ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

(Dis)information Warfare

Why online disinformation is able to prosper and how to fight it

Lucille Van Vooren
Cybersecurity and Cybercrime
University of Bologna
2021-2022

Big data, autonomy, machine learning, social sciences, social media and global connectivity all play an increasingly important role in our lives. And if used against us, form the basis of information warfare.

~Colonel Caroline Woodbridge-Lewin,

Head of the Information Warfare Group at the Defence Academy

Table of Contents

Introduction

In the 21st century, the familiar form of warfare, inflicting physical damage to opposing forces and infrastructure, has made room for a new and less visible form of attack. The use of cyberweapons has taken on a central role in modern warfare where nations increasingly launch non-lethal attacks on enemy information systems. We are witnessing the rise of an information warfare in cyberspace.

Disinformation is central to the arsenal of current information warfare. Social networks tremendously increased the potency of disinformation and its manipulative power. In result, disinformation is being transmitted at an unprecedented pace, safeguarding nobody from any potential influence of the attacker. In 2020, 81 countries were found guilty of spreading disinformation on social media, and this is increasing every year (Bradshaw et al., 2020). Our world is dominated by a flow of disinformation, with social networks being the main culprits of proliferation.

Paradoxically, disinformation can be considered the most visible, yet invisible method of attack. Its ubiquity is precisely what makes it so hard to recognize. In consequence, disinformation attacks have been able to perpetrate every sphere of society and cause damage and polarization among citizens. Our democracy is succumbing to the current information warfare, with the citizens as the main victims. It is said that a team is only as strong as its weakest link, and that is no different in the context of the current information war. Therefore it is essential to arm the people themselves in order to stand firm against disinformation.

This paper starts by explaining the concept of information warfare and what it entails. Further, it focuses on the role of disinformation as a cyberweapon within this war and the different methods of attack. To contextualize the previous, disinformation attacks are then placed within a broader journalistic framework, followed by the outlining of effects on our democracy. To conclude, this paper looks at how disinformation is generally counteracted by actors in society and stresses the necessity for adequate education in order to protect the people and preserve a healthy society.

Information Warfare

Information warfare (IW) can generally be understood as any operation in order to obtain an information advantage over the opponent. As described by the NATO (2020): “It consists in controlling one’s own information space, protecting access to one’s own information, while acquiring and using the opponent’s information, destroying their information systems and disrupting the information flow”. In summary techniques of IW may include (Burns, 1999):

- The tactical collection of information;
- Ensuring the validity of one’s own information;
- The dissemination of propaganda or disinformation to demoralize or manipulate the enemy and the public;
- The safe transfer of information;
- The disturbance, degradation or denial of information, which are all means to prevent the opponent from gathering correct and complete information.

However IW is not a new phenomenon, these techniques are now applied to modern information and communication technologies (ICT) such as the Internet. As a result, modern IW has risen to a whole new level. The mass-integration of ICT has led to an unprecedented global interconnectedness and elevated all physical barriers of communication. McLuhan (1962) referred to this development as the “Global Village”, which indicates the daily consumption and production of media by a global audience. This new digital reality makes the dissemination of information much faster, cheaper and more large-scale. As a result, the consequences of IW are also more far-reaching.

Contemporary Issues of Information Warfare

The information revolution has advanced the ways in which IW can be fought. The most prevalent revolutions come in the form of cyberattacks, automated robots and communication management. However, these new attacking methods also engender new issues and moral ambiguities.

1. Cyberattacks are significantly less risky for the attacker than traditional attacks, making them far more attractive to hostile organizations. As a result, attacks are carried out easier and more frequently than in traditional warfare (Ajir & Vailliant, 2018).

2. Since ICT are so interwoven in modern life, almost any technology can be targeted by a cyberterrorist attack. Especially civilian technologies are a common target of attack. These attacks can even be potentially launched through personal computers or websites. In addition, control over civilian infrastructure is harder to enforce since it can raise ethical concerns about the right to privacy (Editoral Team, 2022).

3. New technological possibilities for automation and robotic weapons are challenging our ability to measure and assess accountability for the actions of computer systems. Moreover, in the case of cyberattacks it can sometimes be virtually impossible to detect the initiator of an attack (Taddeo, 2012).

4. In IW the manipulation of information is aimed to steer the target into making decisions against their best interest without any awareness. As a result, it is often difficult to pinpoint when IW begins, when it ends, or how destructive it is (Editoral Team, 2022).

5. Global interconnectedness can easily turn over into instability, or even chaos. Modern ICT has many strengths regarding the spread of information. However, this also includes that false information and fear can be disseminated more rapidly and widespread. Therefore creating the possibility to affect the well-being of citizens on a very large scale (Stupples, 2015).

These issues reveal the multidimensional nature of IW. It integrates operations from cyberwarfare, electronic warfare and psychological warfare. The next paragraph dives deeper into each of these adjacent concepts.

Anatomy of Information Warfare

The battlefield of IW has extended into the realms of cyberwarfare, electronic warfare and psychological warfare. Each form of warfare contributes certain aspects to the whole of what is IW.

Cyberwarfare

Cyberwarfare (CW) is generally defined as the use of cyberattacks on the computer system of an opponent. These attacks can range from small disruptions in an enemy's system, to complete destruction of technical infrastructure. Yet it is important to note that cyberattacks not only target computer systems. Attacks are also directed towards power grids or industrial control systems used in manufacturing plants. Some examples of CW are (Hanna et al., 2021):

- Hacking and theft of critical data from an opponent;
- Distributed denial-of-service (DDoS) attacks that prevent legitimate users from accessing targeted computer networks or devices;
- Viruses, phishing computer worms and malware that can take down critical infrastructure;
- Spyware or cyber espionage that results in the theft of information that compromises national security and stability;
- Ransomware that holds control systems or data hostage.

However despite many efforts, there is still no consensus regarding a uniform definition of CW. Simply put, we could distinguish CW from IW due to its mere technical nature. Where CW uses technology to target systems, IW revolves around the use of data and information as a weapon. CW can thus be considered as the technical dimension of IW.

Electronic Warfare

Next, IW also integrates electronic warfare (EW). Modern communication heavily relies on electromagnetic transmissions, such as signals of radio, infrared or radar. EW refers to the ability to use the electromagnetic spectrum to support, protect or attack these signals (Gordon, 1981). A common practice of EW is jamming. The purpose of jamming of is to limit an enemy's ability to exchange information by overriding radio transmissions or by sending signals to prevent radar detection or convey false information. Simply put, EW is mainly focused on disrupting or neutralizing communication signals via the electromagnetic spectrum.

Psychological Warfare

Last but not least, IW implies the conduct of psychological warfare (PW). As mentioned before, IW includes the manipulation of information with the intent of harming the well-being and morale of people. Similary, PW refers to the tactical use of propaganda, threats, and other psychological techniques to mislead, intimidate, demoralize, or otherwise influence the thinking or behavior of an opponent (Encyclopaedia Britannica, n.d.). Some examples of PW are (Longley, 2019):

- Demoralization, for example through the distribution of pamphlets or flyers that encourage the opponent to surrender;
- Propaganda radio stations;
- Sleep deprivation of the enemy through the use of loud sound speakers;
- "False flag" events (attacks, operations or incidents), which are employed to give the opponent the impression that they were carried out by other nations or groups;
- The visual "shock and awe" technique to scare the enemy based on the use and display of spectacular force (e.g. using technologically advanced weapons).

In the context of IW, disinformation campaigns are the central psychological element. The manipulation of perception forms one of the main drivers of IW. Therefore knowledge of psychology is extremely relevant during IW in order to adequately influence people's emotions and behavior towards the desired direction. PW thus concerns the psychological dimension of IW, mainly by use of disinformation campaigns.

Psychological Warfare Then vs. Now

PW has been documented throughout all of history. In ancient times, PW was limited to face-to-face and verbal communication only. But starting from the 20th century, the possibilities and effects of PW greatly expanded due to the rise of mass media. Traditional techniques were now being applied to new forms of media such as the radio, newspapers or television.

Generally the origins of contemporary PW can be traced back to World War I (Fritz, 2014). Propaganda was being used by the belligerent countries to influence the public's view and mobilize the total forces of the land in support of its goals. The British however, had several advantages in their battle for world opinion. They had one of the most reputable news systems and controlled an advanced transnational communication system. These two factors are said to have greatly contributed in their victory against the Germans. Moreover, it emphasized the importance of propaganda and a news system in the waging of war.

Over the past few years, PW has moved to new battlefields because of digitalization. Especially nowadays, a continuous PW is being fought in cyberspace. The Internet and social media have shown to be very effective tools of large-scale influence and manipulation. However cognitively, people now aren't any less vulnerable to disinformation than people during WWI. Humans maintain a cognitive vulnerability to IW and the manipulation of perception. These cognitive vulnerabilities form the baseline for disinformation campaigns. Cyber technologies have just merely changed the stage on which PW is fought.

An example of present PW is the war of Russia against Ukraine and Western Nations (Abrams, 2022). Putin's strategies include the framing of messages in terms of power dynamics. Ukraine and Western Nations are painted as evil and immoral, while Russia is merely a victim of their exploitation. Russia has been repeating these narratives over the past few years, leading its citizens to believe in the justification of revenge. For example, claims of "Russophobia" (Figure 1.) resurge among various topics whenever Russia wants to portray itself victim.

Figure 1. Retrieved from DFRLab (2018)

Although many Westerners would easily dismiss such claims, it's important to consider that many Russian citizens lack access to independent and social media, which could provide counterinformation. On the counterpart, Ukraine has also been pushing wartime narratives whose veracity is questionable.

We can conclude that PW is an inextricable part of a larger IW that is primarily held in cyberspace. For this reason, it is wrong to make clear distinctions between these dimensions.

Essentially information warfare weaponizes information in order to gain a competitive advantage over the opponent, whether it's through cyberattacks or psychological operations or a combination. Continuing, this paper will look deeper into this combination of operations and focus on the use of disinformation in cyberattacks.

Disinformation

The term disinformation might not immediately ring a bell, but the term “Fake News” undoubtedly does. Ever since the 2016 US presidential elections the term fake news has become extremely popularized. Following this, other buzzwords like disinformation, misinformation, malinformation have been used interchangeably, eroding any underlying nuances between these terms. The common denominator, is that they all refer to content of which the veracity is considered false and they’re all part of the larger issue: the manipulation of public opinion in order to affect the real world.

The Cambridge Dictionary (2020) defines fake news as “false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke.” However this term is too vague and is so overused that it commonly refers to any news a person dislikes, disregarding whether the content is true or not. Therefor this paper distances itself from using the term fake news, as it’s too ambiguous and contested.

In the debate of fake news the concepts of disinformation, misinformation and malinformation are often confused or wrongly seen as one. To avoid misunderstandings, the underlying differences are shortly clarified (Wardle & Derakhshan, 2017).

Disinformation:	false information deliberately made to harm a person, social group, organization or country.
Misinformation:	false information, but not made with the intent to harm any person, social group, organization or country. The disseminator sees this information as the truth.
Malinformation:	truthful information, intentionally used to harm a person, social group, organization or country.

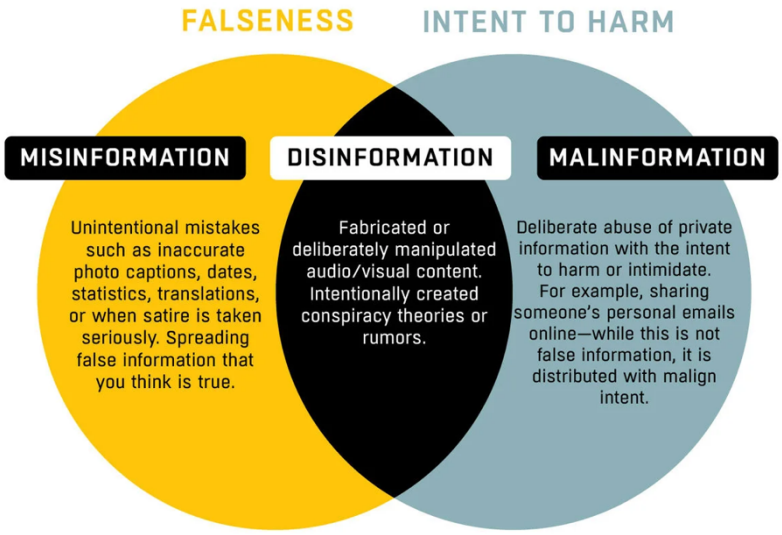

Figure 2. retrieved from Educational Era (2022)

Thus, while clear distinctions can be made between the different types of fraudulent and harmful news, the consequences are similar. Some expressions may exhibit combinations of these three conceptualizations. Individual instances of misinformation, disinformation or malinformation are often part of a broader information strategy (i.e. information warfare), and are often accompanied by other manifestations of mis-, dis- and malinformation (e.g. on other platforms or in different messages). This paper lays its emphasis specifically on disinformation, used as a cyberattack in information warfare.

Disinformation as a Cybersecurity Threat

In current information warfare, social media has shown to be a potent and effective battlefield. Social media is characterized by a variety of digital tools (e.g. bots, algorithms, deep fake…) which help facilitate the conduct of disinformation attacks on platforms such as Facebook, Youtube and Twitter. Therefore many advocate the recognition of disinformation as a cybersecurity threat .

This need for recognition is substantiated by the parallel growth of disinformation- and cyberattacks. With the Internet exponentially expanding, the recognition of malicious content becomes increasingly more difficult. In result, end-users and cybersecurity professionals often remain blind to new weaknesses and risks. Official recognition of disinformation as a cybersecurity threat however, is crucial for the development of more resilient private actors, state-actors and stakeholders from the disinformation and technological field.

The EU DisinfoLab (2021) listed several reasons to why disinformation is a threat to cybersecurity. Drawing upon their research, they discovered four areas of convergence between disinformation and cybersecurity: the "terrain" on which disinformation is distributed, the "tactics" which merge disinformation into cyberattacks, the "targets" being both victims of disinformation campaigns and cyberattacks, and what they call the "temptation", or the appealing nature of this kind of warfare.

1. **Terrain**: while disinformation campaigns have received a lot of attention due to their use of platforms such as Facebook and Twitter, they inherently rely on a distributed network of servers and routers to disseminate false information. Social media networks serve as gateways and amplifiers of disinformation attacks. This implicates the private sector and the internet technical community to share a role in countering disinformation and cybersecurity threats.

2. **Tactics**: cybersecurity and disinformation tools have become immensely intertwined. Disinformation is increasingly used as part of cyberattacks to deliver malware via the manipulation of people's emotions (e.g. fearware, which uses the feelings of fear and urgency to lurk people into clicking on malicious content). In addition, the proliferation of hybrid attacks (i.e. warfare methods that combine human and technological aspects) underpin this convergence.

3. **Targets**: disinformation attacks and cyberattacks cause similar damage and are usually combined to reach the same target. For example, actions such as data breaches (i.e. hackers stealing or manipulating sensitive information) or the manipulation of information are both intended to compromise the integrity of data.

4. **Temptations**: activities of cybercrime and manipulation operations are very appealing to perpetrators due to their high profit margins and insufficient consequences.

In conclusion, the challenge of disinformation is a matter of cybersecurity governance. Therefore cybersecurity and disinformation should be addressed in the same breath in order to safeguard the health of our digital infrastructure.

Methods of Disinformation Attacks

Disinformation attacks primarily take place within social networks. They offer various tools to carry out attacks and serve as an accelerator of extremism because they connect people instantaneously. Some of the most prevalent methods are the use of bots, algorithms, deep fake technology and humans.

The potency of these attacking methods is magnified by the fact that falsified information tends to outperform authentic stories. Research has proven that false stories are more likely to go viral. Disinformation is said to reach 1500 people 6 times faster, on average, than a truthful story (Meyer, 2018). This problem is even exacerbated when the story concerns politics. The next paragraphs dive deeper into these methods of attack.

Bots

Bots have taken on a central role in cyberspace. These software programs are designed to perform specific tasks online, that otherwise humans would have to do (Howard et al., 2018). They were initially designed to perform simple regulatory tasks, however their utility and deployment quickly shifted towards more serious goals.

Nowadays bots are a strong asset within the arsenal of disinformation attacks. Many actors, such as governments or political organizations worldwide have been reinforcing their information warfare capabilities by using bots for both defensive and offensive goals. Bots amplify messages by increasing the speed and number of people it reaches (Howard et al., 2018). In this way, they are able to influence public opinion, disrupt debate and muddy political issues (Woolley & Howard, 2016).

We can distinguish different types of bots:

Social bot: social bots mimic real users on social media platforms by undertaking specific tasks and interacting with other user accounts. They are programmed to automatically advocate certain ideas and spread disinformation or to boost the popularity of social media profiles by creating fake accounts (e.g. fake followers).

Political bots: political bots are social bots that are used for political purposes. Political bots are often caught exaggerating the popularity of certain politicians, while smudging the name of others. Other practices include the drowning of political hashtags in nonsense, or the immediate rebuttal of political claims using disinformation (Fernquist et al., 2018).

Spam bot: spam bots generally spread spam on the internet, such as online comment sections, email inboxes... This can take on the form of disinformation campaigns.

Because of their pace of information parsing and organization, bots save significant time and energy for human authors. For this reason, their potential as weapons may not be underestimated. Bots have skewed multiple discourses and political elections over the few years and have caused serious damage on a global scale. A memorable example are the US presidential elections of 2016. Research by Bessi and Ferrara (2016) indicated that around one out of five election-related tweets were generated by bots during their period of study (16/09-21/10). This leads to almost four million tweets by more than 400,000 bots distorting public discussion on the elections.

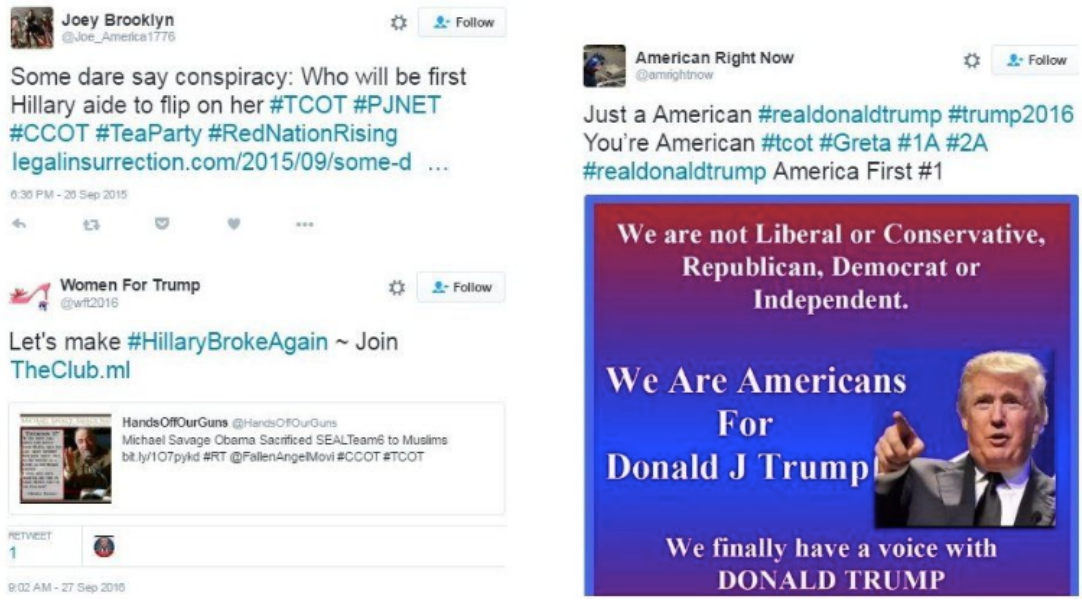

Figure 3. Tweets from active pro-Trump bots according to Woolley and Howard (2018)

Lastly there are also hybrids, which are a combination of both automatic and human curation (Fernquist et al., 2018). The use of hybrids can make awareness of potential disinformation attacks even harder.

Cyborgs: in cyborg accounts a human periodically takes over a bot account in order to disguise the account and increase its credibility.

Sybils:	sybils take over a person's account and try to connect with the real user's social network by impersonating the owner. The perpetrator takes advantage of a user's reputation. Sybil accounts are sometimes operated by bots to share disinformation on a large scale.

Algorithms

Algorithms dominate our flow of (dis)information. They play a decisive role in prioritizing news, determining where news appears online and who does or does not reach the news, based on the user's engagement levels (Devito, 2017; Nechushtai & Lewis, 2019; Wallace, 2017). Exactly because algorithms present us content based on our own interaction with them, they can function as radicalization pipelines. The dynamics of algorithmic news curation leads them to be the ideal gateway for disinformation attacks.

As mentioned before, disinformation attacks thrive on the exploitation of human biases. Algorithms reinforce these biases. People naturally tend to engage more with shocking, radical and click-bait content (Soroka et al., 2019). Algorithms, in consequence, amplify these tendencies leading to higher engagement levels of attention-grabbing posts. As a result, disinformation attacks often leverage algorithms to boost their extremist content and instigate online radicalization (Nemr & Gangwire, 2019)

The potential of algorithms reaches even further than solely being a great tool for rapid dissemination of disinformation. These tools have the power to create an online environment where users only encounter disinformation. Algorithmic news curation can lead to one-sided news consumption and isolate people from a broader spectrum of information that might challenge their beliefs. This is commonly described as the echo chamber effect (Sunstein, 2002) or the filter bubble (Pariser, 2011). Within these information bubbles, there is less room for chance encounters with news and conflicting views. In result users can get trapped in the illusion of disinformation being reality.

Evidently repeated consumption of personalized news can have detrimental effects on people, democracy and our global society. These effects are discussed later on in this paper.

Deepfake

Deepfakes are a recently developed software technology that uses deep machine learning and artificial intelligence to create false imagery (Albahar & Almalki, 2019). Although the idea of manipulating images is not new, the rise of deepfakes initiates a turning point in image modification. Because of recent advancements in neural networks, images and videos can be copied, imitated or changed in such a realistic manner, that it frequently becomes impossible to detect its inauthenticity. Deepfakes therefore, hold an extreme disinformation potential whereas people can be staged to say or do anything within any context.

The rapid emergence of deepfakes tends to be one of the most alarming methods of attack. Although people already have a relative awareness regarding fake news, they are much more vulnerable to fake videos or imagery because of their high accessibility and credibility. The line between "real" and "tricked" is so obscured that even the best detection software cannot recognize certain videos as falsified (Zagers, 2021). Deepfakes are used to disseminate disinformation, defame individuals, cause societal distress and simply have the potential of seriously harming our democracies.

These deepfake attacks are quite common. The internet provides open access to powerful tools such as TensorFlow or Keras making it relatively easy for anyone to generate any kind of false imagery**.** One of the most viral deepfake videos is where former US President Barack Obama uncharacteristically uses insulting vocabulary and curses Donald Trump (BuzzFeedVideo, 2018).

Human Troll Armies

Humans themselves are also part of the disinformation arsenal. When the internet came to be, so did internet trolls. A troll is a person who posts on the internet to provoke predictable emotional responses such as anger, irritation or sadness by intentionally misinforming people or pretending to be different.

The act of trolling is usually done with the sole intention of offending people and provoking discussions for own amusement. However, many countries and institutions have started to weaponize trolls in order to strengthen themselves within the war of information. This phenomenon is referred to as the formation of troll farms or armies. A troll army is an institutionalized group of internet trolls hired to disrupt political sceneries and manipulate public opinion (The Cambridge Dictionary, 2020). These 'keyboard' warriors are paid to spread disinformation, create illusory support and wreak total havoc within the public sphere.

Recently, research funded by the UK government has allegedly found evidence for a troll factory based in Saint Petersburg (The Guardian, 2022). The study reports that online operatives are being paid to spread pro-Russia war lies and target social media accounts of world leaders such as Boris Johnson, Olaf Scholz and Josep Borrell. The troll army is being deployed to spread patriotic narratives and justify the military operations in Ukraine. Moreover, according to the Industrialized Disinformation report (2020) of the Oxford Internet Institution, 59 countries used state-sponsored trolls to attack political opponents. The use of internet trolls is therefore very common within IW.

Human Psychology

Human psychology is the driving force underlying all disinformation attacks. Disinformation prospers because it's spread by humans. Technology would never be as effective without the exploitation of fundamental human psychology, more specifically cognitive vulnerabilities. Therefore, to fully grasp disinformation attacking methods, it's essential to understand the converging factors of media, technology and human psychology.

Cognitive vulnerabilities are psychological factors in human beings which make them more susceptible to disinformation (Pantazi et al., 2021). Cognitive vulnerabilities drive the perception of objectivity while it diminishes the ability of people to rationally analyze a situation (Castanedo, 2021). Information is fueled by this reduction in objectivity. In addition, authors of disinformation usually hide their identity. Reduced objectivity in combination with anonymity, facilitates people to process information and make decisions more subjectively. In consequence, cognitive vulnerabilities can lead to the acceptance and support of radical ideas (Yang, 2019). The adequate exploitation of cognitive vulnerabilities in disinformation attacks are therefore the key to winning an information warfare.

In their research, Caleb & Silva (2022) provide a list (Figure 4.) of possible cognitive vulnerabilities which can be exploited in disinformation attacks.

Confirmation bias	The act of searching evidence to support existing bias or expectations (Nickerson, 1998); Also referred to as selective exposure, this phenomenon makes us blind to information that contradicts our beliefs in order to minimizing cognitive dissonance (Silverman, 2015).
Motivated reasoning	The tendency to "scrutinize ideas more carefully" if we do not agree with them (Marcus, 2009). In other words, our ability to reason is unconsciously affected by our preexisting values, identities, and attitudes (Silverman, 2015; Slothuus & de Vreese, 2010).
Biased assimilation	A process related to motivated reasoning in which people interpret new information in a biased way, in accordance with their own beliefs (Silverman, 2015). This phenomenon explains why individuals "readily accept confirming evidence while critically examining disconfirming evidence" (Dandekar et al., 2013).
Hostile media effect	An effect related to the bias perceived by individuals from their preexisting stance towards the news source. Because of this effect, people with opposing views, when accessing the same reports, tend to perceive these reports as biased against their own opinions (Arpan & Raney, 2003; Gunther & Liebhart, 2006).
Repeated exposure	Repetition leads to familiarity and people use familiarity as a proxy for credibility. It increases the processing fluency (the ease of information recall), which is perceived as discrepant from a comparison standard and may affect truth judgments (Berinsky, 2017; Dechêne et al., 2010)

Denial transparency	This phenomenon portrays the ineffectiveness of denying a proposition. It is attributed to the way people cumulatively process information, always appending new pieces to their "store of knowledge", without deleting previous information (Wegner et al., 1985).
Backfire effect	This effect highlights the increase of people's acceptance of challenged beliefs when presented to contradictory evidence (McRaney, 2011). It may occur as a result of repeated exposure.
Group polarization	It is explained through the predictably behavior of group members adopting a more extreme stance after group deliberation (Sunstein, 2002). Groups of like-minded people reverberate messages, such as in an echo chamber, with a social function to legitimize each other, reinforcing individuals' opinion (Jamieson & Cappella, 2010).
Casual inference making	The act of attributing unwarranted cause–effect relationships to contiguous events. After the occurrence of an event, people tend to mistake their inferences with real memories of the event, yielding auto-suggestion errors (Principe et al., 2008).
Emotion	Previous research indicates that the accuracy of personal beliefs and resulting attitudes can be shaped by a person's emotional state and by the prevalent tone of media coverage (Anderson et al., 2018; Scheufele & Krause, 2019)

Figure 4. retrieved from Caled and Silva (2022)

The proliferation of the current information warfare is parallel-linked to the progressive degradation of journalism and the general impoverishment of the news landscape. News is always a product of the socio-cultural and economic context in which it evolves. Studying the news in isolation of social developments is therefore incorrect (Paulussen, 2004). This makes it relevant to briefly place this information warfare within a broader journalistic framework and link it to concurrent social shifts.

Journalistic Perspective

The arrival of the Internet late 20th century induced the transition from mass society to today's network society (Van Dijk, 2012). Ever since, the journalistic sector struggles to keep up with technological advancements while maintaining the same quality of news.

From Mass to Network Society

In mass society, traditional news organizations had a monopoly on news production and news distribution. News was collected by a few centralized players, then filtered and distributed in a linear process to a mass audience with little or no opportunity for feedback (McQuail, 1987). News production was limited by boundaries of time and space which resulted in a focus on quality rather than quantity. The verification of sources, impartiality and professional ethics were cornerstones of journalism (Coggiola & Siroli, 2018). In short, journalism in mass society was characterized by linear and centralized information flows, passive mass audience, scarcity of time and space, quality in news production and active news consumption (Loisen et al., 2016).

The advent of the Internet and the elimination of time and space boundaries ushered in the network society. Globalization, digitalization and far-reaching user participation challenged the status quo (Castells, 2000). The one-way traffic has evolved into a chaotic news environment characterized by non-linear and decentralized information flows towards a fragmented audience (McNair, 2006). We see an evolution towards network journalism characterized by rapid information exchange among an immeasurable number of information nodes worldwide. The distinction between journalists and amateurs has tightened and citizens can now take part in the news production process (Heinrich, 2012).

The multiplicity of actors gave rise to commercialization or market driven journalism. Additionally, the growing reliance on social media as news platforms has prompted a shift from quality to quantity, and relevance to popularity (McManus, 1994). As a result, the reliability of news has come under pressure spurred by the rise of fake news (McNair, 2018). This evolution further fostered the disintegration of meaning, credibility and reliability of circulating content and journalists. Journalism is now characterized by a simplification of news production, consumption and distribution through digitization (Paulussen, 2004), whilst also setting off commercialization and erosion of news and journalism as a profession (Deprez & Van Leuven, 2020).

The state of the current news landscape makes fighting disinformation very difficult, if not almost impossible. While disinformation has historically been spread by governments, militaries and religious or economic institutions, the internet has enabled anyone with a computer to engage in this activity (Coggiola & Siroli, 2018). Social media lack the control mechanisms that used to be part of the journalistic deontology, and pave the way for disinformation to prosper. Disinformation is ubiquitous and there is no escaping to it.

The proliferation of disinformation, together with the deterioration of journalism, have made a strong impact on our democracy. The next paragraph elaborates further on these outcomes.

Effects on Democracy

IW has put our democracies under severe pressure. Liberal democracy essentially implies the separation of the three institutional powers, namely the legislative, executive and judicial power. The media, in turn, is considered as a fourth institutional power supplementing the other three by providing checks and balances. This fourth power is responsible for providing citizens with all information necessary to make well-informed decisions in a democracy and stimulate public debate (Team Media Texthack, 2014). Although, beautiful in theory, practice points to a different reality.

The scale on which IW is happening today is overshadowing our institution as being a true liberal democracy. The ubiquity of disinformation attacks proof that the separation of media from other institutional powers is an illusion. The 2020 report of Industrialized Disinformation (Bradshaw et al., 2020) highlights that cyber troop activity continues to rise globally each year. Evidence among 81 countries was found for the use of social media to spread computational propaganda and disinformation about politics. These trends emphasize that information has increasingly become a weapon of the government to control the people, rather than a weapon of the people to control the government.

Polarization

One of the main effects (and goals) of information warfare is polarization. The 2020 report of Industrialized Disinformation (Bradshaw et al., 2020) found that a concerning 48% of all studied countries (n = 81) had used disinformation campaigns to drive division and polarize citizens. Polarization discourages debate in the public sphere and is used to drive people apart, often pushing them to extremist viewpoints (Borgesius et al., 2016). In consequence people have less shared experiences and the 'social glue' is erased, which is considered to be necessary in democracy.

The EU High Level Group argues: "The concern is people forgetting that alternatives do exist and hence becoming encapsulated in rigid positions that may hinder consensus-building in society" (Vīķe-Freiberga et al., 2013, pp. 27–28).

Especially the use of algorithms amplify polarization. As mentioned before, algorithms have the power to imprison people in filter bubbles where they get stuck in a spiral of attitudinal reinforcement (Borgesius et al., 2016). However, Sunstein (2002) argues that coming across diverse opinions is necessary for the development of people in a democracy. Thus, extensive algorithmic news curation greatly affects democracy because it prevents the development of well-informed citizens and leads to knowledge gaps in society.

Additionally, polarization in combination with repeated exposure to online disinformation, generates problematic competing narratives. Repeated exposure has the power to generate deep convictions of information being accepted, regardless if it's truthful or not (Lecheler & de Vreese, 2011). People start to view opposing narratives as highly negative and tend to disregard potential alternatives to resolve societal problems. The full exercise of democracy is therefore hindered because citizens are compromised in their critical judgement, political knowledge and access to accurate information (Caled & Silva, 2022).

All of the above covers a larger social issue of general distrust. The credibility of the media is in constant decline and people have lost confidence in institutional powers. In other words, the foundations of our democracy have collapsed. In fact, is it even fair to say that we still live in a democracy?

Countering Disinformation

The effects of disinformation attacks perpetrate all spheres of society. In order to effectively respond to this, the problem must be tackled from all points of view necessary. State-actors, private-actors, journalists, digital platforms and cybersecurity professionals, are all on the front lines of combatting disinformation globally.

Some examples of common strategies:

Governmental perspective	State-led responses usually include legal measures such as regulations or punitive strategies (Caled & Silva, 2022). For example, the imposition of sanctions on social media platforms that spread disinformation (e.g. fines in order to remove misleading content). However, legal measures can also be used as a mechanism for abuse and oppression (e.g. censorship) and eventually foster dissatisfaction among citizens towards the government.
Journalistic perspective	Within journalism fact-checking has become a frequent initiative for countering disinformation. As defined by The American Press Institute, "fact-checkers investigate verifiable facts, and their work is free of partisanship, advocacy, and rhetoric" (AJn, 2014). This solution, however, has major limitations due, firstly, to the vastness of the Internet content to be checked, and secondly, to the question of the reliability of human or algorithmic fact-checkers (Coggiola & Siroli, 2018).

Digital platforms' perspective	Digital platforms usually turn to fact-checking initiatives, content moderation and the promotion of quality news, while also attempting to reduce the visibility of websites sharing disinformation (Caled & Silva, 2022). However, these responses are limited by similar problems as those posed by state-actors or journalists. Digital platforms remain commercial entities driven by personal interest, which makes their impartiality questionable.
Cybersecurity perspective	Solutions generally include computational methods as a standalone tool or to assist other actors such as journalists, digital platforms or private-actors (Caled & Silva, 2022). These tools are based on machine learning technology in order to automatically detect disinformation or provide indicators of veracity. However, mistakes can be very costly and lead to unjust censorship of truthful stories or the dissemination of false ones (Alaphilippe et al., 2019).

Whatever measures state-actors, private-actors, digital platforms or journalists may implement, disinformation will always find its way to the audience. Ultimately, the resilience of society towards disinformation attacks depends on the resilience of the people. As these attacks are usually aimed to fool people, the people themselves have to be prepared to resist them.

Nevertheless, a lot of studies fail to recognize the vital role of individuals to halt disinformation. This academic problem mirrors our society. The ubiquity of technology and media leaves the impression that everyone has developed knowledge and media and technology can be found everywhere, including in education. Unfortunately, this impression is false. Current education fails to keep up with rapid digitalization, and in consequence doesn't properly assist in counteracting disinformation. As a result, humans remain the weakest link within cybersecurity.

In order to win this war, the people should properly be armed towards disinformation. The next paragraphs emphasize the necessity of a good education system as a form of defense and lay focus on media literacy and digital literacy.

Educational Perspective

The crucial role of education cannot be underestimated. Research found media literacy and information literacy to be important factors in the recognition of misinformation (Kahn & Idris, 2019), and emphasizes the importance of media education in the fight against disinformation (Shapovalova, 2020). Moreover, low-educated people are often found to be more vulnerable to disinformation (University of Kansas, 2019). The problem should therefore be tackled from the ground up by educating the people on the converging factors of media, technology and their own human behavior. This is where education on media literacy and digital literacy comes into place.

Media literacy

Media literacy looks at media in its entirety and how it can affect our image of reality. It is the set of competences that enables a person to interpret media products and settings, to produce media themselves and to recognize and confront the social and political biases of the media (Grisham, 2021). Media literacy encourages critical thinking and allows them to take control over media, rather than it to be the other way around.

In a society where war is fought by the use of media biases, media literacy among citizens is necessary to maintain a healthy democracy. Education has the possibility to neutralize many cognitive vulnerabilities by making people aware of media bias, as well as their own bias. It allows them to analyze, understand and evaluate disinformation more deeply, and provides them with the necessary skepticism. Education should therefore lay a higher emphasis on media literacy in order to create critical citizens and contribute to a more healthy society and digital environment.

However media literacy can never fully prevent or undo of media bias, it does help create a counterweight to the rising of disinformation. This counterweight is reinforced with additional digital literacy in education. Digital literacy is an additional skill needed in order to fight disinformation attacks.

Digital Literacy

Digital literacy can be seen as a technical extension of media literacy. Digital literacy focuses on understanding digital tools such as websites, apps and social media platforms and how they affect our society and digital media. Whereas media literacy is about critical consumption of digital media, digital literacy provides a set of competences to safely and consciously navigate and participate in digital media (Hobbs, 2010).

Nevertheless, digital literacy is generally included within education. However, the curriculum frequently needs to be updated in order to match the speed of technological advancements. This is where our education system fails. Digital literacy courses often fall short on subjects such as cybersecurity and algorithmic literacy (Koenig, 2020). In consequence, current education still doesn't properly prepare individuals for the threats of the current IW.

A consequence of this, for example, is the frequent occurrence of filter bubbles. Essentially, filter bubbles arise when individuals don't consciously interact with algorithms, allowing these technologies to amplify media biases. In addition, various studies confirm the existence of knowledge gaps on digital literacy among people (Cotter & Reisdorf, 2020; Henderson et al., 2020; Swart, 2020). Even the youngest generations, who are expected to be the most digitally literate, seem to lack the knowledge to consciously navigate through the current digital news landscape. These tendencies embody the shortcomings of current education.

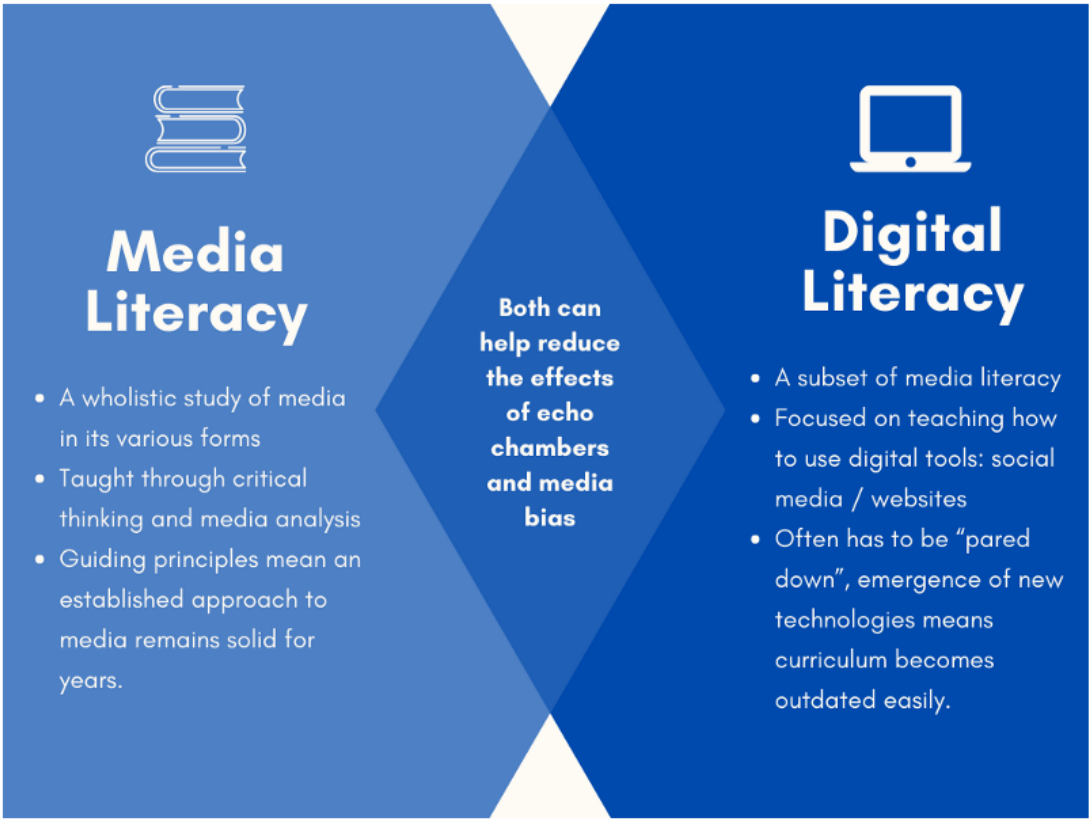

Figure 5. retrieved from Grisham (2021)

In summary, education should focus on including both media literacy and digital literacy, whilst also ensuring that these courses are frequently updated in line with technological advancements of IW. Education on media literacy needs to ensure critical engagement with mass media and education on digital literacy needs to provide the technological, personal and intellectual skills for living in a digital society.

However, education is more focused on the long term, it is a prerequisite for building collective resilience in society. Media and digital literacy should become cornerstones within our educational curricula. Without it, countries will never be able to fully arm themselves against the dangers of disinformation attacks and other cybersecurity threats, regardless of any other measures taken.

Conclusion

Concluding, information warfare is both a war in cyberspace as a war on ideas. States or organizations try to gain a competitive advantage over the enemy through the weaponization of information, by using psychological attacks, cyberattacks or a combination. The emphasis of this paper lays on the combination of both psychological and cyber methods through the conduct of online disinformation attacks.

These attacks generally happen in social networks, because they serve as optimal gateways for the rapid and large-scale spread of disinformation. By using digital tools such as bots, algorithms, troll armies and human biases, perpetrators globally infect social networks with disinformative narratives in order to manipulate the public's view in their own interest.

These technological innovations have pushed journalism into an epistemological crisis, leading towards a general deterioration of the journalistic sector. The diminishing of quality news combined with the proliferation of online disinformation, have caused serious damage to our democracy. People have lost their trust in their governments and the news media. For this reason it is debatable whether we still live in a democracy or not.

The counteraction of disinformation, in consequence, has become a global top-priority in policymaking among governments, private actors, journalists, digital platforms and cybersecurity professionals. However, a team is only as strong as its weakest link, which in this case are the citizens. Whatever measures stakeholders may take, disinformation still finds its ways to the public and is able to prosper.

The resilience of society ultimately relies on the people. Unfortunately the general public lacks critical understanding of technology, media and their own human behaviour. These problems can be attributed to an outdated education system that does not meet the needs of today's digital society.

It is rather unrealistic to expect from to learn people what IW and disinformation attacks are, how they work, and why they are important, without sufficient exposure to the topic in school curricula (Powers, 2017). This paper therefore argues for the inclusion and emphasis of media and digital literacy within educational attainment levels. This should equip young people to efficiently and consciously navigate an increasingly personalized online news landscape (Swart, 2020). Redirecting literacy within the perspective of young people will contribute to a healthier future for the internet, better informed citizens and the maintenance of democracy.

Bibliography

Abrams, Z. (2022). The role of psychological warfare in the battle for Ukraine. *Monitor on Psychology APA*, *53*(4). https://html5-player.libsyn.com/embed/episode/id/22707503/height/90/theme/custom/thumbnail/no/direction/backward/render-playlist/no/custom-color/87A93A/

Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, *12*(3), 70–89.

AJn, J. (2014, May 20). *Who are you calling a fact checker?* American Press Institute. https://www.americanpressinstitute.org/fact-checking-project/fact-checker-definition/

Alaphilippe, A., Gizikis, A., Hanot, C., & Bontcheva, K. (2019). *Automated tackling of disinformation: Major challenges ahead.* [Technical Report]. European Parliamentary Research Service. https://data.europa.eu/doi/10.2861/368879

Albahar, M., & Almalki, J. (2019). Deepfakes: Threats and Countermeasures Systematic Review. *Journal of Theoretical and Applied Information Technology*, *97*(22), 3242–3250.

Anderson, A. A., Yeo, S. K., Brossard, D., Scheufele, D. A., & Xenos, M. A. (2018). Toxic Talk: How Online Incivility Can Undermine Perceptions of Media. *International Journal of Public Opinion Research*, *30*(1), 156–168. https://doi.org/10.1093/ijpor/edw022

Arpan, L. M., & Raney, A. A. (2003). An Experimental Investigation of News Source and the Hostile Media Effect—Laura M. Arpan, Arthur A. Raney, 2003. *Journalism & Mass Communication Quarterly*, *80*(2), 265–281.

Berinsky, A. J. (2017). Rumors and Health Care Reform: Experiments in Political Misinformation. *British Journal of Political Science*, *47*(2), 241–262. https://doi.org/10.1017/S0007123415000186

Bessi, A., & Ferrara, E. (2016). *Social Bots Distort the 2016 US Presidential Election Online Discussion* (SSRN Scholarly Paper No. 2982233). https://papers.ssrn.com/abstract=2982233

Borgesius, F. J. Z., Trilling, D., Möller, J., Bodó, B., Vreese, C. H. de, & Helberger, N. (2016). Should we worry about filter bubbles? *Internet Policy Review*, *5*(1). https://doi.org/10.14763/2016.1.401

Bradshaw, S., Bailey, H., & Howard, P. (2020). *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Computational Propaganda Research Project). Oxford Internet Institute. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/#continue

Burns, M. (1999). *Information Warfare: What and How?* Information Warfare: What and How? https://www.cs.cmu.edu/~burnsm/InfoWarfare.html

BuzzFeedVideo. (2018, April 17). *You Won't Believe What Obama Says In This Video!* 😉. https://www.youtube.com/watch?v=cQ54GDm1eL0

Caled, D., & Silva, M. J. (2022). Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, *5*(1), 123–159. https://doi.org/10.1007/s42001-021-00118-8

Castanedo, I. C. D. (2021, November 24). Cognitive vulnerabilities: Information Warfare 'Then Vs. Now.' *Grey Dynamics*. https://greydynamics.com/cognitive-vulnerabilities-information-warfare-then-vs-now/

Castells, M. (2000). *The Rise of the Network Society*. Blackwell Publishers.

Coggiola, M. G., & Siroli, G. piero. (2018). Fake news: Propaganda e disinformazione all'epoca di Internet. *Sapere. Idee e progressi della scienza*, *2*, 32–36.

Cotter, K., & Reisdorf, B. C. (2020). Algorithmic Knowledge Gaps: A New Horizon of (Digital) Inequality. *International Journal of Communication*, *14*(0), 21.

Dandekar, P., Goel, A., & Lee, D. T. (2013). Biased assimilation, homophily, and the dynamics of polarization. *Proceedings of the National Academy of Sciences*, *110*(15), 5791–5796. https://doi.org/10.1073/pnas.1217220110

Dechêne, A., Stahl, C., Hansen, J., & Wänke, M. (2010). The Truth About the Truth: A Meta-Analytic Review of the Truth Effect. *Personality and Social Psychology Review*, *14*(2), 238–257. https://doi.org/10.1177/1088868309352251

Deprez, A., & Van Leuven, S. (2020). *Journalistiek in maatschappelijk perspectief: Een inleiding tot journalistieke theorie en onderzoek*. Academia Press. https://biblio.ugent.be/publication/8646744

Devito, M. (2017). From Editors to Algorithms: A values-based approach to understanding story selection in the Facebook news feed. *Digital Journalism*, *5*(6). https://www.tandfonline.com/doi/full/10.1080/21670811.2016.1178592?casa_token=vptwOPBYmnIAAAAA%3Ap3mS0CcpBcYIoLAMkX3bdCK8MbbjC4YZC_X_fwcvSaqGzkjUr4urxWbBYUGAD8iNfO8uCjO9beo

DFRLab. (2018). *#PutinAtWar: How Russia Weaponized "Russophobia."* https://web.archive.org/web/20220109055041/https:/medium.com/dfrlab/putinatwar-how-russia-weaponized-russophobia-40a3723d26d4

Editoral Team. (2022). *Information Warfare: Manipulation of Information in a War*. Unrevealed Files. https://www.unrevealedfiles.com/information-warfare-manipulation-of-information-in-a-war/

Educational Era. (2022). *Part A: What is Disinformation*. Very Verified: A Course on Media Literacy. https://verified.ed-era.com/manipulation/part-a

Encyclopaedia Britannica. (n.d.). *Psychological warfare*. Britannica. Retrieved June 20, 2022, from https://www.britannica.com/topic/psychological-warfare

EU DisinfoLab. (2021). *Why Disinformation is a Cybersecurity Threat*. EU DisinfoLab. https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/

Fernquist, J., Kaati, L., & Schroeder, R. (2018). Political Bots and the Swedish General Election. *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 124–129. https://doi.org/10.1109/ISI.2018.8587347

Fritz, J. (2014, June 7). *Propaganda: Psychological warfare in the First World War* [Text]. Der Erste Weltkrieg. https://ww1.habsburger.net/en/chapters/propaganda-psychological-warfare-first-world-war

Gordon, D. E. (1981). CHAPTER I - Introduction. In *Electronic Warfare: Element of Strategy and Multiplier of Combat Power* (pp. 1–13). Pergamon. https://doi.org/10.1016/B978-1-4831-9722-7.50004-2

Grisham, J. (2021). *Echo Breaking News | Media Literacy and Digital Literacy: How they differ and why they matter*. Echo Breaking News. https://echo-breaking-news.com/blog/media-literacy-vs-digital-literacy/

Gunther, A. C., & Liebhart, J. L. (2006). Broad Reach or Biased Source? Decomposing the Hostile Media Effect. *Journal of Communication*, *56*(3), 449–466. https://doi.org/10.1111/j.1460-2466.2006.00295.x

Hanna, K. T., Ferguson, K., & Rosencrance, L. (2021). *What is cyberwarfare?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/cyberwarfare

Heinrich, A. (2012). What is 'Network Journalism'? *Media International Australia*, *144*(1), 60–67.

Henderson, M. J., Shade, L. R., & Mackinnon, K. (2020). EVERY CLICK YOU MAKE: ALGORITHMIC LITERACY AND THE DIGITAL LIVES OF YOUNG ADULTS. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2020i0.11233

Hobbs, R. (2010). *Digital and media literacy: A plan of action*. The Aspen Institue.

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, *15*(2), 81–93. https://doi.org/10.1080/19331681.2018.1448735

Jamieson, K. H., & Cappella, J. N. (2010). *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*. Oxford University Press.

Kahn, M. L., & Idris, I. K. (2019). Recognise misinformation and verify before sharing: A reasoned action and information literacy perspective. *Behaviour & Information Technology*, *38*(12), 1194–1212.

Koenig, A. (2020). The Algorithms Know Me and I Know Them: Using Student Journals to Uncover Algorithmic Literacy Awareness. *Computers and Composition*, *58*. https://www.sciencedirect.com/science/article/abs/pii/S8755461520300724

Lecheler, S., & de Vreese, C. H. (2011). Getting Real: The Duration of Framing Effects. *Journal of Communication*, *61*(5), 959–983. https://doi.org/10.1111/j.1460-2466.2011.01580.x

Loisen, J., Joye, S., & Verstraeten, J. (2016). *Communicatie en media: Een inleiding tot communicatiewetenschappen. Onderzoek en theorie*. Acco.

Longley, R. (2019). *An Introduction to Psychological Warfare, From Genghis Khan to ISIS*. ThoughtCo. https://www.thoughtco.com/psychological-warfare-definition-4151867

Marcus, G. F. (2009). *Kluge: The Haphazard Evolution of the Human Mind*. Houghton Mifflin Harcourt. https://www.amazon.it/Kluge-Haphazard-Evolution-Human-Mind/dp/054723824X

McLuhan, M. (1962). *The Gutenberg Galaxy: The Making of Typographic Man*. University of Toronto Press.

McManus, J. H. (1994). *Market-Driven Journalism: Let the citizen beware?* (6th ed.). Sage Publications Inc.

McNair, B. (2006). *Cultural Chaos: Journalism, News and Power in a Globalised World*. Routledge Taylor & Francis Group.

McNair, B. (2018). *Fake News: Falsehood, Fabrication and Fantasy in Journalism*. Routledge Taylor & Francis Group.

McQuail, D. (1987). *Mass communication theory: An introduction* (2nd ed., pp. xvi, 352). Sage Publications, Inc.

McRaney, D. (2011). *You Are Not So Smart: Why You Have Too Many Friends on Facebook, Why Your Memory Is Mostly Fiction, and 46 Other Ways You're Deluding Yourself*. Gildan Media Corporation. https://www.ibs.it/you-are-not-so-smart-libro-inglese-david-mcraney/e/9798200561247?gclid=CjwKCAjwwdWVBhA4EiwAjcYJECCgtWFhtKsegUoLdbhigBHJnOgb0vjWzyOP6rZeyT9tcqUTLhzL9hoCprUQAvD_BwE

Meyer, R. (2018, March 8). *The Grim Conclusions of the Largest-Ever Study of Fake News*. The Atlantic. https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/

NATO. (2020). *MEDIA-(DIS)INFORMATION-SECURITY INFOGRAPHICS*. Defence Education Enhancement Programme. https://deepportal.hq.nato.int/eacademy/courses/

Nechushtai, E., & Lewis, S. (2019). What kind of news gatekeepers do we want machines to be? Filter bubbles, fragmentation, and the normative dimensions of algorithmic recommendations. *Computers in Human Behavior*, *90*, 298–307.

Nemr, C., & Gangwire, W. (2019). *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*. Parks Advisors. https://2017-2021.state.gov/weapons-of-mass-distraction-foreign-state-sponsored-disinformation-in-the-digital-age/index.html

Nickerson, R. S. (1998). Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, *2*(2), 175–220. https://doi.org/10.1037/1089-2680.2.2.175

Pantazi, M., Hale, S., & Klein, O. (2021). Social and Cognitive Aspects of the Vulnerability to Political Misinformation. *Political Psychology*, *42*(S1), 267–304. https://doi.org/10.1111/pops.12797

Pariser, E. (2011). *The Filter Bubble: What The Internet Is Hiding From You*. Penguin UK. https://books.google.it/books/about/The_Filter_Bubble.html?hl=it&id=-FWO0puw3nYC&redir_esc=y

Paulussen, S. (2004). Online News Production in Flanders: How Flemish Online Journalists Perceive and Explore the Internet's Potential. *Journal of Computer-Mediated Communication*, *9*(4), 00–00. https://doi.org/10.1111/j.1083-6101.2004.tb00300.x

Principe, G. F., Guiliano, S., & Root, C. (2008). Rumor mongering and remembering: How rumors originating in children's inferences can affect memory. *Journal of Experimental Child Psychology*, *99*(2), 135–155. https://doi.org/10.1016/j.jecp.2007.10.009

Scheufele, D. A., & Krause, M. N. (2019). Science audiences, misinformation, and fake news. *Proceedings of the National Academy of Sciences*, *116*(16), 7662–7669. https://doi.org/10.1073/pnas. 1805871115

Shapovalova, E. (2020). Improving Media Education as a Way to Combat Fake News. *Media Education*, *60*(4), 730–735.

Silverman, C. (2015). *Lies, Damn Lies and Viral Content* (Tow Center for Digital Journalism Publications). Tow Center for Digital Journalism, Columbia University. https://doi.org/10.7916/D8Q81RHH

Slothuus, R., & de Vreese, C. H. (2010). Political Parties, Motivated Reasoning, and Issue Framing Effects. *The Journal of Politics*, *72*(3), 630–645. https://doi.org/10.1017/S002238161000006X

Soroka, S., Fournier, P., & Lilach, N. (2019). Cross-national evidence of a negativity bias in psychophysiological reactions to news | PNAS. *Proceedings of the National Academy of Sciences*, *116*(38), 18888–18892.

Stupples, D. (2015). *What is information warfare?* World Economic Forum. https://www.weforum.org/agenda/2015/12/what-is-information-warfare/

Sunstein, C. (2002). The Law of Group Polarization -. *Ournal of Political Philosophy*, *10*(2), 175–195.

Swart, J. (2020). TACTICS OF ALGORITHMIC LITERACY: HOW YOUNG PEOPLE UNDERSTAND AND NEGOTIATE ALGORITHMIC NEWS SELECTION. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2020i0.11342

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. *Philosophy & Technology*, *25*(1), 105–120. https://doi.org/10.1007/s13347-011-0040-9

Team Media Texthack. (2014). *Media Studies 101*. BCcampus. https://opentextbc.ca/mediastudies101/

The Cambridge Dictionary. (2020). In *The Cambridge Advanced Learner's Dictionary & Thesaurus*. Cambridge Univesity Press.

The Guardian. (2022, May 1). 'Troll factory' spreading Russian pro-war lies online, says UK. *The Guardian*. https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk

University of Kansas. (2019). *Study shows vulnerable populations with less education more likely to believe, share misinformation*. Phys.Org. https://phys.org/news/2020-05-vulnerable-populations-misinformation.html

Van Dijk, J. (2012). *The Network Society* (3rd ed.). Sage Publications Ltd. https://www.torrossa.com/en/resources/an/4913638

Vīķe-Freiberga, V., Däubler-Gmelin, H., Hammersley, B., & Pessoa Maduro, L. M. P. (2013). *A free and pluralistic media to sustain European democracy*. Resource Center on Media Freedom in Europe. https://www.rcmediafreedom.eu/Publications/Reports/A-free-and-pluralistic-media-to-sustain-European-democracy

Wallace, J. (2017). Modelling Contemporary Gatekeeping: The rise of individuals, algorithms and platforms in digital news dissemination. *Digital Journalism*, *6*, 1–20. https://doi.org/10.1080/21670811.2017.1343648

Wardle, C., & Derakhshan, H. (2017). *INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making*. Council of Europe.

Wegner, D. M., Coulton, G. F., & Wenzlaff, R. (1985). The transparency of denial: Briefing in the debriefing paradigm. *Journal of Personality and Social Psychology*, *49*(2), 338–346. https://doi.org/10.1037/0022-3514.49.2.338

Woolley, S., & Howard, P. N. (2016). Social media, revolution, and the rise of the political bot. In *Routledge Handbook of Media, Conflict and Security* (1st ed., p. 11). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315850979-33/social-media-revolution-rise-political-bot-samuel-woolley-philip-howard

Woolley, S., & Howard, P. N. (Eds.). (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press. https://doi.org/10.1093/oso/9780190931407.001.0001

Yang, A. (2019). Reflexive Control and Cognitive Vulnerability in the 2016 U.S. Presidential Election. *Journal of Information Warfare*, *18*(3), 99–122.

Zagers, G. (2021, March 16). *We moeten het eens hebben over deepfakes (en nee, dit is niet Tom Cruise)*. Focus. https://focus.knack.be/meer/online/we-moeten-het-eens-hebben-over-deepfakes-en-nee-dit-is-niet-tom-cruise/