [33,42]). A good example of human threats would be social engineering, while examples of technological threats can be malware or worms. The actor can also be divided into the individual type and entity type: individual actors include the abusive user, the cyber-bully, the cyber-criminal, cyber-fighter, cyber-terrorist, the hacktivist, the insider, the online social hacker, the script kiddie, and the sexually deviant user, while entity actors include organizations and states or countries [44]. The DBIR reports usually categorize threat agent sources as external actors and internal ones, which is consistent with the characterization of Jouini et al. [33]. In terms of the characteristics of the threat agent, the difference between an error and an attack is the malicious intent of the actor(s).

Different goals also differentiate among cyber threats, that is, what the threat agent wants to achieve from the cyberattack. Many typical goals have been discussed in the literature, such as creating fearful and threatening situations [43], directly punishing a person [45], personal satisfaction, or recompense [42]. As we mentioned earlier, most attackers are driven by financial gains, while some others are driven by espionage [22]. Therefore, another important criterion is the ***motivation of attackers***, either malicious or non-malicious [42].

Researchers also use different terms to describe the ***target(s)***, which are the attacked hosts within the attacked entity, including the operating system, network, local computer, user, and application [37]. The targets are sometimes referred to as security layers (application, transport, network, data link, physical, etc.) [46]. Within attack vectors, some research also categorizes cyber threats based on security levels (data, access, and network) [46].

The ***impact***, which is usually negative, typically includes the financial loss and reputational damage of the target. Simmons et al. [37] further distinguished operational impact from informational impact. In their description of the two categories of impact, operational impact refers to the effects on the daily operation of the information systems and the business, such as the inability to access systems, while the informational impact relates more to the effects on the sensitive information itself. The impacted assets can be subject to different damage based on their three attributes—confidentiality, integrity, and availability, according to the C.I.A. 31st Triad. Heartfield et al. [43] focused on attack vectors and the impact of cyber threats; they separately discussed the impact on systems, including physical impact and cyber impact, and the impact on individual users. In addition to the breach of physical privacy and unauthorized, incorrect, delayed, or disrupted operations, cyberattacks also harm users' experiences and emotions [43].

Defense methods, including ***mitigation and remediation strategies*** [37], are also an important source that has been used to classify different cyber threats in the recent decade. Table 1 shows the classification criteria summary for the mentioned sources.

Table 1. Summary of Cyber Threat Classification Criteria.

	Threat Agent				Attack Vector	Target	Impact		Defense	
	Actor	Source	Motivation	Goal			Systems	Users	Mitigation	Remediation
Hansman and Hunt (2005)	0	0	0	0	1	1	1	0	0	0
Kjaerland (2006)	1	1	1	0	1	1	1	0	0	0
Simmons et al., (2014)	0	0	0	0	1	1	1	1	1	1
Jouini et al., (2014)	1	1	1	1	0	0	1	0	0	0
Heartfield et al., (2018)	0	0	0	0	1	0	1	1	1	0
Tsakalidis and Vergidis (2019)	1	1	1	0	1	1	1	1	1	1
Humayun et al., (2020)	1	0	0	0	1	1	0	0	1	0
Almaiah et al., (2021)	0	1	1	1	1	1	1	0	0	0
DBIR 2021	1	1	0	0	1	1	1	0	0	0

1 = The corresponding study applies this criterion in their classification of cyber threats; 0 = The corresponding study does not apply this criterion in their classification of cyber threats.

Interestingly, there are other aspects of the criteria that researchers and institutions use to classify cyber threats. The DBIR 2021 report also discusses the cyber threats according to the timeline in terms of which breach types take the longest to discover. In the work of King et al. [47], the attack pre-conditions are captured, which is defined as the presence of all the information needed for the successful undertaking of a cyberattack. In addition to the harm to systems and users proposed by Heartfield et al. [43], Tsakalidis and Vergidis [44] point out the inchoate harm that is inflicted by inchoate cybercrimes, i.e., the potential for harm due to incomplete cybercrimes. Moreover, recent work tends to focus on AI-based cyber threats due to the fact that the advancements in A.I. have enabled "more sophisticated, highly targeted, well-trained, and large-scale" cyberattacks [41] (p. 2), such as stealthy spyware, DeepLocker, PassGAN, and others.

In this study, we analyze the threat of disinformation and how it is comparable to other known cyber threats in the aspects of the threat agent, attack vector, target, impact, and defense. The detailed criteria are presented below in Table 2; descriptions of the items with the criteria are largely based on mentioned resources.

Table 2. Analysis Criteria for Disinformation and Other Cyber Threats.

Criteria		Description
Threat Agent	Actor	The agents that cause threats including human and technological agents; human agents can be at the individual level or entity level
	Source	The origin of threat, either internal or external
	Motivation	Whether the objective of threat actors is malicious or non-malicious
	Goal	The objectives or the type of damage that the actor wants to achieve out of the cyberattack
Attack Vector		The path that attackers use to exploit the vulnerabilities of the target
Target		The attacked hosts within the attacked entity, sometimes known as security layers, including operating system, network, local computer, user, application, transport, network, data link, etc.
Impact	System	Negative impact on the target's operations and information confidentiality, integrity, and availability.
	Users	Negative impact on user assets, experience, socialization, and/or emotions, etc.
Defense	Mitigation	Procedures employed prior to vulnerability exploitation or during an attack to mitigate the negative impact
	Remediation	Steps used by defenders to correct the situation prior to or during an exploitation

3. Methods

Overview

In addition to the epistemological definitions presented above, we have analyzed the publicly available cybersecurity knowledge systems through manuals and literary works and compiled their definitions of a cyber threat. In their respective content, we have also examined the inclusion of the phenomenon of Disinformation in the explicitly classified threat list, including the closely related synonyms such as Fake News and Misinformation. We divided these artifacts into two categories: (1) The most recent works in Table 3 and (2) the prevailing authoritative standards and manuals in Table 4.

Table 3. Recent Sources and Definitions of Cyber Threat.

Source	Definition of Cyber Threat	Inclusion of Disinformation
Enisa Thread Landscape (2021) [9]	Incidents that are usually not restricted to one particular sector and in most cases affect more than one of them. This is indeed true since in many cases the threats manifest themselves by exploiting vulnerabilities in underlying ICT systems that are being used in a variety of sectors.	One record found
NARUC Cybersecurity Manual (2021) [48]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through an I.T. and I.C.S. via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	None found
The Australian Cyber Security Centre (ACSC)'s Information	Any circumstance or event with the potential to harm systems or data.	None found

Security Manual (I.S.M.) (2021) [49]		
Canadian Centre for Cybersecurity's an Introduction to The Cyberthreat Environment (2021) [50]	An activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.	None found
CyBOK: The Cyber Security Body of Knowledge v1.1 (2021) [51]	An individual, event, or action that has the capability to exploit a vulnerability. Threats are also socio-technical and could include hackers, disgruntled or poorly trained employees, poorly designed software, a poorly articulated or understood operational process, etc. To give a concrete example that differentiates vulnerabilities from threats—a software interface has a vulnerability in that malicious input could cause the software to behave in an undesirable manner (e.g., delete tables from a database on the system), while the threat is an action or event that exploits the vulnerability (e.g., the hacker who introduces the malicious input to the system).	One record found
FFIEC Information Technology Examination Handbook Information Security (2021) [52]	An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.	None found

Table 4. Authoritative Sources and Definitions of Cyber Threat.

Source	Definition of Cyber threat	Inclusion of Disinformation
Cybersecurity and Infrastructure Security Agency (CISA) [53]	A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.	None found
Committee on National Security Systems (CNSS) [54]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	None found
National Institute of Standards and Technology (NIST) [55]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	None found
United States Department of Homeland Security [56]	Indication of potential harm to life, information, operations, the environment, and/or property may be a natural or human-created occurrence and includes capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm.	None found
Escal Institute of Advanced Technologies (SANS Institute) [57]	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.	None found
Information Systems Audit and Control Association (ISACA) [58]	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.	None found
Internet Engineering Task Force (IETF) [59]	A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. Any circumstance or event with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service.	None found

4. Results and Analyses

Using the most recent and authoritative sources discussed above, we coded and analyzed the main cyber threat vectors. Based on the findings in previous tables, we discuss how disinformation makes sense to be included alongside the commonly referenced cyber threats in Table 5.

Table 5. Summary of Cyber Threats.

Threats	Threat Agent				Attack Vector	Target Layer(s) from OSI	Impact		Defense	
	Actor	Source	Motivation	Goal			System	Users	Mitigation	Remediation
Disinformation	States, adversarial networks	Internal or external	Radicalism, interference in elections, cyberwarfare	Shape public perception	Advertisements, web searches, social networking platforms	Application	Reputational and economic damage; systemic deception	Negative user psychological effects, social conflicts	Fake news detection, astroturf (bots) removal	Public awareness on proper user recognition of content legitimacy
Phishing	Nation-state attackers, criminal organizations	External	Financial gain, trade secrets, social and political reasons, a competitor's loss of reputation	Impersonate victims and access important online accounts	Fake emails, fake SMS or instant messages, and fake websites that may look authentic	Application	Disruption of system operations; alter, damage, steal, or disrupt data	Identity theft; loss of money, intellectual property and customers; reputational damage; heavy regulatory fines	Security measures deployed by modern browsers (blacklists and visual indicators) that highlight the top-level domain of a URL; anti-phishing training; and public awareness	Strong firewall and IPS protection on the network perimeter; strengthen password policies; monitor all database access

								campaigns that sensitize and teach users to spot phishing URLs	
Social engineering	Largely nation-states, cybercriminals and criminal organizations, some hacktivists, or even individuals	External (invaders) or internal (saboteurs)	Financial gain, trade secrets, social and political reasons, a competitor's loss of reputation	Trick targets into divulging sensitive information or performing certain actions	Psychological manipulation of targeted individuals	Front-end users, data	Disruptions of system operations; alter, damage, steal, or disrupt data	Loss of money and intellectual property; reputational damage	Train employees about password confidentiality and security protocols and enforce these protocols	Strong firewall and IPS protection on the network perimeter; strengthen password policies; monitor all database access; top-down approach with security measures in case saboteurs could be from all privilege levels

Web application attacks	Nation-states, cybercriminals	Internal	Disruption	Gain access to sensitive information, profit	Program alterations, unauthorized software code injections	Application, presentation, session	Can alter, damage, steal, or disrupt systems or data; lock access to or release system information or data	Steal personal information (i.e., financial or health); falsify or modify personal data; lock access to or release sensitive information to the public	Software updates; anomaly detection; software quality checks/assurance	Correction of compromised software components; backup versions rollback
Distributed denial of service (DDoS)	Nation-states, cybercriminals	External	Operational disruption	Impair systems	Overwhelming a target device, network, or web program/software with traffic	Network, transport	Network outage, operational disruption, financial loss	Lock out of networks/systems; productivity loss	Frequent network traffic monitoring; regular update of authorized traffic sources	Enforce access control lists; filter unauthorized traffic from networked attackers
Malware	Nation-states, cybercriminals	Internal or external	Ideology, profit	Gain access to sensitive information, damage	Viruses, worms, trojans; viruses are executable programs that insert codes into legitimate	Application, presentation, session	Can alter, damage, steal, or disrupt systems or data Lock	Steal personal information (i.e., financial or health);	Anomaly detection; misuse detection approach; host-based	Update firewall and network intrusion detection system rules

				systems or data	programs.Worms are self-replicating programs that spread in systems to drain their resources. Trojans are malicious programs disguised as legitimate software aimed at damaging a system.		access to or release system information or data	falsify or modify personal data; lock access to or release sensitive information to the public	monitoring of system activities; network-based monitoring of traffic; machine learning security detection analysis; employee training	at local network access point; take down malware command and control infrastructure at internet service providers of top-level domain; perform attack attribution to identify culprits; machine learning–based detection approaches
Ransomware	Nation-states, cybercriminals	External	Ideology, profit	Extortion: block access to data or systems, or lock systems until	A Trojan or a worm is deployed via phishing or visiting a compromised website, where malicious	Application, presentation, session	Lock system until ransom is paid	Expose sensitive, personal, or embarrassing information unless	Anomaly detection; misuse detection approach; host-based monitoring of system	Prepare recovery plan, protect privileged roles, incrementally remove risks

				ransom is paid	software installs on a system or computer, causing that system or information to be encrypted. Upon encryption, a ransom message is displayed stating the deadline for monetary payment (often in bitcoin). Once paid, an encryption key is provided to unlock the system.			ransom is paid	activities; network-based monitoring of traffic; machine learning security detection analysis; employee training	
Advanced persistent threats (APTs)	Nation-states or state-sponsored groups	External	Malicious, geopolitical	Stay undetected to steal data	Spear phishing for initial network entry	Application	Disruption, data breach	Financial damage, data exfiltration	Malicious traffic detection, access control, user education	Threat intelligence
Polymorphic threats	Nation-states or state-	External	Geopolitical	Gain access to sensitive	Social engineering or phishing	Application	Disruption	Financial damage	Behavior-based detection,	Behavior blocking and containment

	sponsored groups			information, damage system or data					user education	
Zero-day threats	Cyber criminals, hacktivists	Internal	Financial gain, ideology	Gain access to sensitive information	Unknown software vulnerability, social engineering, or phishing	Application	Disruption, data breach	Financial damage, identity theft	Traffic monitoring, malware detection, user education	Patch
Composite threats	Organizations, cyber criminals	External	Financial gain, disruption	Gain access to sensitive information, damage system or data	Social engineering or phishing	Multiple layers	Disruption, destruction	Data exfiltration	User education, intrusion prevention, continuous monitoring	Network behavior analysis

5. Discussion

5.1. Disinformation, Phishing, Social Engineering

Since phishing is essentially a major technique of social engineering, they are the same in a lot of aspects [16]. The threats of phishing and social engineering both target security layers of data and users, both of them directly manipulate victims to divulge sensitive information [51]. Social engineering/phishing and disinformation are similar in terms of their threat actors, impact, and defense methods. All these threats involve nation-state attackers, reputational and economic damage, and the defense methods of public education and detection measures for suspicious activities. In addition, both social engineering/phishing and disinformation directly trick front-end users. Human weaknesses, traditionally targeted by attackers, are consistent between disinformation and phishing. Research has found that intuitive thinking style and willingness to share personal information significantly lead to a higher risk of phishing [60]. This is similar to the disinformation trap given Pennycook et al., (2020) [61] in their finding that disinformation is driven by victims' cognitive laziness. While social engineering/phishing attacks are more driven by economic gains, disinformation is more motivated by radicalism, interference in elections, or cyberwarfare. The different motivations lead to the distinct goals of these attacks—while social engineering/phishing aims at obtaining sensitive information and make money from the attack, disinformation is used to achieve the goal of reshaping public perception. The attack vectors for social engineering are mainly communications through email or phone messages, while for disinformation they could be through various approaches, such as advertisements, web searches, and social media. Overall, our findings lend support to Caramancion 's (2020) [8] argument that disinformation should be classified as a cyber threat.

5.2. Disinformation and Web Application Attacks

The commonality of web application and disinformation attacks is their characteristic and design for hiding behind a legitimate surface vector. Whereas the former is usually embedded in software and its components, the latter is usually engineered to appear as a legitimate authoritative source of news information. To lure users, they both rely on the human contextual vulnerability to trust familiar procedures and interfaces. It should further be emphasized that they are both carefully engineered to deceive, and as such, recognition of their true nature remains elusive unless a user is trained and familiar with them.

5.3. Disinformation and Distributed Denial of Service (DDoS)

The common ground between disinformation and distributed denial of service (DDoS) rests upon the coordinated acts of propaganda on the part of the threat enforcers, which can either be humans or their mechanical counterparts. While DDoS attacks aim at the disruption of services, disinformation's goal is to reshape public perception. Furthermore, they can be both commonly funded by adversarial entities such as nations or institutions due to the costs associated with their massive deployments on a global scale. Preventive mechanisms on both of their phenomena require prompt detection. While DDoS are typically recognized through intrusion detection/prevention systems, disinformation instances are typically detected in the automated detectors in social platforms after a reporter (or crowd reporters) notify the involved providers. Finally, strategies for their remediation are geared more towards developers and providers since these threats operate at the level of the medium itself.

5.4. Disinformation, Malware, and Ransomware

Malware is malicious software or firmware that gains unauthorized access to a system affecting the confidentiality, integrity, or availability of that system or data [48]. Ransomware, in turn, is one of the "most profitable" and "popular forms" of malware that gains unauthorized access to a system holding it hostage until demands, typically monetary, are met [62]. The threats of malware and ransomware are similar in that they both target data and users, both seeking to trick users into opening an attachment or clicking a link containing malicious code. Malware in its various forms, as well as ransomware, is similar to disinformation in terms of threat actors, targets, impacts, and defense mechanisms. The impact of malware is much like disinformation in that it can lead to reputational damage, economic loss, or loss of public trust. For example, if a hospital faces a ransomware attack, disinformation about the hospital's practices can hurt its reputation and cause the loss of its ability to perform at optimal capacity, resulting in economic loss, or even worse, physical lives lost. Alongside this loss of reputation, the public may not feel secure or safe seeking medical treatment at that hospital. In addition, malware and disinformation both trick front-end users. Such deception in malware is found via email attachments, malicious advertising (malvertising), fake software installations, infected USB drives, infected applications, phishing emails, and more [62]. Much like disinformation preys on human weaknesses, so too does malware. While forms of malware, including ransomware, are more driven by profit, disinformation seeks to reshape public perception or fulfill a preset agenda. In terms of defense, both malware and disinformation can be mitigated via machine learning or analogy, or disinformation detection. Similarly, for remediation and to mitigate the threats to various systems, addressing humans via public awareness and, more importantly, employee training is becoming commonplace. In this, bring your own device programs, safe email attachment practices, or training on depicting scams, or suspicious emails are seen across organizations, universities, and governments. Much like the defense mechanisms for countering disinformation, to protect against malware, it is recommended that you be careful online, where the risk of contracting malware or falling victim to misinformation is more common.

5.5. Disinformation, Zero-Day Attacks, and New Generation Threats

New generation threats are multi-vectored and often multi-staged. Advanced persistent threats (A.P.T.s) (also known as advanced targeted attacks, or A.T.A.s) are sophisticated network attacks in which an unauthorized person gains access to a network and stays undetected for a long period of time [63]. The A.P.T.s and disinformation share persistence as a common trait. These threats spread through networks, where disinformation is most commonly spread on social media. They can often be funded and used by nations or nation-funded organizations.

A polymorphic threat is a cyberattack—such as a virus, worm, spyware, or Trojan—that constantly changes ("morphs"), making it nearly impossible to detect using signature-based defenses [63]. Polymorphic threats and disinformation are difficult to spot. A network or social media platform can block activities based on behaviors.

A zero-day threat is a cyberattack on a publicly unknown operating system or application vulnerability, so named because the attack was launched on (or increasingly before) "day zero" of public awareness of the vulnerability [63].

Both zero-day threats and disinformation can impact organizational reputation and influence public opinion negatively. While the outcome can be costly, both financially and socially, the threats often are not discovered until the damage has been done.

Another new generation threat is composite threat. The composite threats are also called blended threats, which combine syntactic and semantic attack approaches [64]. Composite threats and disinformation have the commonality of using multiple media or methods. Disinformation can be spread through various communication platforms, such as social media or private messaging. Composite threats utilize a mix of malicious tools and exploits multiple vulnerabilities.

Many of the new generation threats and disinformation have similar threat actors, impacts, and they call attention to the importance of user education. As with other cyber threats, it is important for users to be aware of disinformation as a threat and be educated about new risks.

6. Conclusions and Future Works

As nations and organizations seek increased cybersecurity, it is essential for them to take into consideration all risks that may play on human weaknesses or affect their functional operations, reputation, or public safety. The findings of this study lend support to Caramancion 's (2020) [8] argument that disinformation should be classified as a cyber threat. As signified in this study, most, if not all, cyber threats play on human weaknesses, at least to some degree. Much like phishing, DDOS, malware, or A.P.T.s, disinformation too plays on human weaknesses. It is critical that as information threats increase, practitioners and academics alike begin to view disinformation through the lens of a critical cyber threat.

In the future, we recommend that cybersecurity threats are updated in manuals, and disinformation is better understood and discussed in the context of the harm it may present to particular individuals, groups, organizations, or governments. Disinformation must be discussed outside of political realm, to encompass the threats it poses to cybersecurity and daily decisions. Beyond simply defining disinformation and outlining what it consists of, one must properly stipulate its role in society and how disinformed individuals threaten businesses, processes, or the very government on which a country relies. The goal of this paper is to raise awareness on disinformation and cyber threats by providing a novel approach to categorizing it as a cyber threat with regard to the impact of and defense mechanisms needed to mitigate the harm. In the midst of a global pandemic, increasing inequalities, and widening digital divides emphasize the need for a better understanding of the threats the world faces, especially as more turn to technology for work and leisure, we must properly define, protect against, and mitigate cybersecurity threats. Thus, the disinformation infodemic requires a calculated and coordinated effort by governments, businesses, and the public to create robust standards and implement stronger human-centric defenses.

Author Contributions: Conceptualization, K.M.C.; methodology, K.M.C. and E.S.J.; formal analysis, K.M.C., Y.L., E.D. and E.S.J.; investigation, K.M.C. and Y.L.; resources, K.M.C.; data curation, Y.L.; writing—original draft preparation, K.M.C., Y.L., E.D. and E.S.J.; writing—review and editing, K.M.C.; visualization, K.M.C. and Y.L.; supervision, K.M.C.; project administration, K.M.C.; funding acquisition, K.M.C. 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.

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

References

1. McCorkindale, T. IPR Disinformation in Society Report; p. 23. 2019. Available online: https://instituteforpr.org/ipr-disinformation-study (accessed on 11 December 2021).
2. Coble, S. Cybersecurity Community Concerned about Misinformation. Available online: https://www.infosecurity-magazine.com/news/us-concerned-about-misinformation (accessed on 10 December 2021).
3. Wardle, C.; Derakshan, H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*; Council of Europe: Strasbourg, France, 2017.
4. Jaiman, A. Disinformation Is a Cybersecurity Threat. The Startup. Available online: https://medium.com/swlh/disinformation-is-a-cybersecurity-threat-335681b15b48 (accessed on 12 December 2021).
5. Pendell, K. LibGuides: Identify & Challenge Disinformation (aka Fake News): Examples. Portland State University. Available online: https://guides.library.pdx.edu/fakenews (accessed on 12 December 2021).
6. CISA. COVID-19 Disinformation Activity. May 2020. Available online: https://www.cisa.gov/publication/covid-19-disinformation-activity (accessed on 12 December 2021).
7. National Academies of Sciences, Engineering, and Medicine. *Appendix A—Categorized List of Cybersecurity Threats.* In *Guidebook on Best Practices for Airport Cybersecurity*; The National Academies Press: Washington, DC, USA, 2015. https://doi.org/10.17226/22116.

8. Caramancion, K.M. An exploration of disinformation as a cybersecurity threat. In Proceedings of the 2020 3rd IEEE International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; pp. 440–444.
9. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2021: April 2020 to Mid July 2021*; European Union Agency for Cybersecurity: Attiki, Greece, 2021. Available online: https://data.europa.eu/doi/10.2824/324797 (accessed on 13 March 2022).
10. Joshua, H.-C. Stop talking about fake news! *Inquiry* **2019**, *62*, 1033–1065.
11. Caramancion, K.M. Understanding the Impact of Contextual Clues in Misinformation Detection. In Proceedings of the 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021; pp. 1–6.
12. Stahl, B.C. On the difference or equality of information, misinformation, and disinformation: A critical research perspective. *Informing Sci. Int. J. Emerg. Transdiscipl.* **2006**, *9*, 83–96. https://doi.org/10.28945/473.
13. Howard, P.N.; Bradshaw; S. The global organization of social media disinformation campaigns. *J. Int. Aff.* **2019**, *71*, 23–32.
14. Larry, C. *Cyber-Risk Oversight, Director's Handbook Series*; Internet Security Alliance: Arlington, Virginia, 2017. Available online: https://regents.universityofcalifornia.edu/regmeet/july18/b4attach1. pdf (accessed on 10 December 2021).
15. Hill, J. The 4 Levels of Cybersecurity Readiness. (n.d.). Available online: https://www.business.att.com/learn/research-reports/the-4-levels-of-cybersecurity-readiness.html (accessed on 12 December 2021).
16. NIST. *Special Publication 800-30 Revision 1—Guide for Conducting Risk Assessments*; NIST Special Publication: Gaithersburg, MD, USA, 2012.
17. Ross, R.; Michael, M.; Janet, O. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*; No. NIST Special Publication (SP) 800-160 (Withdrawn); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
18. Brauch, H.G.; Úrsula, O.S.; Czeslaw, M.; John, G., Patricia, K.-M.; Béchir, C.; Pál, D.; Joern, B. *Coping with Global Environmental Change, Disasters and Security: Threats, Challenges, Vulnerabilities and Risks*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011; Volume 5.
19. Sinanaj, G.; Zafar, H. Who wins in a data breach?—A comparative study on the intangible costs of data breach incidents. In Proceedings of the Pacific Asia Conference on Information Systems, PACIS 2016, Chiayi, Taiwan, 27 June–1 July 2016; p. 60.
20. Taylor, T. How Reputational Damage from a Data Breach Affects Consumer Perception. Available online: https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception (accessed on 10 December 2021)
21. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001.
22. Verizon. *Verizon: 2021 Data Breach Investigations Report*; Computer Fraud & Security: New York, NY, USA, 2021; https://doi.org/10.1016/s1361-3723(21)00061-0.
23. Goel, S.; Shawky, H.A. Estimating the market impact of security breach announcements on firm values. *Inf. Manag***. 2019**, *46*, 404–410.
24. Goel, S.; Shawky, H.A. The impact of federal and state notification laws on security breach announcements. *Commun. Assoc. Inf. Sys*. **2014**, *34*, 1–3.
25. Rosati, P.; Cummins, M.; Deeney, P.; Gogolin, F.; van der Werff, L.; Lynn, T. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *Int. Rev. Financ. Anal.* **2017**, *49*, 146–154. https://doi.org/10.1016/j.irfa.2017.01.001
26. Thales; Verint. The CyberThreat Handbook. Available online: https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who (accessed on 10 December 2021)
27. Verizon. Data Breach Investigations Report. 2019G02G15. 2018. Available online: https://enterprise.verizon.com/resources/reG-ports/dbir (accessed on 10 December 2021)
28. Verizon. *Verizon Data Breach Investigations Report*; Verizon: New York, NY, USA, 2020.
29. Prasad, R.; Rohokale, V. Cyber Threats and Attack Overview. In *Springer Series in Wireless Technology*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2019; pp. 15–31.
30. Seemma, P.S.; Nandhini, S.; Sowmiya, M. Overview of cyber security. *Int. J. Adv. Res. Comput. Commun. Eng.* **2018**, *7*, 125–128.
31. Jagatic, T.N.; Johnson, N.A.; Jakobsson, M.; Menczer, F. Social phishing. *Commun. ACM* **2007**, *50*, 94–100. https://doi.org/10.1145/1290958.1290968.
32. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005.
33. Jouini, M.; Rabai, L.B.A.; Ben Aissa, A. Classification of security threats in information systems. *Procedia Comput. Sci.* **2014**, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452.
34. Alhabeeb, M.; Almuhaideb, A.; Le, P.D.; Srinivasan, B. Information security threats classification pyramid. In Proceedings of the 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, Los Alamitos, CA, USA, 20–23 April 2010; pp. 208–213.
35. Gerić, S.; Željko, H. Information system security threats classifications. *J. Inf. Organ. Sci.* **2007**, *31*, 51–61.
36. Amer, S.H.; Hamilton, J.A., Jr. Intrusion detection systems (IDS) taxonomy—A short review. *J. Softw. Technol.* **2010**, *13*, 1–3.
37. Simmons, C.; Charles, E.; Sajjan, S.; Dipankar, D.; Qishi, W. AVOIDIT: A cyber attack taxonomy. In Proceedings of the 9th Annual Symposium on Information Assurance, Kyoto, Japan, 4–6 June 2014; pp. 2–12.

38. Al Hwaitat, A.K.; Almaiah, M.A.; Almomani, O.; Al-Zahrani, M.; Al-Sayed, R.M.; Asaifi, R.M.; Adhim, K.K.; Althunibat, A.; Alsaaidah, A. Improved security particle swarm optimization (pso) algorithm to detect radio jamming attacks in mobile networks. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2020**, *11*, 614–624.
39. Fenz, S.; Andreas, E.; Thomas, N. Information security risk management: In which security solutions is it worth investing? *Commun. Assoc. Inf. Sys.* **2011**, *28*, 1–3.
40. Farahmand, F.; Shamkant, B; Navathe, G.; Sharp, P.; Enslow, P.H. A management perspective on risk of security threats to information systems. *Inf. Technol. Manag.* **2005**, *6*, 203–225.
41. Nektaria, K.; Li, J. The ai-based cyber threat landscape: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–34.
42. Almaiah, M.A.; Al-Zahrani, A.; Almomani, O. Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer: Cham, Switzerland, 2021; pp. 107–123.
43. Heartfield, R.; Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R.; Filippoupolitis, A.; Roesch, E. A taxonomy of cyber-physical threats and impact in the smart home. *Comput. Secur.* **2018**, *78*, 398–428. https://doi.org/10.1016/j.cose.2018.07.011
44. Tsakalidis, G.; Kostas, V. A systematic approach toward description and classification of cybercrime incidents. *IEEE Trans. Sys. Man Cybern. Sys.* **2017**, *49*, 710–729.
45. Kang, C. A Tweet to Kurt Eichenwald, a Strobe and a Seizure. Now, an Arrest. Available online: https://www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html (accessed on 22 February 2022).
46. Tomić, I.; McCann, J.A. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet Things. J.* **2017**, *4*, 1910–1923.
47. King, J.; Lakkaraju, K.; Slagell, A. A taxonomy and adversarial model for attacks against network log anonymization. In Proceedings of the Proceedings of the 2009 ACM symposium on Applied Computing, New York, NY, USA, 8–12 March 2009; pp. 1286–1293.
48. National Association of Regulatory Utility Commissioner (NARUC). NARUC Cybersecurity Manual. 2021. Available online: https://www.naruc.org/cpi-1/critical-infrastructure-cybersecurity-and-resilience/cybersecurity/cybersecurity-glossary (accessed on 10 December 2021)
49. Australian Cyber Security Centre (ACSC). Information Security Manual. 2021. Available online: https://www.cyber.gov.au/acsc/view-all-content/ism (accessed on 10 December 2021)
50. Canadian Centre for Cybersecurity. An Introduction to the Cyberthreat Environment. 2021. Available online: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment (accessed on 10 December 2021)
51. Bristol Cyber Security Group. CyBOK: The Cyber Security Book of Knowledge v1.1. 2021. Available online: https://www.cybok.org (accessed on 10 December 2021)
52. Federal Financial Institutions Examination Council. Information Security. 2021. Available online: https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf (accessed on 10 December 2021)
53. CISA. Cybersecurity Glossary. National Initiative for Cybersecurity Careers and Studies, n.d. Available online: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary (accessed on 10 December 2021)
54. CNSS. Committee on National Security Systems (CNSS) Glossary, n.d. Available online: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (accessed on 10 December 2021)
55. NIST. Guide for Conducting Risk Assessments—NIST, n.d. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed on 10 December 2021)
56. United States Department of Homeland Security. DHS Lexicon Terms and Definitions, n.d. Available online: https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf (accessed on 10 December 2021)
57. SANS. Glossary of Security Terms. Glossary of Security Terms | SANS Institute, n.d. Available online: https://www.sans.org/security-resources/glossary-of-terms (accessed on 10 December 2021)
58. ISACA. Isaca Interactive Glossary & Term Translations. ISACA, n.d. Available online: https://www.isaca.org/resources/glossary (accessed on 10 December 2021)
59. IETF. RFC4949. Document Search and Retrieval Page, n.d. Available online: https://datatracker.ietf.org/doc/html/rfc4949 (accessed on 10 December 2021)
60. Tjostheim, I.; Waterworth, J.A. Predicting personal susceptibility to phishing. In *International Conference on Information Technology & Systems*; Springer: Cham, Switzerland, 2020; pp. 564–575.
61. Pennycook, G.; Adam, B.; Evan, T.C.; David, G.R. The implied truth effect: Attaching warnings to a subset of fake news headlines increases perceived accuracy of headlines without warnings. *Manag. Sci.* **2020**, *66*, 4944–4957.
62. McAfee. What Is Malware and Why Do Cybercriminals Use Malware? 2021. Available online: https://www.mcafee.com/en-us/antivirus/malware.html (accessed on 10 December 2021)
63. Piper, S. *Definitive Guide™ to Next-Generation Threat Protection;* CyberEdge Group, LLC: Annapolis, MD, USA, 2013.
64. Choo, K.-K.R.; Smith, R.G; McCusker, R. *Future Directions in Technology-Enabled Crime: 2007–2009*; Australian Institute of Criminology: Canberra, Australia, 2007.