Jared Wayne York

Safeguarding Democracy from Disinformation: A Transatlantic Comparative Analysis of Policy Tools

Master Thesis

at the Chair for Information Systems and Information Management
(Westfälische Wilhelms-Universität, Münster)

Supervisor: Prof. Dr. Steven Van de Walle

Presented by: Jared Wayne York
Rue des Commerçants 32
1000 Brussels
+32 491 935857

Date of Submission: 2023-06-05

Abstract

This master's thesis provides a comparative analysis of U.S. and EU approaches in response to the challenge of disinformation and its threats to democracy. Through an analysis of the content of public policy documents and supplementary expert interviews, it establishes a taxonomy of disinformation policy instruments based on Hood's (1986) 'NATO' model, addressing three major questions. Firstly, it analyses the specific threats disinformation presents to democratic processes, such as the destabilization of political discourse and decision-making. Secondly, it examines the distinct policy responses of the U.S. and EU. The U.S. emphasizes legislative action, focusing on transparency in digital political advertising and platform accountability, whereas the EU adopts a broad collaborative approach prioritizing education, public-private partnerships, and international cooperation. Lastly, it extrapolates four best practices from the studied policies: transparency, collaboration, public education, and adaptability, all crucial for effective disinformation policymaking. The findings offer a nuanced perspective on U.S. and EU disinformation countermeasures, beneficial for both comparative policy research and future policymaking processes in other democratic nations. The study underscores the need for constant vigilance, innovation, and global cooperation to preserve democratic integrity against disinformation in a rapidly evolving digital landscape.

Acknowledgement

First and foremost, my sincerest appreciation is extended to my supervisor, Prof. Dr. Steven Van de Walle, whose unwavering support and guidance throughout this journey have helped make what once seemed an unsurmountable task into an achievement that I am proud of. Prof. Van de Walle's wisdom in the field of public administration helped me shape the framework and structure of this thesis, serving as a beacon and guiding my research and thought processes in the most constructive and enriching manner. This accomplishment would not have been possible without their mentorship.

The PIONEER programme, including all of my fellow Pioneers, deserves heartfelt recognition for fostering an environment of collaboration and intellectual growth. Among them, I want to extend a profoundly personal thank you to my husband, Kai Zhang. Kai, your strength, love, and continuous support have been my pillar of motivation. The Pioneers started this journey together in Leuven, and while we finish it in different parts of the world, the relationships we have formed together keep us all tightly connected.

My gratitude extends to the EBSI team at NTT DATA for their incredible support and understanding. Balancing an internship with the rigors of research was made possible thanks to their flexibility. Their accommodation allowed me to dive deeply into my thesis, providing a unique perspective on the interplay between academic investigation and industry experience by giving me the opportunity to work for the European Commission Directorate General of Informatics on real-world digital transformation and cross-border digital public service projects.

A special thanks to the experts who generously gave their time and shared their knowledge for this research. Their insights have played a pivotal role in shaping the depth and breadth of this study.

Finally, this research journey has been more than an academic exercise; it has been a personal and professional growth experience. The insights I have gained and the relationships I have built through this process have underscored the importance of interdisciplinary and international cooperation in the face of modern challenges like disinformation. It is my hope that the findings of this research will contribute to our collective efforts in preserving the integrity of our democratic processes all over the globe.

Thank you all for being part of this journey!

Content

List of Tables and Figures

Abbreviations

AI	artificial intelligence
CCS	comparative case study
CPC	crisis pregnancy center
CSC	Cyberspace Solarium Commission
CSCC	Center for Strategic Counterterrorism Communications
CISA	Cybersecurity and Infrastructure Security Agency
DHS	U.S. Department of Homeland Security
DMA	Digital Markets Act
DSA	Digital Services Act
EEAS	European External Action Service
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GEC	Global Engagement Center
INGE	Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation
RAS	Rapid Alert System
SAD	Stop Antiabortion Disinformation
SOMA	Social Observatory for Disinformation and Social Media Analysis
VLOP	very large online platform

1 Democracy and Disinformation in the Digital Age

From Russian interference in the 2016 U.S. elections to more recent propaganda surrounding the unjust war in Ukraine, the plight of disinformation campaigns and their impact on democracy continues to serve as a focus for national and international political discussions. The ever-growing threat landscape encompasses malignant actors of both international and domestic origin. Scholars Miller and Vaccari point out that "disinformation is not simply a foreign threat" and that "domestic purveyors of disinformation" are leveraging traditional media outlets such as newspapers, radio stations, and television news media to disseminate false information (Miller and Vaccari 2020). Other scholars have argued that newer forms of online social media undermine democratic oversight by displacing traditional media with algorithmic systems and reducing speech accountability due to users' anonymity (McKay and Tenove 2020). With an ever-growing threat landscape, citizens and governments alike are beginning to recognize the harmful effects that disinformation can pose on states operating under democratic institutions.

As a result, governments have responded with a wide range of policies to address concerns about the potential threats that disinformation poses to democracy. Despite this, it appears that there is little agreement in elite policy discourse or academic literature as to what it means for disinformation to threaten democracy and how different policies might help to counter its negative implications (Tenove 2020). To further investigate this knowledge gap, this research will conduct a comparative analysis of disinformation policies within the U.S. and EU employing a document analysis.

1.1 Motivation

The motivation for this research topic stems from an internship at the United States Commercial Service and International Trade Association under the U.S. Mission to the European Union pursued by the researcher following the end of the first semester of this master's program. This governmental organization promotes U.S. business interests in the European Union through advocacy, information dissemination, and cooperation between transatlantic public and private organizations. During this internship, the researcher's main tasks included monitoring, researching, and analyzing EU legislation concerning U.S. business interests. The researcher reported on legislative developments regarding digital policies such as the Digital Markets Act and Digital Services Act and served as rapporteur for parliamentary meetings by the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE). During these INGE holdings, the researcher became aware of

the threats that disinformation poses to democracies around the world, thus sparking their interest in conducting further research on this topic.

1.2 Formulation of Research Questions

This research aims to answer the following research question:

How are governments responding to the threat of disinformation as a means of undermining democracy?

The following three additional sub-questions are introduced to address the proposed research objectives and add greater granularity to the focus and scope of the research:

1. What threats do disinformation, misinformation, and online propaganda pose to democracy?

2. What specific policy actions have the U.S. and the European Union taken in response to these threats?

3. What best practices can be construed and applied to future developments in disinformation policies?

To address the research questions, this research will pursue the following *research objectives*:

1. Identify the disinformation threat landscape concerning the institutions, processes, and citizens of democratic nations;

2. Analyze the disinformation policy tools implemented in response to disinformation threats in the United States and the European Union; and

3. Extrapolate best practices to provide insight for the development of future disinformation policies.

The present study seeks to comprehensively understand disinformation and its implications for democracy by examining the policy responses in two major democratic regions: the United States and the European Union. These regions have been chosen due to their distinct political, legal, and cultural contexts and contrasting approaches to regulating disinformation. By comparing the policy measures adopted in the U.S. and the EU, this research aims to identify best practices and areas for improvement in addressing disinformation and its potential threats to democracy.

1.3 The Research Structure

This study will be structured as follows: first, this research will construct a theoretical framework based on the existing literature on disinformation and its impact on democracy, focusing on democratic theory and empirical findings that have emerged in recent years regarding the negative impacts of disinformation in the U.S. and the EU. This will help to contextualize the debate on disinformation and provide a solid foundation for the comparative analysis. Additionally, a brief literature review of similar studies will be conducted to identify the gap in research on the topic.

Next, the methodology employed in this research will be detailed, outlining the document analysis and semi-structured interviews that will be used to gather data on the policy responses in the U.S. and the EU. This section will also discuss the challenges and limitations of the chosen methods, as well as the steps taken to ensure the reliability and validity of the findings.

The subsequent section will present the results of the comparative analysis, highlighting the similarities and differences between the policy measures adopted by the U.S. and the EU in addressing disinformation. This will include examining the different governmental resources, legislature, and policy instruments implemented by the U.S. and the EU to combat disinformation and the various initiatives to ensure the continuation of democratic institutions and processes.

Finally, the study will conclude by discussing the implications of the findings for democratic theory and practice and by offering recommendations for U.S. and EU policymakers. The goal of this research is not only to enhance the understanding of disinformation and its impact on democracy but also to contribute to the development of more effective policy responses that can safeguard the integrity of democratic processes and institutions in an increasingly interconnected and digitalized world.

2 Disinformation and Democracy: A Theoretical Framework

The digital age, marked by the rapid development of computerized manufacturing, ubiquitous internet access, and the increasing interconnectedness of societies across the globe, has transformed various aspects of modern life, including communication, work, and leisure (Dawes 2009; Hanna 2018; Nath 2011). This technological revolution has fostered a paradigm shift from traditional media, such as newspapers, radio, and television, to new media platforms primarily characterized by user-generated content, social networking, and real-time communication (Hayes et al. 2007; Vukanovic 2009).

Social media, a dominant form of new media, has been widely celebrated for its potential to promote transparency, strengthen connectivity, and foster citizen engagement in political processes (Bertot et al. 2010; Dewan and Ramaprasad 2014; DiStaso and Bortree 2012). These platforms allow individuals to access information, share opinions, and participate in public debates, contributing to a more inclusive and vibrant democratic space. However, the rise of social media has also been accompanied by various risks and challenges, including cyber harassment, privacy infringement, and reputational damage (Akram and Kumar 2017; Putnam 2000). These platforms' unprecedented speed and reach have amplified the potential consequences of such negative aspects, raising questions about their overall impact on the health of democratic societies.

In the forthcoming sections, this research will delve into the intricate relationship between democratic theory and disinformation, exploring how these concepts intersect and influence one another in the context of democratic societies in the digital age. This analysis will cover key theoretical perspectives on democratic theory and the mechanisms through which disinformation can undermine democratic processes, such as participation in elections, public opinion formation, and the empowerment of societal actors. Furthermore, the research will assess the diverse political toolset of government resources available in the policy environment, such as legal and regulatory frameworks, media literacy initiatives, public awareness campaigns, and collaborations with private sector actors like social media platforms and technology companies. The effectiveness and potential drawbacks of these policy measures will be evaluated in light of the broader challenges posed by disinformation and the need to balance freedom of expression and democratic deliberation with the imperative of safeguarding the integrity of democratic processes.

2.1 Overview of the Threat Landscape Posed by Disinformation

Accurate information is critical for the operational efficacy of both traditional and new media outlets. It forms the backbone of their credibility, enabling them to disseminate

information, shape public opinion and influence societal norms (Arias et al. 2019). Beyond media, the broader health of democratic societies also hinges significantly on the accuracy of information. The transparency, informed decision-making, and accountability that form the bedrock of democratic societies are all predicated on the availability and circulation of accurate information (Gingras 2012; Héritier 2011).

Conversely, the implications of inaccurate information can be quite dire, especially during crises such as the Covid-19 pandemic. This is highlighted in the work of Baines and Elliott (2020), which underlines the severity of the repercussions. One key consequence is the erosion of public trust. When misinformation or disinformation becomes prevalent, it can undermine the credibility of media outlets and public institutions, causing a gradual or even swift erosion of trust among citizens (Rodriguez-Morales and Franco 2021).

Inaccurate information can spread mass panic among the general population (The Lancet 2020; Wu et al. 2022). During a crisis, panic can have serious implications, escalating an already precarious situation into a full-blown catastrophe. This is particularly true when misinformation fuels fears or misunderstandings about the crisis, leading to irrational behavior or reactions that can further exacerbate the situation (Sherman et al. 2021).

Furthermore, inaccurate information can severely undermine public health measures. In the context of the Covid-19 pandemic, misinformation surrounding the virus, its transmission, or the effectiveness of health measures can deter people from adhering to guidelines set by health authorities (Baines and Elliott 2020). This can impede efforts to control the virus's spread, prolonging the crisis and causing unnecessary harm. Therefore, the importance of accurate information cannot be overstated, given its serious impact on the health of democratic societies and their ability to manage crises effectively.

2.1.1 Defining Disinformation

False information takes various forms, including misinformation, malinformation, and disinformation. This research will focus on disinformation, the strategic dissemination of false information to cause public harm (Baines and Elliott 2020; Humprecht et al. 2020; Shu et al. 2020; Wardle and Derakhshan 2017). Disinformation can be distinguished from other forms of false information by its intent. While misinformation refers to the unintentional sharing of false information, disinformation involves deliberately creating and disseminating false or misleading content, often with political, economic, or social motivations (Wardle and Derakhshan 2017). Disinformation campaigns can be orchestrated by state or non-state actors, including foreign governments, political parties,

extremist groups, and even individuals seeking to manipulate public opinion or disrupt democratic processes (Colomina et al. 2021; Schiffrin 2017).

The arrival of the digital age and the mass adoption of social media platforms by people globally have dramatically increased the speed and scale at which disinformation can spread (Allcott and Gentzkow 2017; Tucker et al. 2018). These platforms often prioritize content that generates user engagement, inadvertently promoting sensationalist or polarizing disinformation over more accurate and nuanced information (Vosoughi et al. 2018). Moreover, the anonymity provided by online platforms enables malicious actors to obscure their identities and intentions, making it difficult for users to discern the credibility of information sources (Woolley and Howard 2016).

2.1.2 Disinformation in the U.S. and the EU

Cases of disinformation are widely documented in both the U.S. and the EU. In the U.S., the 2016 presidential election brought disinformation to the spotlight, as foreign interference campaigns aimed to manipulate public opinion and create discord among American voters (Jamieson 2021; Special Counsel's Office 2019). In the years since, disinformation has persistently undermined trust in the American government, intensified political polarization, and degraded the quality of public discourse throughout the nation (Guess et al. 2019; Lewandowsky et al. 2017). In addition to the 2016 election, the U.S. has experienced numerous disinformation campaigns surrounding topics such as the Covid-19 pandemic, climate change, and social justice movements like the Black Lives Matter movement, deepening social divisions and furthering misinformation in crucial public debates (Allcott and Gentzkow 2017; Baines and Elliott 2020).

Similarly, disinformation campaigns have targeted elections, referenda, and public opinion on diverse policy issues in the EU. These campaigns aim to destabilize the democratic institutions and values that make up the EU and promote the interests of foreign powers or extremist groups (Colomina et al. 2021; Polyakova and Boyer 2018). For example, the Brexit referendum in the United Kingdom experienced widespread dissemination of disinformation related to the potential consequences of leaving the EU, leading to confusion and misinformation among voters (Hobolt 2016).

Disinformation has also affected national elections in EU member states, such as the 2017 French presidential election, where malicious actors targeted Emmanuel Macron's campaign with hacking attempts and spreading fake news (Ferrara 2017a). Moreover, disinformation campaigns have sought to manipulate public opinion on migration, climate change, and EU integration, exacerbating tensions and fostering divisions within the EU (Humprecht et al. 2020).

These examples highlight disinformation's wide-ranging and pernicious impact on democratic processes in the U.S. and the EU, highlighting the urgent need for effective policy responses to address this growing threat. However, before disinformation can be linked to negative impacts on democracy, it is crucial first to examine and identify the key qualities and functions that constitute a healthy democracy. The following section explores the origins and interpretations of democratic theory to isolate key democratic functions in society.

2.2 Democratic Theory: Foundations and Variations

Democratic theory has undergone significant transformations and refinements throughout history, reflecting the changing social, political, and economic contexts in which it has been embedded (Bohman 1990; Krouse 1982). As societies have evolved, so too have the ideas and principles that underpin the democratic process, resulting in a myriad of conceptualizations and interpretations. To understand the contemporary challenges that disinformation poses to democracies, it is important first to examine the developments in democratic theory to formulate a solid foundation for identifying the key areas of democratic functioning that may be at risk and for developing effective strategies to preserve the integrity of democratic processes in an increasingly interconnected and digitalized world (Monsees 2021).

Democratic theory encompasses diverse practices and outcomes, with no single unique set of institutions (Schmitter and Karl 2017). As democratic theory has evolved, so too have the definitions and expectations surrounding what constitutes a healthy democracy. These changes are often attributed to the shifting priorities and concerns of different historical periods and cultural contexts (Staats 2004). The classical doctrine of democracy, originating in ancient Greece, primarily involved electoral processes, with citizens directly participating in decision-making (Pettit, 2019). This notion of direct democracy later gave way to more indirect forms of democratic governance, such as representative democracy, in which elected representatives act on behalf of the citizens (Besley and Coate 1997; Schumpeter 1976).

2.2.1 A Problem-Based Approach to Understanding Democracies

In the ever-evolving field of political science, the definitions of democracy remain numerous and often contradictory. In response to the diverse and often conflicting definitions of democracy, Associate Professor of Government at Georgetown University, Mark E. Warren, founded a new problem-based approach to support the conceptualization of democracy and democratic theory (He and Warren 2012; Warren 2017). Rather than prescribing a fixed set of institutions or practices, this approach focuses on three specific

problems that a democratic political system must solve to be considered democratic, namely: (1) empowered inclusion, (2) collective agenda and will formation, and (3) collective decision making (Warren 2017, p.41). By identifying and focusing on these core problems, Warren argues that scholars can better understand how democratic systems operate and identify potential systemic deficits or shortcomings. This approach allows for a more flexible analysis that is not confined to a single definition of democracy but can be applied across different contexts and historical periods (Beauvais and Warren 2019).

2.2.2 Empowered Inclusion: Ensuring Equal Participation

When considering the key functions of democratic processes, the principle of inclusion and equal participation is the foundation for other democratic functions (Warren 2017). This function stems from the normative "all affected interests" principle, which proposes that anyone potentially affected by collective decisions should be allowed to influence those decisions (Goodin 2007). This principle is popularly cited in various scholarly works such as those by Näsström (2011), Owen (2012), and Koenig-Archibugi (2017). This represents a universally embraced notion in democratic societies that the people, who stand to be impacted by the collective decisions, should be granted a voice, or at the very least, a potential avenue to express their opinions on the matters at hand.

However, democracies should not merely promote inclusion – they must actively empower it. This distinction is crucial, for it is insufficient for a government to merely consult its citizens in a tokenistic manner (Manor 2007). Members of a democratic society who are normatively entitled to inclusion must be vested with the powers that enable them to insist upon and enforce their right to be included in decision-making processes (Andersen and Siim 2004). This empowerment could be in the form of voting rights, legal standing, representation, the ability to veto decisions, and the capacity for organized opposition. Numerous scholars in the fields of political science and democracy studies support the viewpoint that individuals who stake a claim for inclusion, owing to their potential to be affected by collective decisions, must be equipped with the powers of expression, voting, representation, and dissent (Enslin et al. 2001; Goodin 2007; Kelly 1998; Skrtic et al. 1996; Young 2002). These scholars all agree in unison on the importance of these powers in ensuring the effectiveness of democratic inclusion.

Finally, it is important to consider the moral and ethical dimensions of democratic inclusion. These involve recognizing each individual's inherent dignity and worth, which is the foundation for their right to be included (Ober 2012). This also justifies how the powers and opportunities for inclusion are distributed across society. This ethical consideration emphasizes the necessity for a just and fair distribution of power and rights

to enable effective and empowered inclusion in democratic processes (Modise 2017; Mueller and Stratmann 2003).

2.2.3 Collective Agenda and Will Formation: Shaping Public Discourse

In the realm of democratic processes, once the individual or group-specific interests, perspectives, values, and preferences are included within a collective framework via the function of empowerment described above, an important next step is to communicatively shape these diverse elements into collective agendas and wills (Beauvais and Warren 2019; Warren 2017). This transformative process primarily employs tools such as advocacy, argument, negotiation, persuasion, and bargaining, which can all be broadly categorized under the umbrella of deliberation (Cohen 2005).

This guiding principle, which posits that individual preferences need to be communicatively connected to collective judgments, can be found at the heart of modern theories of deliberative democracy (Bohman 1999; Cohen 2005). The overarching idea is to extend the concept of individual self-governance into the realm of collective self-governance (Pitt and Ober 2019). To achieve self-rule within a collective, individuals must understand the interplay between their preferences and collective judgments and comprehend the reasons underpinning these collective judgments (McAfee 2022).

In the modern era, digital technologies, particularly social media, have played a transformative role in collective will and agenda formation (Berg and Hofmann 2021). They have considerably amplified and diversified the platforms for public discourse, extending its reach beyond traditional boundaries. The advent of social media platforms, such as Facebook, Twitter, Instagram, and others, has democratized the process of inclusion and empowerment in unprecedented ways (Jennings et al. 2020). They offer interactive spaces where interests, perspectives, values, and preferences of individuals from various classes and backgrounds can be freely expressed and included within the larger social dialogue (Halpern and Gibbs 2013). The collective will, thus, is no longer limited to being shaped in physical town halls or legislative chambers but also in the virtual realm of likes, shares, comments, and tweets.

Governments, legislative bodies, and other civic institutions worldwide are also increasingly acknowledging the transformative potential of digital platforms, particularly social media, as an effective platform for direct communication with their constituents (De Rosario et al. 2016). This transition, which represents a significant departure from traditional modes of public engagement, heralds a new era in collective agenda and will formation. Leveraging the power and reach of social media platforms, institutional bodies can engage with citizens directly, gaining immediate insights into their interests,

concerns, and aspirations (Freeman 2016). This interactive relationship fosters a more dynamic and responsive governance model, enhancing these institutions' ability to reflect their constituents' collective will in their decision-making processes. Furthermore, social media channels provide a platform for institutions to disseminate information swiftly and broadly, thus increasing transparency and accountability (Lev-On and Steinfeld 2016). Simultaneously, these platforms offer citizens a means to voice their opinions, participate in public discourse, and actively shape collective agendas.

2.2.4 Collective Decision Making: Maintaining Trust and Integrity

The collective decision-making process, akin to the principle of inclusion, primarily concerns empowerment, yet it extends beyond the formation of collective will (Warren 2017). While empowered inclusion focuses on the individual, collective decision-making emphasizes collective empowerment, namely, when groups can establish and enforce binding decisions to accomplish common objectives (Christiano 1990; Issacharoff 2008). This capacity for collective decision-making empowers communities to secure common goods and protections and regulate and manage semi-independent systems such as markets. Furthermore, it equips a collective with the means to establish the conditions for empowered inclusion and collective will formation (Beauvais and Warren 2019; Warren 2017). A failure within political systems to facilitate these constitutional moments equates to a failure to empower communities as collective entities.

Collective decision-making is fundamentally linked to voting in a democratic society. Voting is one of the most significant tools for making collective decisions, especially in democratic settings (Tideman 2016). It provides a practical mechanism that allows every eligible citizen to have a say in important issues, from selecting leaders in government to making decisions on public policies and laws. Every vote contributes to forming a collective will, which should ideally reflect the desires and needs of the majority, but also consider the interests of minority groups (Jacob 2015). Thus, voting is an exercise of personal choice and a contribution to the larger collective decision-making process.

In the context of the digital age, the link between collective decision-making and voting has been further reinforced. Digital platforms have introduced new opportunities for voting and participation in collective decisions, often allowing a broader and more diverse segment of society to be part of decision-making processes (Hilbert 2009; Macintosh et al. 2003). Online voting systems, digital town halls, and e-petitions show how digital technology has revolutionized collective decision-making (Macintosh 2004).

Examining the three core functions of democracy described above—empowered inclusion, collective will and agenda formation, and collective decision-making—

provides a comprehensive and nuanced framework to investigate the impact of disinformation on democratic processes. This framework will be applied to investigate how disinformation can critically undermine each of these functions, obstructing the inclusiveness of democratic processes, distorting the formation of collective will and agenda, and contaminating the integrity of collective decision-making, particularly voting. In a world increasingly navigating the digital landscape, where the spread of disinformation can be swift and pervasive, understanding the interplay of these functions enables a more in-depth understanding of the specific mechanisms through which disinformation threatens democracy. This comprehensive view also facilitates the creation of targeted strategies and policies to counteract the negative effects of disinformation, thereby protecting and strengthening the democratic process in the digital age.

3 Literature Review: Disinformation and its Impact on Democracy

While bringing profound advancements in communication and information sharing, the digital age has also ushered in a challenging new landscape marked by the proliferation of disinformation. This phenomenon presents an increasingly intricate and alarming threat to the very core of democratic societies worldwide. This threat necessitates a rigorous examination of the underlying factors that contribute to the spread and impact of disinformation and the measures that can be taken to mitigate its detrimental effects.

This literature review embarks on a comprehensive exploration of previous scholarly works focused on this pressing issue. It delves into the intricate web of disinformation, its genesis, and its multifaceted manifestations across various digital platforms. An integral part of this review is understanding the role of new technologies such as artificial intelligence (AI), social bots, and sophisticated targeting algorithms in propagating disinformation. While promising on many fronts, these technologies have unfortunately also been exploited as tools of deception, manipulation, and political subversion.

Deepfake technology is a particular area of concern in this intricate landscape. This novel AI-driven technology, capable of generating highly realistic but entirely fabricated audio-visual content, represents a new frontier in disinformation. The literature under review examines the potential of deepfakes as potent instruments of disinformation, their potential implications for various aspects of a democratic society, and the challenges they pose to journalism.

Additionally, the review delves into the policy dimensions of disinformation. With the rise of AI-enabled disinformation, there is an emergent need to formulate and implement robust policy and legislative responses to safeguard democratic processes. By examining the existing body of literature, this review sheds light on such initiatives, their effectiveness, and the areas that require further attention.

3.1 The Role of Artificial Intelligence and Social Media in Disinformation

Artificial intelligence and social media intersection have significantly influenced the proliferation of disinformation in the digital age. Scholar García-Orosa (2021) discusses several phenomena that are impacting the formation of public opinion in the digital age, including the role of digital platforms as political actors, the use of AI and big data in political strategies, and the employment of falsehoods via fake news and deepfakes as a political strategy. While previous studies focus primarily on textual disinformation, scholars Dan et al. (2021) acknowledge the effect of visual information on social media

platforms on how individuals consume, process, and respond to information. This viewpoint has been corroborated by various scholars researching the behavioral response to misinformation presented in a visual media format (Cao et al. 2020; Matthes et al. 2021; Powell et al. 2015).

Another popular topic under discussion by several scholars is the implications of social bots – AI systems designed to mimic human behavior and interact with users on social media platforms – and their spread of disinformation (Ferrara 2017b; Hajli et al. 2022; Wang et al. 2018; Wiesenberg and Tench 2020). These bots are often deployed to manipulate public opinion, spread disinformation, and create an illusion of popular consensus or sentiment, a practice referred to as astroturfing (García-Orosa 2021; Kovic et al. 2018). This manipulation of public opinion has been seen in various contexts, including election campaigns, public health crises, and climate change debates, leading to increasing polarization and misinformation among citizens.

Additionally, in the seminal work "Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting," scholar Brkan (2019) delves into the role of AI in tailoring disinformation for specific target audiences. Scholars have conducted similar research that discusses how AI algorithms can analyze vast amounts of data to identify individuals' political leanings, biases, and vulnerabilities, then deliver tailored disinformation that exploits these characteristics (Agudo and Matute 2021; Peters 2022). This form of targeted disinformation can be particularly potent, as it can reinforce existing beliefs, sow division, and undermine democratic discourse.

3.2 Deepfake Technology: The New Frontier of Disinformation

Deepfake technology, a notable advancement in the field of artificial intelligence described above, has significantly amplified the complexity and potential threats associated with disinformation (Temir 2020). These technologies can create hyper-realistic videos of individuals appearing to say or do things they never did, posing profound implications for public discourse, individual reputations, and even geopolitical stability. Several scholars foresee the possibility of deepfakes becoming a predominant form of fake news, undermining public trust in authority figures and institutions at large (Brown 2020).

This perspective is echoed and expanded in "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics" (Chesney and Citron 2019). The authors further warn of the potential for deepfakes to ignite geopolitical conflicts or tarnish reputations. Meanwhile, Temir (2020) adds another dimension to this discourse, suggesting that the proliferation of deepfakes could fundamentally undermine the

credibility of journalism as it becomes increasingly challenging to distinguish fact from fiction.

Building upon these concerns, scholar Pawelec (2022) presents a comprehensive framework for understanding democracy and its vulnerabilities to deepfake disinformation. Drawing from the work of Warren (2017) and other democratic theorists, Pawelec integrates three core democratic functions to construct a robust and adaptable model. By applying this model to deepfakes, Pawelec illuminates how disinformation and hate speech enabled by this technology can pose significant threats to democratic functioning. This analytical framework also offers a valuable foundation for further exploration of the relationship between disinformation and democratic theory, underlining the key areas of democratic functioning that may be susceptible to the corrosive effects of false and misleading information.

3.3 Literature Gap: Taxonomy of Policy Responses to Combat Disinformation

Despite the growing body of literature discussing the impact of disinformation on democracy, there appears to be a significant gap in the academic exploration of systematic, comprehensive taxonomies of government policy responses to counter disinformation and promote democratic resilience.

While individual studies have focused on elements of policy responses, such as the role of education in fostering digital literacy (Dame Adjin-Tettey 2022; Dell 2019; Hwang et al. 2021) or the necessity for social media platform accountability (De Blasio and Selva 2021; Reisach 2021; Saurwein and Spencer-Smith 2020), a comprehensive, comparative study or taxonomy categorizing and evaluating diverse governmental policy responses to disinformation appears to be absent from the scholarly discussion.

Such a taxonomy could identify a range of concrete policy options, analyze their effectiveness, and consider their applicability across different political and cultural contexts. It could also study the interaction and coordination between policy areas (e.g., education, technology regulation, legal reform) in a holistic strategy to combat disinformation. The absence of this research prevents a comprehensive understanding of how different government policies can be applied, what has been effective, and where further efforts need to be concentrated. This gap in the literature underscores the need for further research in this area to provide policymakers with a more robust toolset to counter disinformation and promote democratic resilience.

4 Methodology

This research adopts the comparative case study (CCS) approach for examining policy formation and implementation in the context of disinformation and its impact on democratic systems, focusing on the United States and the European Union as the two primary cases (Bartlett and Vavrus 2016; Maxwell 2013). These cases have been selected based on factors that render them suitable and representative of democratic systems. They are also particularly relevant for studying policy responses to disinformation (Dahl 1998; Hix 2005; Moravcsik 2006).

The U.S. and the EU possess well-established, complex, and diverse democratic structures, which provide a rich context for analyzing policy formation and implementation (Dahl 1998; Hix 2005). Furthermore, these two entities exhibit distinct political and administrative systems, allowing for a more nuanced understanding of how democratic systems respond to policy challenges, such as disinformation (Huntington 1966). The U.S. and the EU have global significance as economic and political powers, and their policy decisions often have far-reaching implications on the international stage (Nye 2005). This prominence underscores the importance of analyzing policy processes in these two cases, as they may serve as influential models for other nations and regions.

Additionally, the U.S. and the EU have been primary targets of disinformation campaigns orchestrated by foreign actors (Fletcher et al. 2018; Pollicino and Bietti 2019). Studying these cases can offer valuable insights into the effectiveness and limitations of different approaches to addressing disinformation in democratic societies. The advanced technological infrastructures and highly digitalized societies in the U.S. and the EU also make them particularly vulnerable to disinformation spread through online platforms (Howard and Kollanyi 2016). Analyzing the policy responses in these two cases allows for examining the complex interplay between public institutions, private entities, and civil society in addressing disinformation and mitigating its impact on democratic processes (Helberger et al. 2017).

The researcher’s internship at the U.S. Mission to the EU provides familiarity with the inner workings of both entities, contributing to a deeper and more insightful analysis of the policy processes in question. This first-hand experience can provide valuable context for interpreting policy documents and understanding the complex interplay between various stakeholders.

4.1 Data Collection

This research employs a combination of two primary data sources to effectively address the research questions: official documents, websites, and publications published by relevant EU and U.S. government institutions, alongside five semi-structured expert interviews with key stakeholders from government institutions, the private sector, and non-governmental institutions. Institutional documents, websites, and publications are considered rich and reliable data sources due to their high-quality content and the direct involvement of governmental authorities in producing and disseminating them (Danto 2008).

A systematic search strategy will be employed to locate and analyze relevant documents, websites, and publications from U.S. and EU government institutions. This search strategy will involve identifying key governmental agencies, departments, and organizations in the U.S. and EU responsible for developing and implementing policies related to disinformation. These may include, but are not limited to, the European Commission, the European Parliament, the U.S. Department of State, and the U.S. Federal Communications Commission. Once identified, their official websites and online databases will be searched using specific keywords and search terms related to disinformation, such as “disinformation,” “misinformation,” “fake news,” “information manipulation,” and “online information integrity.” This approach will help ensure the comprehensiveness and relevance of the data collected for this study.

Given the top-down nature of the European Union’s legislative framework and the limited scope of individual member-state policies, this research will prioritize policy documents from the European Commission and other EU-level institutions. Similarly, the research will focus on federal-level policies and initiatives in the U.S., as these are more likely to provide a comprehensive and coherent understanding of the country’s approach to disinformation.

Interviews are also an effective form of data collection, as they provide deeper insights and overviews of issues under study, particularly when conducted with experts or individuals directly involved in relevant areas (Bolderston 2012). In this research, interviews will be conducted with professionals and individuals with experience or direct involvement in U.S. and EU disinformation policies, contributing to the in-depth analysis of the subject. As a form of socio-psychological communication, interviews are influenced by factors such as question order and quality, interview setting, interviewer preparedness, and interviewee’s emotional and psychological conditions (Bolderston 2012). While interviews are more time-consuming and costly than questionnaires, they are often preferred for firsthand data collection due to their ability to provide unbiased

information about personal experiences, behaviors, and opinions of research subjects (Mathers et al. 2000). Furthermore, interviews minimize non-response cases, as interviewers and respondents maintain direct contact.

The interactive nature of interviews presents several advantages. For instance, interviewees can request clarifications or repeat questions in case of misunderstandings, and the order of questions can be changed according to the needs of researchers and interviewers. Additionally, interviews can provide in-depth overviews and deep insights from individuals while allowing the interviewer to analyze the behaviors and emotional conditions of respondents to evaluate the reliability and validity of the obtained data.

In this study, semi-structured interviews were conducted, which combined the advantages of both structured and unstructured interviews (Schmidt 2004). This approach allowed for predetermined interview questions while permitting the interviewer to ask unplanned yet relevant questions that seemed important during the conversation. Semi-structured interviews enable respondents and interviewers to express their opinions and ask questions, encouraging a more open exchange of views and fostering a deeper understanding of various topics. The questions were constructed based on four key sub-topics:

1. **Sub-topic 1: Disinformation Sources & Tactics**: Examining the various sources of disinformation, their methods, and the scope of their impact on democratic processes;

2. **Sub-topic 2: Public Perception & Democracy**: Investigating disinformation's influence on public opinion, political polarization, and citizens' trust in democratic institutions;

3. **Sub-topic 3: Regulatory Frameworks & Policy Approaches**: Comparing the legal and policy frameworks in the US and the EU and their effectiveness in protecting democracy; and

4. **Sub-topic 4: Future Strategies & Collaborative Efforts**: Exploring potential US-EU collaborative efforts to combat disinformation and strengthen democratic resilience.

The individual questions include open-ended questions relating to the impact of disinformation on democratic processes and institutions within the U.S. and the EU, as well as specific policy tools implemented by the government in response to disinformation threats. The experts were identified based on a snowball approach and through mutual connections from previous professional and academic experiences. The

goal was to provide insight from the perspectives of key actors in a democratic society, with findings aiming to corroborate the results from the content analysis. The content analysis also informed some of the interview questions, while the insights from the interview also served to complement the content analysis as interviewees identifyed key documents that may have been overlooked by the researcher. A summary of the interview subjects can be found in Table 4.2 below, identifying their alias, function, and organization, as well as the date that the interview was conducted.

Name	**Function**	**Organization**	**Date of Interview**
Interviewee 1	(1) Research Associate; (2) Chair of the Supervisory Board	(1) University of Oxford; (2) eGovernance Non-Profit Foundation	09 May 2023
Interviewee 2	(1) Business Founder; (2) Former Channel Manager	(1) Cybersecurity Communication Company; (2) Microsoft	17 May 2023
Interviewee 3	Disinformation Analyst	European Parliament	19 May 2023
Interviewee 4	Disinformation Analyst	Debunk EU (NGO)	20 May 2023
Interviewee 5	Associate, and Member of the Advisory Board	Harvard University – Davis Center for Russian and Eurasion Studies	25 May 2023

Table 4.1 Interview Respondents

4.2 Data Analysis

In this research, the policy tools identified during the data collection phase and semi-structured interview transcripts will be subject to a qualitative data analysis process, which has gained widespread acceptance in social science research (Allan 2020).

Qualitative data analysis allows for a deeper understanding of complex issues and provides valuable insights into the intricacies of policy tools and their implementation.

A key aspect of analyzing qualitative data involves using codes to categorize and make sense of the collected data. Coding enables researchers to condense large amounts of information, identify significant patterns and relationships, and extract meaning, thereby facilitating the emergence of a logical chain of evidence (Linneberg and Korsgaard 2019). To streamline this process, the latest version of the qualitative data analysis software, NVivo 11, will be utilized for coding. This software improves the quality of research by automating labor-intensive tasks and allows researchers to assess the data better, identify relationships and trends, and ultimately, form well-grounded conclusions (Wong 2008).

The deductive approach to coding employed in this study ensures a top-down analysis of policy documents and interview transcripts by applying pre-determined codes to the data. This method maintains alignment with the research questions and objectives, focusing on the research's purpose (Azungah 2018). Furthermore, deductive analysis facilitates the coherent application of the conceptual framework on the data (Crabtree and Miller 1999). Consequently, the coding process will begin by classifying the documents' contents based on Hood's (1983) four resources of governments: (1) nodality, (2) authority, (3) treasure, and (4) organization. The contents will then be classified as either effectors or defectors, and the actions described in the content will then be assigned the codes associated with the key functions of democracies from Warren (2017): (1) empowered inclusion; (2) collective agenda and will formation; and (3) collective decision-making. These codes will be applied to both cases to assess the extent to which the conceptual framework can be observed. The code tree can be seen in the table below.

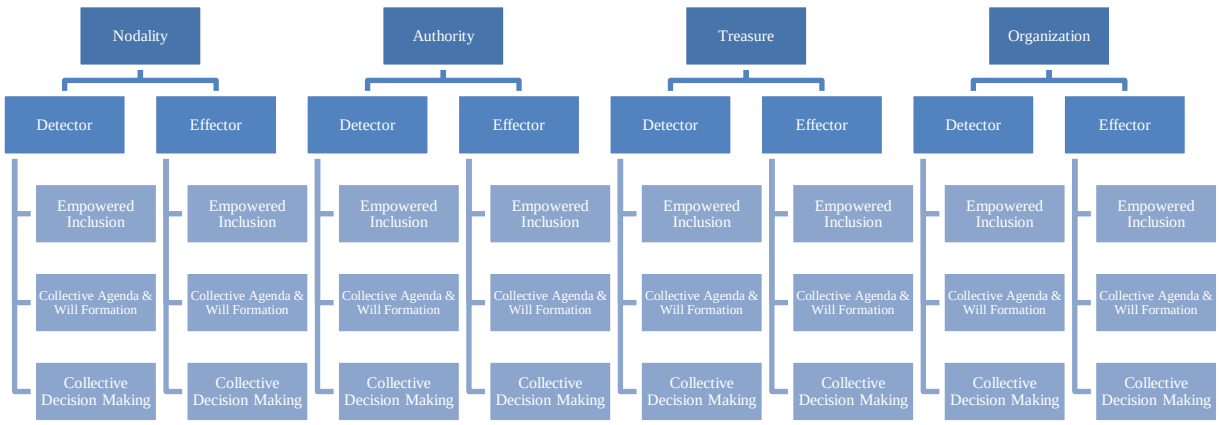


Figure 4.1 Code Tree Hierarchy Diagram

The coding process for policy instruments and interview transcripts will be carried out in two phases. In the first phase, the content of the policy instruments and related documents will be thoroughly reviewed to gain a comprehensive understanding of the disinformation policy environment in the U.S. and EU. After the initial readings, the content will be coded based on the a-priori codes. This phase will be completed before conducting the interviews, as the patterns and trends identified in the documents will provide valuable insights and inform the formulation of interview questions.

The interview transcripts will be coded according to the established codes in the second phase. The insights from the interviews will complement the initial findings from the first phase of policy document coding, resulting in a more robust and comprehensive analysis of the disinformation policy landscape in the U.S. and EU. By employing this rigorous, systematic approach to data analysis, this research aims to provide a nuanced understanding of the various strategies and resources utilized by these entities in addressing the complex issue of disinformation.

4.3 Data Categorization

Furthermore, classifying the content identified in documents, websites, and publications utilizes Christopher Hood's taxonomy of substantive policy instruments, providing an extensive framework for organizing disinformation-related policy tools in the U.S. and EU (Hood 1983). Hood's taxonomy distinguishes policy instruments based on the resources they depend on and whether the instrument aims to effect or detect changes in a policy environment. Hood (1983) identifies four key resources available to governments:

Nodality: Nodality refers to a government's unique position at the center of social and political networks. This central position allows governments to gather, disseminate, and leverage information and knowledge as valuable resources. In policy instruments, nodality influences behavior, spreads awareness, and communicates essential information to various stakeholders involved in the policy environment.

Authority: Authority represents the government's power to enforce rules, regulations, and legal frameworks. This power is derived from the legitimacy granted by the governed population and enables governments to establish, implement, and enforce standards, guidelines, and sanctions. Authority, as a resource, is employed in policy instruments to ensure compliance with rules, create obligations, and impose penalties for non-compliance.

Treasure: Treasure refers to a government's financial resources, which can be used to influence policy outcomes. This resource encompasses various financial allocations, including grants, loans, taxes, and expenditures. Governments can use their treasure to incentivize or penalize specific actions, support initiatives, or finance programs that align with policy objectives.

Organization: Organization pertains to a government's capacity to design, develop, and manage structures, programs, and initiatives that contribute to policy outcomes. This resource includes the bureaucratic apparatus, personnel, and institutional arrangements that facilitate the implementation of policy instruments. Organizations enable governments to execute strategies, coordinate with stakeholders, and monitor progress toward policy objectives.

To thoroughly analyze and categorize the diverse policy instruments employed by the U.S. and EU in addressing disinformation, it is also crucial to understand the distinction between Effectors and Detectors and the resources they employ within Hood's (1983) taxonomy. Prior research has demonstrated the utility of Hood's taxonomy in examining policy instruments across various contexts (Howlett 2000; Salamon 2002).

Effectors are policy instruments designed to facilitate change in a policy environment. These instruments can be categorized based on the resource they employ. For instance, nodality-based effectors leverage a government's central position in social and political networks, using information and knowledge to provide advice, issue guidelines, and offer training programs to address disinformation (Howlett 2000). Authority-based effectors capitalize on the government's power to enforce rules and regulations, which can include licenses, user charges, and certification processes that govern the dissemination of information and establish standards for online platforms (Peters 2000). Treasure-based effectors utilize a government's financial resources to influence the policy environment through grants, loans, taxes, and expenditures that support initiatives countering disinformation or promoting digital literacy (Bemelmans-Videc et al. 2017). Lastly, organization-based effectors depend on a government's organizational capacity to develop and manage programs, such as administrative measures, public enterprises, and collaborations with private sector entities to combat disinformation (Salamon 2002).

In contrast, Detectors are policy instruments designed to monitor and identify changes in a policy environment, and they can also be divided based on the resource they use. Nodality-based detectors gather information and knowledge through reporting mechanisms and registration systems, monitoring social media platforms, and tracking the spread of disinformation. Authority-based detectors exercise government power to collect data through legal means, such as census taking and consultations with experts or

stakeholders in disinformation (Peters 2000). Treasure-based detectors employ financial resources to conduct polling, policing, or other monitoring activities that help assess disinformation's impact and countermeasures' effectiveness (Bemelmans-Videc et al. 2017). Finally, organization-based detectors rely on a government's organizational capabilities to maintain records and conduct surveys to evaluate the prevalence and consequences of disinformation and the success of implemented policies (Howlett 2000).

Hood's (1983) taxonomy thus provides a coherent and comprehensive framework for examining the diverse policy instruments used by the U.S. and EU to address disinformation. This approach facilitates a more nuanced understanding of the various strategies and resources to tackle this complex issue within their democratic systems. Examples of detectors and effectors can be seen in table 4.1 below.

	Government Resources			
Principle Use:	**Nodality**	**Authority**	**Treasure**	**Organization**
Detectors (Detect Change)	Surveys Public consultation Registration Reporting	Registers Inspection Interrogation	Rewards Focus Groups Public Poll	Surveillance Investigation Security Check
Effectors (Effect Change)	Communication Advisory Searchable Database Training	Regulation Certification Ban Law	Contracts Gift Payments Grants Taxes	Custody Quarantine Detention Law Enforcement

Source: Hood (1983), p. 9-10

Table 4.2 Examples of Government Policy Tools

4.4 Advantages and Disadvantages of Methods

The CCS approach adopted in this research offers several advantages, such as providing a rich context for analyzing policy formation and implementation within diverse and complex democratic systems, as well as offering valuable insights into the effectiveness and limitations of different approaches to addressing disinformation (Bartlett and Vavrus 2016; Maxwell 2013). The selection of the United States and the European Union as the primary cases is well-founded, given their global significance, vulnerability to disinformation campaigns, and the researcher's familiarity with their inner workings

through an internship (Dahl 1998; Fletcher et al. 2018; Hix 2005; Moravcsik 2006; Pollicino and Bietti 2019).

However, this methodology also has its limitations. Focusing only on the two cases of the U.S. and EU may limit the generalizability of the findings, as they may not be directly applicable to other nations or regions with different political and administrative systems (Seawright and Gerring 2008). Additionally, CCS is sensitive to context, and the unique characteristics of the selected cases may influence the research findings, limiting their applicability to other contexts (Ragin 2014).

The data collection methods employed in this research, namely the analysis of official documents, websites, and publications, as well as semi-structured expert interviews, offer various advantages. Official documents are considered rich and reliable data sources, while semi-structured interviews provide deeper insights and overviews of the issues under study (Bolderston 2012; Danto 2008). The systematic search strategy for locating and analyzing relevant documents, websites, and publications ensures the comprehensiveness and relevance of the collected data.

These data collection methods also come with limitations. For instance, the search strategy may miss important documents if the selected keywords or search terms do not cover only some relevant aspects of disinformation policy. Moreover, the reliability and validity of interview data can be influenced by various factors, such as question order and quality, interview setting, interviewer preparedness, and the interviewee's emotional and psychological conditions (Bolderston 2012).

The data analysis process, which involves qualitative data analysis and coding, offers several advantages. For example, qualitative data analysis allows for a deeper understanding of complex issues and provides valuable insights into policy tools and their implementation (Allan 2020). The deductive approach to coding ensures alignment with the research questions and objectives (Azungah 2018). Additionally, using NVivo 11, a qualitative data analysis software tool, enhances the quality of the research and allows for more efficient coding (Wong 2008).

Nevertheless, there are limitations to this data analysis approach. The qualitative nature of the research may make it more subjective and open to interpretation, affecting the findings' reliability and validity (Golafshani 2003). Additionally, the deductive approach to coding, which relies on pre-determined codes, may limit the exploration of unanticipated themes or issues that could emerge from the data (Fereday and Muir-Cochrane 2006). Future research could explore additional cases or adopt a mixed-

methods approach to address these limitations to provide a more comprehensive understanding of disinformation policy.

5 Case Findings: Analysis of Disinformation Policy Responses

In this hyperconnectivity and information overload era, disinformation has emerged as a critical challenge to democratic societies worldwide. As such, it is critical to understand how governments respond to disinformation through different policy actions to ensure continued democratic resilience. In this context, this research presents a comprehensive analysis of the policy tools employed by the U.S. and the EU in their fight against disinformation.

This analysis is grounded in Hood's (1983) innovative framework of viewing government as a 'toolkit' comprising four key resources – Nodality, Authority, Treasure, and Organization – which can be deployed to detect and effect changes in the policy environment. Each of these resources represents different facets of governmental power and influence, contributing uniquely to countering disinformation.

- Nodality refers to the government's role as a hub of information and networks.
- Authority represents the legal and moral weight that governments carry.
- Treasure encapsulates the financial resources at the government's disposal.
- Organization denotes the structural capacity and bureaucratic machinery that enable policy implementation.

The 'government-as-a-toolkit' framework provides a useful lens through which to examine and compare the nuanced strategies deployed by the U.S. and EU in their battle against disinformation.

Subsequent sections will explore these resources and their principal use as employed by the U.S. and the EU. Furthermore, it will analyze how each policy tool, in its unique capacity as either a detector or effector, contributes to the core functions of democracy as outlined by Warren (2017): empowered inclusion, which relates to the right and ability of citizens to participate in public affairs; collective agenda and will formation, which is the process of creating a shared sense of priorities and collective intention; and collective decision making, the procedure by which a group decides on a course of action.

This meticulous analysis offers a comprehensive picture of the contemporary policy landscape. It will provide clarity and nuanced understanding of the various strategies and policy tools deployed and illuminate the potential impacts and implications of these strategies. The objective is to unravel the complexities of the responses to disinformation,

illustrating the inherent challenges and opportunities and contributing to a more informed and robust dialogue on this critical issue in our contemporary world.

5.1 Analysis of U.S. Policy Tools

TITLE	Date	Source	Resource	Use
About us - global engagement center	03/2016	U.S. Department of State Website	Organization	Effector
Executive order 13721- developing an integrated global engagement center	03/2016	U.S. National Register Website	Authority	Effector
S.3274 - countering foreign propaganda and disinformation act	07/2016	U.S. Congress Website	Authority	Effector
National defense authorization act for fiscal year 2017	12/2016	U.S. Congress Website	Authority; Treasure	Effector
H.R.3364 - countering America's adversaries through sanctions act	08/2017	U.S. Congress Website	Authority	Effector
John S. McCain national defense authorization act for fiscal year 2019	08/2018	U.S. Congress Website	Authority; Treasure	Effector
Serial no. 116-55 (house hearing) - Russian disinformation attacks on elections: lessons from Europe	07/2019	U.S. Congress Website	Nodality	Effector
Cyberspace solarium commission: march 2020 csc report	03/2020	Cyberspace Solarium Commission	Organization	Effector
S.4499 - covid–19 misinformation and disinformation task force act of 2020	08/2020	U.S. Congress Website	Organization	Effector
Serial no. 117-19 (house hearing) - disinformation nation: social media's role in promoting extremism and misinformation	03/2021	U.S. Congress Website	Nodality	Effector
Treasury escalates sanctions against the Russian government's attempts to influence U.S. elections	04/2021	U.S. Department of the Treasury Website	Authority	Effector
The U.S. surgeon general's advisory on building a healthy information environment	07/2021	HHS.gov Website	Nodality	Effector
Cyberspace solarium commission white paper #6: countering disinformation in the United States	12/2021	Cyberspace Solarium Commission	Organization	Effector
S.3608 - social media nudge act	02/2022	U.S. Congress Website	Authority	Effector
CISA strategic plan 2023 - 2025	09/2022	CISA Website	Organization	Detector; Effector
PSA: foreign actors likely to use information manipulation tactics for 2022	10/2022	CISA Website	Nodality	Effector

midterm elections				
S.394 - digital citizenship and media literacy act	02/2023	U.S. Congress Website	Authority; Treasure	Effector
S.406 - promoting public health information act	02/2023	U.S. Congress Website	Authority; Treasure	Effector
S.1231 - sad act	04/2023	U.S. Congress Website	Authority	Effector
H.R.2599 - honest ads act	04/2023	U.S. Congress Website	Authority	Effector

Table 5.1 U.S. Policy Tools Overview

This study involved a meticulous collection and systematic analysis of data obtained from 20 documents. These documents were primarily derived from U.S. Federal Government websites and other government agency platforms. These agencies included, but were not limited to, the U.S. Department of State, U.S. National Register, U.S. Congress, U.S. Department of Treasury, U.S. Department of Health and Human Services, Cyberspace Solarium Commission (CSC), and the Cybersecurity and Infrastructure Security Agency (CISA).

The selection of the said documents was executed by employing a strategic keyword search methodology. Keywords such as “disinformation”, “misinformation”, and “false information” were used in this search process. The timeframe encompassed by the published dates of these selected documents extended from March 2016 to April 2023. A condensed overview of the identified policy tools has been conveniently provided in Table 5.1.

The content of these sourced documents was thoroughly coded using NVivo, a qualitative data analysis software. The coding was primarily based on three distinctive dimensions:

1. The main resource harnessed by the government, classified under Nodality, Authority, Treasure, and/or Organization;

2. The intended utilization of the resource, determined as either detector or effector;

3. Specific actions focused on the three core democratic functions: empowered inclusion, collective agenda and will formation, and/or collective decision-making.

The findings derived from this comprehensive content analysis have been exhaustively presented and discussed in the subsequent sections of this thesis.

5.1.1 Tools of Nodality

In the context of this analysis, the utilization of the government's resource of nodality was prominent in four policy tools, as evidenced by 37 distinct code references. These policy tools span a variety of topics, with particular emphasis on disinformation and misinformation within the sphere of elections and social media. The referenced documents are as follows:

1. *Serial No. 116-55 (House Hearing) - Russian Disinformation Attacks on Elections: Lessons from Europe*
2. *Serial No. 117-19 (House Hearing) - Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation*
3. *The U.S. Surgeon General's Advisory on Building a Healthy Information Environment*
4. *PSA: Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections*

Following this, the succeeding section will delve into a detailed analysis of these policy tools, drawing upon specific excerpts from the documents to better understand their context and implications.

The content analysis did not reveal any detector policy tools typically employed to gather information or intelligence. Instead, the four policy tools under scrutiny leverage the government's resource of Nodality as an effector policy tool. The subsequent sections delve deeper into each document, shedding light on how the government strategically uses Nodality to tackle the pressing issue of disinformation.

Serial No. 116-55 (House Hearing) - Russian Disinformation Attacks on Elections: Lessons from Europe

Through this hearing, the U.S. government uses the resource of nodality to identify and expose the tactics of Russian disinformation campaigns targeting elections. The references focus on understanding the nature of the threat, learning from the European Union's experiences and counterstrategies, and discussing potential collaborative efforts (U.S. Government Publishing Office 2019). The committee points out that *"The United States lags behind the EU, both in conceptual framing of the issue and systemic actions to deal with it,"* attributing the policy challenge to uneven leadership and an approach

"hampered by what could be called partisan reactions to the problem" (U.S. Government Publishing Office 2019, p. 12).

The hearing serves as a platform and group-targeted message to other members of congress to promote awareness and strategic preparedness against foreign information manipulation tactics, underlining the government's nodal role in providing credible information and shaping policy discourse. It calls on the U.S. Federal Government and supporting agencies to "*get organized to contend with Russian and other disinformation"* by leveraging the expertise and mandates proposed by *"U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the State Department (especially the Global Engagement Center)"* (U.S. Government Publishing Office 2019).

Serial No. 117-19 (House Hearing) - Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation

In this hearing, the U.S. government explores the role of social media platforms in promoting misinformation and extremism. The references highlight the need for greater transparency from tech companies and a robust oversight mechanism (House of Representatives 2021). The committee emphasizes the role of tech companies and the need for their active involvement in combating misinformation, encouraging self-regulation in the technology sector and fostering a culture of information responsibility. House lawmakers directly address the chief executives of Google, Facebook, and Twitter, *"You can take this content down […], but you choose not to,"* accusing them of *"picking engagement and profit over the health and safety of [their] users, our Nation, and our democracy"* (House of Representatives 2021, p. 7-8). The House calls for regulation that *"should not attempt to limit constitutionally protected freedom of speech";* rather, the aim is to *"hold platforms accountable when they are used to incite violence and […] spread misinformation"* (House of Representatives 2021, p. 13).

The U.S. Surgeon General's Advisory on Building a Healthy Information Environment

In this advisory, the U.S. Surgeon General's office uses Nodality to call for a societal effort in combating health misinformation, particularly in light of the COVID-19 pandemic (Office of the U.S. Surgeon General 2021). The advisory, directed at the general American public, outlines the actions of various stakeholders, from individuals to educators and health professionals, declaring that *"addressing health misinformation will require a whole-of-society effort"* (Office of the U.S. Surgeon General 2021). It calls on American society, emphasizing the importance of improving media literacy, proactive engagement with the public by health professionals, and the need for tech platforms to

slow the spread of misinformation. The advisory illustrates the government's role as a nodal point for information, broadcasting strategies to a wide audience that encourage resilience against health misinformation.

PSA: Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections

This public service announcement warns about foreign information manipulation in the U.S. 2022 mid-term elections (Cybersecurity and Infrastructure Security Agency 2022). The announcement is an example of the government using Nodality to raise awareness about the threat of foreign interference, advocating for vigilance and informed skepticism among the public, warning that *"foreign actors can use a number of methods to […] spread false claims and narratives about malicious cyber activity, voting processes, and results surrounding the midterm election cycle"* (Cybersecurity and Infrastructure Security Agency 2022, p. 1). It also promotes reliance on trustworthy sources for election information, encouraging the public to *"make use of in-platform tools offered by social media for reporting elections related disinformation"* (p. 2), further emphasizing the government's nodal role in promoting accurate information dissemination.

5.1.2 Tools of Authority

This section analyzes ten policy tools implemented in the U.S., all characterized as effectors of authority. In addition, three of these tools share characteristics of treasure, indicating the involvement of resources or finances.

The policy tools range from executive orders, such as Executive Order No. 13721 (2016) titled "Developing an Integrated Global Engagement Center," issued in March 2016, to legislative acts passed by the U.S. Congress. These include the Countering Foreign Propaganda and Disinformation Act (2016), and National Defense Authorization Act for Fiscal Year 2017 (2016), both of which also involve the government's budgetary allocations for disinformation-related activities.

Four bills were also introduced in U.S. Congress between 2022 and 2023, including S.3608 (2022) – "Social Media NUDGE Act", Digital Citizenship and Media Literacy Act (2023), Promoting Public Health Information Act (2023) and SAD Act (2023). Lastly, the Honest Ads Act (2023) was introduced in April 2023. All these legislative acts function as authority effectors, primarily involving regulation and law. The following sections will present these tools of authority in chronological order, distinguishing between legally-binding laws and proposed bills that have yet to become laws.

Federal Laws

Executive Order No. 13721 – Developing an Integrated Global Engagement Center

In March 2016, President Barack Obama signed Executive Order No. 13721 into law, ordering the establishment of the Global Engagement Center (GEC), which *"shall lead the coordination, integration, and synchronization of Government-wide communications activities […] to counter the messaging and diminish the influence of international terrorist organizations"* (Executive Order No. 13721 2016, p. 14685). While the initial responsibilities assigned to the center were largely focused on coordinating counter-terrorism activities, this executive order serves as the precedent for later legislation; namely, the National Defense Authorization Act for Fiscal Year 2017 discussed below, that would add further responsibilities directed at foreign state and non-state propaganda and disinformation operations.

S.2943 – National Defense Authorization Act for Fiscal Year 2017

The National Defense Authorization Act for Fiscal Year 2017 was introduced in May 2016 and became law in December of the same year, with its main purpose being to *"authorize appropriations for fiscal year 2017 military activities"* (National Defense Authorization Act for Fiscal Year 2017 2016, p. 2000). This law also extended the original responsibilities of the Global Engagement Center identified above in Executive Order No. 13721 (2016) to *"lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts"* (p. 2546). These additional responsibilities reflect the current mission of the Global Engagement Center today.

H.R.3364 – Countering America's Adversaries Through Sanctions Act

The Countering America's Adversaries Through Sanctions Act (2017) was first introduced by the House of Representatives in July 2017 and became law the following month. This act highlighted findings made by Congress surrounding the Russian Federation's efforts to *"routinely traffic in anti-Western disinformation, while few independent, fact-based media sources provide objective reporting for Russian-speaking audiences"* (Countering America's Adversaries Through Sanctions Act 2017, p. 925). To counter this, Section 255 requests that the U.S. president *"submit to the appropriate congressional committees a report that includes a description of media organizations that are controlled and funded by the Government of the Russian Federation"* (p. 930). In addition to countering Russian interference in cyber security, human rights abuses, and corruption, the law also called for sanctions against Iran's destabilization activities and North Korean goods produced employing North Korean convicts or forced laborers.

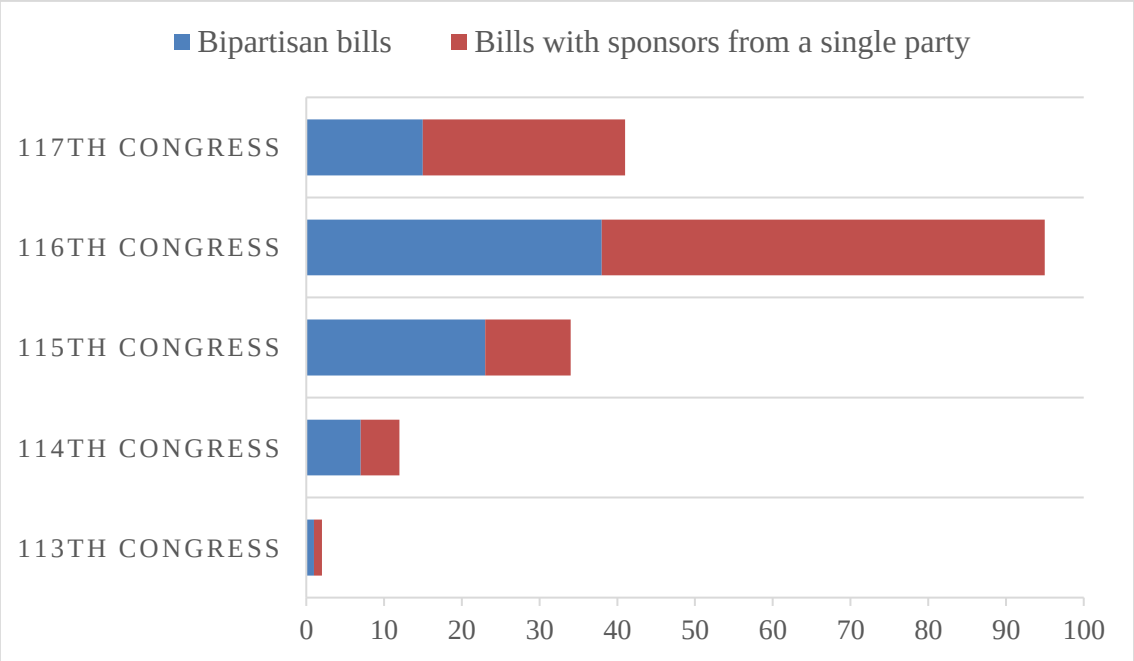
H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019

The law John S. McCain National Defense Authorization Act for Fiscal Year 2019 (2018) pertains to the further refinement of the Global Engagement Center's responsibilities and mission. As per the reference, the law amends the purpose of the Center to *"lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States"* (John S. McCain National Defense Authorization Act for Fiscal Year 2019 2018, p. 2076). It also specifies that the Center should track and evaluate counterfactual narratives abroad that threaten the US and its allies, identify current and emerging trends in foreign propaganda and disinformation, and support the promotion of credible, fact-based narratives and policies to audiences outside the US. The reference further discusses measuring and evaluating the Center's activities and using information from appropriate interagency entities to identify susceptible and likely impacted populations.

Proposed Legislature

According to the sixth white paper by the CSC titled "Countering Disinformation in the United States," the 117th Congress saw the introduction of over 40 bills specifically mentioning "misinformation" or "disinformation" (Cyberspace Solarium Commission 2021). Additional bills discussed related themes, including foreign influence, civic education, and media and social media regulation, though these did not explicitly mention disinformation. The number and range of proposed bills indicate Congress's increased commitment to addressing disinformation. These legislative efforts aim to tackle disinformation and foreign interference with various strategies. Yet, partisan politics is prevalent, with about two-thirds of these relevant bills not having bipartisan co-sponsorship.

Since the 2016 elections, when Russian meddling raised public concern, the Congressional focus on disinformation has amplified. In the 113th Congress (2013-14), only two bills mentioned "misinformation," and none mentioned "disinformation." Interest in the subject grew, and during the 116th Congress (2019-21), nearly 100 bills referenced "misinformation" or "disinformation." This session marked a significant change as less than half of the related bills had bipartisan support. These results are summarized in the table adapted from the CSC below. This section will explore several of the key proposed legislatures, with some acts from as recent as April 2023.



c.f. Cyberspace Solarium Commission (2021), p. 16

Figure 5.1 Bills Introduced That Mention "Disinformation" or "Misinformation"

S.3274 – Countering Foreign Propaganda and Disinformation Act

The Countering Foreign Propaganda and Disinformation Act bill comprises several references that discuss establishing a Center for Information Analysis and Response to counter foreign disinformation and propaganda. It calls for the Center *to "coordinate the sharing among government agencies of information on foreign government information warfare efforts"* as well as to *"establish a process for integrating information on foreign propaganda and disinformation efforts into national strategy"* (Countering Foreign Propaganda and Disinformation Act 2016, p. 2). According to the bill, the Center is to be established not later than 180 days after the enactment of the Act.

This bill was introduced in the U.S. senate in July 2016 in the 114th Congress. It was read twice before being referred by the Senate to the Committee on Foreign Relations. While the bill was not enacted, its legislative text was re-introduced and included in the National Defense Authorization Act for Fiscal Year 2017, discussed above, which later became law in December 2017.

S.3608 – Social Media NUDGE Act

The Social Media NUDGE Act, proposed in the Senate in February 2022, references the need for the Federal Trade Commission to identify content-agnostic platform interventions to reduce the harm of algorithmic amplification and social media addiction

on covered platforms (Social Media NUDGE Act 2022). The bill points out that *"viral harmful content often spreads on social media platforms"*, claiming this is because *"Social media platforms do not consistently enforce their terms of service and content policies, leading to supposedly prohibited content often being shown to users and amplified by such platforms"* (p. 2).

The bill also calls for a study to be conducted and led by the Director of the National Science Foundation, in agreement with the National Academies of Sciences, Engineering, and Medicine, to identify content-agnostic interventions *"that covered platforms could implement to reduce the harms of algorithmic amplification […] on covered platforms"* (p. 4). The bill claims that significant research previously found that these interventions, which include nudges to users, increased platform viewing options, labels and alerts requiring users to review content before sharing, prompts to help users identify manipulative advertisements and other research-supported content-agnostic interventions, may help mitigate these issues. The Act also mandates that within 60 days of receiving notice from the Commission, the covered platform must submit a plan to implement each content-agnostic intervention and provide evidence if it chooses not to implement a given intervention mechanism.

S.394 - Digital Citizenship and Media Literacy Act

The Digital Citizenship and Media Literacy Act, introduced in February 2023, comprises several references discussing the promotion of digital citizenship and media literacy (Digital Citizenship and Media Literacy Act 2023). The Act emphasizes the importance of media literacy education in building national resilience to foreign disinformation campaigns, citing the success of such programs in countries like Estonia, Finland, and Ukraine (Digital Citizenship and Media Literacy Act 2023). The Act also acknowledges the role of media literacy and digital citizenship as a means that *"empowers young people and is critical to improving their health and safety, preventing cyberbullying, and enabling young people to make informed decisions about products and services, including advertisements and controlled substances"* (p. 4).

The Act provides definitions for the concepts of "digital citizenship" and "media literacy", which encompass a wide range of skills and abilities, including the responsible and ethical use of communication technologies, critical analysis of media content, and protection from online content that presents a clear risk to health and safety. Furthermore, it calls on the Assistant Secretary to promote these two concepts by establishing a program to award grants to entities with a plan for organizing activities supporting enhanced digital citizenship and media literacy.

S.406 – Promoting Public Health Information Act

Also proposed in February 2023, the Promoting Public Health Information Act calls for establishing the Public Health Information and Communications Advisory Committee (Promoting Public Health Information Act 2023). This committee makes recommendations and reports to provide *"strategies to improve communication and dissemination of scientific and evidence-based public health information to the public, and, as appropriate, to address misinformation during public health emergencies"* (p. 3). This covers aspects like the role and impact of misinformation on the response to such public health emergencies and the role of risk communication before and during these emergencies.

Additionally, the Committee is to ensure that official scientific and public health guidance is accessible and effectively communicated to the public, particularly focusing on underserved populations or low health literacy. Activities should be tailored towards subgroups targeted for health misinformation and disinformation, or those particularly susceptible to health misinformation and disinformation, in a culturally- and linguistically-appropriate manner.

S.1231 - SAD Act

Short for the Stop Antiabortion Disinformation, the "SAD Act" proposed in April 2023 calls for the prohibition of disinformation in the advertising of abortion services (SAD Act 2023). The act reiterates that abortion services are an essential component of reproductive health care, noting that the Supreme Court's overruling of Roe v. Wade in the case of Dobbs v. Jackson Women's Health Organization has resulted in immediate and disastrous effects, including the unavailability of abortion in 14 states as of January 2023. This has increased the burdens associated with accessing an abortion facility, including time off from work or school, lost wages, transportation, lodging, child care, and other ancillary costs.

The Act states that *"the freedom to decide whether and when to have a child is key to the ability of an individual to participate fully in our democracy"* (p. 3). It also criticizes crisis pregnancy centers (CPCs), which are anti-abortion organizations that present themselves as comprehensive reproductive health care providers to discourage people from having abortions. CPCs reportedly use deceptive tactics, including making false claims about reproductive health care and providers and disseminating inaccurate and misleading information on the risks of abortion and contraception.

The Act expressly prohibits *"deceptive advertising about the reproductive health services offered by the person"*, including advertising that intends to deceive by falsely stating that a person *"offers or provides contraception or abortion services […] or employs or offers access to licensed medical personnel"* (p. 5). Violations of this section or a regulation promulgated under this section are punishable by a civil penalty that should not exceed the greater of $100,000 or 50 percent of the revenues earned by the ultimate parent entity of a person during the preceding 12-month period.

H.R.2599 - Honest Ads Act

Another act proposed in April 2023 is the Honest Ads Act, which emphasizes enhancing transparency and accountability for online political advertisements (Honest Ads Act 2023). This act aims to protect the integrity of American democracy and national security by improving disclosure requirements for online political advertisements to align with the Supreme Court's standard that the electorate has the right to be fully informed.

The Act emphasizes that it is crucial to extend to online internet platforms the same political advertisement disclosure requirements applicable to broadcast television and radio stations and cable and satellite television providers. Effective transparency for voters must include information about the true and original source of money spent on online political advertisements. The Act also requires the disclosure of information *"to inform the voting public of who is behind digital advertising disseminated to influence their votes and to enable the Federal Election Commission and the Department of Justice to detect and prosecute illegal foreign spending on local, State, and Federal elections and other campaign finance violations"* (p. 3).

It also points out the difference between paid advertising on large online platforms and other common media due to factors such as the low cost of reaching large numbers of people, the availability of advanced microtargeting, and the ease with which online advertisers can evade disclosure requirements. It mentions that the public nature of broadcast television, radio, and satellite ensures publicity for any political advertisement. However, social media platforms can target portions of the electorate with direct, temporary advertisements, often employing private information the platform collects on individuals.

The act proposes expanding the definition of public communication in the "Federal Election Campaign Act of 1971" to include paid internet and digital communication. This category also includes any news story, commentary, or editorial disseminated utilizing any broadcasting station, print, online, or digital newspaper, magazine, publication,

periodical, blog, or platform, unless owned or controlled by any political party, political committee, or candidate.

5.1.3 Tools of Treasure

This section presents an analysis of the content of four legislative documents characterized as possessing tools of treasure, namely, the National Defense Authorization Act for Fiscal Year 2017, the John S. McCain National Defense Authorization Act for Fiscal Year 2019, S.394 - Digital Citizenship and Media Literacy Act, and S.406 - Promoting Public Health Information Act. While also functioning as tools of authority, these acts demonstrate the use of financial resources or allocations aimed at countering disinformation activities.

S.2943 – National Defense Authorization Act for Fiscal Year 2017

The National Defense Authorization Act for Fiscal Year 2017, as detailed in the previous section on tools of authority, calls for establishing the Global Engagement Center (National Defense Authorization Act for Fiscal Year 2017 2016). In addition to outlining the center's responsibilities and key tasks, the act also details the financial provisions for the Center for both the fiscal year 2017 and the fiscal year 2018. The Act authorizes the transfer of funds from the Department of Defense (DoD) to the Department of State, should the appropriations for the GEC be according to the following requirements:

1. For the fiscal year 2017: If the funds authorized for the operations of the GEC are less than $80,000,000, *"the Secretary of Defense is authorized to transfer, from amounts authorized to be appropriated by this Act for the Department of Defense for fiscal year 2017, to the Secretary of State an amount, not to exceed $60,000,000, to be available to carry out the functions of the Center"* (National Defense Authorization Act for Fiscal Year 2017 2016, p. 2547).

2. For the fiscal year 2018: A similar provision is made, where if the funds authorized for the GEC are less than $80,000,000, the Secretary of Defense can transfer up to $60,000,000 from the DoD's budget for the fiscal year 2018 to the Secretary of State for the GEC's functions.

These provisions aim to ensure that the GEC has sufficient funding to carry out its functions, particularly in recognition, understanding, exposing, and countering foreign propaganda and disinformation.

H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019

The John S. McCain National Defense Authorization Act for Fiscal Year 2019, enacted in August 2018, further highlights using financial resources to counter disinformation. The act allocated funding for the continuation and expansion of projects started under the 2017 National Defense Authorization Act. It stipulates that for fiscal years 2019 and 2020, The Secretary of Defense is authorized to transfer *"not more than $60,000,000, to carry out the functions of the Center"* from the Department of Defense's appropriated budget to the Secretary of State (John S. McCain National Defense Authorization Act for Fiscal Year 2019 2018, p. 2077). This transfer ensures the GEC has the necessary funds to perform its functions.

This act also authorizes the GEC to extend financial support through grants or contracts to various entities. These include civil society groups, media content providers, non-governmental organizations, federally funded research and development centers, private companies, and academic institutions. This funding is intended to *"support local entities and linkages among such entities, including independent media entities, that are best positioned to refute foreign propaganda and disinformation in affected communities"* (p. 2077). Furthermore, these grants aim to facilitate collecting and storing *"examples of print, online, and social media disinformation and propaganda directed at the United States or United States allies and partner nations"* (p. 2077). This could serve as an archive or database to better understand and address the strategies of foreign disinformation.

Another key aspect of the grants is to promote the analysis and reporting on *"tactics, techniques, and procedures of foreign information warfare and other efforts with respect to disinformation and propaganda"* and *"to support efforts by the Center to counter efforts by foreign entities to use disinformation and propaganda to undermine or influence the policies, security, and social and political stability of the United States and United States allies and partner nations"* (p. 2077). This indicates the intention to enhance the Center's ability to mitigate the impact of disinformation on national security and stability.

S.394 - Digital Citizenship and Media Literacy Act

The S.394 - Digital Citizenship and Media Literacy Act, introduced in February 2023, serves as another tool of treasure, as it involves the allocation of funding to promote media literacy (Digital Citizenship and Media Literacy Act 2023). It calls on the Assistant Secretary of State to establish a program to promote media literacy, through which the Assistant Secretary shall award grants to eligible entities to enable them to engage in media literacy-related activities. These activities are described in detail in Section 4 subsection (c) *"Use of Funds"*, which identities four types of entities that are eligible to

receive funding, namely, State educational agencies, local educational agencies, public libraries, and qualified nonprofit organizations (Digital Citizenship and Media Literacy Act 2023, p. 9-16). The following regulations outline the scope of grant funds that can be administered:

1. **State educational agencies** are eligible to receive a grant for establishing a media literacy advisory council to *"provide recommendations about digital citizenship and media literacy guidelines"*, which includes conducting research and collecting data to assess the media literacy capabilities of students and teachers, as well as providing reporting (p. 9-10).

2. **Local educational agencies** may receive funding for *"incorporating digital citizenship and media literacy into the existing curriculum or establishing new educational opportunities to learn about media literacy"* (p. 14). They may also receive funding for *"employing specialized instructional support personnel"* and *"other activities, including student led efforts, to support, develop, or promote the implementation of media literacy education programs, policies, teacher preparation, curriculum, or standards"* (p. 14).

3. **Public libraries** can receive grants *"to carry out activities that enhance digital citizenship and media literacy skills in children"* (p. 15).

4. **Qualified nonprofit organizations** are qualified to receive grants for media literacy activities for children in kindergarten through grade 12, as well as *"other activities to support, develop, or promote the implementation of media literacy education programs, policies, teacher preparation, curriculum, or standards relating to enhancing digital citizenship and media literacy skills for children"* (p. 15).

S.406 – Promoting Public Health Information Act

Finally, the S.406 - Promoting Public Health Information Act, also introduced in February 2023, serves as a tool of treasure that involves allocating funding to promote accurate health information and combating health misinformation and disinformation. The act proposes to authorize *"$45,000,000 for each of fiscal years 2023 through 2027"* for educational initiatives aimed at promoting *"fact-based public health and medical science information to the public and educate the public on how to identify misinformation, disinformation, and credible information"* (Promoting Public Health Information Act 2023, p. 5).

5.1.4 Tools of Organization

To address the increasing threat landscape of disinformation, the U.S. has implemented tools of organization that allocate and operationalize governmental resources, personnel, and public and private sector experts through establishing inter-governmental agencies and taskforces. Four of these organizations, identified by analyzing the content of key documents, stand out: the GEC (previously introduced in the "Tools of Authority" section), the CSC, the Misinformation and Disinformation Task Force, and the Cybersecurity and Infrastructure Security Agency. The following section will present the findings of key documents relating to establishing the organizations mentioned above.

Global Engagement Center (GEC)

The GEC is a key apparatus within the U.S. Department of State tasked with coordinating and leading efforts to identify and counteract foreign propaganda and disinformation attempts, both from state and non-state actors, aimed at *"undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations"* (U.S. Department of State n.d.). Rooted in a vision of being a data-driven body, GEC is committed to preemptively addressing the attempts of foreign adversaries to compromise U.S. interests through disinformation and propaganda.

The establishment of the Global Engagement Center can be traced back to 2011 and Executive Order 13584, which initially established the Department of State the Center for Strategic Counterterrorism Communications (CSCC) for *"supporting agencies in Government-wide public communications activities targeted against violent extremism and terrorist organizations"* (The White House 2011). However, the evolution of the GEC came about through Executive Order 13721 in 2016, which transformed the CSCC into the GEC, keeping its counterterrorism mission unchanged.

A pivotal development in GEC's mission occurred with enacting the National Defense Authorization Act for Fiscal Year 2017, which expanded its scope of duties to include addressing other foreign state and non-state propaganda and disinformation activities. The John S. McCain National Defense Authorization Act for Fiscal Year 2019 further refined this mission, providing it with a mandate reflected in the present mission statement of GEC. This expansion and refinement of GEC's mandate demonstrates the evolving nature of its role and responsibilities in countering disinformation and propaganda.

The operational architecture of GEC is designed around five distinct yet interconnected lines of effort: Analytics and Research, International Partnerships, Programs and Campaigns, Exposure, and Technology Assessment and Engagement.

1. Under **Analytics and Research**, GEC's analysts and data scientists gather and scrutinize data from foreign state and non-state actors. They aim to produce an analysis of these entities' malicious information influence narratives, tactics, and techniques. Notably, GEC's analyses are shared internally and with U.S. embassies, interagency groups, and international partners.

2. The **International Partnerships** aspect of GEC's operations highlights the importance of collective global action against disinformation. The GEC actively nurtures coalitions and collaborations with other national governments, enhancing the coordination of counter-disinformation analyses and actions.

3. **Programs and Campaigns** are a unique component of GEC's operations where dedicated teams focus on specific regions or nations—Russia, the People's Republic of China, Iran, and Counterterrorism being the key focuses. These teams work towards building societal and institutional resilience to foreign propaganda and disinformation efforts abroad. These initiatives are tailored to the specific challenges encountered in various overseas information environments and involve coordination within the Department and with interagency and international partners.

4. The **Exposure** line of effort exemplifies GEC's commitment to transparency and public awareness, with the Center's participation in the public disclosure of foreign information influence operations, including the use of proxy sites and social media networks overseas.

5. Lastly, under **Technology Assessment and Engagement**, GEC engages with the private sector to host technology demonstrations, assess counter-disinformation technologies against specific challenges, and scout for technological solutions via technology challenge programs.

CSC

The CSC is a pivotal body established in 2019 under the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (John S. McCain National Defense Authorization Act for Fiscal Year 2019 2018). Its primary objective is to *"develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences"* (p. 2141). This strategic mandate focuses on

establishing a collective understanding of the defensive strategies required to safeguard U.S. interests in the cyber domain, particularly against significant cyber threats and attacks.

On March 11, 2020, the CSC published a report offering detailed insights, analysis, and recommendations on cyber defense strategy (Cyberspace Solarium Commission 2020). This public report provided over 80 recommendations for action in the public and private sectors, highlighting key areas including deterrence in cyberspace, importance of a resilient economy, government reform and public-private partnership, and stated that *"election security must become a priority"* (p. vi).

Following the presentation of the report, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 reauthorized the Commission with extended responsibilities (William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 2021). These include collecting and assessing feedback on the analysis and recommendations contained within the final report, an indication of the commission's openness to ongoing input and refinement of its strategic approach. The reauthorization also mandates the CSC to review the implementation of the recommendations contained within the final report. It involves an ongoing supervisory role for the commission in ensuring the effective application of its recommendations, thus facilitating a responsive and adaptive approach to the evolving landscape of cyber threats.

Additionally, the "Countering Disinformation in the United States" white paper published by the CSC in December 2021 focused on cyber-enabled disinformation, aiming to outline steps the United States could take to strengthen resilience against such disinformation, specifically when originating from foreign actors (Cyberspace Solarium Commission 2021). The white paper is a culmination of careful research and deliberation by the CSC staff and commissioners, identifying seven key recommendations, each of which is designed to decrease the prevalence of disinformation in the information ecosystem and build upon both individual and societal resilience to disinformation and malign foreign influence:

- ***Recommendation 1****: Congress should establish a Civics Education Task Force, enable greater access to civics education resources, and raise public awareness about foreign disinformation.*

- ***Recommendation 2****: Congress should ensure material support to non-governmental disinformation researchers*

- ***Recommendation 3****: Congress should fund the Department of Justice to provide grants to nonprofit centers seeking to identify, expose, and explain malign foreign influence campaigns to the American public*

- ***Recommendation 4****: Congress should create a capability within DHS to actively monitor foreign disinformation*

- ***Recommendation 5****: Congress should create a grants program at the Department of Homeland Security designed to equip SLTT governments with the personnel and resources necessary to identify foreign disinformation campaigns and incorporate countermeasures into public communications strategies*

- ***Recommendation 6****: Congress should reform the Foreign Agents Registration Act and direct the Federal Communications Commission to introduce new regulations in order to improve media ownership transparency in the United States*

- ***Recommendation 7****: Congress should grant a federal entity the authority to publish and enforce transparency guidelines for social media platforms* (p. 2-3).

The white paper's recommendations summarize their research-based comprehensive strategy to counter foreign disinformation. These recommendations aim to empower citizens, support research, improve transparency, and establish countermeasures, emphasizing the need for a multi-pronged response vital for the U.S. to address disinformation effectively.

CISA

CISA was established in November 2018 when U.S. President Trump signed the "Cybersecurity and Infrastructure Security Agency Act of 2018" into law (Cybersecurity and Infrastructure Security Agency Act of 2018 2018). CISA's inaugural comprehensive Strategic Plan for 2023-2025, CISA identifies its overarching strategy and targets since its establishment in 2018 (Cybersecurity & Infrastructure Security Agency 2022). Building upon the foundation laid by the CISA Strategic Intent released in August 2019, the strategic plan focuses on streamlining the agency's work and establishing unity of effort. As the national cyber defense agency and the national coordinator for critical infrastructure security, CISA interacts daily with critical infrastructure partners to respond to an evolving threat landscape.

CISA's Strategic Plan emphasizes its collective approach to mitigate risks and build resilience against cyber and physical threats to the nation's infrastructure. It highlights four ambitious goals: three targeting *"how"* the agency will reduce risk and build

resilience, and the fourth emphasizing internal readiness to execute the Strategic Plan as *"One CISA"* (p. 2). CISA aims to drive change over the next three years in four primary areas:

1. Spearheading the national effort to ensure the defense and resilience of cyberspace. As stated in the plan, *"As America's cyber defense agency, we must build the national capacity to defend against, and recover from cyberattacks […] and we must partner with the private sector and SLTT governments to detect and mitigate cyber threats and vulnerabilities before they become incidents"* (p. 1).

2. Reducing risks and strengthening the resilience of America's critical infrastructure. CISA declares to *"proactively reduce risk to infrastructure and systems while also building our stakeholders' capacity to safeguard their infrastructure from cyber and physical threats and risks"* (p. 2).

3. Strengthening whole-of-nation operational collaboration and information sharing. CISA's strategy states that *"securing our nation's cyber and physical infrastructure is a shared responsibility"* that requires the collaboration between government, industry, academic and international partners (p. 2).

4. Unifying as One CISA through integrated functions, capabilities, and workforce. CISA commits to *"building a culture of excellence based on core values and core principles that prize teamwork and collaboration, innovation and inclusion, ownership and empowerment, and transparency and trust"* (p. 2).

The Strategic Plan underscores the development of internal performance and effectiveness measures better to track progress toward risk reduction and goal achievement. As the plan concludes, *"identifying appropriate measures is not a simple task, […] it will require an ongoing effort throughout the performance period of the plan, and we will refine them as needed"* (p. 9).

Misinformation and Disinformation Task Force

The Federal Interagency COVID-19 Misinformation and Disinformation Task Force was a government initiative designed to counter misinformation and disinformation related to COVID-19 (COVID–19 Misinformation and Disinformation Task Force Act of 2020 2020). It was proposed to be established as described in the bill "Covid–19 Misinformation and Disinformation Task Force Act of 2020". Its roles and responsibilities were to include *"coordinating the analysis of COVID–19 misinformation and disinformation by agencies across the Federal Government […] developing, […] and*

disseminating information literacy, including digital literacy and media literacy, and information resilience public awareness campaigns relating to pandemics" (p.11-12).

Comprised of representatives from various agencies, including the Federal Communications Commission and the Centers for Disease Control and Prevention, the proposed task force aimed to promote media literacy, civil engagement, and educated decision-making based on trustworthy information sources. The task force has the mandate to communicate with both the public and relevant congressional committees; Specifically, it is required to publish on a publicly accessible website a report summarizing the analyses developed by the task force and provide congressional briefings.

The task force was expected to play a significant role in ensuring that public communications related to the analysis of COVID-19 misinformation and disinformation are effectively disseminated, *"specifically focus on ethnic and racial minority, rural, and other underserved populations, including communities without widespread internet access, including local news organizations, local radio organizations, and other non-digital media organizations"* (p. 17).

5.2 Analysis of EU Policy Tools

TITLE	Date	Source	Resource	Use
European council conclusions, 19-20 march 2015	**03/2015**	**European Council Website**	**Nodality**	**Effector**
Action plan on strategic communication	**06/2015**	**European External Action Service Website**	**Nodality**	**Effector**
EUvsDisinfo	**N/A**	**EUvsDisinfo Website**	**Organization**	**Effector**
In video veritas – verification of social media video content for the news industry	**05/2017**	**EC CORDIS**	**Treasure; Nodality**	**Effector**
2018 code of practice on disinformation	**10/2018**	**European Commission Website**	**Authority**	**Effector**
Flash eurobarometer 464 fake news and disinformation online	**03/2018**	**European Union Website: Eurobarometer**	**Nodality**	**Detector**
A multi-dimensional approach to disinformation - report of the independent high level group on fake news and online disinformation	**03/2018**	**Publications Office of the European Union**	**Nodality**	**Detector**
Communication - tackling online disinformation: a european approach	**04/2018**	**EUR-Lex Website**	**Nodality**	**Effector**

Synopsis report of the public consultation on fake news and online disinformation	**04/2018**	**European Commission Website**	**Nodality**	**Detector**
Communication action plan against disinformation	**12/2018**	**EUR-Lex Website**	**Nodality**	**Effector**
Rapid alert system (ras)	**03/2019**	**European External Action Service Website**	**Organization**	**Effector**
Setting up a special committee on foreign interference in all democratic processes in the european union, including disinformation	**06/2020**	**European Parliament Website**	**Nodality; Organization**	**Detector**
Communication on the european democracy action plan	**12/2020**	**EUR-Lex Website**	**Nodality**	**Effector**
European democracy action plan - making eu democracies stronger press release	**12/2020**	**European Commission Website**	**Nodality**	**Effector**
Communication european commission guidance on strengthening the code of practice on disinformation	**05/2021**	**European Commission Website**	**Authority**	**Effector**
Media literacy in Europe and the role of EDMO	**09/2021**	**EDMO Website**	**Organization**	**Effector**
Questions and answers about the east stratcom task force	**10/2021**	**European External Action Service Website**	**Treasure; Organization**	**Effector**
Social observatory for disinformation and social media analysis	**02/2022**	**EC CORDIS**	**Treasure; Organization**	**Effector**
2022 strengthened code of practice on disinformation	**06/2022**	**European Commission Website**	**Authority**	**Effector**
Regulation (EU) 2022/2065 digital services act	**10/2022**	**EUR-Lex Website**	**Authority**	**Effector**

Table 5.2 EU Policy Tools Overview

This section comprises a rigorous accumulation and systematic evaluation of the information drawn from 20 EU policy and institutional documents. These documents were principally sourced from various EU institutions' and agencies' online platforms, including but not limited to the European Council, European External Action Service (EEAS), European Commission, and the European Parliament. The period covered by these documents stretches from March 2015 to October 2022.

A strategic keyword search was performed to select these documents, with keywords such as "disinformation", "misinformation", and "false information" guiding the process. A concise summary of the identified policy instruments is presented in Table 5.2 for reference. Using Nvivo, the content from these documents was meticulously coded

following the same process introduced and implemented in the U.S. policy tools analysis above.

The comprehensive analysis of these documents has yielded findings that will be thoroughly presented and discussed in the following sections of this thesis. After classifying and introducing each policy tool based on its primary resource and intended use, references to the three core democratic processes will be introduced.

5.2.1 Tools of Nodality

In the detailed examination of EU policies on misinformation and disinformation, nodality emerges as a frequently employed resource. In eleven documents containing identified policy tools, nodality is employed to effect and detect disinformation policy outcomes.

This group identifies seven policy tools as effectors designed to enact specific outcomes. These encompass:

1. “European Council conclusions, 19-20 March 2015”
2. “Action Plan on Strategic Communication”
3. “In Video Veritas – Verification of Social Media Video Content for the News Industry”
4. “Communication – Tackling online disinformation: a European approach”
5. “Communication Action Plan Against Disinformation”
6. “Communication on the European Democracy Action Plan”
7. “European Democracy Action Plan - making EU democracies stronger Press Release”

In contrast, four policy tools utilize nodality as a detector, gathering information or intelligence in the fight against disinformation. These include:

1. “Flash Eurobarometer 464 Fake news and disinformation online”
2. “A multi-dimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation”

3. "Synopsis report of the public consultation on fake news and online disinformation"

4. "Setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation"

Detailed exploration of these documents in subsequent sections, starting with effectors, then continuing to detectors, will illuminate the strategic use of nodality by the EU in countering disinformation.

Nodality Effectors

"European Council conclusions, 19-20 March 2015"

The "European Council conclusions, 19-20 March 2015" communication directed at EU Delegations offers insights into the gathering of the 28 EU leaders in Brussels on March 19th and 20th, 2015, highlighting the EU's awareness and response to disinformation campaigns, primarily originating from Russia, as outlined in point 13 of the document (European Council 2015). The Council unequivocally recognizes the need to confront Russia's ongoing disinformation campaigns, distorting information and sowing discord within the EU. The communication states, *"The European Council stressed the need to challenge Russia's ongoing* disinformation *campaigns and invited the High Representative, in corporation with Member States and EU institutions, to prepare by June an action plan on strategic communication"* (p. 5).

This proposal affirms the EU's recognition of the vital role of communication in countering disinformation. It also states that *"the establishment of a communication team is a first step in this regard"* (p. 5). This alludes to the establishment of the East Statcom Task Force.

Action Plan on Strategic Communication

The "Action Plan on Strategic Communication" represents the EU's comprehensive approach to addressing disinformation campaigns and ensuring the accurate conveyance of its policies and values, particularly towards the Eastern neighborhood (European External Action Service 2015). In the context of dramatic political, economic, and security-related developments in the region, the European Council identified the crucial role of strategic communication, emphasizing *"the need to challenge Russia's ongoing disinformation campaigns"* and preparing an action plan to counter such activities (p. 1).

This plan was designed by the newly established East StratCom Team, a testament to the Council's commitment to challenging disinformation. As the document outlines, this team was formed to *"maintain an overall coordinating and monitoring role in relation to its implementation"* (p. 1). This represents an acknowledgment of the need for specialized structures in combating disinformation campaigns, mirroring the establishment of a communication team as stated in the Council's conclusions of 20 March 2015 (European Council 2015).

The Action Plan highlights strategic communication as a crucial tool to further EU policy objectives in the Eastern neighborhood, stating that it is aimed at *"building a common area of shared democracy, prosperity, stability, and increased cooperation"* based on *"mutual interests and commitments"* (p. 1). This positive narrative is intended to resonate with citizens, illustrating the tangible benefits EU policies can have on their lives. Furthermore, the Action Plan underscores the necessity to increase public awareness of disinformation activities by external actors. This objective showcases the EU's determination to react to and anticipate such activities. The document commits to responding to disinformation relating to the EU, emphasizing the necessity for the EU to *"be prepared to anticipate and respond to disinformation"* (p. 2).

In practice, the East StratCom Team is tasked to develop dedicated communication materials to improve EU strategic communication, especially in areas where the EU is subject to disinformation campaigns. The Action Plan identifies the importance of media freedom and freedom of expression, highlighting the need to train journalists and media actors, support pluralism in the Russian language media space, and increase media literacy. These points underline the EU's broader approach to mitigating disinformation: creating an environment where the truth can prosper and citizens can discern the difference between valid information and disinformation.

In Video Veritas – Verification of Social Media Video Content for the News Industry

The InVID project was established in the context of the digital media revolution, where *"social media with broadband wired and wireless connectivity [...] are bringing breaking news to online video platforms"* (European Commission 2018a). It aimed to tackle the challenge of verifying user-generated video content shared on social media. According to the report, *"the access to increasingly sophisticated video editing and content management tools, and the ease in which fake information spreads over the internet, make necessary the verification of any third-party content by news outlets and media organizations before publishing it"* (para. 1). To combat this, InVID built a platform to

provide services for the *"detection, authentication and assessment of the reliability and accuracy of newsworthy video files and video content spread via social media"* (para. 1).

InVID *"developed techniques for breaking news monitoring, content acquisition and indexing, fragment-level video conceptual annotation"* (European Commission 2018a). Moreover, they "*built a toolset for video verification by means of forensic analysis, near-duplicate detection, video logo detection and identification, location detection, and context aggregation and analysis"* (para. 2). The culmination of this work comprised 4 integrated technologies:

1. The InVID Verification Plugin: a globally accessible browser add-on utilized by over 9,800 users, which assists journalists in verifying facts and debunking misinformation;

2. The InVID Multimodal Analytics Dashboard: a unified online platform designed to gather and identify newsworthy video content;

3. The InVID Verification Application: a comprehensive online tool designed for the sophisticated verification of video content; and

4. The InVID Mobile App: a mobile application designed to quickly deliver verified and noteworthy content for reporting breaking news stories.

"The integrated InVID applications are new services for the management and verification of user-generated video (UGV), exploiting in full the convergence of broadband, broadcast and social media" (para. 3). These novel tools developed in close collaboration with journalists have potential to improve productivity, counter disinformation, and increase revenue opportunities for both media organizations and UGV owners.

Communication – Tackling online disinformation: a European approach

The European Commission's communication on "Tackling online disinformation: a European approach" is rooted in recognition of online platforms' important role in countering the spread of online disinformation (European Commission 2018b). The communication, directed at the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, brings awareness to the other EU institutions of the threat of disinformation, highlighting that disinformation can be amplified via social media and other online media, primarily driven by three types inherent mechanics that support these platforms:

1. Algorithm-based: Algorithms support the platform's business model, often prioritizing sensational content that is most likely to grab the attention of a large crowd of users. These algorithms can *"indirectly heighten polarization and strengthen the effects of disinformation"* (p. 5).

2. Advertising-driven: In today's business model, advertising companies shoot for content that will generate the most clicks, facilitating *"the placement of ads based on websites that publish sensationalist content appealing to users' emotions, including disinformation"* (p. 5).

3. Technology-enabled: New digital technology, such as "bots", can be used to automate services and *"artificially amplify the spread of disinformation"* (p. 5).

In response to the developing threat of disinformation to European society, the Commission proposed a policy response based on four overarching principles and objectives, namely, *(1) "to improve transparency regarding the origin of information and the way it is produced […]; (2) to promote diversity of information […]; (3) to foster credibility of information by providing an indication of its trustworthiness […]; [and] (4) to fashion inclusive solutions"* (p. 6).

In the effort to achieve objectives for the first front, creating "a more transparent, trustworthy and accountable online ecosystem", the Commission "calls upon platforms to decisively step up their efforts to tackle online disinformation [by using] self-regulation" (p. 7). To achieve this, the Commission calls on developing a "Code of Practice" that will be used to commit online platforms and advertising organizations to practices that limit the dissemination of disinformation (to be discussed further in the section on Tools of Authority).

Communication – Action Plan against Disinformation

The Joint Communication "Action Plan against Disinformation" presented by the European Commission and High Representative of the Union for Foreign Affairs and Security Policy in December 2018 to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions serves as an answer to the European Council's call for measures to *"protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections"* (European Commission 2018c). Building on the work of the East Strategic Communication Task Force (see the section below on Tools of Organization), this communication identifies four pillars on which the coordinated

response actions the Commission aims to take to combat the threat of disinformation are based:

1. *"Improving the capabilities of Union institutions to detect, analyze and expose disinformation;*
2. *Strengthening coordinated and joint responses to disinformation;*
3. *Mobilizing private sector to tackle disinformation;*
4. *Raising awareness and improving societal resilience"* (p. 5).

Two specific actions identified under the first pillar involve reinforcing the capabilities of the Strategic Communication Task Forces of the EEAS, Union Delegations, and the EU Hybrid Fusion Cell. The first action mentions providing support through *"additional staff and new tools which are necessary to detect, analyze and expose disinformation activities"* (p. 6). The second action involves the High Representative, tasking it with reviewing *"the mandates of the Strategic Communications Task Forces for Western Balkans and South to enable them to address disinformation effectively in these regions"* (p. 6).

Three actions are presented under the second pillar to strengthen coordinated and joint responses to disinformation. The first calls for the establishment of the Rapid Alert System (RAS) (discussed in the section below on Tools of Organization) *"for addressing disinformation campaigns"* (p. 8). The second action aims to bolster the Commission's communication efforts *"on Union values and policies"* in preparation for upcoming European elections (p. 8). This pillar's third and final action states that *"the Commission and the High Representative, in cooperation with Member States, will strengthen strategic communications in the Union's neighborhood"* (p. 8).

Only one action is presented under the third pillar directed at mobilizing the private sector to tackle disinformation. The Commission vows to *"ensure a close and continuous monitoring of the implementation of the Code of Practice"* (discussed in the following section on Tools of Authority) (p. 9). The Commission will *"push for rapid and effective compliance" and "carry out a comprehensive assessment at the conclusion of the Code's initial 12-month period of application"* (p. 9). Based on this assessment, the Commission will decide whether further regulatory actions are necessary.

The fourth and final pillar entails four actions to raise awareness and improve societal resilience to disinformation. To this effort, the first action proposes the organization of *"targeted campaigns for the public and trainings for media and public opinion shapers*

in the Union and its neighborhood to raise awareness" (p. 11). In the second action, the Commission calls on Member States to *"support the creation of teams of muti-disciplinary independent fact-checkers and researchers"* with knowledge of disinformation campaigns prevalent in online social media (p. 11). The third action aims to *"support cross-border cooperation amongst media literacy practitioners as well as the launch of practical tools for the promotion of media literacy for the public"* (p. 11). Considering the 2019 European elections, the final action calls on Member States to *"ensure effective follow-up of the Elections Package"* (p. 11).

Communication – On the European democracy action plan

The communication "On the European democracy action plan" in December 2020 highlighted the implications of digital transformation within democracies and the threats thereof posed by disinformation (European Commission 2020a). This action plan proposes specific actions to reinforce the EU policy framework, specifically through measures to *"promote free and fair elections and strong democratic participation; support free and independent media; and counter disinformation"* (p. 3). The plan contains 79 references to disinformation, including references in the context of election integrity, democratic participation, and media freedom, as well as a specific section on countering disinformation.

The action plan calls for *"closer cooperation within the EU, with relevant stakeholders in civil society, academia and private industry, and with international partners"* to pool existing knowledge on the new threat landscape across different sectors (p. 20). Additional measures involve developing *"the EU's toolbox for countering foreign interference and influential operations […] as well as strengthening the EEAS strategic communication activities and taskforces"* (p. 21). The Commission also aims to *"develop a common framework and methodology for collecting systematic evidence on foreign interference and a structural dialogue with civil society, private industry actors and other relevant stakeholders"* (p. 21).

European Democracy Action Plan: making EU democracies stronger

The European Commission, in its press release, announced the presentation of its European Democracy Action Plan, the comprehensive strategy to empower citizens and bolster democracies across the EU presented in the communication above (European Commission 2020b). The initiative was prompted by rising extremism, disinformation, and the perceived gap between people and politicians.

The press release addresses the Action Plan's measures to foster free and fair elections, reinforce media freedom, and counteract disinformation. The press release explicitly announces the Commission's aim to propose legal actions concerning political advertising, addressing various stakeholders, including online platforms, advertisers, and political consultancies.

European Commission President Ursula von der Leyen emphasized the importance of free speech in the digital age and the need for distinguishing facts from fiction, stating, *"With the digital revolution under way, citizens must be able to make choices where views can be expressed freely. Facts have to be distinguished from fiction, and free media and civil society must be able to participate in an open debate, free from malign interference"* (para. 3). She further asserted that the EU is taking action to enhance the resilience of democracies in the EU.

Věra Jourová, Vice-President for Values and Transparency, highlighted that democracy needs to be nurtured and protected. She shared, *"Our plan aims at protecting and promoting meaningful participation of citizens, empowering them to make their choices in the public space freely, without manipulation. We need to update the rules to harness the opportunities and challenges of the digital age"* (para. 4).

The press release underscores that the challenges faced by the EU extend beyond its borders, implying that the impact of their actions would have international repercussions. It also shares the three pillars around which the European Democracy Action Plan is structured: "promoting free and fair elections, strengthening media freedom and pluralism, and countering disinformation" (para. 6-13). Each of these pillars encompasses specific initiatives and actions aimed at enhancing democracy, ensuring the safety and integrity of journalists, and tackling disinformation.

The press release concludes that the European Commission will implement the European Democracy Action plan gradually until 2023, with progress assessments determining any need for additional steps. It also reaffirms the Commission's commitment to continued engagement with various stakeholders, including the European Parliament, the Council, and a wide circle of national actors, both public and private, all of which are key to strengthening the resilience of EU's democracies.

Nodality Detectors

Flash Eurobarometer 464 Fake news and disinformation online

A Eurobarometer survey is a series of public opinion surveys conducted regularly on behalf of the European Commission since 1973 (European Parliament n.d.). These

surveys address various topical issues, providing comprehensive studies of the state of public opinion in the European Union member countries. It is a key tool for tracking public sentiment and trends, often used to influence policy-making within the EU.

One of the Eurobarometer surveys, "Flash Eurobarometer 464 - fake news and disinformation online," focused on the perception and impact of misinformation or 'fake news' in the online space (European Union 2018). The survey's findings present a strong public sentiment on the issue, with 83% of the respondents expressing their belief that fake news poses a significant threat to democracy (p. 4).

The survey further revealed that the respondents held particular concerns about the existence of fake news as a problem in their country and for democracy in general, where *"more than eight in ten respondents (85%) think that the existence of fake news is a problem in their country"*, reflected consistently across all Member States, *"with at least 70% in every country seeing fake news as a problem in their country"* (p. 4).

Another key aspect of the survey was its insight into the public's trust in various news sources. Traditional media outlets, including radio, TV, and print, were held in high regard by the respondents, with trust ratings of 70%, 66%, and 63%, respectively. This underscores the continuing relevance and importance of traditional media as reliable sources of information in the eyes of the public.

On the contrary, online sources of news and video hosting websites lagged significantly in terms of public trust. They were considered the least trusted news source, with 26% and 27% trust rates, respectively. This low level of trust in online sources reveals a prevailing skepticism among the public about the credibility of news disseminated through these platforms, demonstrating the necessity for robust measures to combat online disinformation.

A multi-dimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation

At the beginning of 2018, the European Commission established an advanced expert panel known as "the HLEG" to guide policy actions to mitigate disseminating false information and disinformation online (European Commission and Directorate-General for Communications Networks 2018). The panel, led by Prof. Dr. Madeleine de Cock Buning, comprised 39 members who brought a diverse array of perspectives from various sectors such as academia, journalism, print and broadcast media, online platforms, and civil society and fact-checking institutions. Their tasks included *"to advise the Commission on all issues arising in the context of false information spread across*

traditional and social media and on possible ways to cope with its social and political consequences" (p. 5). The primary deliverable of this group was this report, which identifies a multi-dimensional approach to combat disinformation that is based on five pillars:

1. Increasing the transparency of online news, which includes sharing suitable and privacy-compliant data regarding the systems that facilitate their online dissemination;

2. Advocating for media and information literacy as a means to counter disinformation and to assist users in navigating the digital media landscape;

3. Creating tools that empower both users and journalists to combat disinformation and stimulate positive interaction with rapidly evolving information technologies;

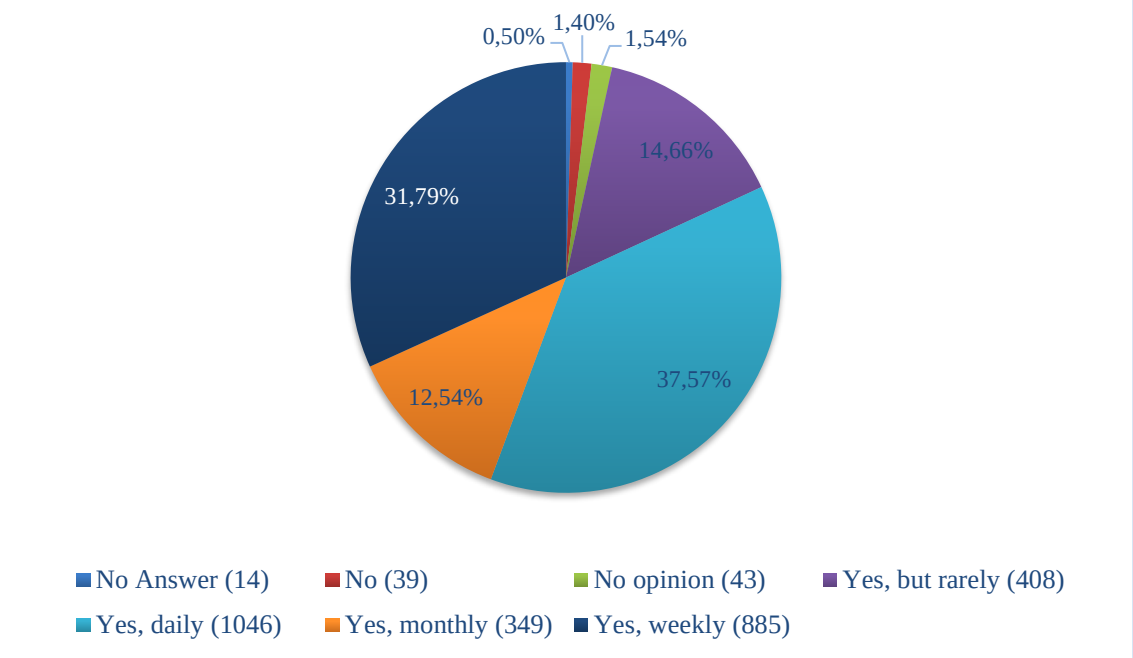
4. Ensuring the diversity and sustainability of the European news media ecosystem; and

5. Encouraging ongoing research into the effects of disinformation in Europe to assess the actions taken by various players and continually fine-tune the necessary responses.

Synopsis report of the public consultation on fake news and online disinformation

The public consultation on fake news and online disinformation occurred between November 2017 and February 2018. It aimed *"to help assess the effectiveness of current actions by market players and other stakeholders, the need for scaling them up and introducing new actions to address different types of fake news"* (European Commission 2018d, para. 1). It involved two different questionnaires designed for citizens and for legal persons/journalists, respectively, with a total of 2986 responses received from individuals and legal organizations and journalists.

One notable finding was that over 97% of the respondents claim to have been confronted with fake news, with 38% of them daily and 32% of the respondents every week. These results can be seen summarized in Figure 5.2 below.



c.f. European Commission (2018d), para. 2

Figure 5.2 Responses to the question "Have you ever come across fake news?"

The consultation aimed to gain insights on three aspects: the definition of fake information and its online spread, the effectiveness of measures taken by various stakeholders to counter the spread of fake information online, and the potential for future actions to strengthen quality information and prevent the propagation of disinformation online.

The key findings from the consultation revealed that there was a *"common perception amongst all respondents that fake news in general is highly likely to cause harm to society, in particular in areas such as political affairs, immigration, minorities and security"* (para. 6). It was also found that *"Fact-checking through independent news organisations and civil society organisations is considered the method that better contributes to counter the spread of disinformation online"* (para. 7).

Furthermore, the respondents *"agreed that more should be done to reduce the spread of disinformation online"* (para. 8). It was also emphasized that any approach to tackling fake news should respect fundamental rights such as freedom of expression and not promote censorship.

The consultation concludes, *"Together with the results of the Eurobarometer, and the report of the High-Level group, the results of the public consultation feed into the Commission Communication on tackling online disinformation"* (para. 12). This indicates

that the findings from this consultation will be used to inform future policies and strategies for addressing online disinformation.

Setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation

In response to increasing concerns about foreign interference in the democratic processes of the European Union, the European Parliament decided to establish a special committee in June 2020, as proposed by the Conference of Presidents (European Parliament 2020a). The special committee will consist of 33 members and will operate for a term of 12 months, starting from its first meeting. It may present a mid-term report to Parliament and is expected to present a final report containing factual findings and recommendations regarding the measures and initiatives to be taken.

The committee, which will later be known as INGE, addresses foreign interference across various fronts, including disinformation campaigns on traditional and social media, cyber-attacks targeting critical infrastructure, and indirect financial support of political actors, among others.

In its mandate, the special committee is tasked with responsibilities that cover a broad spectrum of democratic processes. The committee is expected to *"conduct a thorough analysis of the investigations showing that crucial electoral rules have been breached or circumvented, in particular the existing provisions on the transparency of campaign financing,"* as per the decision document (sec. 1.a). To prevent foreign interference in democratic processes, the committee will also aim to *"identify possible areas which would require legislative and non-legislative actions,"* these actions will not only involve public authorities, but also social media platforms, technology companies, and the private sector at large (sec. 1.b).

The committee is directed to assess national actions that provide strict restrictions on the sources of political funding, with the goal of circumventing covert support from foreign actors. The decision document states that *"foreign actors have found legal and illegal ways to circumvent national legislations and have offered covert support to their allies by taking out loans with foreign banks, providing in-kind things of value, through purchase and commercial agreements, through shell companies, through non-profit organisations,"* among others (sec. 1.d).

Furthermore, the committee is charged with proposing *"coordinated action at EU level for tackling hybrid threats, including cyber-attacks on military and non-military targets,"* as well as investigating the EU's dependence on foreign technologies in critical

infrastructure supply chains (sec. 1.e). This is to counter the strategic communication of hostile third parties and to support coordination between Member States to counter threats and address current deficiencies. Interviewee 3 corroborates this claim, stating that the special committee was tasked with *"investigating how much disinformation is a problem within the European institutions, especially targeting the Parliament."* Interviewee 3 also mentions that the department focused on disinformation where the interviewee works at the European Parliament was established based on the recommendations and findings of INGE.

5.2.2 Tools of Authority

This section examines four policy tools implemented in the EU, all typified as effectors of authority. The policy tools encompass a range of measures, from industry self-regulation codes to comprehensive regulations issued by the European Commission.

These include the 2018 Code of Practice on Disinformation, a voluntary framework devised by online platforms, leading social networks, advertisers, and the advertising industry to address the spread of disinformation (European Commission 2018e). Following this, the European Commission released Communication Guidance on Strengthening the Code of Practice on Disinformation to improve the effectiveness of the initial Code (European Commission 2021). This then led to the 2022 Strengthened Code of Practice on Disinformation, reflecting the updated commitment of signatories to more effectively combat disinformation (European Commission 2022a).

In addition to these self-regulatory measures, legislative authority was invoked through the implementation of Regulation (EU) 2022/2065, also known as the Digital Services Act (European Parliament and Council of the European Union 2022). This comprehensive regulation was introduced to better manage the digital space, including areas related to disinformation. This regulation also involves the EU's budgetary allocations for disinformation-related activities.

Each of these policy tools functions as an authority effector, primarily involving regulation, guidance, and law. The following sections will present these tools in chronological order.

2018 Code of Practice on Disinformation

The first of its kind, the European Union Code of Practice on Disinformation is a self-regulatory framework established in October 2018 to manage the spread of disinformation within the EU (European Commission 2018e). The signatories of the code, according to Section I, are online platforms, leading social networks, advertisers, and the

advertising industry. The code defines 'disinformation' and 'political advertising,' among other terms, and makes it clear that disinformation *"does not include reporting errors, satire and parody, or clearly identified partisan news and commentary"* (p. 1).

In Section II, signatories commit to various practices organized under five main headings: "Scrutiny of ad placements", "Political and issue-based advertising", "Integrity of services", "Empowering consumers", and "Empowering the research community". Examples of these commitments include the pledge to implement *"clear policies regarding identity and the misuse of automated bots on their services and to enforce these policies within the EU"* (p. 6) and to *"support good faith independent efforts to track Disinformation and understand its impact"* (p. 8).

Section III, "Measuring and Monitoring the Code's Effectiveness", outlines that *"Relevant Signatories commit to write an annual account of their work to counter Disinformation in the form of a publicly available report reviewable by a third party"* (p. 8). The World Federation of Advertisers and the European Association of Communications Agencies, among other organizations, are designated to provide aggregated reports on brand safety activities and policies.

According to Section IV, there will be an *"assessment period of 12 months"* following the signing of the Code of Practice (p. 9). During this time, the signatories will regularly assess progress, implementation, and functioning. After this period, annual meetings will be held to review the code and make necessary amendments. In Section V, the document lays out the conditions under which new signatories can join or existing signatories can withdraw from the Code. It is also stated that if a signatory fails to respect its commitments under the code, after all reasonable avenues have been explored, the other signatories may invite such a signatory to withdraw from the Code.

Communication European Commission Guidance on Strengthening the Code of Practice on Disinformation

The "Communication European Commission Guidance on Strengthening the Code of Practice on Disinformation", as its name implies, proposes reinforcements to the Code of Practice discussed above (European Commission 2021). The communication states that *"the commitments of the current Code of Practice are not sufficiently effective in providing a comprehensive response to the disinformation phenomena"*, asserting that there are still gaps related to specific commitments and new and emerging risks (p. 4).

Additionally, the communication proposes that, *"while the main target remains disinformation in the narrow sense"*, the scope of the Code should commit to employ

"appropriate policies and take proportionate actions to mitigate the risks posed by misinformation" when public safety is at risk, such as with the misinformation campaigns during COVID-19 (p. 5). The Commission also recommends including "a broader participation of stakeholders from the advertising ecosystem beyond the circle of the Code's current signatories" including brands, ad-tech providers, communication agencies, and e-payment services, among others (p. 6). This action is aimed at increasing the impact of the Code on the demonetization of disinformation activities.

Furthermore, another proposed key addition to the Code involves empowering users with *"a better understanding of the functioning of online services, as well as tools that foster more responsible behavior online or that enable users to detect and report false and/or misleading content"* in order to reduce the spread of disinformation (p. 13). Relevant proposals include commitment to media literacy enhancing measures and safe service design of online platforms.

2022 Strengthened Code of Practice on Disinformation

Introduced on 16th June 2022, the 2022 Code of Practice on Disinformation represents a collaborative effort by major online platforms, emerging and specialized platforms, players in the advertising industry, fact-checkers, research and civil society organizations to strengthen countermeasures against online disinformation (European Commission 2022a).

The road to the strengthened Code began with the 2018 Code of Practice on Disinformation, which was the first initiative to unite industry players in combating disinformation. In response to the Commission's Assessment of its initial implementation period, the Commission issued detailed Guidance in May 2021 to address the 2018 Code's shortcomings. This led to the current Strengthened Code, created in collaboration with signatories of the 2018 Code and a diverse group of potential signatories.

The strengthened Code comprises of 44 commitments and 128 specific measures across several domains, including demonetisation of disinformation dissemination, transparency of political advertising, service integrity, user empowerment, research facilitation, and fact-checker cooperation. To ensure adaptability to technological, societal, market and legislative developments, signatories have established a permanent Task-force and a Transparency Centre to provide the public with clear, regularly updated insights into the policies implemented to uphold these commitments.

Regulation (EU) 2022/2065 Digital Services Act

The European Union's Digital Services Act (DSA), into force as of November 2022, is a comprehensive legislation that seeks to provide updated rules governing digital services across the Union, addressing emerging issues surrounding digital platforms, particularly Very Large Online Platforms (VLOP) (European Parliament and Council of the European Union 2022). The DSA, alongside the Digital Markets Act (DMA), was developed to enhance the protections and rights of users in the digital space, with its focus on bringing greater transparency, accountability, and user control into the operations of VLOPs.

The regulation specifically targets major issues like the handling of illegal content and addressing systemic risks. This is reiterated by Interviewee 1, who mentions that the DSA does not aim to regulate content itself, but rather *"regulating the way"* that content is dealt with. It proposes changes in the responsibility structure for digital service providers, ensuring they act with due diligence to mitigate the spread of illicit content. The DSA's new procedures encompass faster response times to reported illegal content, clear procedures for challenging decisions made by online platforms, and transparency obligations.

Furthermore, the DSA establishes a range of rules for targeted advertising and recommender systems, particularly with regard to data privacy. It requires VLOPs and very large search engines to *"ensure public access to repositories of advertisements presented on their online interfaces to facilitate supervisoion and research into emerging risks […] in relation to illegal advertisements or manipulative techniques and disinformation,"* and this information should contain the content of advertisements, particularly where targeted advertising is employed (p. 26). The DSA reinforces some core principles of the General Data Protection Regulation (GDPR) and also attempts to fill in gaps that the GDPR leaves, notably in the area of profiling. Article 26 of the DSA requires transparency of platforms concerning online advertisement activities, while stricter regulation on online targeted advertising and profiling, particularly regarding minors and special categories of personal data, are pursued.

5.2.3 Tools of Treasure

This section provides an examination of three EU policy instruments characterized by the deployment of tools of treasure, specifically, 'In Video Veritas – Verification of Social Media Video Content for the News Industry', 'Questions and Answers about the East StratCom Task Force', and the 'Social Observatory for Disinformation and Social Media Analysis'. While some of these tools are also identified as tools of nodality and organization, this section analyzes these policy instruments in the context of the application of financial assets or allocations aimed at tackling disinformation activities.

In Video Veritas – Verification of Social Media Video Content for the News Industry

The "In Video Veritas" project, introduced in the Tools of Nodality section above, was funded under the Horizon 2020 EU research and innovation funding programme (European Commission 2018a). The project belonged to the "INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies" objective of the funding programme and received a total contribution of €3,115,737.50 from EU funding for work carried out from 1 January 2016 to 31 December 2018.

The Horizon 2020 funding programme represents a pivotal instrument for the European Union in fostering innovation and research. As the largest public research funding programme in the world, Horizon 2020, operating from 2014 to 2020, was equipped with nearly €80 billion in funding to distribute over its seven-year tenure (European Commission n.d.) As the European Commission states, *"Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness"* ("Horizon2020 - EURADA - EURADA" n.d.). The programme sought to address critical societal challenges, drive industrial leadership, and enhance excellence in Europe's science base.

Questions and Answers about the East StratCom Task Force

The East StratCom Task Force, founded in September 2015, was created as part of the EEAS in an effort to combat Russia's ongoing disinformation campaigns (European External Action Service 2021). The Task Force, which comprises personnel from EU institutions and national experts seconded from Member States, operates within the EU's strategic communications budget. This budget has seen substantial growth, from a 2018 allotment of €1.1 million from the European Parliament's Preparatory Action to address pro-Kremlin disinformation, to €4 million in 2020 (European External Action Service 2021). By 2021, the total budget dedicated to the EEAS Strategic Communications and Information Analysis Division for countering disinformation and manipulative interference, and enhancing strategic communication capabilities, reached €11.1 million.

This funding is allocated to support several initiatives, including professional monitoring of media, disinformation and data analysis, the design and execution of communication campaigns, and the creation and translation of content designed to raise awareness of disinformation into various EU and neighbouring languages. It is also used for the development of training programs and simulations on responding to disinformation. As quoted, *"The objective is to gain a more comprehensive, up-to-date and in-depth picture of foreign disinformation campaigns, to reach out with awareness campaigns to new*

audiences and to increase the EU's and its neighbours' resilience to disinformation" (para. 18).

Social Observatory for Disinformation and Social Media Analysis

Similar to the "In Video Veritas" project introduced above, the "Social Observatory for Disinformation and Social Media Analysis (SOMA)" project also received funding from the European Commission, aiming to establish an observatory within the EU that targets disinformation activities (European Commission 2022b). The project began in 1 November 2018 and continued until 30 April 2021, receiving a total contribution of EU funds for the amount of €987,437.50. For a detailed description of the work achieved and tasks of the observatory, see the section below on "Tools of Organization".

5.2.4 Tools of Organization

In response to the growing challenge of disinformation, the EU has put into operation tools of organization that marshal governmental resources, personnel, and expertise from both the public and private sectors. These tools are primarily manifest in the establishment of intergovernmental agencies and taskforces. Notably, five entities stand out upon review of pertinent documents: EUvsDisinfo, the Special Committee on Foreign Interference in all Democratic Processes in the EU including Disinformation, RAS, the European Digital Media Observatory (EDMO), and the East StratCom Task Force. This subsequent section will unpack the findings from key documents related to the inception and roles of the above-mentioned entities.

EUvsDisinfo

EUvsDisinfo is a flagship initiative by the East StratCom Task Force of the EEAS, formed in 2015 (EUvsDisinfo n.d.). This project emerged as a response to the persistent disinformation campaigns by the Russian Federation that have been impacting the EU, its Member States, and countries within the neighbouring region. EUvsDisinfo primarily aims to enhance public awareness and comprehension of the Kremlin's disinformation operations. Interviewee 4 also points out that the disinformation efforst of the group extend to narratives and threats from China and Iran as well. Moreover, it aspires to assist citizens in Europe and beyond in cultivating resilience against digital information manipulation and media subversion.

In terms of functionality, EUvsDisinfo utilizes media monitoring services and data analysis in 15 languages to pinpoint, aggregate, and disclose instances of disinformation that originate from pro-Kremlin media and disseminate across the EU and Eastern Partnership countries (EUvsDisinfo n.d.). The project's monitoring capabilities, since

2019, extend to the uncovering of disinformation disseminated in the Western Balkans and the EU's Southern neighbourhood. These identified instances of disinformation, along with their debunking, are archived in the EUvsDisinfo database, which is hailed as *"the only searchable, open-source repository of its kind,"* containing more than 15,000 examples of pro-Kremlin disinformation. The database undergoes weekly updates, which are complemented by a concise summary of trends (para. 3).

Beyond maintaining the database, EUvsDisinfo regularly generates articles and analyses on novel trends in disinformation practices and methodologies and collates pioneering international research in the field (EUvsDisinfo n.d.). The project also focuses on one of the gravest threats to democratic societies – electoral interference – by providing educational resources under the Elections section of its webpage.

Setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation

On June 18, 2020, the European Parliament decided to establish a special committee known as the Special Committee on Foreign Interference in all Democratic Processes in the European Union, Including Disinformation (INGE) (European Parliament 2022). The primary goal of this initiative was to facilitate a *"common, holistic, long-term approach to addressing evidence of foreign interference in the democratic institutions and processes of the EU and its Member States"* (European Parliament 2020b, p. 1). It was recognized that incidents of foreign interference represented a systematic pattern that has been recurring over recent years. State and non-state actors from third countries were identified as being behind these attempts, which threatened democracy in the EU and its Member States and were part of a wider trend experienced by democracies worldwide.

To combat these developments, the committee has several responsibilities, including conducting an in-depth analysis of violations of crucial electoral rules, particularly regarding the transparency of campaign financing (European Parliament 2020b). It is also tasked with identifying areas requiring legislative and non-legislative action, such as potential interventions by social media platforms to label content shared by bots or to make algorithms as transparent as possible.

Moreover, the committee aims to *"contribute to the ongoing debate on how to enhance the responsibility for countering foreign interference in all democratic processes in the European Union"* (p. 2). The Parliament recognizes that this task is not solely for public authorities but also requires cooperation with technology companies, social media platforms, and the wider private sector. Another significant duty of the committee is to assess national actions to provide strict restrictions on the sources of political funding.

This includes identifying possible areas that would require actions regarding the funding of political parties and political campaigns.

Factsheet: Rapid Alert System

The European Union's RAS is a critical component in the fight against disinformation. Enacted as part of the "Action Plan against Disinformation approved by the European Council in December 2018", the RAS is designed to bolster coordination and create joint responses to disinformation (European External Action Service 2019). At its core, the RAS serves as a network between EU institutions and Member States that facilitates the exchange of insights related to disinformation campaigns and helps orchestrate collective responses. According to the factsheet, the RAS aims for *"time and resource efficiency"* and a *"coordinated response"* to disinformation threats (p. 1).

The system is not limited to internal EU sources, but it also incorporates external insights. As the factsheet notes, the RAS is *"based on open-source information and will also draw upon insights from academia, fact-checkers, online platforms and international partners"* (European External Action Service 2019).

Three key functions characterize the work of the RAS:

1. Alerts: The RAS facilitates the sharing of instances of disinformation campaigns, ensuring that relevant stakeholders are promptly informed about disinformation threats.

2. Discussing Best Practices: The system provides a platform for stakeholders to discuss and share best practices in countering disinformation, promoting collective learning and improvement of response strategies.

3. Regular Sharing of Analysis, Trends, and Reports: The RAS fosters a collaborative environment through the regular sharing of analysis, trends, and reports related to disinformation.

The RAS constitutes a crucial intiative of the EEAS, and serves as a key organizational instrument for strengthening coordinated and joint responses to disinformation in the European Union.

European Digital Media Observatory: Media literacy in Europe and the role of EDMO

EDMO represents a concerted effort by a multidisciplinary community of experts to understand, analyze, and counter disinformation (European Digital Media Observatory

n.d.). This diverse community includes fact-checkers, media literacy experts, academic researchers, media organizations, and media literacy practitioners. They come together under the EDMO banner to pursue a deeper understanding of disinformation – its actors, vectors, tools, methods, dissemination dynamics, targets, and impact on society.

EDMO serves as a cornerstone of the EU's efforts to foster media literacy and build societal resilience to disinformation. Through a public portal, EDMO provides an array of resources aimed at equipping media practitioners, teachers, and citizens with the necessary information to understand and counteract the disinformation problem (Goodman 2021). As per the tender specifications, this public portal is envisioned to *"become the reference point for promoting European and national media literacy activities related to the disinformation problem and provide evidence for future-proof policies on disinformation"* (p. 8).

A crucial part of EDMO's strategy is to create *"searchable directories aggregating fact-checks and media literacy material from external repositories"* (Goodman 2021, p. 9) These directories are expected to hold at least 200 pieces of media literacy material, which must be continuously and systematically reviewed and updated. However, members of the EDMO Advisory Group on Media Literacy cautioned against the creation of a mere repository of media literacy activities, stressing instead the importance of considering the target audience and the benefits of such an effort. They urged EDMO to reflect on what has already been accomplished in this field and consider the other organizations currently at work in the area. They also acknowledged the challenge of creating a centralized resource that is genuinely searchable and, more importantly, encouraging people to use it.

In terms of audience, EDMO primarily serves media literacy stakeholders across Europe, including practitioners, policymakers, regulators, funders, and others. National hubs, which are planning media literacy activities, are a key part of EDMO's audience and strategy (Goodman 2021). EDMO's direct links with national contexts via these hubs represent one of the strengths of its model. Rather than creating its own media literacy resources, EDMO aims to support these hubs in their efforts, promoting the exchange of knowledge and ideas, and highlighting valuable initiatives. This is aligned with the statement in the European Democracy Action Plan that EDMO will provide support to national media literacy campaigns to strengthen citizens' ability to assess the quality and veracity of online information. Interviewee 3 also added that EDMO is taksed to "coordinate fact checkers within each Member State", claiming that this task can prove difficult to respond to due to the multilingual environment of the EU.

Questions and Answers about the East StratCom Task Force

The East StratCom Task Force is a specialized group established by the EU to address ongoing disinformation campaigns, particularly those from Russia. Created in March 2015, the Task Force is a component of the Strategic Communications and Information Analysis Division of the EEAS (European External Action Service 2021). The East StratCom Task Force operates under three key objectives*: "Effective communication and promotion of EU policies towards the Eastern Neighbourhood; Strengthening the overall media environment in the Eastern Neighbourhood and in the EU Member States, including support for media freedom and strengthening independent media; and Improved EU capacity to forecast, address and respond to disinformation activities by external actors"* (para. 4).

To counteract disinformation, the Task Force develops communication products and campaigns, working closely with other EU institutions and Delegations in the Eastern Partnership countries, Central Asia, and the Russian Federation (European External Action Service 2021). Its mission is to better explain EU values, interests, and policies, as well as to strengthen the media environment in these regions. As noted in their official webpage, *"The Task Force reports on and analyses disinformation trends, explains and exposes disinformation narratives, and raises awareness of the negative impact of disinformation that originates in pro-Kremlin sources"* (para. 7).

The team comprises sixteen full-time staff, as of March 2021, who have various professional backgrounds in communications, journalism, and social sciences. This group of experts has been instrumental in transforming the EU Delegations' approach to communication in the Eastern Partnership countries since its inception. The Task Force also collaborates with other international organisations and entities to tackle disinformation and ensure a holistic approach to this global challenge.

In addition, the Task Force plays a vital role in strengthening the media environment in the Eastern Neighbourhood. For instance, it has supported the development of an €11-million regional programme for independent media in Eastern Partnership countries and helped shape the Commission's bilateral media support programmes (European External Action Service 2021).

Social Observatory for Disinformation and Social Media Analysis

SOMA, a project funded by the European Commission, is a bold initiative aimed at combating disinformation at a pan-European level. With its focus on establishing and operating a European Observatory against Disinformation, SOMA engages in a broad spectrum of activities aimed at fostering a reliable and secure information space (European Commission 2022b). The primary objectives of SOMA encompass *"setting*

up the necessary technological infrastructure, attracting the relevant community, training the corresponding stakeholder groups, coordinating the operation of the observatory, setting up national centers that can act as satellite nodes with a multiplying effect, and finally assessing the impact both of disinformation, as well as of our intervention" (para. 2).

In its concerted effort to build a reselient community against disinformation, SOMA managed to create a network consisting of *"100 members featuring 38 think-tanks/research centers/NGOs; 13 fact-checking organizations; 12 companies (9 of which are tech); 11 freelancers; 8 associations/networks of orgs; 7 media literacy organisations; 6 media companies; 5 governmental or state-connected entities"* (para. 3). SOMA's initiative led to significant advancements, such as the establishment of three Centers of Excellence, the creation of the DisInfoNet toolbox for analysts, experts, and journalists, and the development of comprehensive impact assessment strategies against disinformation. The project also invested in mapping research activities around disinformation and organising media literacy events. During the project, the SOMA community has been actively engaged in *"20 collaborative investigations through the SOMA Observatory platform"* and 14 stakeholder events across multiple locations (para. 11). Its work went beyond traditional geographic boundaries, including events in Belgium, Slovenia, Denmark, Italy, and South Africa.

5.3 References to Key Democratic Functions

5.3.1 Empowered Inclusion

U.S. Policy Tools

Serial No. 116-55 House Hearing - Russian Disinformation Attacks on Elections: Lessons from Europe

In the "Serial No. 116-55 House Hearing - Russian Disinformation Attacks on Elections: Lessons from Europe", it is noted that there's no panacea for disinformation. The fight against it requires long-term social resilience, rooted in *"teaching everyone from – civil servants to children"* how to discern disinformation (U.S. Government Publishing Office 2019, p. 16). This empowers individuals through inclusion in the fight against disinformation. It's not just a matter for the federal government or social media companies but also requires *"state, local, territorial, tribal, private, nonprofit, and research partners to explore the impact of health misinformation, identify best practices to prevent and address it, issue recommendations, and find common ground on difficult questions"* (p. 16).

The U.S. Surgeon General's Advisory on Building a Healthy Information Environment

The "U.S. Surgeon General's Advisory on Building a Healthy Information Environment" provides a detailed blueprint of how the inclusion of the public is integral to addressing health misinformation, especially during the COVID-19 pandemic. The advisory proposes a similar "whole-of-society" approach, where citizens are equipped with tools to recognize and address health misinformation (Office of the U.S. Surgeon General 2021). This approach is reflected in multiple instances throughout the document. It emphasizes the role of trusted community members, *"such as professionals, faith leaders, and educators"*, in speaking directly to their communities, thus acknowledging the value of inclusion at the grassroots level (p. 6). It proposes to equip Americans with the tools to identify misinformation and address it in their communities, highlighting the importance of empowering individuals to act.

S.406 – Promoting Public Health Information Act

The "Promoting Public Health Information Act" emphasizes the importance of inclusive communication strategies in the context of public health emergencies. Specifically, the act focuses on the need to identify effective methods for disseminating public health information during emergencies and tailoring these methods *"to populations that may be impacted by such [health] misinformation"* (Promoting Public Health Information Act 2023, p. 3).

It also highlights the need to ensure scientific and public health guidance is *"accessible and communicated effectively to the public with specific focus on populations that are underserved or* with low health literacy" while also ensuring that informational activities focus on *"subgroups that are being targeted for health misinformation and disinformation, or are especially susceptible to health misinformation and disinformation, in a culturally- and linguistically-appropriate manner"* (p. 6).

S.394 - Digital Citizenship and Media Literacy Act

The Digital Citizenship and Media Literacy Act (2023), also emphasizes the importance of empowered inclusion by promoting media literacy and digital citizenship to the wider public. This act acknowledges the crucial role of media literacy education in enhancing national resilience against foreign disinformation campaigns. It encourages the implementation of educational programs to empower individuals, making them well-equipped to engage with digital content critically and thereby promoting their inclusion in the digital world. This focus is a clear testament to the act's commitment to empowered

inclusion by enabling individuals to be active, informed, and discerning participants in the digital sphere.

Furthermore, the act recognizes the effect of media literacy and digital citizenship education, stating that it *"empowers young people"*, helping them to improve health and safety, prevent cyberbullying, and enable informed decision-making about online information (p. 4). The Act aims to ensure active and informed inclusion in the digital world by equipping young people with these skills.

CISA

Empowerment is one of CISA's core strategic principles driving its mission to secure elections and promote safe cyber practices (Cybersecurity & Infrastructure Security Agency 2022). This includes empowering *"state and local officials"* to address disinformation in their communities and recognizing that *"empowering trusted voices is critical to ensuring that accurate information is available on our core democratic processes"* (p. 22). CISA also brings empowerment internally to the agency, as it believes *"people are CISA's most valuable asset";* therefore, they *"prioritize an environment of psychological safety where [people] feel cared for, supported, [and] empowered"* (p. 33).

EU Policy Tools

Action Plan on Strategic Communication

In the "Action Plan on Strategic Communication", the EU underscores the significance of enhancing *"public awareness of disinformation activities by external actors"* and strengthening the *"EU capacity to anticipate and respond to such activities"* (European External Action Service 2015, p. 1). The plan also calls for supporting *"pluralism in the Russian language media space"* to ensure citizens have access to information in their local language (p. 3). The EU further stresses the importance of working with Member States to *"raise awareness of disinformation activities amongst the general public"* and to put *"media literacy actions at all levels"* (p. 3).

Communication – Tackling online disinformation: a European approach

The "Communication – Tackling online disinformation: a European approach" document discusses the significance of creating *"inclusive solutions"*, *"awareness-raising activities"* on disinformation and *"fostering a critical awareness of citizens – in particular, young people – of the digital environment"* (European Commission 2018b, p. 13). It also emphasizes the importance of sharing knowledge and building cooperation among various stakeholders including *"public authorities, online platforms, advertisers,*

trusted flaggers, journalists and media groups" (p. 6). The document further highlights the lifelong development of *"critical and digital competences, in particular for young people, is crucial to reinforce the resilience of our societies to disinformation"* (p. 12).

European Democracy Action Plan - making EU democracies stronger Press Release

Lastly, in the "European Democracy Action Plan - making EU democracies stronger Press Release", the Commission presents the plan *"to empower citizens and build more resilient democracies across the EU"* (European Commission 2020b, para. 1). Vice-President for Values and Transparency, Věra Jourová states, *"Our plan aims at protecting and promoting meaningful participation of citizens, empowering them to make their choices in the public space freely, without manipulation"* (para. 4). This emphasizes the need to empower citizens and ensure their meaningful participation in public and democratic processes.

A Multi-Dimensional Approach to Disinformation - Report of the Independent High Level Group on Fake News and Online Disinformation

From the "A Multi-Dimensional Approach to Disinformation - Report of the Independent High Level Group on Fake News and Online Disinformation," it is evident that there is an emphasis on the promotion of media and information literacy as a key approach to counter disinformation (European Commission and Directorate-General for Communications Networks 2018). This strategy is seen as helping users navigate the dynamic digital media environment. It is stated that empowering users and journalists through the development of tools to combat disinformation and encouraging positive interaction with rapidly evolving information technologies is essential. Media and information literacy, in the modern information age, is seen as crucial as traditional educational competences were in the industrial age. These competencies are necessary for the active and responsible participation in the online public sphere, underpinned by fundamental rights like freedom of expression.

The document also recommends that media and information literacy should be implemented on a large scale in school curricula and teacher training curricula to be effective. It suggests that users of platforms' services, including both citizens and media professionals, should be empowered to increase society's resilience to various forms of disinformation. There is also an emphasis on platforms providing their users with advanced settings and controls to allow them to customize their online experiences.

5.3.2 Collective Agenda & Will Formation

U.S. Policy Tools

Serial No. 116-55 House Hearing - Russian Disinformation Attacks on Elections: Lessons from Europe

"Serial No. 116-55 House Hearing - Russian Disinformation Attacks on Elections: Lessons from Europe" points out the need for social media companies to continuously clean their platforms and address the issue of algorithmic bias (U.S. Government Publishing Office 2019). The hearing calls on social media platforms to *"[establish] common transparency standards to deal with suspicious accounts or deceptive sites, and reassessing online anonymity"* (p. 14). The hearing also calls on the Administration and Congress to adhere to *"the principles of transparency and authenticity on social media"* rather than engage in censorship or content control (p. 6). The committee suggests mandating standard definitions of an impersonator and inauthentic accounts across social media companies and exploring ways to counter the algorithmic bias.

The U.S. Surgeon General's Advisory on Building a Healthy Information Environment

Turning to "The U.S. Surgeon General's Advisory on Building a Healthy Information Environment", there are several references that describe actions taken by researchers, media organizations, and technology platforms, such as identifying misinformation "super-spreaders", devoting resources to debunk misinformation, and improving efforts to monitor and address misinformation, all of which are aimed at ensuring users have access to accurate information (Office of the U.S. Surgeon General 2021). The Surgeon General calls on journalists and media organizations to *"provide the public with context to avoid skewing their perceptions about ongoing debates on health topics"* (p. 11). They also suggest avoiding shocking or provoking headlines in leu of headlines that inform the reader, asking them to *"lead with the truth instead of simply repeating details of the rumor"* (p. 11).

S.1231 - SAD Act

The "SAD Act" contributes to collective agenda and will formation by providing the public with accurate and credible information about reproductive health services (SAD Act 2023). It aims to combat disinformation in the advertising of abortion services to facilitate informed public discourse around abortion services and access, helping citizens to formulate an informed opinion on these topics. The prohibitions against deceptive

advertising further promote transparency and accuracy of information, which are crucial for collective agenda.

S.406 – Promoting Public Health Information Act

The Promoting Public Health Information Act establishes the Public Health Information and Communications Advisory Committee for making recommendations and reporting on critical aspects of communication and *"dissemination of scientific and evidence-based public health information during public health emergencies"* (Promoting Public Health Information Act 2023, p. 2). The act aims to ensure the public is aware of the importance of both *"the role and impact of misinformation on the response to such public health emergencies [and] the role of risk communication before and during such public health emergencies"* (p. 2). Through these efforts, the committee contributes to a collective agenda and will formation by promoting transparency and ensuring the public is equipped with scientifically-backed information, facilitating informed public discourse.

S.3608 – Social Media NUDGE Act

Finally, the Social Media NUDGE Act seeks to inform public will and agenda formation among social media platform users through enhanced transparency in how user data is used and how information is presented on these platforms (Social Media NUDGE Act 2022). By promoting accurate information about data usage and algorithmic transparency, the Act supports informed public discourse about digital privacy and the role of social media platforms in society.

EU Policy Tools

Communication - Tackling online disinformation: a European approach

This document reiterates the indispensable role of media and transparency in democratic societies. It holds that media helps keep public authorities accountable while providing the information citizens need to form their own views on societal issues and participate actively and effectively in democracy (European Commission 2018b). This sentiment is captured in the statement, *"Media have traditionally played a key role in holding public authorities to account and in providing the information that enables citizens to form their own views on societal issues and actively and effectively participate in democratic society"* (p. 1). In enhancing transparency, the document underscores the necessity to improve the understanding of the origin of information and how it is produced, sponsored, disseminated, and targeted, thus enabling citizens to assess content they access online, highlighting potential attempts at manipulation.

A multi-dimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation

The importance of transparency in addressing digital disinformation is emphasized in this document. It articulates that transparency in news production and distribution can help users differentiate between journalistic quality content and disinformation (European Commission and Directorate-General for Communications Networks 2018). This assertion is found in the statement, *"Transparency is a key element in the response to digital disinformation. It is a cross-cutting issue that concerns the whole digital media value chain and aims at making news production and distribution less opaque with a view to supporting users' ability to better discern between journalistic quality content and various kinds of disinformation"* (p. 22). Moreover, the document advocates for platforms to enhance the visibility of reliable news and provide user-friendly tools to connect with trusted fact-checking sources, thereby empowering users in the democratic process of collective agenda and will formation.

Flash Eurobarometer 464 Fake news and disinformation online

This survey report reveals that European citizens express concern over media independence, and their trust levels in media, especially online sources, are low (European Union 2018). The data suggest that respondents trust traditional media more than their online counterparts, a sentiment that is presented in the statement, A significant proportion of survey participants express complete or partial trust in the news and information delivered through radio (70%), television (66%), and print media (63%). Conversely, less than half of the respondents (47%) place their trust in online newspapers and magazines. Interviewee 2 highlights that readers of traditional media may also be more vulnerable to disinformation due to their lack of exposure to disinformation on social media. This trust declines even further for video hosting websites and podcasts (27%), as well as for online social networks and messaging apps (26%). These findings indicate the challenges and uncertainties citizens face in the digital age when forming collective agendas and wills, further underlining the need for enhanced transparency and media literacy.

2018 Code of Practice on Disinformation

In this document, several commitments are set forth by the signatories to counter disinformation, focusing on enhancing transparency, ensuring authenticity, and promoting accuracy (European Commission 2018e). The document suggests various strategies, such as closing fake accounts, establishing clear rules for bots, prioritizing authentic and accurate information in search feeds, and disrupting advertising incentives

for misrepresenting information. One prominent commitment states, *"Relevant Signatories will use commercially reasonable efforts to implement policies and processes; not to accept remuneration from, or otherwise promote accounts and websites which consistently misrepresent information about themselves"* (p. 4). These commitments and actions are geared towards fostering an informed and accurate public discourse, a cornerstone of collective agenda and will formation.

5.3.3 Collective Decision-Making

U.S. Policy Tools

PSA: Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections

In the "PSA: Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections", both the Federal Bureau of Investigation and the CISA provide recommendations to avoid foreign influence in the 2022 U.S. midterm elections. They state, "*For information about registering to vote, voting, and election results, rely on state and local government election officials"* (Cybersecurity and Infrastructure Security Agency 2022, p. 2). They also encourage voters to be cautious of *"websites not affiliated with local or state government that solicit voting information, like voter registration information"* and to use websites that end in the ".gov" domain instead (p. 2). Furthermore, the FBI reminds voters to report any suspected election crimes, including *"intentional disinformation about the manner, time, or place of voting,"* to the nearest FBI Field Office (p. 2).

H.R.2599 - Honest Ads Act

Of the legislature presented above, the Honest Ads Act contains the most references to strengthening and securing the key collective decision-making process of a democratic society: elections. The act enhances transparency and accountability for online political advertisements, empowering citizens to make informed decisions in democratic elections. It highlights the need for voters to have access to *"information about the true and original source of money given, transferred, and spent on political advertisements made online"* (Honest Ads Act 2023, p. 3) and the importance of such disclosure to inform the voting public and enable the Federal Election Commission and the Department of Justice to detect and prosecute illegal foreign spending and other campaign finance violations.

The Act acknowledges social media platforms *"can target portions of the electorate with direct, ephemeral advertisements often on the basis of private information the platform has on individuals, enabling political advertisements that are contradictory, racially or*

socially inflammatory, or materially false" (p. 5). The Act aims to ensure the voting public has complete information about who is trying to influence their votes and to aid enforcement of other laws, including the prohibition of foreign money in domestic campaigns.

CISA

In CISA's strategic plan, Objective 2.6 supports risk management to enhance election infrastructure security (Cybersecurity & Infrastructure Security Agency 2022). This support has evolved alongside the disinformation risk landscape and includes *"contextualizing existing resources and capabilities for effective application to the Election Infrastructure Subsector's risk management activities"* (p. 22). Insights gathered from federal partners such as the FBI, the U.S. Election Assistance Commission, and the Intelligence Community *"drive the development of innovative solutions that improved its ability to respond to election stakeholder needs"* (p. 22). CISA's efforts have resulted in two key representative outcomes:

1. *CISA's services, products, and guidance are responsive to stakeholder needs and improve iteratively based on its evolving understanding of risks to election infrastructure;* and

2. *Lessons learned from risk and vulnerability trends are applied across the Election Infrastructure Subsector* (p. 22). '

To account for the impact of these outcomes, CISA will take part in measuring its reach to state, local, tribal, and territorial (SLTT) governments and private sector election stakeholders *"with products and guidance appropriate for their risk profile and organizational capabilities"* (p. 22).

EU Policy Tools

Communication - Tackling online disinformation: a European approach

This document presents disinformation as a factor that *"erodes trust in institutions and in digital and traditional media, and harms our democracies by hampering the ability of citizens to take informed decisions"* (European Commission 2018b, p. 1). It underscores the role of disinformation in disrupting *"election processes, in particular in combination with cyberattacks"* (p. 2). A European approach is suggested to handle the cross-border nature of online disinformation, ensuring *"effective and coordinated action"* to protect EU institutions and its citizens (p. 3). The document also promotes the diversity of information to facilitate informed decisions based on critical thinking. Notably, the

document outlines the use of disinformation as a tool for manipulating electoral processes, requiring concerted efforts for detection and response.

Communication on the European democracy action plan

The document outlines the intent to propose a new EU mechanism to *"support resilient electoral processes"* and deal with issues like *"the cybersecurity of elections and online forensics"* (European Commission 2020a, p. 6). The Commission identities social media as one of the key channels *"for attempts to manipulate public opinion, discourage participation in elections and cast doubt on the integrity of election processes"* (p. 3). The Commission also aims to foster better cooperation between Member States and regulatory authorities on achieving balanced media coverage during elections. An action plan is mentioned, including creating a joint operational mechanism for promoting resilient electoral processes and protective measures against cyber-attack threats. Additionally, two key actions are identified to protect election integrity and promote democratic participation by (1) planning to introduce legislation in 2021 that will increase transparency surrounding financially-backed political content (also known as 'political advertising') and (2) implementing aid measures and guidance for political parties and Member States.

European Democracy Action Plan - making EU democracies stronger Press Release

This press release emphasizes enabling citizens to freely express their views and make informed decisions, distinguishing facts from fiction in an open debate (European Commission 2020b). It also reveals plans to propose legislation regarding the transparency of sponsored political content and revise the rules for financing European political parties. It emphasizes the need for active citizen participation during elections and as a continual part of the democratic process. It vows to *"organise a high-level event bringing together various authorities to address the challenges related to electoral processes as well as empowering citizens to participate as voters and candidates in the democratic process"* (para. 8). The Action Plan suggests enhancing the current EU's resources to combat external interference, incorporating novel tools designed to levy penalties on offenders. The Commission aims to transform the Code of Practice on Disinformation into a joint regulatory structure which holds online platforms accountable and is consistent with the impending Digital Services Act. For this purpose, the Commission plans to release guidelines to fortify the Code of Practice in spring 2021 and establish a sturdier framework for overseeing its enforcement. Additionally, the Commission and the High Representative intend to implement extra measures to boost the resilience of our societies and encourage global collaborations.

6 Comparison of U.S. and EU Disinformation Policy Perspectives

This research aimed to provide a comprehensive understanding of how governments, particularly the U.S. and the EU, counter the rising menace of disinformation and its potential implications on democratic institutions and processes. This discussion summarizes the findings, situating them in the context of the research questions and objectives outlined at the onset of this study.

To adequately address the primary research question – *how are governments responding to the threat of disinformation as a means of undermining democracy?* – a dual-faceted approach was adopted. First, the disinformation threat landscape was analyzed, and second, the disinformation policy responses of the U.S. and the EU were analyzed.

6.1 Disinformation Threat Landscape

Starting with the first objective, following an in-depth literature review and analysis of policy responses, the research has demonstrated that disinformation poses a significant threat to the institutional and procedural dimensions of democratic governance. Disinformation, misinformation, and online propaganda disseminated on social media platforms can severely compromise collective intelligence, agenda-setting, and decision-making processes, key pillars that uphold democratic societies (Warren 2017).

Disinformation acts as a corrosive agent, eroding public trust in institutions, invoking social divisions, and impairing the public's ability to make informed decisions. This, in turn, threatens the vitality of democratic governance as it undermines the premise of an informed citizenry, which is essential for the effective functioning of a democracy. Disinformation also exacerbates societal polarization and discord, contributing to instability and weakening the social fabric (The Lancet 2020). These effects illustrate how disinformation can be a strategic tool in the hands of malicious actors aiming to destabilize democratic societies.

6.2 Disinformation Policy Instruments and Responses: the U.S. vs the EU

The second objective of the research was to analyze the disinformation policy tools implemented in the U.S. and the EU. Both entities have exhibited awareness and responsiveness to the disinformation threats, as reflected in their deployment of various policy tools. These range from legislative measures to strategic communication efforts and codes of practice, all of which aim to reinforce democratic processes' integrity against the onslaught of disinformation.

6.2.1 Comparison of U.S. and EU Nodality Tools

The EU and U.S. both use nodality, i.e., the utilization of their central position in a network to gather and disseminate information. However, they differ in their initiatives' specific tactics and focus.

U.S.'s Approach to Nodality

The U.S. takes a slightly different approach with nodality, using it more for group-targeted messaging than broad public communication. Congressional hearings like "Russian Disinformation Attacks on Elections: Lessons from Europe" and "Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation" are indicative of this approach (House of Representatives 2021; U.S. Government Publishing Office 2019). These hearings are not merely disseminating information but are also forums for questioning and accountability, igniting political discussion and the policymaking process.

EU's Approach to Nodality

The EU frequently employs direct notification as a nodality tool. For example, the "Action Plan on Strategic Communication" and "Communication Action Plan Against Disinformation" demonstrate this by outlining structured communication blueprints to tackle disinformation (European Commission 2018c; European External Action Service 2015). Direct notification is also seen in the establishment of a special committee on foreign interference in democratic processes, further emphasizing the EU's commitment to sharing information openly.

The EU also utilizes prompted query responses, like establishing the EUvsDisinfo platform, which offers a searchable database to counter disinformation narratives (EUvsDisinfo n.d.). Public opinion surveys and public consultations, like the Flash Eurobarometer 464 and the public consultation on fake news and online disinformation, show that the EU values feedback from the public in formulating its policies (European Commission 2018d; European Union 2018).

The EU appears to be more proactive in directly notifying the public about disinformation and soliciting their input, while the U.S. focuses more on targeted discussions within specific groups. Both approaches have their merits: the EU's approach may be more effective at promoting public awareness, while the U.S.'s approach can facilitate deeper, more focused discussions.

6.2.2 Comparison of U.S. and EU Authority Tools

Both the U.S. and EU use authority tools, i.e., their ability to enact legislation and regulations. However, their approaches diverge considerably.

U.S.'s Approach to Authority

Contrarily, the U.S.'s approach to authority is predominantly legislative. Numerous acts and executive orders, such as "S.3274 - Countering Foreign Propaganda and Disinformation Act" and "Executive Order 13721-Developing an Integrated Global Engagement Center," demonstrate a preference for regulatory measures (Executive Order No. 13721 2016; Countering Foreign Propaganda and Disinformation Act 2016). They show a strong reliance on legislative action to counteract disinformation.

EU's Approach to Authority

The EU's approach to authority is marked by a balance between regulatory measures and encouraging voluntary adherence. For instance, the Code of Practice on Disinformation, issued in 2018 and later strengthened in 2022, acts as a voluntary framework for major tech companies to commit to reducing disinformation (European Commission 2018e, 2022a). On the other hand, they have also utilized regulations like the Digital Services Act, suggesting a willingness to use authoritative measures when needed (European Parliament and Council of the European Union 2022). Interviewee 1 suggests that this may stem from voluntary efforts not achieving the results expected in addressing disinformation on large social media platforms.

The EU leans more towards voluntary frameworks and collaboration with private entities, whereas the U.S. prefers legislation and executive orders. The EU's approach can foster cooperation but might face limitations if companies do not adhere to voluntary guidelines. The U.S.'s approach ensures compliance but might lead to criticism over freedom of speech.

6.2.3 Comparison of EU and U.S. Organization and Treasure Tools

Organizational and treasure tools represent physical resources, financial assets, and the structure of organizations. The EU and U.S. both use these tools but differ in their implementation.

U.S.'s Approach to Organization and Treasure

The U.S., similar to the EU, has established specific entities like the Global Engagement Center and proposed task forces such as the COVID–19 Misinformation and

Disinformation Task Force (COVID–19 Misinformation and Disinformation Task Force Act of 2020 2020; U.S. Department of State n.d.). However, they also tie disinformation countermeasures into broader legislative efforts, as seen in acts like the National Defense Authorization Act for Fiscal Year 2017 and 2019, which includes provisions and funding aimed at establishing and increasing the responsibilities of specific organisations, such as the GEC, in order to counter disinformation (John S. McCain National Defense Authorization Act for Fiscal Year 2019 2018; National Defense Authorization Act for Fiscal Year 2017 2016).

EU's Approach to Organization and Treasure

The EU often sets up specific entities or funds projects to address disinformation, like the East StratCom Task Force, Social Observatory for Disinformation and Social Media Analysis, and RAS (European Commission 2022b; European External Action Service 2019, 2021). These tools showcase the EU's approach of creating specialized bodies and funding research to handle disinformation.

While both the EU and the U.S. set up specialized entities, the EU appears to focus more on funding specific projects and research. The U.S., on the other hand, often ties their organizational efforts into broader legislative packages related to military funding.

6.2.4 Key Differences in Policy Responses to Disinformation

In the U.S., legislation has been a key component of the policy response to disinformation. Proposed acts such as the Honest Ads Act, SAD Act, and Promoting Public Health Information Act, while not yet legally binding, represent a legislative commitment and active political discourse aimed to address the disinformation challenge head-on (*Honest Ads Act* 2023; *Promoting Public Health Information Act* 2023; *SAD Act* 2023). These bills focus on fostering transparency, ensuring data security, and promoting accurate information dissemination, all crucial to combating disinformation.

Upon a closer examination, the study reveals critical differences between the U.S. and the EU in their policy responses to disinformation. The U.S. tends to prioritize legislative proposals and laws that mandate transparency and data security. The emphasis is on rules and regulations that protect the integrity of information, especially in the sphere of political advertising, which is evident in its application of a total of seven tools of authority compared to the EU's use of four tools of authority. Interviewee 5 points out that discourse surrounding the topic of disinformation remains in a *"bubble"* dominated by elites in educational institutions such as Harvard and bureaucrats in political institutions.

The EU, on the other hand, has a slightly different approach, characterized by collaborative efforts and joint communication between the various EU institutions and EU citizens, emphasis on media literacy, and strengthening the regulatory environment. The EU's policy tools, such as the Code of Practice on Disinformation and the European Democracy Action Plan, underscore the importance of transparency, media literacy, and credibility of news sources. These efforts reflect a more holistic approach that acknowledges the complex and multi-faceted nature and need for a whole-of-society approach to conquer the disinformation challenge.

The EU's approach leans more toward a combination of regulation, collaboration, and public education, invoking a total of eleven tools of nodality. Interviewee 3 highlights that disinformation campaigns can be tailored to *"specific demographics"*; therefore, all members of civil society must be addressed. Thus, the EU policies stress collaboration among all stakeholders, enhancing media literacy, and refining the regulatory environment. The EU's approach acknowledges the intertwined nature of the digital information ecosystem, suggesting that an effective response requires not just regulation, but also cooperation and education.

6.3 Best Practices and Future Directions

This research's third and final objective was to extract and extrapolate best practices from the disinformation policies of the U.S. and the EU, highlighting the most successful strategies for navigating the increasingly complex landscape of disinformation and democracy.

A critical element in the battle against disinformation, as indicated by the policy responses of both the U.S. and the EU, is the principle of transparency. This extends across multiple facets of the digital environment, with concrete instances of its implementation found in policies and initiatives to enhance public trust and accountability. For instance, the Honest Ads Act in the U.S. imposes rigorous transparency requirements on digital political advertisements, mandating platforms to disclose who paid for the ads and whom they are targeted at (Honest Ads Act 2023). This transparency enables users to evaluate the credibility and potential biases of the information they consume, reinforcing democratic discourse. The EU's Code of Practice on Disinformation also emphasizes transparency, specifically around algorithmic processes and data collection (European Commission 2018e, 2022a). By demanding that signatories provide clearer explanations about how algorithms rank and recommend news, the code encourages the digital platforms to be more open about their operations, allowing users to understand better how information is curated and presented to them.

Collaboration, both within and across national borders, emerges as a second critical best practice. The EU's Action Plan against Disinformation epitomizes this approach, involving collaboration at various levels. It calls for an operational task force, comprised of representatives from member states, to detect and respond to disinformation. It also advocates for a more robust partnership between public authorities and the private sector and stresses the importance of sharing insights and strategies with international partners (European Commission 2018c). The U.S. SAD Act echoes the necessity of a coordinated response, mandating a whole-of-society approach involving both public and private stakeholders in order to tackle disinformation effectively (SAD Act 2023). Interviewee 2 corroborates these findings stating that, *"if the users are not aware and knowledgeable about the dangers, about online disinformation, then then all these steps taken by other stakeholders will be in vain."* This underlines the importance of shared responsibilities and collaborative solutions in combating the complex, cross-border challenge of disinformation.

The importance of public education and media literacy, particularly in the digital age, is a recurring theme in the policies of both entities. For example, the EU's European Democracy Action Plan highlights the need for improved media literacy as a proactive measure against disinformation, fostering a more discerning public capable of critically analyzing digital content (European Commission 2020b). Interviewee 1, however, points out that while these media literacy campaigns can be promoted at the EU level, they cannot be imposed on member states due to the treaties of the EU. Similarly, the U.S. Promoting Public Health Information Act emphasizes the role of education, mandating the Department of Health and Human Services to conduct a national awareness campaign about the importance of factual health information (Promoting Public Health Information Act 2023). However, like the EU, it is mainly the responsibility of local state-level governments within the U.S. to implement media literacy initiatives in school curriculums. These initiatives underline the importance of equipping citizens with the skills to differentiate between reliable information and disinformation, reinforcing the resilience of democratic processes.

The final best practice centers around the necessity for proactive, adaptable strategies. Interviewee 4 acknowledges that technological developments, such as those related to AI, allow for *"disinformation actors to use this technology to amplify their messages."* Given the rapidly evolving digital landscape, policies combating disinformation must remain dynamic and flexible, ready to adapt to new forms and techniques of disinformation. For instance, the European Democracy Action Plan's commitment to regularly reviewing the Code of Practice on Disinformation reflects this ethos of adaptability, ensuring that the Code remains effective against new disinformation threats (European Commission 2018e,

2020b). Similarly, the U.S. Honest Ads Act's provision for the Federal Election Commission to review and revise the regulations periodically demonstrates an understanding that strategies must evolve to keep pace with technological advancements and changing disinformation tactics (Honest Ads Act 2023).

In conclusion, the analysis of U.S. and EU policy responses to disinformation illuminates four best practices: (1) prioritizing transparency; (2) fostering collaboration; (3) enhancing public education and media literacy; and (4) adopting proactive, adaptable strategies. These practices are significant in the current struggle against disinformation and crucial for informing future policy development in the context of digital disinformation and its impact on democratic processes. Additionally, future research could explore more in-depth the policy response tools identified in this study and form comparisons with other democratic nations to determine whether other tools implemented within other nations should also be taken into consideration. It will also be important to revist the topic once future regulations and proposed acts in the U.S. and the EU have been legally adopted in order to evaluate their efficacy at addressing the threats of disinformation.

7 Conclusion

This research identifies a taxonomy of the strategies and tools employed by the U.S. and EU in response to the threat of disinformation as a means of undermining democracy. This is achieved by conducting a content analysis of policy documents and publications from public institutions in the U.S. and EU, and the findings are supplemented and corroborated by five semi-structured expert interviews. With the intent to answer the research question: *How are governments responding to the threat of disinformation as a means of undermining democracy* and three subquestions, a comprehensive comparative analysis was conducted focusing on three primary areas: the threats disinformation poses to democracy, the specific policy actions taken by the U.S. and EU, and the best practices that could guide future disinformation policy development.

The first sub-question, *what threats do disinformation, misinformation, and online propaganda pose to democracy,* was answered in the literature review and systematic analysis of the policy tools, which identified the challenge disinformation presents to democratic processes, with detrimental effects on public empowerment, political discourse and opinion development, and stability of democratic decision-making processes. Utilizing digital technologies and large social media platform ecosystems, disinformation has become a convoluted issue requiring a multi-faceted and whole-of-society response.

For the second sub-question, *what specific policy actions have the U.S. and the European Union taken in response to these threats,* the investigation of specific policy actions revealed the diversity of strategies and tools employed by the U.S. and EU. The U.S. has introduced legislative measures such as the Honest Ads Act and Countering Foreign Propaganda and Disinformation Act, both of which emphasize the transparency in digital political advertising and the responsibility of digital platforms to combat disinformation. On the other hand, the EU's approach has been collaborative and wide-ranging, emphasizing the education of all stakeholders involved in the digital ecosystem as echoed in communications such as the European Democracy Action Plan and the Code of Practice on Disinformation, both of which underscore public-private partnerships, media literacy, and international cooperation.

Finally, in response to the third sub-question, *what best practices can be construed and applied to future developments in disinformation policies,* four key best practices were extrapolated from the examined policies: transparency, collaboration, public education and media literacy, and adaptability. Each of these practices was observed to be integral to a robust and effective disinformation policy. Transparency bolsters trust and empowers citizens. Collaboration amplifies the impact of collective resources and expertise. Public

education enhances media literacy, enabling citizens to actively participate in democratic resilience. The need for adaptability emphasizes that disinformation policies must evolve alongside the ever-changing digital landscape.

The findings of this research contribute a nuanced analysis and taxonomy of policy instruments employed by the U.S. and the EU that can serve as a valuable point of reference both in comparative policy research and disinformation-related policymaking processes. It is important to note that these findings suggest that while the U.S. and EU policies may offer valuable guidance, the battle against disinformation mandates continuous vigilance, innovation, and global cooperation of the public sector, private sector, civil society and international partnerships. These findings also serve as a reminder that as the digital landscape continues to develop, efforts to maintain the integrity of democratic processes must adapt and expand to counter the disruptive influence of disinformation.

References

Agudo, U., and Matute, H. 2021. "The Influence of Algorithms on Political and Dating Decisions," *PLOS ONE* (16:4), Public Library of Science, p. e0249454. (https://doi.org/10.1371/JOURNAL.PONE.0249454).

Akram, W., and Kumar, R. 2017. "A Study on Positive and Negative Effects of Social Media on Society," *International Journal of Computer Sciences and Engineering* (5:10), ISROSET: International Scientific Research Organization for Science, Engineering and Technology, pp. 351–354. (https://doi.org/10.26438/IJCSE/V5I10.351354).

Allan, G. 2020. "Qualitative Research," *Handbook for Research Students in the Social Sciences*, Routledge, pp. 177–189. (https://doi.org/10.4324/9781003070993-18).

Allcott, H., and Gentzkow, M. 2017. "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* (31:2), American Economic Association, pp. 211–36. (https://doi.org/10.1257/JEP.31.2.211).

Andersen, J., and Siim, B. 2004. "Introduction: The Politics of Inclusion and Empowerment — Gender, Class and Citizenship," *The Politics of Inclusion and Empowerment*, Palgrave Macmillan, London, pp. 1–18. (https://doi.org/10.1057/9781403990013_1).

Arias, E., Cloward, K., Lonardo, L. Di, Egan, P., Gottlieb, J., Humphreys, M., Lierl, M., Linardi, S., Potter, A., Rosendorff, P., Satyanath, S., Stasavage, D., and Tyson, S. 2019. "How Does Media Influence Social Norms? Experimental Evidence on the Role of Common Knowledge," *Political Science Research and Methods* (7:3), Cambridge University Press, pp. 561–578. (https://doi.org/10.1017/PSRM.2018.1).

Azungah, T. 2018. "Qualitative Research: Deductive and Inductive Approaches to Data Analysis," *Qualitative Research Journal* (18:4), Emerald Group Holdings Ltd., pp. 383–400. (https://doi.org/10.1108/QRJ-D-18-00035/FULL/XML).

Baines, D., and Elliott, R. J. R. 2020. "Defining Misinformation, Disinformation and Malinformation: An Urgent Need for Clarity during the COVID-19 Infodemic," *Discussion Papers of the Department of Economics, University of Birmingham*, Department of Economics, University of Birmingham. (https://ideas.repec.org/p/bir/birmec/20-06.html).

Bartlett, L., and Vavrus, F. 2016. "Rethinking Case Study Research: A Comparative Approach," *Rethinking Case Study Research: A Comparative Approach*, Taylor and Francis Inc., pp. 1–132. (https://doi.org/10.4324/9781315674889).

Beauvais, E., and Warren, M. E. 2019. "What Can Deliberative Mini-Publics Contribute to Democratic Systems?," *European Journal of Political Research* (58:3), John Wiley & Sons, Ltd, pp. 893–914. (https://doi.org/10.1111/1475-6765.12303).

Bemelmans-Videc, M. L., Rist, R. C., and Vedung, E. 2017. "CARROTS, STICKS and SERMONS: Policy Instruments and Their Evaluation," *Carrots, Sticks and Sermons: Policy Instruments and Their Evaluation*, Taylor and Francis, pp. 1–281. (https://doi.org/10.4324/9781315081748).

Berg, S., and Hofmann, J. 2021. "Digital Democracy," *Internet Policy Review* (10:4), Alexander von Humboldt Institute for Internet and Society. (https://doi.org/10.14763/2021.4.1612).

Bertot, J. C., Jaeger, P. T., Munson, S., and Glaisyer, T. 2010. "Social Media Technology and Government Transparency," *Computer* (43:11), pp. 53–59. (https://doi.org/10.1109/MC.2010.325).

Besley, T., and Coate, S. 1997. "An Economic Model of Representative Democracy," *The Quarterly Journal of Economics* (112:1), pp. 85–114. (https://doi.org/10.1162/003355397555136).

De Blasio, E., and Selva, D. 2021. "Who Is Responsible for Disinformation? European Approaches to Social Platforms' Accountability in the Post-Truth Era," *American Behavioral Scientist* (65:6), SAGE PublicationsSage CA: Los Angeles, CA, pp. 825–846. (https://doi.org/10.1177/0002764221989784).

Bohman, J. F. 1990. "Communication, Ideology, and Democratic Theory," *American Political Science Review* (84:1), Cambridge University Press, pp. 93–109. (https://doi.org/10.2307/1963631).

Bohman, James. W. R. 1999. "Deliberative Democracy: Essays on Reason and Politics," *Political Theory* (Vol. 109).

Bolderston, A. 2012. "Conducting a Research Interview," *Journal of Medical Imaging and Radiation Sciences* (43:1), J Med Imaging Radiat Sci, pp. 66–76. (https://doi.org/10.1016/J.JMIR.2011.12.002).

Brkan, M. 2019. "Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting," *Delphi - Interdisciplinary Review of Emerging Technologies* (2:2), Lexxion, pp. 66–71. (https://doi.org/10.21552/DELPHI/2019/2/4).

Brown, N. I. 2020. “Deepfakes and the Weaponization of Disinformation,” *Virginia Journal of Law & Technology* (23). (https://heinonline.org/HOL/Page?handle=hein.journals/vjolt23&id=1&div=&collection=).

Cao, J., Qi, P., Sheng, Q., Yang, T., Guo, J., and Li, J. 2020. “Exploring the Role of Visual Content in Fake News Detection,” in *Disinformation, Misinformation, and Fake News in Social Media. Lecture Notes in Social Networks.*, K. Shu, S. Wang, D. Lee, and H. Liu (eds.), Springer, Cham, pp. 141–161. (https://doi.org/10.1007/978-3-030-42699-6_8/FIGURES/9).

Chesney, R., and Citron, D. 2019. “Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics,” *Foreign Affairs* (98). (https://heinonline.org/HOL/Page?handle=hein.journals/fora98&id=149&div=&collection=).

Christiano, T. 1990. “Freedom, Consensus, and Equality in Collective Decision Making,” *Ethics* (101:1), University of Chicago Press , pp. 151–181. (https://doi.org/10.1086/293265).

Cohen, J. 2005. “DELIBERATION AND DEMOCRATIC LEGITIMACY,” in *Debates in Contemporary Political Philosophy* (1st Edition.), Routledge, pp. 352–370. (https://doi.org/10.4324/9780203986820-28).

Colomina, C., Sánchez Margalef, H., and Youngs, R. 2021. “The Impact of Disinformation on Democratic Processes and Human Rights in the World | Think Tank | European Parliament,” , April. (https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653635).

Crabtree, B. F., and Miller, W. L. 1999. *Doing Qualitative Research*, London: Sage Publications. (https://books.google.com/books/about/Doing_Qualitative_Research.html?id=MEd2AwAAQBAJ).

Cybersecurity & Infrastructure Security Agency. 2022. “2023-2025 Strategic Plan | CISA,” , September. (https://www.cisa.gov/strategic-plan).

Cybersecurity and Infrastructure Security Agency. 2022. “PSA: Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections | CISA,” , October 6. (https://www.cisa.gov/resources-tools/resources/psa-foreign-actors-likely-use-information-manipulation-tactics-2022).

Cyberspace Solarium Commission. 2020. “Cyberspace Solarium Commission - March 2020 Final Report,” , March. (https://www.solarium.gov/#h.p_rK7mL_1MeZw7).

Cyberspace Solarium Commission. 2021. “Countering Disinformation in the United States,” *Cyberspace Solarium Commission White Paper #6*, , December. (https://www.solarium.gov/public-communications/disinformation-white-paper, accessed May 19, 2023).

Dahl, R. A. 1998. *On Democracy*, Yale University Press.

Dame Adjin-Tettey, T. 2022. “Combating Fake News, Disinformation, and Misinformation: Experimental Evidence for Media Literacy Education,” *Cogent Arts & Humanities* (9:1), Cogent. (https://doi.org/10.1080/23311983.2022.2037229).

Dan, V., Paris, B., Donovan, J., Hameleers, M., Roozenbeek, J., van der Linden, S., and von Sikorski, C. 2021. “Visual Mis- and Disinformation, Social Media, and Democracy,” *Journalism and Mass Communication Quarterly* (98:3), SAGE Publications Inc., pp. 641–664. (https://doi.org/10.1177/10776990211035395/ASSET/IMAGES/LARGE/10.1177_10776990211035395-FIG2.JPEG).

Danto, E. 2008. *Historical Research: Pocket Guides to Social Work Research Methods*, New York: Oxford University Press.

Dawes, S. S. 2009. “Governance in the Digital Age: A Research and Action Framework for an Uncertain Future,” *Government Information Quarterly* (26:2), JAI, pp. 257–264. (https://doi.org/10.1016/J.GIQ.2008.12.003).

Dell, M. 2019. “Fake News, Alternative Facts, and Disinformation: The Importance of Teaching Media Literacy to Law Students,” *Touro Law Review* (35). (https://heinonline.org/HOL/Page?handle=hein.journals/touro35&id=635&div=&collection=).

Dewan, S., and Ramaprasad, J. 2014. “Social Media, Traditional Media, and Music Sales,” *MIS Quarterly* (38:1), pp. 101–121. (https://www.jstor.org/stable/26554870).

DiStaso, M. W., and Bortree, D. S. 2012. “Multi-Method Analysis of Transparency in Social Media Practices: Survey, Interviews and Content Analysis,” *Public Relations Review* (38:3), JAI, pp. 511–514. (https://doi.org/10.1016/J.PUBREV.2012.01.003).

Enslin, P., Pendlebury, S., and Tjattas, M. 2001. “Political Inclusion, Democratic Empowerment and Lifelong Learning,” *International Handbook of Lifelong Learning*, Springer, Dordrecht, pp. 61–78. (https://doi.org/10.1007/978-94-010-0916-4_4).

European Commission. 2018a. “Periodic Reporting for Period 2 - InVID (In Video Veritas – Verification of Social Media Video Content for the News Industry) | H2020 | CORDIS | European Commission,” , December 31. (https://cordis.europa.eu/project/id/687786/reporting, accessed May 20, 2023).

European Commission. 2018b. “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling Online Disinformation: A European Approach, COM/2018/236 Final,” Brussels, April 26. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236).

European Commission. 2018c. “JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Action Plan against Disinformation, JOIN/2018/36 Final,” Brussels, December 5. (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1615890082555&uri=CELEX%3A52018JC0036).

European Commission. 2018d. “Synopsis Report of the Public Consultation on Fake News and Online Disinformation | Shaping Europe’s Digital Future,” *Consultation Results | Publication 26 April 2018*, , April 2018. (https://digital-strategy.ec.europa.eu/en/library/synopsis-report-public-consultation-fake-news-and-online-disinformation, accessed May 21, 2023).

European Commission. 2018e. *2018 Code of Practice on Disinformation*, Brussels: European Commission. (https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation).

European Commission. 2020a. “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS On the European Democracy Action Plan, COM/2020/790 Final,” Brussels, December 3. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423).

European Commission. 2020b. “European Democracy Action Plan,” *European Democracy Action Plan: Making EU Democracies Stronger*, , December 3. (https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250, accessed May 21, 2023).

European Commission. 2021. “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, European Commission Guidance on Strengthening the Code of Practice on Disinformation,” Brussels, May 26. (https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation).

European Commission. 2022a. “2022 Strengthened Code of Practice on Disinformation,” Brussels, June. (https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation).

European Commission. 2022b. “Periodic Reporting for Period 2 - SOMA (Social Observatory for Disinformation and Social Media Analysis) | H2020 | CORDIS | European Commission,” , February 25. (https://cordis.europa.eu/project/id/825469/reporting, accessed May 27, 2023).

European Commission. (n.d.). “Horizon 2020,” *Funding Programmes and Open Calls: Horizon 2020*. (https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en, accessed May 27, 2023).

European Commission, and Directorate-General for Communications Networks, C. and T. 2018. *A Multi-Dimensional Approach to Disinformation : Report of the Independent High Level Group on Fake News and Online Disinformation*, Publications Office. (https://doi.org/doi/10.2759/739290).

European Council. 2015. “European Council, 19-20 March 2015,” *European Council Conclusions, 19-20 March 2015*, , March 19. (https://www.consilium.europa.eu/en/meetings/european-council/2015/03/19-20/, accessed May 20, 2023).

European Digital Media Observatory. (n.d.). “EDMO at a Glance – EDMO.” (https://edmo.eu/edmo-at-a-glance/#page, accessed May 27, 2023).

European External Action Service. 2015. “Action Plan on Strategic Communication.”

European External Action Service. 2019. “Factsheet: Rapid Alert System | EEAS,” , March 15. (https://www.eeas.europa.eu/node/59644_en).

European External Action Service. 2021. “Countering Disinformation: Questions and Answers about the East StratCom Task Force | EEAS,” , October 27. (https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en, accessed May 27, 2023).

European Parliament. 2020a. *P9_TA(2020)0161, Setting up a Special Committee on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation, and Defining Its Responsibilities, Numerical Strength and Term of Office*, Brussels: European Parliament. (https://www.europarl.europa.eu/doceo/document/TA-9-2020-0161_EN.html).

European Parliament. 2020b. *European Parliament Decision of 18 June 2020 on Setting up a Special Committee on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation, and Defining Its Responsibilities, Numerical Strength and Term of Office*

(2020/2683(RSO)), Brussels: European Parliament. (https://www.europarl.europa.eu/doceo/document/TA-9-2020-0161_EN.html).

European Parliament. 2022. "Special Committee on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation," , April 28. (https://www.europarl.europa.eu/committees/en/inge/home/highlights, accessed May 27, 2023).

European Parliament. (n.d.). "Eurobarometer." (https://www.europarl.europa.eu/at-your-service/en/be-heard/eurobarometer, accessed May 21, 2023).

European Parliament, and Council of the European Union. 2022. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014).

European Union. 2018. "Flash Eurobarometer 464 - Fake News and Disinformation Online," , April. (https://europa.eu/eurobarometer/surveys/detail/2183).

EUvsDisinfo. (n.d.). "About - EUvsDisinfo." (https://euvsdisinfo.eu/about/?_gl=1*kgy8zt*_up*MQ..*_ga*MTAzMjY3MTI0Mi4xNjgyODYyMDcx*_ga_9SH0NZ5558*MTY4Mjg2MjA3MS4xLjAuMTY4Mjg2MjA3MS4wLjAuMA.., accessed May 27, 2023).

Executive Order No. 13721, 81 Fed. Reg. 2016. pp. 14685–14688. (https://www.federalregister.gov/documents/2016/03/17/2016-06250/developing-an-integrated-global-engagement-center-to-support-government-wide-counterterrorism).

Fereday, J., and Muir-Cochrane, E. 2006. "Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development," *International Journal of Qualitative Methods* (5:1). (https://doi.org/10.1177/160940690600500107).

Ferrara, E. 2017a. "Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election," *First Monday* (22:8), First Monday. (https://doi.org/10.5210/FM.V22I8.8005).

Ferrara, E. 2017b. "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election," *First Monday* (22:8), First Monday. (https://doi.org/10.5210/fm.v22i8.8005).

Fletcher, R., Cornia, A., Graves, L., and Nielsen, R. K. 2018. "Measuring the Reach of 'Fake News' and Online Disinformation in Europe," *Australasian Policing* (10:2), Pascoe Vale South,, VIC, Australia: Australasian Institute of Policing, p. 25. (https://search.informit.org/doi/10.3316/informit.807732061612771).

Freeman, J. 2016. "Digital Civic Participation in Australian Local Governments: Everyday Practices and Opportunities for Engagement," in *Social Media and Local Governments* (Vol. 15), M. Sobaci (ed.), Springer, Cham, pp. 195–218. (https://doi.org/10.1007/978-3-319-17722-9_11/TABLES/3).

García-Orosa, B. 2021. "Disinformation, Social Media, Bots, and Astroturfing: The Fourth Wave of Digital Democracy," *Profesional de La Información* (30:6), El Profesional de la Informacion, pp. 1699–2407. (https://doi.org/10.3145/EPI.2021.NOV.03).

Gingras, A. M. 2012. "Access to Information: An Asset for Democracy or Ammunition for Political Conflict, or Both?," *Canadian Public Administration* (55:2), John Wiley & Sons, Ltd, pp. 221–246. (https://doi.org/10.1111/J.1754-7121.2012.00215.X).

Golafshani, N. 2003. "Understanding Reliability and Validity in Qualitative Research," *The Qualitative Report* (8:4), Nova Southeastern University, pp. 597–606. (https://doi.org/10.46743/2160-3715/2003.1870).

Goodin, R. E. 2007. "Enfranchising All Affected Interests, and Its Alternatives," *Philosophy & Public Affairs* (35:1), John Wiley & Sons, Ltd, pp. 40–68. (https://doi.org/10.1111/J.1088-4963.2007.00098.X).

Goodman, E. 2021. "Media Literacy in Europe and the Role of EDMO," , September. (https://edmo.eu/wp-content/uploads/2022/02/Media-literacy-in-Europe-and-the-role-of-EDMO-Report-2021.pdf).

Guess, A., Nagler, J., and Tucker, J. 2019. "Less than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook," *Science Advances* (5:1), Sci Adv. (https://doi.org/10.1126/SCIADV.AAU4586).

Hajli, N., Saeed, U., Tajvidi, M., and Shirazi, F. 2022. "Social Bots and the Spread of Disinformation in Social Media: The Challenges of Artificial Intelligence," *British Journal of Management* (33:3), John Wiley & Sons, Ltd, pp. 1238–1253. (https://doi.org/10.1111/1467-8551.12554).

Halpern, D., and Gibbs, J. 2013. "Social Media as a Catalyst for Online Deliberation? Exploring the Affordances of Facebook and YouTube for Political Expression," *Computers in Human Behavior* (29:3), Pergamon, pp. 1159–1168. (https://doi.org/10.1016/J.CHB.2012.10.008).

Hanna, N. 2018. “A Role for the State in the Digital Age,” *Journal of Innovation and Entrepreneurship* (7:1), SpringerOpen, pp. 1–16. (https://doi.org/10.1186/S13731-018-0086-3/FIGURES/3).

Hayes, A. S., Singer, J. B., and Ceppos, J. 2007. “Shifting Roles, Enduring Values: The Credible Journalist in a Digital Age,” *Journal of Mass Media Ethics* (22:4), Taylor & Francis Group , pp. 262–279. (https://doi.org/10.1080/08900520701583545).

He, B., and Warren, M. E. 2012. “When, Where and Why Do We Need Deliberation, Voting, and Other Means of Organizing Democracy? A Problem-Based Approach to Democratic Systems,” *Perspectives on Politics* (9:2), pp. 269–289. (https://doi.org/10.1017/S1537592711000892).

Helberger, N., Pierson, J., and Poell, T. 2017. “Governing Online Platforms: From Contested to Cooperative Responsibility,” *Https://Doi.Org/10.1080/01972243.2017.1391913* (34:1), Routledge, pp. 1–14. (https://doi.org/10.1080/01972243.2017.1391913).

Héritier, A. 2011. *Composite Democracy in Europe: The Role of Transparency and Access to Information*, (10:5), Taylor & Francis , pp. 814–833. (https://doi.org/10.1080/1350176032000124104).

Hilbert, M. 2009. “The Maturing Concept of E-Democracy: From E-Voting and Online Consultations to Democratic Value Out of Jumbled Online Chatter,” *Journal of Information Technology & Politics* (6:2), Taylor & Francis Group , pp. 87–110. (https://doi.org/10.1080/19331680802715242).

Hix, S. 2005. *The Political System of the European Union*, (2nd ed.), Palgrave Macmillan.

Hobolt, S. B. 2016. “The Brexit Vote: A Divided Nation, a Divided Continent,” *Journal of European Public Policy* (23:9), Routledge, pp. 1259–1277. (https://doi.org/10.1080/13501763.2016.1225785/SUPPL_FILE/RJPP_A_1225785_SM3636.ZIP).

Hood, C. 1983. *The Tools of Government*, Macmillan.

“Horizon2020 - EURADA - EURADA.” (n.d.). (https://www.eurada.org/projects/horizon2020, accessed May 27, 2023).

House of Representatives. 2021. “‘Disinformation Nation: Social Media’s Role in Promoting Extremism and Misinformation,’” in *House Hearing, 117th Congress*, , March. (https://www.congress.gov/event/117th-congress/house-event/111407).

Howard, P. N., and Kollanyi, B. 2016. “Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum,” *SSRN Electronic Journal*, Elsevier BV. (https://doi.org/10.2139/SSRN.2798311).

Howlett, M. 2000. “Managing the ‘Hollow State’: Procedural Policy Instruments and Modern Governance,” *Canadian Public Administration* (43:4), John Wiley & Sons, Ltd, pp. 412–431. (https://doi.org/10.1111/J.1754-7121.2000.TB01152.X).

H.R.2599 – 118th Congress (2023-2024): Honest Ads Act. 2023. House, Congress. (https://www.congress.gov/bill/118th-congress/house-bill/2599/text?s=6&r=8&q=%7B%22search%22%3A%5B%22Disinformation%22%5D%7D).

H.R.3359 – 115th Congress (2017-2018): Cybersecurity and Infrastructure Security Agency Act of 2018. 2018. (http://www.congress.gov/).

H.R.3364 – 115th Congress (2017-2018): Countering America’s Adversaries Through Sanctions Act. 2017. Senate, Congress. (https://www.congress.gov/bill/115th-congress/house-bill/3364/text?s=5&r=6&q=%7B%22search%22%3A%5B%22Disinformation%22%5D%7D).

H.R.5515 – 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019. 2018. House, Congress. (https://www.congress.gov/bill/115th-congress/house-bill/5515/text).

H.R.6395 – 116th Congress (2019-2020): William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. 2021. (https://www.congress.gov/bill/116th-congress/house-bill/6395).

Humprecht, E., Esser, F., and Van Aelst, P. 2020. “Resilience to Online Disinformation: A Framework for Cross-National Comparative Research,” *The International Journal of Press/Politics* (25:3), SAGE PublicationsSage CA: Los Angeles, CA, pp. 493–516. (https://doi.org/10.1177/1940161219900126).

Huntington, S. P. 1966. “Political Modernization: America vs. Europe,” *World Politics* (18:3), Cambridge University Press, pp. 378–414. (https://doi.org/10.2307/2009762).

Hwang, Y., Ryu, J. Y., and Jeong, S. H. 2021. “Effects of Disinformation Using Deepfake: The Protective Effect of Media Literacy Education,” *Cyberpsychology, Behavior, and Social Networking* (24:3), Mary Ann Liebert, Inc., publishers 140 Huguenot Street, 3rd Floor New Rochelle, NY 10801 USA , pp. 188–193. (https://doi.org/10.1089/CYBER.2020.0174).

Issacharoff, S. 2008. “Democracy and Collective Decision Making,” *International Journal of Constitutional Law* (6:2), Oxford Academic, pp. 231–266. (https://doi.org/10.1093/ICON/MON003).

Jacob, D. 2015. “Every Vote Counts: Equality, Autonomy, and the Moral Value of Democratic Decision-Making,” *Res Publica* (21:1), Kluwer Academic Publishers, pp. 61–75. (https://doi.org/10.1007/S11158-014-9262-X/METRICS).

Jamieson, K. H. 2021. “Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don’t, Can’t, and Do Know,” *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don’t, Can’t, and Do Know*. (https://doi.org/10.1093/oso/9780190058838.001.0001).

Jennings, F. J., Suzuki, V. P., and Hubbard, A. 2020. “Social Media and Democracy: Fostering Political Deliberation and Participation,” *Western Journal of Communication* (85:2), Routledge, pp. 147–167. (https://doi.org/10.1080/10570314.2020.1728369).

Kelly, R. M. 1998. “An Inclusive Democratic Polity, Representative Bureaucracies, and the New Public Management,” *Public Administration Review* (58:3), JSTOR, p. 201. (https://doi.org/10.2307/976560).

Koenig-Archibugi, M. 2017. “How to Diagnose Democratic Deficits in Global Politics: The Use of the ‘All-Affected Principle,’” *International Theory* (9:2), Cambridge University Press, pp. 171–202. (https://doi.org/10.1017/S1752971916000312).

Kovic, M., Rauchfleisch, A., Sele, M., and Caspar, C. 2018. “Digital Astroturfing in Politics: Definition, Typology, and Countermeasures,” *Studies in Communication Sciences* (18:1), HBZ Open Publishing Environment, pp. 69–85. (https://doi.org/10.24434/j.scoms.2018.01.005).

Krouse, R. W. 1982. “Polyarchy & Participation: The Changing Democratic Theory of Robert Dahl,” *Polity* (14:3), The University of Chicago Press, pp. 441–463. (https://doi.org/10.2307/3234535).

Lev-On, A., and Steinfeld, N. 2016. “Social Media and the City: Analyzing Conversations in Municipal Facebook Pages,” in *Social Media and Local Governments: Theory and Practice*, M. Z. Sobaci (ed.), Cham: Springer International Publishing, pp. 243–261. (https://doi.org/10.1007/978-3-319-17722-9_13).

Lewandowsky, S., Ecker, U. K. H., and Cook, J. 2017. “Beyond Misinformation: Understanding and Coping with the ‘Post-Truth’ Era,” *Journal of Applied Research in Memory and Cognition* (6:4), Elsevier Inc., pp. 353–369. (https://doi.org/10.1016/J.JARMAC.2017.07.008).

Linneberg, M. S., and Korsgaard, S. 2019. “Coding Qualitative Data: A Synthesis Guiding the Novice,” *Qualitative Research Journal* (19:3), Emerald Group Holdings Ltd., pp. 259–270. (https://doi.org/10.1108/QRJ-12-2018-0012/FULL/XML).

Macintosh, A. 2004. “Characterizing E-Participation in Policy-Making,” *Proceedings of the Hawaii International Conference on System Sciences* (37), pp. 1843–1852. (https://doi.org/10.1109/HICSS.2004.1265300).

Macintosh, A., Robson, E., Smith, E., and Whyte, A. 2003. “Electronic Democracy and Young People,” *Social Science Computer Review* (21:1), SAGE Publications, pp. 43–54. (https://doi.org/10.1177/0894439302238970).

Manor, J. 2007. “Democratisation with Inclusion: Political Reforms and People’s Empowerment at the Grassroots,” *Journal of Human Development* (5:1), United Nations Development Programme , pp. 5–29. (https://doi.org/10.1080/14649880310001660193).

Mathers, N., Fox, N., and Hunn, A. 2000. *Using Interviews in a Research Project*, pp. 113–134.

Matthes, J., Schmuck, D., and von Sikorski, C. 2021. “In the Eye of the Beholder: A Case for the Visual Hostile Media Phenomenon,” *Communication Research*, SAGE PublicationsSage CA: Los Angeles, CA. (https://doi.org/10.1177/00936502211018596).

Maxwell, J. A. 2013. *Qualitative Research Design: An Interactive Approach (Applied Social Research Methods)*. (https://mrcppu-covid.bio/sites/default/files/signed_mtas/qualitative-research-design-an-interactive-approach-applied-soc-joseph-a-maxwell-8a0ba43.pdf).

McAfee, N. 2022. “Democracy without Shortcuts: A Participatory Conception of Deliberative Democracy,” *Contemporary Political Theory* (21:S2). (https://doi.org/10.1057/s41296-021-00519-4).

McKay, S., and Tenove, C. 2020. “Disinformation as a Threat to Deliberative Democracy,” *Https://Doi.Org/10.1177/1065912920938143* (74:3), SAGE PublicationsSage CA: Los Angeles, CA, pp. 703–717. (https://doi.org/10.1177/1065912920938143).

Miller, M. L., and Vaccari, C. 2020. “Digital Threats to Democracy: Comparative Lessons and Possible Remedies,” *Https://Doi.Org/10.1177/1940161220922323* (25:3), SAGE PublicationsSage CA: Los Angeles, CA, pp. 333–356. (https://doi.org/10.1177/1940161220922323).

Modise, L. J. 2017. “The Notion of Participatory Democracy in Relation to Local Ward Committees: The Distribution of Power,” *In Die Skriflig/In Luce Verbi* (51:1), AOSIS. (https://doi.org/10.4102/IDS.V51I1.2248).

Monsees, L. 2021. “Information Disorder, Fake News and the Future of Democracy,” *Globalizations* (20:1), Routledge, pp. 153–168. (https://doi.org/10.1080/14747731.2021.1927470).

Moravcsik, A. 2006. “The European Constitutional Compromise and the Neofunctionalist Legacy,” *Journal of European Public Policy* (12:2), Routledge , pp. 349–386. (https://doi.org/10.1080/13501760500044215).

Mueller, D. C., and Stratmann, T. 2003. “The Economic Effects of Democratic Participation,” *Journal of Public Economics* (87:9–10), North-Holland, pp. 2129–2155. (https://doi.org/10.1016/S0047-2727(02)00046-4).

Näsström, S. 2011. “The Challenge of the All-Affected Principle,” *Political Studies* (59:1), SAGE PublicationsSage UK: London, England, pp. 116–134. (https://doi.org/10.1111/J.1467-9248.2010.00845.X).

Nath, J. 2011. “Reimagining Government in the Digital Age,” *National Civic Review* (100:3), John Wiley & Sons, Ltd, pp. 19–23. (https://doi.org/10.1002/NCR.20070).

Nye, J. S. 2005. *Soft Power: The Means to Success in World Politics*, PublicAffairs Books.

Ober, J. 2012. “Democracy’s Dignity,” *American Political Science Review* (106:4), Cambridge University Press, pp. 827–846. (https://doi.org/10.1017/S000305541200038X).

Office of the U.S. Surgeon General. 2021. “Confronting Health Misinformation: The U.S. Surgeon General’s Advisory on Building a Healthy Information Environment.” (https://www.hhs.gov/surgeongeneral/priorities/health-misinformation/index.html).

Owen, D. 2012. “Constituting the Polity, Constituting the Demos: On the Place of the All Affected Interests Principle in Democratic Theory and in Resolving the Democratic Boundary Problem,” *Ethics & Global Politics* (5:3), Routledge, pp. 129–152. (https://doi.org/10.3402/EGP.V5I3.18617).

Pawelec, M. 2022. “Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions,” *Digital Society* (1:2), Springer Science and Business Media LLC. (https://doi.org/10.1007/s44206-022-00010-6).

Peters, G. B. 2000. “Policy Instruments and Public Management: Bridging the Gaps,” *Journal of Public Administration Research and Theory: J-PART* (10:10), pp. 33–47. (https://www.jstor.org/stable/3525810).

Peters, U. 2022. “Algorithmic Political Bias in Artificial Intelligence Systems,” *Philosophy and Technology* (35:2), Springer Science and Business Media B.V., pp. 1–23. (https://doi.org/10.1007/S13347-022-00512-8/METRICS).

Pitt, J., and Ober, J. 2019. “Democracy by Design: Basic Democracy and the Self-Organisation of Collective Governance,” *International Conference on Self-Adaptive and Self-Organizing Systems, SASO* (2018-September), IEEE Computer Society, pp. 20–29. (https://doi.org/10.1109/SASO.2018.00013).

Pollicino, O., and Bietti, E. 2019. “Truth and Deception Across the Atlantic: A Roadmap of Disinformation in the US and Europe,” *Italian Journal of Public Law* (11:1), pp. 43–85. (https://papers.ssrn.com/abstract=3397910).

Polyakova, A., and Boyer, S. P. 2018. “The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition,” , March. (https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/).

Powell, T. E., Boomgaarden, H. G., De Swert, K., and de Vreese, C. H. 2015. “A Clearer Picture: The Contribution of Visuals and Text to Framing Effects,” *Journal of Communication* (65:6), Oxford Academic, pp. 997–1017. (https://doi.org/10.1111/JCOM.12184).

Putnam, R. D. 2000. “Bowling Alone: The Collapse and Revival of American Community,” in *Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work*, CSCW ‘00, New York, NY, USA: Association for Computing Machinery, p. 357. (https://doi.org/10.1145/358916.361990).

Ragin, C. C. 2014. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*, University of California Press.

Reisach, U. 2021. “The Responsibility of Social Media in Times of Societal and Political Manipulation,” *European Journal of Operational Research* (291:3), North-Holland, pp. 906–917. (https://doi.org/10.1016/J.EJOR.2020.09.020).

Rodriguez-Morales, A. J., and Franco, O. H. 2021. “Public Trust, Misinformation and COVID-19 Vaccination Willingness in Latin America and the Caribbean: Today’s Key Challenges,” *The Lancet Regional Health - Americas* (3), Elsevier Ltd, p. 100073. (https://doi.org/10.1016/j.lana.2021.100073).

De Rosario, A. H., Martín, A. S., and Pérez, M. D. C. C. 2016. “The Use of Facebook to Promote Engagement with Local Governments in Spain,” in *Social Media and Local Governments* (Vol. 15),

M. Sobaci (ed.), Springer, Cham, pp. 219–241. (https://doi.org/10.1007/978-3-319-17722-9_12/TABLES/10).

S.394 – 118th Congress (2023-2024): Digital Citizenship and Media Literacy Act. 2023. Senate, Congress. (https://www.congress.gov/bill/118th-congress/senate-bill/394/text?s=4&r=17&q=%7B%22search%22%3A%5B%22Disinformation%22%5D%7D).

S.406 – 118th Congress (2023-2024): Promoting Public Health Information Act. 2023. Senate, Congress. (https://www.congress.gov/bill/118th-congress/senate-bill/406/text?s=4&r=16&q=%7B%22search%22%3A%5B%22Disinformation%22%5D%7D).

S.1231 – 118th Congress (2023-2024): SAD Act. 2023. Senate, Congress. (https://www.congress.gov/bill/118th-congress/senate-bill/1231/text?s=1&r=3).

S.2943 – 114th Congress (2015-2016): National Defense Authorization Act for Fiscal Year 2017. 2016. Senate, Congress. (http://www.congress.gov/).

S.3274 – 114th Congress (2015-2016): Countering Foreign Propaganda and Disinformation Act. 2016. Senate, Congress. (https://www.congress.gov/bill/114th-congress/senate-bill/3274/text).

S.3608 – 117th Congress (2021-2022): Social Media NUDGE Act. 2022. Senate, Congress. (https://www.congress.gov/bill/117th-congress/senate-bill/3608/text).

S.4499 – 116th Congress (2019-2020): COVID–19 Misinformation and Disinformation Task Force Act of 2020. 2020. (https://www.congress.gov/bill/116th-congress/senate-bill/4499/text?s=1&r=28).

Salamon, L. M. 2002. *The Tools of Government: A Guide to the New Governance*, Oxford University Press.

Saurwein, F., and Spencer-Smith, C. 2020. "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe," *Digital Journalism* (8:6), Routledge, pp. 820–841. (https://doi.org/10.1080/21670811.2020.1765401).

Schiffrin, A. 2017. "DISINFORMATION AND DEMOCRACY: THE INTERNET TRANSFORMED PROTEST BUT DID NOT IMPROVE DEMOCRACY," *Journal of International Affairs* (71:1), pp. 117–126. (https://www.jstor.org/stable/26494367).

Schmidt, C. 2004. "The Analysis of Semi-Structured Interviews," in *A Companion to Qualitative Research*, U. Flick, E. von Kardoff, and I. Steinke (eds.), Sage Publications, pp. 253–259.

Schmitter, P. C., and Karl, T. L. 2017. "What Democracy Is. . . and Is Not," *Journal of Democracy* (2:3), Johns Hopkins University Press, pp. 75–88. (https://doi.org/10.1353/JOD.1991.0033).

Schumpeter, J. A. 1976. *Capitalism, Socialism and Democracy*, London: Routledge.

Seawright, J., and Gerring, J. 2008. "Case Selection Techniques in Case Study Research," *Political Research Quarterly* (61:2), SAGE PublicationsSage CA: Los Angeles, CA, pp. 294–308. (https://doi.org/10.1177/1065912907313077).

Sherman, C. E., Arthur, D., and Thomas, J. 2021. "Panic Buying or Preparedness? The Effect of Information, Anxiety and Resilience on Stockpiling by Muslim Consumers during the COVID-19 Pandemic," *Journal of Islamic Marketing* (12:3), Emerald Group Holdings Ltd., pp. 479–497. (https://doi.org/10.1108/JIMA-09-2020-0309/FULL/PDF).

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., and Liu, H. 2020. "Combating Disinformation in a Social Media Age," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* (10:6), John Wiley & Sons, Ltd, p. e1385. (https://doi.org/10.1002/WIDM.1385).

Skrtic, T. M., Sailor, W., and Gee, K. 1996. "Voice, Collaboration, and Inclusion: Democratic Themes in Educational and Social Reform Initiatives," *Remedial and Special Education* (17:3), SAGE PublicationsSage CA: Los Angeles, CA, pp. 142–157. (https://doi.org/10.1177/074193259601700304).

Special Counsel's Office, D. of J. 2019. "Report on the Investigation into Russian Interference in the 2016 Presidential Election (Mueller Report)," U.S. Government Publishing Office, April 18. (https://www.govinfo.gov/app/details/GPO-SCREPORT-MUELLER).

Staats, J. L. 2004. "Habermas and Democratic Theory: The Threat to Democracy of Unchecked Corporate Power," *Political Research Quarterly* (57:4), JSTOR, p. 585. (https://doi.org/10.2307/3219820).

Temir, E. 2020. "Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism," *Journal of Selcuk Communication* (13:2), Selcuk University, pp. 1009–1024. (https://doi.org/10.18094/JOSC.685338).

Tenove, C. 2020. "Protecting Democracy from Disinformation: Normative Threats and Policy Responses," *Https://Doi.Org/10.1177/1940161220918740* (25:3), SAGE PublicationsSage CA: Los Angeles, CA, pp. 517–537. (https://doi.org/10.1177/1940161220918740).

The Lancet. 2020. "COVID-19: Fighting Panic with Information," *Lancet (London, England)* (395:10224), Elsevier, p. 537. (https://doi.org/10.1016/S0140-6736(20)30379-2).

The White House. 2011. “Executive Order 13584 --Developing an Integrated Strategic Counterterrorism Communications Initiative | Whitehouse.Gov.” (https://obamawhitehouse.archives.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c, accessed May 19, 2023).

Tideman, N. 2016. “Collective Decisions and Voting: The Potential for Public Choice,” *Collective Decisions and Voting: The Potential for Public Choice* (1st Edition.), London: Routledge. (https://doi.org/10.4324/9781315259963/COLLECTIVE-DECISIONS-VOTING-NICOLAUS-TIDEMAN).

Tucker, J. A., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., and Nyhan, B. 2018. “Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature,” *SSRN Electronic Journal*, Elsevier BV. (https://doi.org/10.2139/SSRN.3144139).

U.S. Department of State. (n.d.). “About Us - Global Engagement Center - United States Department of State.” (https://www.state.gov/about-us-global-engagement-center-2/, accessed May 19, 2023).

U.S. Government Publishing Office. 2019. “RUSSIAN DISINFORMATION ATTACKS ON ELECTIONS: LESSONS FROM EUROPE,” in *House Hearing, 116 Congress*. (https://www.congress.gov/event/116th-congress/house-event/LC64157/text?s=1&r=10).

Vosoughi, S., Roy, D., and Aral, S. 2018. “The Spread of True and False News Online,” *Science* (359:6380), American Association for the Advancement of Science, pp. 1146–1151. (https://doi.org/10.1126/SCIENCE.AAP9559/SUPPL_FILE/AAP9559_VOSOUGHI_SM.PDF).

Vukanovic, Z. 2009. “Global Paradigm Shift: Strategic Management of New and Digital Media in New and Digital Economics,” *International Journal on Media Management* (11:2), pp. 81–90. (https://doi.org/10.1080/14241270902844249).

Wang, P., Angarita, R., and Renna, I. 2018. “Is This the Era of Misinformation yet: Combining Social Bots and Fake News to Deceive the Masses,” *The Web Conference 2018 - Companion of the World Wide Web Conference, WWW 2018*, Association for Computing Machinery, Inc, pp. 1557–1561. (https://doi.org/10.1145/3184558.3191610).

Wardle, C., and Derakhshan, H. 2017. “Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making.” (https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html).

Warren, M. E. 2017. “A Problem-Based Approach to Democratic Theory,” *American Political Science Review* (111:1), Cambridge University Press, pp. 39–53. (https://doi.org/10.1017/S0003055416000605).

Wiesenberg, M., and Tench, R. 2020. “Deep Strategic Mediatization: Organizational Leaders’ Knowledge and Usage of Social Bots in an Era of Disinformation,” *International Journal of Information Management* (51), Pergamon, p. 102042. (https://doi.org/10.1016/J.IJINFOMGT.2019.102042).

Wong, L. P. 2008. “Data Analysis in Qualitative Research: A Brief Guide to Using Nvivo,” *Malaysian Family Physician : The Official Journal of the Academy of Family Physicians of Malaysia* (3:1), Academy of Family Physicians of Malaysia, p. 20. (/pmc/articles/PMC4267019/).

Woolley, S. C., and Howard, P. N. 2016. “Automation, Algorithms, and Politics| Political Communication, Computational Propaganda, and Autonomous Agents — Introduction,” *International Journal of Communication* (10:0), pp. 4882–4890. (https://ijoc.org/index.php/ijoc/article/view/6298).

Wu, G., Deng, X., and Liu, B. 2022. “Managing Urban Citizens’ Panic Levels and Preventive Behaviours during COVID-19 with Pandemic Information Released by Social Media,” *Cities* (120), Pergamon, p. 103490. (https://doi.org/10.1016/J.CITIES.2021.103490).

Young, I. M. 2002. “Inclusion and Democracy,” *Inclusion and Democracy*, Oxford University Press. (https://doi.org/10.1093/0198297556.001.0001).

Appendix

A Interview Outline and Transcripts

A.a Interview Outline: Safeguarding Democracy from Disinformation

Research Topic: Disinformation Policy Tools: A Comparison of the US and the EU

The Impact of Disinformation on Democracy:

Sub-topic 1: Disinformation Sources & Tactics: Examining the various sources of disinformation, their methods, and the scope of their impact on democratic processes.

Sub-topic 2: Public Perception & Democracy: Investigating disinformation's influence on public opinion, political polarization, and citizens' trust in democratic institutions.

The Measures Taken by the Government in Response to Disinformation:

Sub-topic 3: Regulatory Frameworks & Policy Approaches: Comparing the legal and policy frameworks in the US and the EU and their effectiveness in protecting democracy.

Sub-topic 4: Future Strategies & Collaborative Efforts: Exploring potential US-EU collaborative efforts to combat disinformation and strengthen democratic resilience.

Introduction to interviewer:

My name is Jared York, and I am an American student currently pursuing a joint master's degree in Public Sector Innovation and e-Governance at KU Leuven in Belgium.

Description of project/aims:

This research aims to explore the impact of disinformation on democracy and the policy tools that the governments in the US and the EU are using to ensure democratic resilience. These tools may include laws, regulations, the establishment of regulatory bodies, special committees, or information campaigns, among others. By comparing these tools, this research aims to identify successes and challenges associated with various disinformation policy tools and extrapolate best practices to provide insight for the development of future disinformation policies.

Confidentiality:

I would like to record the interview to help with my data analysis. I won't share the interview outside of this master thesis module and your personal details will be concealed. Can I reveal some information about your position/expertise? I will ensure that none of these details are identifying and will be broad descriptions.

Orienting Questions

Q1) What is your role within ...?

Q2) Why did you choose to work/study in ...?

Initial Questions: *Questions relating to the impact of disinformation on democratic processes and institutions within the US and the EU.*

Sub-topic 1: Disinformation Sources & Tactics

1. How does disinformation threaten democratic processes and institutions (i.e., Empowered Inclusion, Collective Will & Agenda Formation, and Collective Decision Making)?

2. In what ways have disinformation sources and tactics evolved in recent years?

3. Can you provide examples of disinformation campaigns that have had significant impacts on democratic processes in the US and/or the EU?

4. How do state-sponsored and non-state actors differ in their disinformation strategies?

5. What are key challenges in identifying and countering disinformation?

Sub-topic 2: Public Perception & Democracy

How does disinformation affect citizens' trust in democratic processes and institutions?

6. To what extent do you think social media plays a role in amplifying disinformation's impact on public opinion and political polarization?

7. In your view, are certain demographic groups more vulnerable to disinformation? Why?

8. Can you provide examples of how disinformation has shaped public opinion and political polarization in the US and/or the EU?

Deeper Questions: *Questions relating to the policy tools implemented by the government in response to disinformation threats.*

Sub-topic 3: Regulatory Frameworks & Policy Approaches

10. What are the main policy tools used in the US and/or the EU to address disinformation's threat to key functions of democracy?

11. To what extent have these policy tools been effective in combating disinformation? Are some policy tools better than others?

12. Are there any notable differences between the US and the EU in terms of their regulatory frameworks and policy approaches?

13. How do the US and the EU strike a balance between freedom of expression and the need to counter disinformation?

Sub-topic 4: Future Strategies & Collaborative Efforts

14. How can the US and the EU collaborate in the development and implementation of more effective disinformation policies?

15. What role do you believe private entities, such as social media platforms, play in countering disinformation. How can they be better incorporated into policy efforts?

16. What lessons can be learned from the successes and challenges of existing disinformation policies in the US and/or the EU?

17. In your opinion, what emerging technologies or trends should policymakers be made aware of when designing disinformation policies for the future?

Wrap up Questions *Any summary questions, sense-checks, and also a question about whether they have anything to add*

Conclusion of interview: *e.g. thank them for their time, ask if they have anything to add*

A.b Interview Transcipt for Interviewee 1

Friday, May 9, 2023 15:00-15:40 • 31:13

SPEAKERS
Jared York, Interviewee 1

Interviewee 1 00:00
Yeah, so a bit of the background, although I'm a professor at KU Leuven, and I think that's in that context that you have been contacting me. And I'm doing research and I'm also affiliated to the Oxford Internet Institute. My background and the focus of my interest is the intersection between technology and International Relations, for example, technology, multilateralism, and in particular digital technologies. So I'm doing academic work, but also advisory work, in that respect, for example, on things like industrial policy or governance of AI or those kinds of things. And my solid longer back as my background as director at the European Commission, where I was responsible in DG Connect, which is the digital policy department of the European Commission, where I had responsibility for a range of policies amongst others related to digital identity and cybersecurity, privacy and, and also responsibility for managing research and development and deployment programs that are operating at European level. So I have been much involved in European policymaking but in direct European policymaking now more will be commenting on or analyzing European policymaking, especially digital policies. Is that okay?

Jared York 01:28
Yes, that's, that's perfect.

Interviewee 1 01:31
On your first subtopic, guide the interviewer as you want to, but I'll leave it to you; how do you want to? Do you want to walk through the various questions?

Jared York 01:41
Sure, we can go from subtopic to subtopic, it's completely at your convenience.

Interviewee 1 01:46
Yeah, disinformation sources and tactics. I find that a difficult one, because as far as I know, much more of the information that I have, would be at most at best anecdotal. Rather than, you know, how does disinformation threaten democratic processes and institutions? You know, the anecdotes yourself, you know, the anecdotal evidence, which goes from Cambridge analytical to disinformation campaigns that have been happening around elections, fueling populism or anti Vax, or those kind of campaigns. And, of course, the things all haven't been heated up very much with the war against Ukraine. So I prefer to kind of go and skip a little bit, these questions, because really, I don't think I can say that much about it. What I found quite interesting is your question about state sponsored versus the non state actors. And there's actually this kind of hybrid form also of non state actors that are state sponsored, where states are probably in the background for sponsoring that, which may be worthwhile to look at. So I think pretty solidly you can say that state actors have two types of objectives. It's either to disrupt other states or to sustain their own state. As simple as that, so there's whereas there isn't much disinformation campaigns are focus on a few days ago, and I anecdotal the disinformation

campaign in Venezuela recent one of depicting the government in a very positive light, that's clearly want to sustain the regime. If you see the disinformation campaigns around Ukraine, that are happening on social media that we might be seeing here. They are clearly to disrupt the West, and the messaging around. The non state actors. I'm really wondering about that, because I was wondering if non state actors are perhaps more issue based or instance based rather than this systematic disruption and the systematic sustaining that state actors do. And I was thinking of the example of, of a research that had been done and information around the Irish referendum. That was the referendum that was held a few years ago in which they had, amongst others also the issue of abortion, a lot of my then colleagues of Oxford's department of Politics and International Relations. Abhishek Gupta, did research into that and found out or was researching how information and that includes disinformation is being spread on social media and to what extent that had an influence and also whether this was human based or bots based based on bots or humans, but it was clearly around the issue at that time of the Irish referendum and particularly the abortion question. So that's an issue based thing I don't know, state actor or were anti abortion groups in the United States, as far as I remember, but you can find the research on the internet. So perhaps interesting research rather kind of quantitative research also that he did. All I can say about it. The I mean, interrupt me and ask me more questions if you want to ensure,

Jared York 05:26
Absolutely, if a question comes to mind I will and I'm taking notes as you speak.

Interviewee 1 05:30
Yeah, and then these key challenges in identifying and countering disinformation, I find that also a difficult one, because I don't have that much experience with it. All I can see at the moment, we are shortly going to have a workshop on AI and democratic sustainability. So about in particular generative AI coming up. And so the challenge, our assumption is that AI and in particular, new forms of AI generative AI can pose a significant challenge in the field of disinformation, because of them being able to present credible stories at a high rate, and the stories are also going to get done again, getting recycled into a database on which these AI systems are based. So some kind of self reinforcing loop might be involved. So AI as a challenge bots, that link to AI as a challenge. And I was actually also wondering, but it's much more speculative, because may, you may know, have kept much more information about it, whether hybrid physical, digital approaches play a role, in other words, state actors that are supporting and disinformation and also creating this information groups or supporting them, for example, financially populist movements that are secretly supported by China or the United or Russia, or Iran or others. And the subtle ways that this can also play a role. As you see, now, you know, regularly something is coming up that even universities are enticed or corrupted, to provide effectively, disinformation. I think just yesterday, it was a case that a number of universities were financially supported by Saudi by Saudi Arabia, I think, in order to publish articles that refer to as the first one, to the university to the University of Saudi Arabia, just to bump them up and ranking well, that's a form of information manipulation, at least. So yeah, that's about it first subtopic. The second sub topic, I must admit, I find it very hard you know, I can say these kind of bland statements like, you know, less informed groups, less educated group might be more vulnerable, etc, etc. But you notice, it doesn't add value to your, to your analysis, and examples, you've got plenty of examples to an including the Cambridge analytical, for example, and two examples around anti Vax in Europe and the United States that indeed have led to polarization. And no wonder that some of the public broadcasters are now actively engaging in debunking like in Belgium, you've got the VRT, who, as its website, but also on the television programs regularly, an analysis of is this true? Or is this false information? And they do an analysis of text and images, video, photos, etc.

Jared York 09:22
And are they do that on their own means, or is that?

Interviewee 1 09:26
Yeah, that's a good point. I've also been wondering, you know, are they incited by the government? Is that are they quite well possible that our government, say public programs, financing that supports that, but I've never seen that. So it might also be that this is that they consider this as part of their journalistic ethics and that they have to do this. I don't know. Perhaps you can find out.

Jared York 09:56
And you mentioned the DSA and the DMA, they're quite controversial topics, at least in the US, because the US believes that this is targeting big tech, it's targeting US firms, they're not really seeing it from the perspective of regulating the platforms and holding them accountable for the information that they share. And then this touches back on to, as well as the First Amendment and freedom of speech. Are we limiting freedom of speech by regulating the platforms. What might be your, your, your opinion on this

Interviewee 1 10:36
I guess that also your analysis, it's good to take these kind of different perceptions on how society should be organized. And I think you're also referring to certain models or models here, I guess that you can take a kind of a regulatory perspective and look at Section 230. And, and, and the European approach, actually being quite hesitant to do something at European level, because there is no mandate, formally around content at European level in the treaty. So you have to be quite careful if you start acting at the European level. And so there's some similarity in that, but they have different kinds of grants in order to hold back in regulating. So you see regulating content is one of the later areas and actually handle acting in the field of digital, you know, things like cybersecurity, which also very sensitive area because it touches national security has actually been much earlier in coming up with hard legislation in Europe, and also hard measures in the United States like presidential executive orders. If you look at content regulation, of course, the platform providers were for a long time shielded by section 230. And that's contested, depending upon the political opinion and the leadership of the FTC, who will are now much more clear that they think this actually should be addressed, that they should be held accountable. And at the European level, it continues to be to some degree contested because of the lack of competences, as they call it the lack of formal mandate at European level. But the case has been made stronger, because voluntary approaches that you can always undertake at European level didn't work. And so the threat to democracy and other threats to actually also to security, they have become more prominent, and so that you get the DSA that says we can regulate this, but we are still not really regulating content, we are actually regulating the way we deal with content. So not the content itself. So we are not going to say what exactly is legal and illegal. But if we do this, then we work together. And interestingly, because it continues, I that's my interpretation. So there is a more harmonized approach to how you deal with illegal and harmful content. But beyond that, it's interesting to see that this common approach is actually also part more than before allocated to be handled at European level, rather than just the coordination between the national levels. So in a certain sense, perhaps comparable to saying you have a federal competence and authority in the United States, rather than that everybody does this at the state level. And in the US. It's very contested look at what is happening around education and information about LGBT or what have you, you know. So the fact it's a remarkable outcome of the DSA negotiations and also DMA negotiations that there has been capacity created at European level at the European Commission in order to help implementing the DSA and the DMA rather than keeping it only at the national level, and I think you can interpret it that the member states who are the decisive factor in this have seen that it is about topics that are indeed really threatening for their sovereignty and that they that these topics are too large to deal with at the national level. And so they are willing to let this happen at the European level. So institutionally, this is a quite different quite important development. I don't know if something similar ultimately also happens at the United States. But of course, you don't get to the second round, the one that you mentioned. Namely, is this

has this is this an issue of economic interference, interfering for economic reasons. And for the DSA, that's a matter of interpretation. But I would say highly unlikely, highly unlikely that it is, it happens to be that big platforms for other reasons are mostly American. But the disinformation rules would apply to anyone. And also the market distortion rules that are in the DMA are applied to everyone. And the European Commission just provided a list of about 20 of these platforms. And amongst these platforms, there's also a number of European platforms because the criteria are just number criteria. They are not nationality criteria. So that you find sure you find Facebook meta, but you also find to booking.com. Spotify probably also, not sure. And you find Tiktok. So they all have to behave. So I think it's a too limited view to see the DSA and DMA as instruments of weaponizing economic competition. It's not that. I mean, they, and it's a bit unrealistic. Also, because if you talk about economic competition, are you talking about? Are you competing in, for example, cloud services? are you competing in AI? are you competing in network technologies or chips. And this specific function that the platforms have in providing information is, of course, very important, but it is only a very limited part of the whole digital world. Okay, so it's a matter of assessment, whether or not you think this is used by the Europeans as a tool to, to unfairly perhaps compete with the American providers. In terms of the regulatory frameworks and policy approaches, and we are talking about it as the as a DMA. Yeah, how do you strike a balance between the EU and US? So it's part of the discussions in the transatlantic Trade & Technology Council (TTC) and the accompanying stakeholder dialogue? Are you attending some of the stakeholder dialogue meetings?

Jared York 17:56
I have in the past, but recently I've not

Interviewee 1 17:59
But you know, about OSHA. So that's where some of these efforts are taking place. And this has also to do with data management, I can send you a paper that I made for the transatlantic cooperation on that aspect of data management. It's about a year old. And if we look a little bit forward, I think you'll see that this is now being put really in the spotlight because of the rise of AI. And the potential use of AI precisely for disinformation and for misleading, perhaps educational purposes, but also disinformation in the context of democracy. And so a common approach to AI is very much in the transAtlantic picture and more than transatlantic, it's very much in the picture of the G7, who recently also declared in the Hiroshima Summit, that they would work together on a responsible AI. And they also put it in the context of democracy and disinformation. So there, I think you see the future strategies and collaborative efforts are indeed about trying to establish compatible approaches around high risk AI. And this ultimately has to be legally compatible, because the approach will have to hold in court. And that means that if there is a responsible AI approach, including how AI might be used for this information. And that's not necessarily AI that has been purposed for disinformation up front, but it might also while it's being used that it shows to be a risk for democracy, then this falls into AI act and are the responsibility of the companies that are that are providing the AI. You have to monitor that as post market surveillance. And that will have a legal framework in Europe, there might be a comparable framework in the United States, but like in the GDPR data protection, it might be put to the test. Is this comparability or actually it's called adequacy. Is this adequacy actually respecting the rights of Europeans? And so I guess we can see that there's a even before there are court cases, there will be test runs to see is the compatibility such that it will stand a test in court and the European Court of Justice in particular. So I think that's the big thing. International AI adequacy in the in a similar sense, as the GDPR, except that there's a big difference, you know, in the GDPR. It's about data protection, personal data protection, per se. You don't need to CSA what is the purpose of it, of that you're collecting the data, but you need to say, but it's the law is not focused on doing a purpose assessment. But in AI, you already have declared the possibility that there is an upfront declared purpose. And because of that declared purpose, you may be falling into a high risk category, and you need to do to take certain steps safeguards under the AI act. And in addition, you need to monitor what is happening to the AI while it's being used. So it has the field of disinformation, AI generated

disinformation, holds a bit the middle between data protection approaches and medical device approaches. So in medical device approaches, you need to upfront say, what is the intention intended purpose of this medical device, and then you do a whole assessment for that. And if there's high risk, you got a class two class three medical device, you do high risk assessment. And then you also need to see does this actually are the negative effects while it's in the market. And in data protection, you do an upfront risk assessment, but it's not per se purpose related. And in AI, I think you've got the combination of an upfront purpose and the use monitoring while the product is in the market, the right products in the market. So perhaps that's this kind of broader approach, you know, so upfront assessment and market monitoring is perhaps something that will be become part of a common international approach.

Jared York 22:59
And a question on, I guess some of the approaches. You mentioned, there's workshops being held on AI, and its impact on disinformation, its relation to disinformation, how it can be used to impact democracy, which you say things like workshops, and mandating, for example, public awareness campaigns or courses and schools. Is this a common approach within the EU? And is this accepted at the individual member state levels, if it's mandated at the EU level? Because one of the issues that the US is facing is, usually it's the state level government that decides what is in the curriculum or anything that deals with schools. So if the federal government were to make a similar mandate, it might not be accepted at the state level.

Interviewee 1 23:58
Yeah, that is a very good comment. So if you deal with if you talk about this information, there is a number of public policy measures that you can take and indeed, awareness and building up education is part of that. And then ultimately, the other side is regulatory approaches. And building awareness and education is outside the EU mandate in terms of imposing it. So you have to look at what the Europe is based upon the treaties, the treaties say, what can you do. And also what is the hardness of the instruments that you can use. And in those areas like awareness and skills, education, the mandate is for the European institutions for Europe, to coordinate, to stimulate, to promote, but not to impose. So it's impossible to make a law that says you must have in the curriculum education about disinformation. What you can do is make funding available to develop such content for education. And this has been there for a long, long time, we have to, for example, safer internet programs, you know, there was a funding program that created awareness campaigns and courses, to educate kids about the internet that's already existing since the early days of the internet. And you can do things like benchmark and comparing countries with each other. And these are soft policy instruments that have some effect. When you then go to the regulatory side, you really need to think about, you know, is it actually possible to act with legislation in this field. And as you cannot fall back onto the part and treaty that is about education, or public health or whatever. You have to use all the articles in the treaty. So you have to use exception measures. For example, if there is a threat to public health, that can be an emergency measure, that you could intervene, if there is a threat to public security. Likewise, these are emergency measures. But they are difficult because they are kind of punctual, they are for that instance, they are not kind of market conditioning or market shaping, or market enabling. If you want to do something that is much more on the structure of the market, then you you don't have that much choice, you can use internal market legislation that harmonizes approaches across Europe. So that's as if you've got a product in the market in Belgium, that has been classified and certified in Belgium as being secure, for example, safe to use, then it cannot be refused. In another country. So it's good enough. In one country that is good enough for the whole internal market. And that means there's free flow of these products and services. That's based upon article 114 of the treaty. And total market. And that's a very powerful article. Thats the article which most European legislation is based, and that leads to, and that's also the legal basis for the DMA and the DSA. So the argument is essentially, you know, if you have, if you think that there's trouble with platforms in your country, and they don't behave, and the way they manage the platform and the conditions that they have for access, and you can impose rules, but these rules are the same across Europe. And they are

European rules. And actually, you are not allowed to impose rules nationally, the rules have to be the same all across Europe. Now, that's a powerful basis that you can use in what they call the ex ante approach. So before products or services are in the market, there are actually market access requirements. You can also do them ex post approach, which is you use competition policy. And then you say, you know, there's a market distortion, for example, there's abuse of dominance. And you would act against that, in some way or another. That in itself is, is an exclusive European competence, meaning it is executed at European level. And so you immediately have a common approach. And it's a hard approach, you know, that's why you get the big fines about, you know, not dealing properly with, for example, consumer, private and personal data. But the disadvantage of that approach is that it is ex post, so after the products or services or the companies are already in the market, and perhaps they are entrenched. And it's hard to undo the damage. So the whole briefing concluding call, the whole question about awareness, and education is highly sensitive and continues to be a national matter. But because countries realize, increasingly the problem is really big. There is some willingness to take European voluntary solutions as the reference point.

Jared York 29:23
Okay. Yeah, to that extent, I think we covered mostly everything. I'm not sure if you have any concluding remarks, but I really appreciate you going into detail on these different subjects and for the insights, if you wouldn't mind. Could you please send me that article you mentioned.

Interviewee 1 29:53
Let me drop you that article or email separately. Yeah, I will do this.

Jared York 30:41
Perfect, thank you so much.

A.c Interview Transcript for Interviewee 2

Wednesday, May 17, 2023 14:00-14:40 • 23:13

SPEAKERS
Interviewee 2, Jared York

Jared York 00:00
Perfect. Could we maybe start talking about how you got involved in cybersecurity, disinformation, AI, that sort of thing, maybe a bit about your background?

Interviewee 2 00:14
Yeah, I was a journalist, in the last decade. And actually, in a nutshell, I was amazed how cybersecurity is transforming the world, power politics. And the nation state, there are a lot of nations state. And it actually happens when I saw when I read about the cyber attacks, especially nation state backed cyber attacks, all these reports about them, these kinds of attacks actually attracted my attention. And at the time, I focused on foreign news, than I think it's probably better to have a more focus on cybersecurity related issues. Because I am a political science graduate in my bachelor, all this kind of nation state and state sovereignty and bureaucritic mechanisms kind of things actually shaped my understanding of the world. But when I consider the developments related to cyber security, I noticed that this is actually a revolutionary thing that may fundamentally change the world, as we see today.

Jared York 01:53

Excellent, very interesting. And I noticed that you even started your own sort of company where you try to explain these difficult technical terms, cybersecurity, to maybe an audience who doesn't really understand all the implications. So could you tell me maybe a bit more about that?

Interviewee 2 02:13
Yeah, actually, at this point, I am trying to combine journalistic skills like storytelling, and I'm targeting an audience with a specific narrative with the cybersecurity terminology that I have learned during the years, working in a semi-governmental organization as a strategic cybersecurity expert, and Microsoft and marketing with some cyber cyber secret startups. Today I am in Estonia I on my company here, and my company offers digital marketing consultation services to cybersecurity startups, the thing is here that there I see an opportunity to grow is that the cybersecurity startups in the founders are mostly technical people with a technical background, mostly Computer Science or Computer Engineering Bachelor's degree, and they are not good at telling something or writing something about on a specific thing, even if it is their product, their own product they develop, they are unable to explain it comprehensively. So, at this point, I guess I my company will be helpful to actually explain their products and services to their target audience in an understandable manner, we which means the decision makers doesn't know how the technical background, how technical infrastructure is working in a product, they are more interested in what kind of benefits the products and services are providing. So my aim is to help them to to explain and make them noticeable, their product noticeable from the eyes of buyer personas.

Jared York 04:28
Ah sure, I understand. Yeah, that's a very good point. Because, indeed, a lot of these business starters or even developers, when they create a product, they're not always the best to explain that product. That's why you hire technical writers or like you said, content writers or digital marketers to get the word out and actually be able to explain it to ultimately the end user or whoever the service is being sold to. So that's that's very cool. That you are doing this with your business and sounds very exciting. I guess maybe to turn it back a bit to disinformation. You said you have experience working in semi governmental organizations, Microsoft, usually in the field of cybersecurity, but could you tell me maybe a bit what you've done on the front of disinformation?

Interviewee 2 05:21
Okay, okay. That's a great question. For me to explain how I am involved with disinformation, especially online disinformation. I actually founded a Turkish website, I will write in the chat its name. Its English translation is cyber bulletin. And it actually has been publishing for for nine years, so far it publishes articles, news analysis on the subject that stems the overlapping section of technology and politics. Of course, when it comes to disinformation, it's also under our scope. Because of the online disinformation campaigns that we have experienced, especially during the second half of last decade, it actually grabs our attention. And and I get a fund from a German foundation to create a specific newsletter for our readers about online disinformation. In this monthly newsletter, there will be news developments, recent regulations, about online disinformation. Since the website is in Turkish, and Turkeye is actually becoming more, let's say dictatorial, ruled by by a president who, who is having increasingly dictatorial tendencies, Lets puts it like this. Online disinformation become really a critical issue for freedom supporters, for those who want Turkey to maintain a democratic state. So this newsletter is just set of news and new ideas for our readers. Maybe they can get some inspiration. Or maybe we can actually coordinate efforts. Create more communication about the groups and people who are working on this field, about online information. Of course, the 2016 elections is a turning point about the utilization of online disinformation campaigns in politics, because as it was later clearly released, that Russia is behind some social media operations, some advertisement and some fake news operations, this kind of things, they were up to actually not influence the outcome of the election, but intervention to the democratic processes. And this is, I think,

actually a fundamental issue. This is extremely significant issue for the part of the world population, that defends for democracy, because what my point is that internet was seen as a facilitator for democracy, because political participation is expected to raise because many people can make their voice heard via online tools, like social media platforms, or the localization of politics is expected to become much easier because of this online facilitator. What what we have today is is that we are seeing you are witnessing, that Internet can be something that can work against democracy in the hands of anti democratic powers. This is actually very, very disappointing for those who thought that the internet will level up democracy in a global scale. But today we have Russia, China, and this Iran, they can actually these states can actually leverage Internet tools online campaign campaigns in a way that strengthens their dictatorial systems.

Jared York 10:29
Right. So what you would say is originally internet was intended to boost participation, make sure that everybody's involved in the democratic processes, but because of this open nature of the internet, it actually allowed more, I guess, malignant or bad actors to use it to then distribute false information.

Interviewee 2 10:56
Exactly, exactly. I mean, because the power balance is not democratic. I mean, there are big tech companies like Facebook, Twitter, Microsoft, and that has some say about how internet will be used by the individuals. And actually, states must see it in a much easier way to conduct the problem or overcome the problem caused by Internet by by discussing the problems with them, not the people. Maybe my point is not clear. But there is also dictatorial tendencies in the era of internet, these are not only the states, but other stakeholders, like the giant tech companies cannot be considered as fully Democratic supporters. So for example, they didn't, they haven't taken necessary steps to prevent online disinformation and dissemination of fake news on the platform's. Facebook is still very passive in this regard. And Twitter, today under Elon Musk, we cannot say that Twitter has portrayed a company that is pro democratic. So, these are very essential questions and in the in the very core of the discussion is that people in democratic systems need to decide who will rule them. In the process of making this decision, ideally, they must be informed well, to make an efficient or an effective decision for the public. But if you poison the sources, the channels, the ways they are formed, then their decision will be manipulated. So, in some cases, we cannot say this decision will be for public good, or the for the good or society they are in because they actually use their freedom to decide freely, because the information sources they feed is actually poisoned by by manipulation. Am I clear?

Jared York 13:50
Indeed. The big tech companies are really monopolizing the space and these with these huge platforms, and really undermining the, I guess, the Democratic, original intention of these social media platforms. But to that question, I know that the EU is starting to take action on this with the Digital Services Act, holding these big tech companies accountable. But how do you see that? Do you think that it is helpful? Do you think that there is more that could be done? What is your opinion?

Interviewee 2 14:29
I mean, I just attended a conference last year about this act. And what I see is what can I say about this regulation is it seems a bit more defensive instead of more proactive, or as an example, if I'm wrong, please correct me but there must be more support from EU to fact checkers. And there must be much severe regulations on those people or groups that disseminate fake news. I mean, still this Act gives some hope. But I don't think it can fully cover all the needs.

Jared York 15:34

And to this point, there is also a lot of discussion about if they use maybe stronger regulations, then there is a question of, is this taking away free speech from people? Is it too strict like censoring? What do you think about that?

Interviewee 2 15:54
Yeah. Actually, this is a very good question. My argument will be like this. I mean, what is at stake is our democracy, the the functioning mechanism, the only element that proves that there is a functional democracy is elections. If elections is under risk, I mean, then there will be a risk to lose a bigger freedom of speech, because elections can also be labeled as a sort of freedom of speech, because as an individual, I go to polls and express my freedom to determine which party or politician will rule, me and my neighborhood, my country. So in this respect, I mean, of course, freedom, media freedom is essential. Of course, freedom of expression is a fundamental human right. But I don't, of course, no one can argue that all these freedoms can be gave up or can be abandoned. And, of course, we must defend them. But one of the effective ways of defending them is actually regulating more fiercely against this kind of manipulation purposes. Campaigns with this manipulation purposes. If we stay silent, then the outcomes will be much more critical. For example, I live in Estonia. And after the start of war, many Russian speaking television channels were closed down, because of the concern that they will disseminate Russian propaganda within the Russian population living in Estonia and other Baltic states. So, you have to make a cost benefit analysis. When you see the this case, from outside, you can just say that this is just against freedom of expression, because media organizations must be kept open. But on the other side, if they start disseminating an aggressors narrative among the Russian population, in the mid and long term outcome will be much more damaging. This is my personal perspective.

Jared York 18:50
And you for that that is a very interesting perspective. And I guess one more question that I'm interested in hearing your perspective is, with regards to disinformation and the impact that it can have on democratic processes. Where do you think the knowledge gap lies? Do you think it's with the politicians? Do you think it's with businesses or citizens? Where do you think there's this lack of understanding about disinformation and its impact on democracy?

Interviewee 2 19:26
From the perspective of the public, an ordinary newspaper reader, I can say that they are sometimes unaware of the danger. I mean, they may see that a lie is just a lie. A fake news is just the fake news. But when we considered the reverse and developments in technology like deep fake, we can actually really predict that the risks and dangers in the future is much bigger. So I think that digital literacy is essential in this regard. And the end users, let's say, are the most responsible part of this equilibrium, I guess, yes, states and companies must take some steps. But at the end of the day, if the users are not aware and knowledgeable about the dangers, about online disinformation, then then all these steps taken by other stakeholders will be in vain. Because if one believes a fake news, or if one clicks a link that one is not supposed to click, or the Facebook ad is convincing for him, without questioning the ad ads being fact or lie, then it will be a trouble for him, then, you know, the rapid speed of dissemination of some news is very, very incremental. So it will be very late to reverse the process back. And so I think the strategic point that should be strengthened in this puzzle is the end user, the voter, the individuals.

Jared York 21:52
That make sense, definitely starting from the bottom and then going up in order to make sure that the end users understand why there are these policies in place and why they are important to protecting their democratic society. That's a very good point. Well, listen, I'm really, really grateful for your time and your insight. I feel like you brought up a lot of really excellent points. And the way you explained it is so clear. Thank you. And if you're interested, when I finished

the study, and I have results and published the paper, I'd be happy to share it with you. It might be interesting for you.

Interviewee 2 22:56
My pleasure. Please keep in touch.

A.d Interview Transcript for Interviewee 3

Friday, May 19, 2023 11:00-11:40 • 26:12

SPEAKERS
Interviewee 3, Jared York

Jared York 00:03
So I was wondering if we might be able to start talking kind of about your background, how you got involved in disinformation? And what sort of, I guess things do you work on in your role currently?

Interviewee 3 00:17
Of course. So, first disclaimer, I only got involved recently. And I, I guess, wasn't brought me there was a traineeship that I did in another unit in the administration of the European Parliament in the public opinion monitoring unit. And then a position opened up in the unit that deals with disinformation within the European Parliament. And I think I got the position because from my background, it fits quite well. I studied behavioral science before. And I have some background in quantitative analysis. And they were looking for a social scientist to join and help a little bit. Bridge the Gap, maybe between the more analytical part and then the more communication side of things. So my job is to help out with with analyzing all the information that we gather, on who targets to Parliament, and then translating that into insights that we can share with a less technical audience. Yeah, that is the overall picture, and if anything is unclear, you know, just let me know. And I'll try to elaborate.

Jared York 01:45
No worries. So it's just disinformation targeting the Parliament, or is it the EU as a whole? Or how does that work?

Interviewee 3 01:54
No, that's so the unit that I work in, they're specifically tasked with dealing with disinformation targeting the European Parliament. But of course, most people don't really distinguish between the European Parliament, the European Commission, all the other institutions. So oftentimes, it's targeted at the EU as a whole or the West as a whole. And then our focus would still be the things that have a direct relation to the Parliament, for example, disinformation that uses MEPs and their speeches in order to advance certain narratives, or that target specific personalities that are more revelant to the Parliament. But there is some sort of divide in who deals with what kind of information because now the EEA, the European External Action Service, they would have to task to look more at disinformation targeted at the EU as a whole coming from foreign actors. And while of course, there's also disinformation targeted to European Parliament coming from foreign actors, we only would look at that when it's just starting the European Parliament. So of course, we need to be aware of what's going on, and what's targeted at the EU as a whole. But it's not necessarily our task to raise awareness about the things that target the EU as a whole. If that makes sense.

Jared York 03:27

Absolutely. That makes perfect sense. Then, I guess moving into subtopic number one, disinformation sources and tactics. What are some, I guess, instances or some common things that you see, I guess, you mentioned one sort of targeting the MEPs. What other I guess tactics do you notice when it comes to disinformation?

Interviewee 3 03:55
I think it's actually, so sometimes MEPs are targeted, but I would argue oftentimes, it's also using speeches from MEPs or snippets of what has been said in Parliament and then portraying that as the opinion of the Parliament as a whole in order to distort the impression of what is the general opinion, maybe within the EU, and thereby influence public opinion. And then yeah, I think that that's actually one of the biggest that we we deal with is taking things that look official and you know, have some credibility because they have a Parliament logo in the background or because they can say you know, it's an MEP or whoever, and making that look as if it is the official Parliament position. So trying to use the credibility the Parliament bestows to propagate niche views, conspiracy theories, and narratives that are conductive to whoever's trying to spread that. And then sometimes we also see, I think, our spokesperson posted two months ago, an attack by a Russian network that uses a video of a German member of the Bundestag, and then he was taking, I think, snuff tobacco or something like that. And then they tried to frame it as if it's parliamentarians in the European Parliament, taking cocaine. So I guess it goes both ways, almost sometimes to take the MEP s and try to represent them in a distorted way. Or they take other people and say, well, you know, these are MEPs doing whatever kind of things who aren't really MEPs, but they're trying to tarnish the reputation of the Parliament.

Jared York 06:06
Right, right. So definitely focused on tarnishing reputation, would you say it's also motivated by trying to sort of shape elections within the EU? Is that something you would say?

Interviewee 3 06:20
Oh, yes. So, elections are coming up. And I would argue for the moment, right now we see more activity, for example, in Poland, because they have elections coming up. And then, it is our expectation that leading up to the elections in June next year, that there will be more disinformation targeted at the European Parliament. But I would argue that tactic, especially of foreign actors is mostly to divide, instill polarization and anti-elitism, you know, discontent with the EU as a whole, and they use different channels for that. You know, we can't always prove it. But when there's protests in France, then it's noticeable that certain actors publish a lot on that and try to maybe inflate the topic, make it bigger, make it to continue, because it might serve their agenda that there's a lot of public unrest, and it looks like the West is in some sort of disorder. So yes, for sure. Coming up to the elections, we see more activity.

Jared York 07:52
Right. And sort of on a similar topic. You mentioned that you're used to work sort of more in that department focused on public opinion. So as some you probably dealt with a lot of different public opinion polls and sort of got to see a bit into that, would you say that disinformation can be wielded in a way that is aimed at affecting citizens trust and lowering that trust in democratic processes and the EU institutions?

Interviewee 3 08:27
Yes, for sure. I would argue that's one of the main goals of disseminating disinformation, at least by certain actors.

Jared York 08:37
Yep. And that's reflected for example, in the EU barometer, right?

Interviewee 3 08:45
Yeah. So I mean, yes. The Euro barometer, tries to gauge public opinion and on various indicators among the interest in the EU institutions and national parliaments, elections and so forth. In our work, we don't make a direct connection and try to you know, following a disinformation campaign, let's see now how trust has changed. It's not granular enough for doing that. But from the broader academic research, I think that's what can be assumed and in general investigations into what especially the Russian actors tried to accomplish with added information at their distributing. That's something that's a working hypothesis we work with and we assume is one of the key purposes of their disinformation campaigns.

Jared York 09:49
Got you, and would you say that there is a certain demographic group that's more vulnerable or more frequently targeted by disinformation?

Interviewee 3 10:00
Oh, that's interesting. One of the techniques disinformation actors are using is definitely trying to target disinformation to specific demographics. And that may change depending on what's convenient right now for the campaign that they're organizing. And they are quite, how you say this, opportunistic when it comes to campaign. So if there's a vote, let's say on some new green energy measures, then they will use that and target it maybe at economically more vulnerable people because they're an easier audience with that. If it's something on women's rights or similar, they would target a more conservative base. So it's, I wouldn't say they choose a specific audience because they think that audience is best suited to disinformation, but they choose it depending on the topic, and then who is most likely to maybe have diverging views from the EU mainstream and try to create polarization wherever they can. So stoke outrage in directions that are easiest, in that specific context.

Jared York 11:33
Right. And maybe moving on to some of the regulatory and policy approaches. I was wondering what tools maybe specifically in the Parliament or maybe the EU in general users to combat disinformation, such as, I don't know, knowledge campaigns to raise awareness? Or are there different nongovernmental organizations? I'm just curious as to that.

Interviewee 3 12:06
That's a very good question. And I'm still trying to get a grip of that myself, because I always like to join. And there's a lot going on. But I will try my best. And then maybe I can share with you some resources afterwards, where you can read a nice overview as presented of all different things that are going on. So how do you go about this? In Parliament, we have this small unit that's tasked with monitoring, analyzing and responding to disinformation. Although the responding part is not that clearly defined. So what we do is basically documenting attacks at Parliament, and then in some instances, trying to raise awareness. And we have increased our awareness raising programs targeted at, for example, journalists, or teachers. So there's like media literacy campaigns shaping up, then within Parliament, we don't do that much other than maybe informing colleagues. Because we don't have a mandate to actively go about and say, you know, this is right, this is wrong, or this is problematic. I would argue that's more for the European External Action Service and the commission to do. So these are the other two key main players within the EU institutions. European External Action Service, actually, I would say is the biggest actor. They have the East STRATCOM Task Force. I think it's about 40 people working directly with this. Maybe you have talked to someone from them, so I'm not going to bore you, because they know much better what they do. And then within the Commission, I find it a bit complicated to understand because they have different DGs dealing with different aspects. And there is someone within communications who are trying to coordinate a network within the Commission and forging their response to disinformation. They are doing some research and actually they just published, or someone from that department, just

published published a book chapter explaining their approach exactly and how they've been working together. I don't know if you who have seen that yet, but could be helpful, maybe interesting because it goes in to quite a lot of detail how they work. And then there is another DG that is responsible for the Code of Conduct. And they are trying to work together with platforms in order to establish some sort of shared rules. And that would guide their work against disinformation and trying to introduce some accountability, make it more easy for researchers to access data in order to then investigate how disinformation spreads, and you know, what can be done about it. And then there's the Digital Service Act that is trying, that is used to legally enforce some of the things that the code of conduct is mentioning, but obviously not binding. So that's a very, like, high level overview. I can, as I said, share with you some more documents, but I don't think I'm qualified to go into more detail what exactly all these different tools are.

Jared York 16:18
No worries, that's, that's perfect. I'm looking exactly for a high level overview, because it's easy to get lost in the details. And especially when I'm comparing two whole democratic systems. It's it's very confusing.

Interviewee 3 16:35
I should have mentioned, sorry, I forgot. There's the alert system. I don't know if you ever heard of that. And it was set up by the EEAS, the European External Action Service, and it's kind of a platform to coordinate between member states, European institutions. And I wonder if the G7 is part of it or not. No, I don't think they're in there. It is used in order to coordinate between them and share alerts in case something happens, and others should maybe know about.

Jared York 17:14
Is that the RAS, I think is the acronym?

Interviewee 3 17:20
Yeah, okay, ARS.

Jared York 17:24
And maybe one last thing in terms of the regulations, you did mention that there is the code of conduct, which is more so like soft regulation, whereas the companies are signing it, and they're agreeing they're going to follow these different, different rules. But the DSA is more of the hard regulatory approach to really combat, I guess, and hold the different social media platforms accountable for what they're doing. Maybe apart from these hard and soft approaches, what else has been done maybe for society as a whole? Are there any I guess, you mentioned media literacy campaigns? There are these campaigns going on right now? Or? Were there some in the past?

Interviewee 3 18:18
Hmm, yes, I am. So I think the Commission especially works very closely together with EDMO, the European Digital Media Observatory, and they coordinate fact checkers within each member state. Because one of the key difficulties, I would say in the European Union is, there's a lot of different languages, and you need someone to kind of respond in 24 different languages to disinformation. And so they build up this network of fact checkers that are supposed to work in the different member states, and they also do media literacy courses. The European Parliament is not usually the institution that gives grants to civil society organizations to do media literacy courses, and so forth. So I'm not entirely sure if who received what kind of funding from European institutions, I think that would be more the Commission that's responsible. Like my unit itself is doing some media literacy courses and raising, but of course, that's like dropping a hot stone. Very small compared to that challenge that's out there. But we

collaborate with other institutions. So for example, we are organizing different events, maybe and then we'll invite fact checkers or civil society outreach institutions that are doing media literacy work and we are in constant exchange with them about new developments and, you know, trying to help each other out, although oftentimes is not maybe such a formalized agreement or exchange. It's more like off the record, how can we better work on this kind of thing. But I'd argue it's quite clearly understood from within Parliament and the other European institutions that it's like a whole of society approach that's needed to combat disinformation. It's not just institutions that need to work to fight that. But we need to work together with civil society and the platforms to do something. Right. And there was also a committee within Parliament wasn't there specifically on disinformation? I think it was a special committee. Yes, INGE. So there was INGE, I'm not even sure what INGE stands for, but it it was supposed to target interference and democracy and foreign stuff, blah, blah, blah, very long title. And then that committee was continued and called INGE2. And it's still unclear whether it will be continued again. Okay, here, I need to be careful, because I'm not yet sure what has been voted on and published and what hasn't been. But the committee was, indeed tasked with investigating how much disinformation is a problem within the European institutions, especially targeting the Parliament. And it is also based on their recommendations and findings that my unit within the administration of the Parliament was set up. So our mandate to monitor and analyze disinformation targeting the Parliament follows from that committee.

Jared York 22:07
Okay, very interesting. Maybe one final question to sum that up, is there any to your knowledge, of course, is there any, I guess, approaches that are joint between the EU and the US? Or are we learning from each other? Do you see collaboration in that area? Or what do you think?

Interviewee 3 22:32
Hmm, good question. Okay, and disclaimer, again, I've only been there for for a month. So maybe I'm not aware of many things. The time that I have spent there for now, I haven't really seen any collaboration with the US for the moment. I would say. But you know, we also work together with NATO and the US is a member of NATO. So I guess there is collaboration, but the parliament itself, my unit in the Parliament, collaborates with the different member states, with the Commission, but not with third member countries that I would know of for the moment. There's sometimes these delegations by Parliament sent to different countries like, I think they call it fact finding missions. And I don't know, maybe the INGE committee and committees tasked with disinformation travel to the US at some point to investigate the matter further. I don't know that. You would probably find it on their website, if you are looking.

Jared York 24:04
All right. Well, well, I think that's all the questions on my side, I if you have anything else to add, you're more than welcome to. I would ask, though, for the, you said there was a new publishing by the commission that sort of talks a bit more on their work, would it be possible for you to maybe forward that link to me?

24:26
Of course, of course, oh, I'm gonna do it right after so I don't forget. And in case they still do, just remind me. And I think it's a chapter in a book called, "Fighting...something with "Infodemics in the 21st century". I will look it up.

Jared York 24:48
Thank you so much for taking the time to speak with me. Very, very enlightening. I have taken quite a few notes and I'm excited to include them in the study. And if you're in Interested and it is something that sounds interesting to you, I can definitely forward you my study when it's finished. And yeah, I'll share that with you. And thank you again so much. I really appreciate it.

25:16
Thank you. That was really, really nice. I hope, you know, my knowledge is still limited, I hope it was at least a little bit useful for you. And I would love to read your study. So if you can forward it, that would be very nice. Indeed. I will make sure to share the link with you and if there's anything coming up, or you would need someone with maybe a bit more expertise and background, let me know and I'll try to find someone and put you in touch. I wish you all the best with your master thesis. I know it's quite a process.

Jared York 25:55
Indeed, indeed. Well, you enjoy the rest of your weekend. Have a good day!

A.e Interview Transcript for Interviewee 4

Saturday, May 20, 2023 11:00-11:40 • 27:56

SPEAKERS
Interviewee 4, Jared York

Jared York 00:34
Maybe we could start, I guess, with a bit about your background sort of how you got involved with disinformation and your interest in it.

Interviewee 4 00:47
Yeah, sure. So, some sometime around one and a half year, 2022 early winter, I joined the Lithuanian independent technology think tank, which researches disinformation and runs educational media literacy campaigns. Why? Because I was following disinformation related developments for some time. Also, because my native language is Russian, like I could see that there is a lot of disinformation coming from, from that direction, from Russian Federation. And I could see that people who I know in Estonia and Finland, they really echoed some of the disinformation narratives. So there is also personal interest. And then I joined to the Lithuanian think tank and I worked with them on on the project. And then shortly after that, I was invited to work on some projects for New York based disinformation analysis company called Graphika.

Jared York 02:28
Sure. So are you originally from Estonia?

Interviewee 4 02:32
I was born in Estonia in a Finnish-Belarusian family with Russian as a native language.

Jared York 02:39
Oh my gosh, quite an international background.

Interviewee 4 02:43
Yeah.

Jared York 02:45
Okay. And so, the Lithuanian research group was that part of debunk, debunk EU?

Interviewee 4 02:54
Debunk EU, yes. Lithuanian Debunk EU, US New York based Graphika.

Jared York 03:03
Got it. And Debunk EU is a nonprofit organization, right?

Interviewee 4 03:12
Yes. I believe they receive probably government grants, and they operate based on that.

Jared York 03:22
Okay, I see. Well, that's really awesome that you have experienced both with an EU organization of disinformation and New York based organization. So maybe could you tell me a bit more about what some of your activities were, for example, starting with Debunk EU? What were some of the things you did to research disinformation? And what were some of the things you've came across while there?

Interviewee 4 03:48
Yeah. So for Debunk, I worked on the project which was analyzing how Russian state television was preparing the domestic audience for the invasion of Ukraine. I can share the link with you for the analysis because it was published on their website. Let me check. Ah, here it is. So the name of the published analysis was "Alternative Universe Kremlin TV Prepped its Russian Audience for a Full Scale Invasion of Ukraine", let me drop a link in the chat. So this one and for Graphika I worked on two projects. Unfortunately, I can't tell you which ones and who were the clients because in this instances, there was a client who ordered from Graphica, New York based disinformation analysis company an analysis of two different topics, I can tell you that one topic was [incomprehensible]. And another one was LGBTQI plus. And then we were we're analyzing what kind of narratives there are regarding LGBTQI plus in a set of countries, and what are the key actors, key narratives, key messages there, and then we present an analysis, but unfortunately, that's everything I can tell you. I have a non-disclosure agreements, so but I think it gives some idea.

Jared York 12:01
Okay. So the question was, how does disinformation, impact democratic processes and democratic institution?

Interviewee 4 12:12
That's a very, very good question. In the short answer is in all possible ways. So the idea is that disinformation, this disinformation has real consequences in the in the lives of people. So despite maybe being spread online consequences are seen in real life. What it means, it means that there are a number of examples, the most clear one is the fact how disinformation can affect the election process in democratic countries. If certain narratives are spread, the voters voting behavior changes, and well, the impacts are real. So this is definitely a risk a threat for the democratic institution and democratic processes.

Jared York 13:46
Do you notice is disinformation activities evolving with time? Are they using new methods that are different from before?

Interviewee 4 13:59
Yes, indeed, very good question as well. Because the technology develops allowing for disinformation actors to use this technology to amplify their messages. For instance, you've probably heard already about the use of AI in spreading disinformation messages, making fake images and all technology for instance, AI helps to reach larger audiences and a multitude of platforms. If you go one step back. You know, the disinformation was there 500 years ago, 1000 years ago, however, you know, it was made via a piece of paper, which was then printed and circulated to the very limited amount of people. And it was the development of the technology

today, we have internet, social media, where messages can spread across the world in the fraction of a second. So what it means it also means that these information messages can reach much, much more people. And the intensity of these messages can be much higher. So definitely the the tactics also evolve, following the technological development.

Jared York 15:51
Right, good point. And you mentioned social media. Do you think that these giant social media platforms should be accountable for the disinformation that spreads on them? Or what is your opinion?

Interviewee 4 16:08
That's a very good question as well. This is the discussion which has been going on for a while now, where is the limits of accountability of social media platforms? So I think there is a large agreement that social media platforms should be accountable for certain extent, what it means, it means that the social media platforms should have moderation which checks, you know that there is no sexual content, videos, or images or messages. There is no violence, messages, videos, images, and also that the images and videos and messages, which are published on social media platforms, they are correct, and they're factual, and they are true. So the social media platforms are accountable to certain extent. However, I think the challenge here is that the amount of messaging and images and videos, disinformation, is so big, it's so vast. So it's simply not possible to be able to monitor in real time, everything that is going on. So it is definitely a challenge for social media platforms. But the help comes from civil society, NGOs, private companies, which do work in the field of disinformation, and which do analyze social media platforms, because it's one of the key playgrounds where disinformation is spread. So social media platforms do something by themselves monitoring, but also the private sector and civil society also help to ensure that the social media platforms sharing as little disnformation as possible.

Jared York 18:32
All right, and would you say that the civil society or society in general, are they aware of disinformation threats? Or do we need to include more media literacy campaigns? Is there still this gap of knowledge? Do you think?

Interviewee 4 18:54
Yes, this is a very important point. So Debunk, I'll send you again the link for Lithuanian disinformation think tank Debunk, because one of the objectives of Debunk is also to raise awareness about disinformation and train, especially young people, teenagers, about how to be literate in information field. This is one of the keys because it won't be probably possible to constantly monitor and flag all the disinformation which is out there. And a lot of responsibility lies within the user of internet or social media or person. So what we want to do, I think we want to train individuals to be critical thinkers, to look into different sources and provide them with some tools for how to be able to spot disinformation, and, you know, protect themselves from it. So definitely media literacy, especially among young people is one of the key elements very important.

Jared York 20:38
All right, and do you know, if this has been driven at the EU level, is it at the national level? Who is driving these media literacy campaigns?

Interviewee 4 20:56
That's a very good question as well. So I will provide you some links. So at EU level, there are definitely y some attempts...Here's the link for what the EU does. So already in 2015, the heads of states and governments at the EU level, they agreed that disinformation campaigns are a risk for democratic society and the European Union. So after that, there was an action plan against

disinformation 2018. And then there was European democracy action plan in 2020. You can see that via the link, which I put put in the chat. And then European External Action Service, which is part of the European Union ecosystem, they have East strategic communication division, which runs website EUversusDisinfo which debunks some of the most prominent disinformation narratives, especially when it comes to countries located east of European Union, but also China, for instance, and and Iran and others. So definitely the European Union invests in to the topic of disinformation, also the European Parliament had a whole special committee related to disinformation and COVID. I will provide you a link for that as well. So the European institutions are looking into this matter and they do actively recognize that disinformation is a threat and something needs to be done. In addition, there is the number of European level civil societies or NGOs, organizations such as, for example, this disinfo.eu, which also there are a number of others in each country. There are several which actively work in that field. So all together, European institutions, civil society, private companies, they create this ecosystem, which tackles disinformation related issues.

Jared York 24:16
Excellent. Thank you for the links. And maybe one more question. Before we finish. Do you notice any differences in the approach between the EU and the US when it comes to disinformation? Are there any examples of lessons that either side could learn from each other or collaboration opportunities? What What is your opinion?

Interviewee 4 24:42
Yeah, this is a very good question. I maybe wouldn't be able to tell you about differences. However, what is certain is that the US and the EU recognize that it is not It's possible to fight, to tackle disinformation in isolation all by itself. So what is important, is international cooperation between democratic countries and democratic institutions. Because the magnitude of disinformation is huge, so the resources of one country, the US or the block of countries comprising the European Union, won't be enough. So it's definitely a great idea to join forces. Because many of the problems related to disinformation, they're similar. For instance, we discussed already media literacy. So you know, US and EU could cooperate in promoting media literacy. So the key here, I would say, is international cooperation between democratic countries. The differences, to be honest, I am not familiar that much with what's going on in the US. But I would maybe highlight cooperation here is very important.

Jared York 26:20
All right, excellent point. Apart from that, I think we covered most of everything. So I don't want to take any more of your time. But I would like to thank you very, very much for your insights. I feel like I got a lot of great information and links from you, that will be very helpful to finish my research. So thank you very much.

Interviewee 4 26:48
Well, Jared, thank you for contacting me it is a pleasure and I wish you all the best successes your master's thesis very important topic I think you chose very important and timely topic. I'm looking with a great interest for publication of your master thesis and feel free to send it to me once it's ready. I will read it with great interest well and success success with your successes, your master program and finalizing your studies and master

Jared York 27:29
Thank you!

Interviewee 4 27:34
you so much. And let me feel feel free to contact me via LinkedIn or email if you need any more. Maybe clarifications or additional details, maybe I could provide some more links. So feel the feel free to contact me in case you need.

Jared York 27:48
Well, they're well there. Thank you again.

Interviewee 4 27:52
Thanks a lot. They have a nice day.

A.f Interview Transcript for Interviewee 5

Thu, May 25, 2023 12:21PM • 38:48

SPEAKERS
Jared York, Interviewee 5

Jared York 00:06
Alright, so, I guess to get started, would you mind maybe introducing a bit your background? Maybe your qualifications and some of your experience working in the field related to disinformation?

Interviewee 5 00:21
Yeah, well, I mean, the disinformation thing isn't really my direct area, obviously, it's just the side interest, as you know, but I don't have any degrees in that. I do have six academic degrees, but none of them fits perfectly to this. But as you know, my primary appointment is a professor of governance at TalTech's Nurkse school. My first sight appointment is as honorary professor and PI at University College London, IIPP. And the third one is at the Davis Center for Russian and Eurasian Studies at Harvard University. And, of course, this is one of the places where you deal with Russian disinformation. And also with the Russian interference in the American elections, for instance, which comes in various degrees and shapes, and is very interesting in this context. Then, you know, I do have a certain interest in the digital, if you will, and the role of social media and the change of both politics and governance, to the point that, you know, Estonia is supposed to be the digital leader. Now, we all know, it's not really but. It's very, very good and advertising itself. And it's not bad. You know, it's certainly in the top. And my two claims to fame for that was that for about half a decade, more than 50% of all Estonians who had a PhD in governance had it under my supervision, that means I started this. And also I taught the first class ever on e-governance in Estonia. And yeah, when I was still at the University of Tartu, so I have been doing that since a long while. Too long I guess it's time to retire. But this entire idea of digitality here is important. Now the Harvard connection also has more than that. The Berkman Kline Center for Internet and Society is probably the leading center in the world dealing with this, and these are good friends and also my own PhD and colleague Kostakis is a fellow there. And I do a lot of stuff, both there and in the Kennedy School. And there is also just the physical proximity that you have in Harvard, in that in our buildings. These are two buildings on Cambridge Avenue, which house the area studies and stuff like that. And somehow a lot of stuff is happening there as well. So you have these kind of lunch talks and brown bags and conferences that just happened literally every day. And that gives you a nice, a nice access. One thing that, as you might know, I have a particular expertise in Southeast Asia. And so the last time I was there, there was actually a meeting on the last Philippine elections where the question was very, very much about this kind of disinformation. And the speaker was Maria Ressa, who was then a fellow and who won. I mean, she's a Nobel Prize winner. And this was typical Harvard thing. 17 people, including one Nobel Prize winner talking about her work. That is, that was really interesting. And that got me if you will to consider what this information versus disinformation really is. I think that was long enough.

Jared York 03:54
All right, perfect overview. I am definitely very curious to hear a bit more in detail, I guess, oh, what's going on at Harvard, in what you've sort of got your hands on there. And I think there is quite a connection between disinformation and e-governance, and especially with the implementation of these technologies being used more and more within government and public administrations. So I think it's an important aspect to consider as well, especially with AI and other legislation that's following that. But yeah, please, if you don't mind, maybe a bit more detail about Harvard and what's been going on there.

Interviewee 5 04:39
So I think one of the biggest issues with your topic is really a definitional one of what you call "disinformation" and what you call "information". For me, there is a parallelity, and that's also not my own idea. I heard that somewhere that "disinformation" is a word like "troll". That means that you use it as an insult with people you don't agree with. So so it's actually, that's, that's a problem I have this tendency to if somebody does three comments on, I mean, recently somebody posted a podcast of mine for German consultancy, one hour podcast on LinkedIn. And then somebody had like three comments on this and really bizarre comments, and I was very tempted to to write as my comment, "don't feed the trolls". But of course, to call somebody a troll is I mean, there might be something to it, it might be an unnerving guy, but it still might not be trolling. And the same thing is with disinformation because it is very, very difficult to do a delineation between propaganda, if you will, and disinformation specifically. And if you do that, of course, both sides have it. And I remember hear the former Estonian minister of defense and former Rector of our own university, Jaak Aaviksoo, who said to the point that scientists have no right in a situation of serious conflict and war to tell the truth, because you're supposed to do propaganda for your country, and that is your first duty. And of course, in the in the current situation with the Ukraine invasion, we are back to that in Estonia, for sure. That means that most people wouldn't see honest information that will endanger the one's own country as legitimate. But then the question is, where is this delineation here? So the question is, really, is this something that has a really strong normative contents? And it is also something that shifts the blame, if you will. Namely, I think that, interestingly enough, there is a political connotation with the term "disinformation". I don't know whether you've seen that. Normally, disinformation is a charge that is brought by people from the political left to the political right, not so much the other way around. Also, you would assume, unless you're a very hardcore person, yourself from the political left, which I'm more or less am, but still, that is quite interesting. You would you would think that the charge happens on both sides. And an explanation for that might be that one of the biggest problems for democracy theorists, and I think you deal primarily with US and Europe, or what was it?

Jared York 07:45
Yes, US and Europe.

Interviewee 5 07:46
Yeah. So the number one topic when I'm at Harvard, where there is the most events, the most talks by the best people is the crisis of democracy. What people are really worried about, people at Harvard, is why is democracy in crisis? If I take the views from research, which is probably the best my colleague from the Kennedy School, on faith and democracy, it is actually I mean, you can justify it left and right, but it is declining. And if you ask litmus questions on Democracy in America, such as my favorite question is a strong capable leader doing his own stuff is more important than the useless bickering of people in parliament, you always get more than 50%. And that is a litmus question that is authoritarian at heart. This conviction. Yeah, there's not being liking to do that. Now. But there is a problem. And it's a problem that the left had always and the left has had. I mean, left in a very, like really the left 50% of the spectrum, not the radical left. And that is that the left is supposed to trust the people. Like the common person in England we say, or used to say "the man on the Clapham bus". That's the bus that brings the suburban workers to the city, right? Something like that. "Lizzie Miller", say in

Germany, Lizzie Miller, because it's a very common name. And the question is whether he was still allowed to say it because it might be gender discriminatory. But anyway, so the problem is that the left should trust the people but can't because very often the people there people vote democratically for results that one doesn't like that is the famous current differentiation between liberal democracy and democracy is such right, that having a minority the majority is not enough to qualify as a democracy. But if we say that if we put the values of your average American political scientist on list and of the four top countries in the world only one is kind of democratic. And that's the US. Because if I put any basic values in India, China and Indonesia are certainly out. I mean, they're not real democracies, they're just democracies. You can't, you can't have a direct impact on what the result is. So, but the problem is what happens. So there's two threats for democracy, right, competitive authoritarian regimes, and people voting for candidates that political scientists don't like, and don't like rightly, Trump being the first example. So you need to have an explanatory for that. And very often, it seems that the term "disinformation" is an excuse that the left half, and in Harvard that will be over 90% of political scientists and digital researchers, put on a discourse for justifying why the people aren't smart enough to vote against authoritarian leaders such as Trump, because if they were smart, they wouldn't. So and that is a that is an interesting point. But there, this is why your research topic is at the core of the current political discourse, but it's very tricky, because it's very sensitive. And, you know, Marx himself was, obviously the founder of the radical left for our times he says that the proletariat doesn't know its political role, and it needs the party to be reminded of what its role is, and what the roles of the individual are to bring about radical change. That was his point. But this is the issue, why communists can say we don't care what the people say, because they don't know. But that is an argument that's very difficult to make for a mainstream Democrat. Because if you say that you actually feed to Trump's. Yeah, if you if you qualify people as deplorable and so on, and so on. And so, is this okay, but I'm talking about does that help you or am I going off on a tangent?

Jared York 12:07
No, absolutely. It's, it's a great perspective to have. Yeah.

Interviewee 5 12:10
Okay. So let me give you a concrete example from this talk with Maria Ressa. So Maria Ressa is a journalist, editor of the Rappler and she's the one who won the Nobel Prize and stuff like that. And you know, that at the last Philippine elections and Philippines, a very large and you have a lot of Pinoy guest workers in the west by now, you know, 1.5 million alone in the American Health sector, which would collapse if people from the Philippines foot go out. And the reason is because of American colonialism that the Philippines, the Philippine people speak basic English. And that gives you a huge advantage, of course, and in the global job market, if you have that right away, and a functional one that and so there was this populist, really bad, mini Trump leader elected and then again Bongbong Marcos, the current president, was the son of the former dictator, Marcos and his wife the famous Imelda, "the iron butterfly". And this is a a family that according to all American legal standards, has stolen billions and billions dozens of billions of dollars from this country and actually, Marcos, the father, is in the Guinness Book of World record as the greatest corrupt person in, I don't know, recorded history that means he's stolen more from his own country than anyone else. And that's something you know, there is a lot of feeds around and and you know, these trials are very clear Imelda, wanted to finish some some house in Manila. And then there was a collapse and workers fell in because it was built for too strong. And since you wanted to finish the house, you said okay, let's put concrete under and leave the corpses in the structure. I mean, she's he was pretty or is that's that's not my point, an important person. Now the important thing is that Bongbong Marcos, the president who was elected is absolutely about not paying back and not owning up to the saying that this takeover against which there was the only really big Philippine Revolution was that nothing really happened and that his father was a great development guy and so on, maybe a bit authoritarian, but in principle, he was the good guy and the revolutionary leaders were the bad ones now, if you want. He won, pretty much in a landslide, right? And there was a counter

candidate, everybodys favorite candidate and she lost. She got a fellowship at Harvard, where also her daughters are studying and so on and so on, Leni Robredo. Any intellectual, anyone with a degree was basically for her. All my friends were. I didn't know a single person in favor of Marcos in my own network, and it's rather large. But how do you explain that? And so at this very discussion, which was actually the last discussion I had at Harvard when I was there physically, because it was on the day I was leaving, and I had the evening plane from Boston back to Frankfurt. And I really found and they were very, very good people present. And that was exactly the question is this based, Philippines is, as you might know, one of the strongest Facebook countries in the world, much, much more Facebook heavy than the US or Estonia or anything like that. And you know, that if you talk about how people get informed through media and through the internet, you really need to differentiate the places there is even such a term called "Facebook racism", because again, Western academics tended before the Musk take over to be on Twitter. And the mastodon move didn't work. But much has been gravitated or towards LinkedIn. But but so there are Twitter thinkers, and there are many Western intellectuals also in Estonia, who also in our departments are indeed who do not have a Facebook account. But all government in the Philippines or in Thailand, or in Cambodia, happens on Facebook. So it's very important where you are, but because of Facebook, and because the Philippines are mixed English and Tagalog, you can actually follow it quite nicely. It's easy to analyze, and not only was Oxford analytical, and so two things are true. The first thing is the propaganda, if you will really did happen on Facebook. So this entire big lie in saying Marcos was not an evil dictator, but friendly developing economies, basically, like Lee Kuan Yew and Singapore may be rough on the edges. But in the end, we're all wealthy, which is of course nonsense. In the Philippines. Nobody is wealthy except the very big plutocrats and the, the families. But so this is the scenario and it's a typical scenario now for Western Digital politics, egovernance, and so on, and so on people in coming in and saying the Philippine elections were lost by the moderate left and the Liberals because of this disinformation. But is this really true? And out of this argument, I would also say that, of course, you go through certain performative gestures, you give a kowtow to what's currently in but that's the same in the US if against certain correct truths you wouldn't be against you can't really do that. I mean, if you're on a certain part of the European spectrum, to say I'm against sustainability, that's just not gonna happen. You're gonna lie about and, you know, the sustainable development goals, how can you argue against those, you're alone, you're a French guy. So But beyond that, if you look at the actual propaganda of the Marcos team, it was actually amazingly honest. And I would have a problem in calling that this information. You Imelda Marcos is still around. She gives these interviews in front of originals by Picasso and Suzanne, which they stole which was paid for by the by the people's money, which is in the New York court. She's supposed to give back. She's just sitting there and she's not giving it back. And she's very open about it. She's very open about it. So you know, this happened and about, you know, this guy Aquino who got shot, and I didn't order him to be shot. But he did talk a little bit much. So anybody can realize what she's saying here. Yeah. So it's a it's a typical example for me the last Philippine elections, where too much simple analysis blames the authoritarian victory on disinformation. But it is really because of a certain complicity with crockery by a large majority of the people who in the end thought that their own lot would increase more with this. And of course, it won't. Of course, they won't help the people for a certain thing, but you do get to certain largess, a certain distribution of money. Like for election press and some stuff like that. But that, for me is a typical example where the "disinformation label" is too lightly used. And in order to be useful, because in the end, I mean, you're looking for it for your thesis, I'm looking at for the site of social analysis. So the there's a beautiful word for that in German "Erkenntnisinteresse", it means the interest to recognize something or to understand something, and you need to describe it very much around whereas in Germany, you have one long word. And that means what what is actually our interest? What is actually the question, and my philosophical teacher, Hans Georg Gadamer, some of his books, you can't really see it on the back thing. He used to say the question in science is, if you see a book, what is the question for which this is the answer? And he says, also, at some point in the sea of words, when a language evolves, we give individual words to phenomena that are so important that they become somehow central to the discourse. So what is the added value of

disinformation? And that was a very theoretical framing. But why are we using this word "disinformation" at all? And I would say, to describe a specific online phenomenon that goes beyond propaganda, and perhaps even beyond a certain form of lying. And it becomes valuable, for instance, now with the AI debate with a deep fakes and so on and so on. But in order for the term to be useful, we need to be precise of what we are saying not because of scientific Fun and Games, that because only then is it useful, analytical tool, and we do have to watch our own biases. This was the point of my previous talk points, that because we want to say the people are smart, but there are tricked by evil manipulators that you realize that no, sometimes they are complicit with authoritarian regimes. That's what you get. They're not tricked, they get this, but they for instance, accept it. Most Filipinos, say, "Sure, Imelda steals stuff. She does that?" Yeah. "So? We're still gonna vote for her family because we're still better off and the other ones can't manage it either." The problem in the Philippines is that the liberals, when they were in government, they didn't help the poor people either. And so you know, for them, that's not an alternative. So I think this is a really important thing here to say, and that is, that is what I meant to say, when I saw your topic.

Jared York 22:55
That's an excellent perspective. And something that I really struggled with in the beginning of this thesis was how can I, in an unbiased way, define this information? And not only that, I'm also measuring its impact on democracy. Well, how do I decide what is determined as a democracy? So after exploring through democratic theory, I came across an interesting approach. That's like, a problem based approach where you essentially look at three key functions within democracy. So you look at whether there is empowered inclusion. So are all of the wider civic civil society being involved in the democracy? There is also collective agenda and will formation. So are people supplied with information that allows them to create these narratives and opinions on their own? And then the third would be collective decision making. So that's more related directly to the elections. Are there things that are impacting their ability to participate in elections, or that are making the elections unfair? So even with this framework it's still up to a lot of interpretation. But it did give me something to sort of look at, okay, these are the areas that we see disinformation impacting. And because I'm looking at the policy responses from the US and EU, these are the approaches they're taking and how they're addressing this issue. But as you said, it is a very sensitive topic, very easy to be influenced by bias. That's an interesting perspective.

Interviewee 5 24:32
Yeah, I mean, the thing is, what you need to do if you deal with something like that, is that you don't claim that anything is the case, including this framework, this definition of democracy you use, it's not uncommon, but it's certainly not held by a majority of political scientists. It's very specific. And of course, you know, that by that definition of democracy, we have less than 10 democratic countries in the world is very small. It's it's a very exclusive definition and actually Most of political science has moved into an acceptance of what's called flawed democracies. So to say that these are still democracies, but with a problem and to talk about the continuum, because otherwise, you're really talking about a bunch of white people in cold climate. Right. I mean, that's, that's what you get, essentially. And the question is whether that's not more problematic than than it is an answer, right. Other than that, the the Ukraine war has given a real booster to Western values and Western identities and something to be defended. But I, I think this makes a lot of sense. But at any given point, you must say, I am in this thesis, adopting for functional reasons like 123, this approach by that and that person, and then go with this. One good thing in the social sciences says is that if you don't claim anything as a fact, but that there are choices, and you take this and not the other, that cannot be faulted. And that is, that is the only way you have that you never talk about reality, but about choices that you make in order to understand basically the heuristics thing. I mean, that is what this area, I would very, very strongly recommend, if you already go to the democracy theory, that is a complete minefield.

Jared York 26:31

Right, right. Professor, maybe one last question before we finish off, because I know you're involved in both the US side with Harvard, and you're also an EU citizen, yourself. I'm just wondering from the citizen point of view, do you notice a difference in the approaches, for example, in policy approaches or approaches to disinformation as it is now? Do you notice differences? Do you think there's maybe something we can learn from each other on either side? What's your opinion?

Interviewee 5 27:05
Yeah. So, that's a good last question. But it may take a while. So let me see how I can do this briefly. So you know, that in principle, on this level, democracy, democracy theory, and so on right now, once again, the EU in general looks down on the US. But I would say that the discourse level, but of course, it's a, it's a bubble thing on the US in the top plates, this is actually higher. And, and the response is actually better. And that's the old problem, you know, with the Lisbon Strategy and other things like that, that in spite of all the criticisms of the US, the US is ahead, militarily, scientifically, education wise, intellectually, only that this happens in a fairly bubbly kind of thing. Again, I recall a Harvard Kennedy School discussion on discussion where my, my good friend, Jane Mansbridge, whom I think has one of the best theories on these things, said after this exactly issue was discussed, you realize that we are here in a room with 200 plus people, and there is not a single Trump supporter. But there was a majority of people who voted for Trump out there. So it's this difference. So in this room, you have a higher level of discursive competence on disinformation that you have anywhere in Brussels, or in one of the member states, we do not have top outfits in Europe that actually deal with that. We do not have an institution anymore that deals with this for the commission, that means what's called J DRC. That just doesn't exist for this topic. And so I think as far as that is concerned, as far as the actual problem analysis, the thinking ahead and so on is concerned, Europe can actually learn from the US. But the problem with this is that there is this old European prejudice to say that we are culture us a civilization, they do the technical stuff, they steal our stuff, although that is not true for a long, long, long time and more. There is actually now if you say Europe, the problem is that I do see a relatively high level of this discussion in the United Kingdom where it's also really needed because you do have a government of gas lighters since a while, I mean, the last three prime ministers incurring, including the current ones now okay, this is a normative statement by myself. But yeah, I would say even beyond personal political preference, this is this is incredible who you have there, but the both the policy think tank and the academic perspective on these matters. In London is very good in the various other top universities, not Oxford Oxford Internet does not that good as people think. But I mean, the other ones are pretty good. And the but the problem is that, of course, England isn't part of political Europe anymore. So this is really out. And if you would ask me who are the top analysts on this topic, and also you know how to formulate a policy response towards the threat that is, if you will emerge in as you rightly said, with AI, if you would say, which is the best place in the EU that deals with this, I would have to think very long. Whereas I could name the places and the people who deal with this in London, and in Boston, and also in Washington, DC and also in Palo Alto, quite quickly. So. And it's I wouldn't say, say that as far as social media involvement, there is really a huge difference if I look at the two. So the problem for the EU is as big, especially as an emerging threat, that it didn't happen right now has something more to do with party structures, and so on and so on. But on the other hand, that is certainly not something to slip on, if you're a responsible politician. Right. So, yeah, I would think that on the policy, policy formulation and policy framing, sight on the topic of disinformation, Anglo America is in the lead.

Jared York 31:40
Very interesting, okay, well, you definitely gave me a lot of food for thought there. In that case, I think we covered a lot. I really appreciate your time. And if you are interested in this topic, which I think you might be, I'm more than happy to share my research after I finish it. I'm planning to submit it and then the defense will be finished by the end of June. So after that, I can share with you my findings. Thank you so much for your time!

Interviewee 5 38:43
Yes, please do. Thank you!