HYBRID WARFARE & DISINFORMATION

Struggles to regulate the new battleground

Aina Laura Errando Calleja

Student Number: 0561159
Course: European Security and Counter-Terrorism
Professor: Raluca Csernatoni

Brussels, 17 January 2021

Abstract

The increasing importance of the role of social media has compelled governments to take action and consider cyberspace as a paramount sphere in which (dis)information can be easily shared.

Disinformation threatens democracy as it has the potential to undermine national security. From a security perspective, this paper focuses on the impact this phenomena has had in the previous years. The author will analyse to what extent disinformation and hybrid warfare pose a threat to democracy and how it has been regulated in Europe. To do so, first, the concept of disinformation and its intricacies will be examined. Secondly, Poststructuralism and Strategic Theory will be used to depict that change towards a 'postmodern' world and what 'hybrid warfare' implies. Thirdly, a short explanation of the development of Information and hybrid warfare is included to describe their characteristics. Fourthly, the French and Spanish attempts to regulate disinformation are shortly explained and, finally, a last section illustrates the implications of Artificial Intelligence in the European context. The article concludes that latest developments have shown that this kind of warfare has opened 'new doors' of conflict and that legal matters remain unclear; however, tackling disinformation requires collective cooperation and further research is needed on the field.

Introduction

Information means power and dominates society. 'Post-truth' was designated the word of the year in 2016 by *Oxford Dictionaries* and 'fake news' was the word of year 2017 for *Collins* Dictionary. This showcases the increasing relevance of disinformation and borderless cyberspace. The World Economic Forum identified online warfare and disinformation as 'one of the top ten global risks' (Golovchenko *et al.*, 2018). The dissemination of disinformation can be carried out by a state, 'purposefully targeting the society of a foreign state' and this has led to 'an international struggle' for geopolitical power (European Parliament, 2019). The information framework becomes 'the *de facto* center of gravity' for conflicts (De Vries, 1996).

Current breakthroughs have made information more accessible. Disinformation has had a clear impact on public discourse and institutional legitimacy can be put in question. Individuals are the target but also a medium to disseminate information as citizens can be more influential than states and traditional media (Golovchenko *et al.,* 2018).

Can a government filter false information, propaganda and disinformation while, at the same time, preserve democratic values that define our societies? The EU has tried to create a robust and harmonized strategy including national governments, citizens and the private sector. Social media do not generate content by themselves but 'transmit, organize and amplify it' (European Parliament 2019). Some EU initiatives have been passed such as 'the Communication of the Commission on Tackling Online Disinformation' or the 'European Parliament Resolution on media pluralism and media freedom in the European Union'. There have also been national attempts to develop legislative initiatives like the French and Spanish ones.

The research question that this paper will address is to what extent have disinformation and hybrid warfare posed a threat to democracy and how this has been regulated so far. To do so, first, the concept of disinformation and its intricacies will be examined. Secondly, Poststructuralism and Strategic Theory will be used to depict the change towards a 'postmodern' world. Thirdly, a short explanation of the development of Information and hybrid warfare is included to describe their characteristics. Fourthly, the French and Spanish attempts to regulate disinformation are shortly explained. A last section is provided briefly illustrating the implications of Artificial Intelligence in the European context. The article concludes that latest developments show that this kind of warfare has opened 'new doors' of conflict and that legal matters remain unclear; however, tackling disinformation requires cooperation and further research is needed on the field.

Disinformation: the challenge of the 21st century

The European Parliament (2019) defines disinformation as 'false or misleading information produces and disseminated to *intentionally* cause public harm or for profit' and it highlights that:

"False information in itself (if it does not violate others' reputation, for example) enjoys the protection of freedom of expression, but when the whole environment of public discourse becomes occupied and dominated by falsehood, it frustrates the primary purpose of freedom of expression".

Disinformation campaigns are aimed at misleading particular or targeted audiences, governments or members of society to exert some kind of influence in the process of policy-making (Lanoszka, 2019). Disinformation can be used to influence and polarize public debates which constitute a 'fertile ground' for foreign influence (NATO, 2015). Disinformation and misinformation are concepts used interchangeably because there has been a lack of consistency. Also, NATO and the European Parliament use the word 'propaganda' together with disinformation too. As Tenove (2020) puts it, disinformation refers to *intentionally* false information whereas misinformation is not intended to cause harm, although it also involves false statements.

When analyzing the 'fake news' phenomena, one important aspect needs to be taken into account: the 'echo chamber' effect. In Communication Sciences, this concept refers to the fact that 'information, ideas or beliefs are amplified due to the transmission and repetition in a "closed system" in which different visions are censured, prohibited or represented' (Terán González, 2019). It contributes to polarization in the public sphere (Domínguez & Nicolás, 2020), proliferation of hate speech, nationalism and the use or abuse of the Internet for adversarial purposes (Helberger, 2020).

The security lens theory: Poststructuralism & Strategic Theory

As Lanoszka (2019) highlights, international disinformation campaigns have generated some sort of anxiety among contemporary defense planners. As Crawford (2003) clarifies, the national security implications of these are now being assumed by national leaders that spend a considerable amount of the governmental budget to collect relevant information and be aware of potential threats.

Security is paramount from a state perspective that goes beyond the traditional understanding of a state having the need to protect itself from external threats (Hansen, 1997). Security is now part of a 'self-referring system which is perceived as more real than reality' and that 'has now entered the realm of hyperreality'. For instance, in the Gulf War we could already see some kind of threat linked to information means such as the television. Thus, as Hansen (1997) concludes, the concept of security is not exclusively related to the military domain, threats can be constructed from a wide range of fields and it is through discourses that material and ideational factors are represented 'for us and by us'. The main IR theories provide somewhat opposing guidance when it comes to analyzing disinformation (Lanoszka, 2019). In the following lines we will briefly focus in Poststructuralism and Strategic Theory.

Poststructuralism contributes to our understanding of security in 'the age of post-truth politics' (Crilley & Chatterje-Doody, 2019), 'alternative facts, truthiness and *fake news*' (Bellis, 2019). It points out the metamorphosis from a 'modern to a postmodern or post-sovereign world' (Hansen, 1997) and focuses on language, practice and emotion. Brexit

or 2016 US elections are examples of 'alternative facts' and 'fake news' that were in the public debate in the context of 'post-truth politics' (Khan & Wenman, 2017).

'Fake news' or false claims have usually more impact than articles aimed at fact-checking so refuting these and asking for objectiveness might not be the solution. As Crilley and Chatterie-Doody (2019) argue, Poststructuralism points at examining how the representation of interests lead to certain actions and have the power to undermine the objective discourse including 'the production of knowledge and identities'.

Strategic Theory provides a comprehensive approach to analyze warfare. Clausewitz gives a clear definition: 'Strategy is the use of the engagements for the purpose of the war' (Clausewitz, 1976: 128); however, as Caliskan (2019) observes, this definition was focused on the use of the military and it has been adjusted to include other 'instruments of national power' besides the military one. War implies combinations of instruments ranging from informational activities to the use of force. Within each dynamic dimension, strategy-making plays a crucial role in conflicts (*see figure 1)*. Conducting an information warfare campaign requires the implication of disciplines such as 'command, communications, operation, logistics and intelligence' (Crawford, 2003).

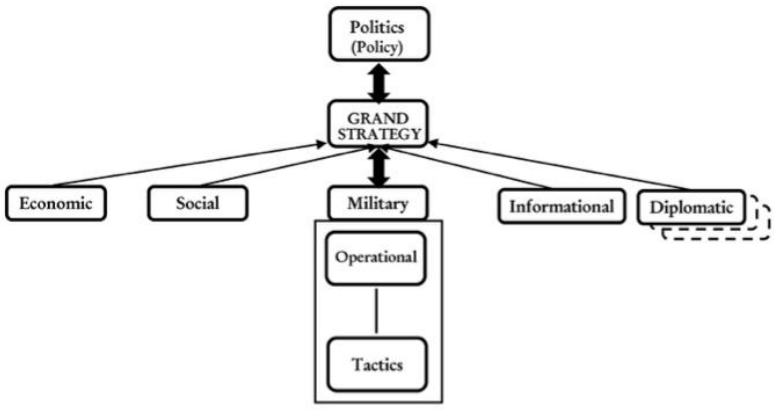

Figure 1. Key dimensions of strategy. Source: Caliskan, 2019.

Considering the strategy approach, the term 'hybrid' implies the emergence of a new kind of warfare (some occasions in which this term has been used are the Crimea war and Israel-Hezbollah in 2006, for instance) but as the next section will further clarify, during the Second World War many 'irregular aspects' were used such as propaganda or subversion (Caliskan, 2019).

Information & hybrid warfare: a new field of war?

Experts have tried to bring some clarity on the concept. 'Hybrid warfare' was first used in 2005 and it is one of the main terms used to explain the implications of contemporary warfare (Caliskan & Cramers, 2018). When Russia's operations in Ukraine took place, it

was referred to as 'the new find of warfare' by NATO, the media and the EU[1]. However, going back to the Napoleonic wars (and before) leaflets were used as non-conventional warfare to confuse the adversary and this had an impact on the outcome of the conflict.

The use of computers as a weapon has introduced concepts and terms for the 'information warrior' (Crawford, 2003). After Russia's war in Ukraine, the concept became more inclusive including non-military elements such as information warfare or cybersecurity.

'Information warfare' is real warfare. It can affect military, political and economic targets. As Crawford (2003) exemplifies, a press conference from a national governmental figure could be 'altered to change its content' or an economy could be sabotaged by 'reducing confidence in a nation's currency'. Strategic Information Warfare can generate a feeling of confusion. As Szafranski (1997) puts it, the main objective is 'to confound the adversary's decision-making process so that the adversary cannot act or behave in a coordinated or effective way'. Here is where the fundamental danger relies. It depicts a fast-paced, uncertain and dynamic environment constantly developing. As De Vries (1997) points out: '*It is about using information to create such a mismatch between us and an opponent that the opponent's strategy is defeated before his forces can be deployed or his first shots fired*'. It is cheap to wage, technology is widely available and it can be conducted by state and non-state actors.

The fact of examining the link between disinformation and international conflicts in the digital age should be done so as to not only analyse *'what* is said' but also '*how* information flows and *who* spreads it' (Commission, 2020). Only that way we can understand how to succeed in the fight against disinformation and, ultimately, grasp who can be considered as 'influential agenda-setter' (Golovchenko *et al*., 2018).

The common elemental characteristics of strategic information warfare are (Molander *et al.*, 1996)[2]:

FEATURES	CONSEQUENCES
1. Low entry cost dramatically multiplies threat	Anybody can attack
2. Blurred traditional boundaries create new problems	You may not know who is under attack, by whom… or who's in charge.
3. Perception management has expanded role.	You may not know what is real.
4. Strategic intelligence is not yet available	You may not know who your adversaries will be or what their intentions or capabilities will be.

[1] The EU developed different mechanisms such as StratCom task force against disinformation or the European Centre of Excellence for Countering Hybrid Threats (*see also* Caliskan & Cramers, 2018).
[2] Molander *et al.*(1996) also emphasize the US case adding one more feature to specify that the American vulnerability may give adversaries leverage. However, it is beyond of the scope of this paper.

5. **Tactical warning and attack assessment are extremely difficult**	You may not know you are under attack, who is attacking or how.
6. **Building and sustaining coalitions is more complicated**	You may depend on others who are vulnerable.

Protecting democracy?: National attempts to regulate disinformation

Online disinformation has been in the spotlight during the last decade. There have recently been some attempts to regulate disinformation in EU MS. National security responses are required to address the risks that disinformation campaigns pose to EU states so 'illegitimate actors' do not interfere undermining democracy (Tenove, 2020): every citizen has the right to receive quality information (Flores Vivar, 2019).

In countries with no freedom of speech or where rights are not granted, government regulations are strict. For instance, the Chinese Communist Party surveils online (social media) content with a mechanism known as 'Golden Shield' (Brown & Peters, 2018). China argues that the West has not effectively tackled the issue but in Western democratic countries, such an approach is not legitimate.

Several MS have made some attempts to legislate and regulate disinformation; however, as Magallón (2020) observes, 'anti-*fake news'* laws end up restricting freedom of information and expression: 'The State should present itself not as the "arbiter of the information" but rather as a guarantor of the principle of pluralism'. Helberger (2020) argues that regulatory proposals at stake are 'desperate attempts by national government to maintain the illusion of control'.

According to the European Parliament (2019), in France, the law against the 'manipulation of information' defines 'fake news' as '"any allegation of a fact that is inaccurate or misleading" which is likely to "distort the fairness of the election", if propagation on the internet was made "deliberately" and "in an artificial or automatized and massive way"'. Notwithstanding, when fake stories are denounced for being false and the story has gone viral, it is too late.

The French President Emmanuel Macron proposed the *Proposition de loi relative à la lute contre la manipulation de l'information'* in January 2018. The law was adopted to combat hate content on the Internet. According to Helberger (2020), France has had a general approach in developing this regulation and cooperating with Facebook. As the author explains, it is based in 5 different pillars:

1. *Broader vision on the role, regulation and realization of public values vis-à-vis social media.*
2. *New accountability regulations with a new duty of care for social media platform at the heart.*
3. *Public stakeholder dialogue under the auspices of the government.*
4. *Specialized regulator.*
5. *European coordination.*

As the Commission (2020) explains, while 'the rationale is similar to what was proposed in France, Spain focuses on the "threat to the institutional stability of the country"'.

In Spain, the rightwing Popular Party (*Partido Popular*) proposed a controversial new legislation in 2017 to fight against disinformation[3]. The Parliament rejected it but it has remained on the political agenda. During 2020, a new initiative was proposed. The government plan to fight disinformation was approved by the National Security Council last October. It was passed by the Socialist Party together with his coalition partner Unidas Podemos.According to the *Boletín Oficial del Estado* (Official State Gazette) it outlines four level of actions[4]:

1. Monitorization and surveillance, participation in the European RAS (Rapid Alert System) and investigation about the origin and aim of the source in question.
2. Evaluation of the alert by the Permanent Commission against disinformation, situation analysis and definition of the action plan, activation (if required) of a coordination cell against disinformation by the National Security Department and public campaign by the Secretary of State for Press depending on the nature of the campaign.
3. Information at a political and strategic level by the secretary of State for Press and evaluation of the alert.
4. Coordination of the response at a political level by the National Security Council.

What were the reactions to this attempt of regulating disinformation? It sparked complaints from opposition leaders as well as journalists and the media. They argue that it seeks to establish an Orwellian 'ministry of Truth'[5] as it limits freedom of expression and the above-mentioned sectors are not represented. It is argued that it is a mere 'political response' as it leaves the power to decide what disinformation is (and what is not) in hands of the government. Nevertheless, the EU Commission backed Spain's plan and defended it was a response to the European call for cooperation[6]. The plan aims at monitoring social media channels to fight against disinformation and describes the way in which bodies - such as the CNI (*Centro Nacional de Inteligencia*) – should proceed.

Future prospects and conclusion: Artificial Intelligence & Cybersecurity.

Artificial Intelligence (AI) is developing fast and poses challenges for essential EU values. Moreover, it remains unregulated: 'Our democracies can yet again afford the risk of a new, pervasive and decisive technology' (Nemitz, 2018). As Flores Vivar (2019) advocates, AI innovations that are taking place would have the capacity to 'read the informational chaos -infoxification-' by warning users about the nature of these sources.

[3] The original name of the proposed law was *Ley relativa al impulso de las medidas necesarias para garantizar la veracidad de las informaciones que circulan por servicios conectados a Internet y evitar injerencias que pongan en peligro la estabilidad institucional en España*.
[4] https://boe.es/diario_boe/txt.php?id=BOE-A-2020-13663
[5] https://www.euronews.com/2020/11/18/spain-divides-opinion-with-strategy-to-combat-online-disinformation
[6] https://english.elpais.com/politics/2020-11-10/eu-commission-backs-spains-protocol-against-disinformation-campaigns.html

Marsden *el al.* (2020) defend that AI is 'in short to medium term highly unlikely to replace human judgement and there is no possibility of restricting disinformation at source such that no-one views it'. AI is not a 'silver bullet' (European Parliament, 2019). This means that their accuracy is limited and they have biases and prejudices. Helberger (2020) states that no proposals exist to limit the use of AI, algorithms and the governments' power to collect data. However, some steps have recently been taken towards Europe's resilience against cyber threats. The European Commission presented last December the *EU's Cybersecurity Strategy in the Digital Decade* but results are still to be seen. AI will change our lives by increasing the security of Europeans and the digital world is becoming an intrinsic part in every day's life (Commission, 2020). AI is characterized by its pervasiveness so it should be analyzed how to use and present this technology to not undermine our EU democratic foundations.

Europe could become a global leader if combining its knowledge and expertise in both regulatory framework and digital tools and mechanisms. Marsden *et al.* (2020) propose co-regulation mechanisms so companies (private sector) regulate their own users and, at the same time, this is approved in a democratic way by national regulators that monitor their effectiveness. This option implies the independence of the regulator from the government so the regulation is subject to 'prior approval of codes of conduct'.

The evolution of Information Warfare has shown that, as Crawford (2003) puts it, it opens 'new doors' of conflict to fulfil the objectives (tactical, operational and strategic). Digital and media literacy, measures towards national security, big data, AI, freedom of expression, regulation of the journalistic discourse come together in the black box of disinformation. A significant amount of legal matters remain unclear or unaddressed as IW is now acquiring relevance in the military and governmental spheres of influence.

Tackling disinformation requires cooperation: public and private sector, NGOs, educational institutions, governments and media. Information means power and those who have the ability (power) to control information are powerful sources.

Further research might be needed on citizen's voting behavior and its connection with disinformation and political beliefs. It might be also of interest to examine the demographic features of those who are more likely to be manipulated by disinformation campaigns or strategies. Lastly, another subject of interest for future research is to analyse the extent to which the exposure to disinformation has an impact on personal beliefs.

Bibliography

Bellis, P. J. (2019). Poststructuralism and paranoia. *Leviathan*, *21*(3), 43–49.

Brown, N. I., & Peters, J. (2018). Say this, not that: Government regulation and control of social media. *Syracuse Law Review*, *68*(3), 521–546.

Caliskan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis*, *35*(1), 40–58.

Caliskan, M., & Cramers, P. A. (2018). What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. *Horizon Insights*, *1*(4), 23–35.

Clausewitz, C. von. (1976). *On War*. Princeton University Press.

Crawford, G. A. (2003). Information Warfare: New Roles for Information Systems in Military Operations. *Encyclopedia of International Media and Communications*, 419–427.

Crilley, R., & Chatterje-Doody, P. (2019). Security studies in the age of 'post-truth' politics: in defence of poststructuralism. *Critical Studies on Security*, *7*(2), 166–170.

De Vries, A. D. (1997). *Information Warfare and its impact on National Security*.

Del Luján Flores, M. (2019). La Desinformación Y La Búsqueda De Respuestas Para Enfrentarla. *Revista de Derecho Público*, *56*, 27–36.

Domínguez, S. C. & Nicolás, M. J. (2020). La Unión Europea ante la desinformación y las fake news. El fact checking como un recurso de detección, prevención y análisis. In *Aproximación periodística y educomunicativa al fenómeno de las redes sociales* (pp. 985–1002). Mc GrawHill.

European Commission. (2020). *White Paper on Artificial Intelligence: A European approach to excellence and trust* (Vol. COM(2020)).

European Parliament. (2019). *Disinformation and propaganda - impact on the functioning of the rule of law in the EU and its Member States*.

Flores Vivar, J. M. (2019). Artificial intelligence and journalism: diluting the impact of disinformation and fake news through bots. *Doxa Comunicación.*, (29), 197–212.

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *International Affairs*, *94*(5), 975–994.

Hansen, L. (1997). A case for Seduction? Evaluating the Poststructuralism Conceptualization of Security. *Cooperation and Conflict*, *32*(4), 369–397.

Helberger, N. (2020). The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power. *Digital Journalism*, *8*(6), 842–854.

Khan, G., & Wenman, M. (2017). The Politics of Poststructuralism Today. *Political Studies Review*, *15*(4), 513–515.

Lanoszka, A. (2019). Disinformation in international politics. *European Journal of International Security*, *4*(2), 227–248.

Magallón, R. (2020). La nueva infonormalidad: no pienses en 'fake news', piensa en desinformación. *Cuadernos de Periodistas*, *40*, 12–21. Retrieved from https://www.researchgate.net/profile/Raul_Magallon_Rosa/publication/343181380_La_nueva_infonormalidad_no_pienses_en_'fake_news'_piensa_en_desinformacion/links/5f1ab5e445851515ef44d94d/La-nueva-infonormalidad-no-pienses-en-fake-news-piensa-en-desinformacio

Marsden, C., & Meyer, T. (2019). *Regulating disinformation with artificial intelligence*. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf

Marsden, C., Meyer, T., & Brown, I. (2020). Platform values and democratic elections: How can the law regulate digital disinformation? *Computer Law and Security Review*, *36*.

Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). Strategic Information Warfare: A New Face of War. (National Defense Research Institute, Ed.).

NATO Strategic Communications Centre of Excellence. (2015). Disinformation in Sweden.

Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 1–25.

Szafranski, C. R. (1997). *A theory of Information Warfare: Preparing for 2020*.

Tenove, C. (2020). Protecting Democracy from Disinformation: Normative Threats and Policy Responses. *The International Journal of Press/Politics*, *25*(3), 517–537.

Terán González, E. (2019). *Desinformación en la UE : ¿Amenaza híbrida o fenómeno comunicativo ? Evolución de la estrategia de la UE desde 2015*. *Unión Europea y Relaciones Internacionales*. Retrieved from https://www.ceuediciones.es/catalogo/libros/politica/desinformacion-en-la-ue-amenaza-hibrida-o-fenomeno-comunicativo-evolucion-de-la-estrategia-de-la-ue-desde-2015/