Influence Operations in Cyberspace – How They Really Work

Pijpers, B.M.J.; Ducheine, P.A.L.

Publication date
2020

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Influence Operations in Cyberspace – how they really work

By: Peter B.M.J. Pijpers and Paul A.L. Ducheine*

(last updated 1 February 2021)

Abstract

1. Introduction

2. Influence Operations in Cyberspace

   2.1. Cyberspace

   2.2. Influence operations

3. Generating Effects

   3.1. Preparing the Influence Operation

      3.1.1. The Intent

      3.1.2. The strategic narrative

      3.1.3. Framing

   3.2. Executing cyber related activities

   3.3. Exploiting social media

4. Reflections and conclusions

Bibliography

* Peter B.M.J. Pijpers, LL.M, MSc is an Associate Professor of Cyber Operations at the Netherlands Defence Academy and PhD researcher at the Amsterdam Centre of International Law, University of Amsterdam. Dr Paul A.L. Ducheine is Professor of Cyber Operations at the Netherlands Defence Academy and Endowed Professor of Military Law of Cyber Operations and Cyber Security at the University of Amsterdam. Corresponding author: b.m.j.pijpers@uva.nl.
Abstract

Covid-19 is the latest, but will not be the last pretext for spreading fabricated information. Topics like Covid-19 can and will be used for influencing foreign States in a deliberate way. So, is this new? No, influencing has been on-going for ages. But what is new, is the domain of cyberspace enabling fabricated news to spread fast and effectively. Much is written about influencing people via social media. But how do influence operations via cyberspace work? And what is the added value of cyberspace in that context?

In the authors’ view, the core tenets of why audiences are susceptible to influence operations in cyberspace are a) the exploitation of social media to magnify and amplify successful messages and b) the ability to craft ‘frames’ or scripts, executed by i.a. disinformation campaigns. A frame couples a specific event such as Covid-19 to a strategic narrative; a divisive societal topic; and audiences’ preferences and heuristics. A frame does not need to be true, but it must appear so.

Influence operations that make use of these frames can therefore be persuasive, coercive but also manipulative, especially if subconscious heuristic techniques are used that lure target audiences to make biased judgements, undermining or even circumventing their deliberate understanding and autonomous decision-making process.

Cyberspace provides an arena of engagement where actors or States can opt-in if their interests coalesce with domestic or other State actor influence operation. Furthermore, cyberspace and social media are conducive in supporting subconscious manipulative influence operations: The added value of cyberspace is the ability to harvest data about the audience, generate audience’s heuristics, and reversely to micro-target the audience with bespoke messages. Finally, the attributes of cyberspace can facilitate the amplifying and multiplying of messages and ‘likes’, thereby increasing familiarity with the topic and creating an illusion of truth, the acme of susceptibility, to initially false and fabricated frames.
1. Introduction

“30 mila soldati dagli Usa in Europa senza mascherina”, “Coronavirus? Macché, la Ue apre alle manovre Usa”, “La manovre Nato sabotate dal virus”. Just three headlines of the Italian news site of the communist daily ‘Il Manifesto’,¹ in which the spread of the coronavirus is somehow magically linked to a military exercise of NATO in Europe and the EU’s approval thereof.

Covid-19 is the latest, but will not be the last pretext for spreading ‘fake news’. The corona pandemic proves to be a popular topic for spreading white lies, polarising or populist outcries. Often these populist outcries are not picked up by the wider audience; they are solely consumed by the converted and will most likely not change people’s perception, let alone their behaviour. But, spreading fabricated information can also come in a more methodical way as part of a deliberate disinformation campaign. Disinformation campaigns, as part of State-led influence operations, use similar platforms and events - including Covid-19, and earlier the downing of the MH-17, the debate about the disintegration of the EU, the effects of 5G,² and the war in Ukraine - but the effect and intent of deliberate disinformation campaigns different substantially from ad-hoc fake news.³

Are disinformation campaigns new? No, influencing audiences via disinformation campaigns has been on-going for ages,⁴ and especially during the Cold War-era both the United States (US) and Soviet Union and their respective allies were constantly spreading misleading information, forgeries or propaganda.⁵ Disinformation, deception and masking the truth were elements of the US ‘political warfare’⁶ and Soviet-Russian ‘active measures’- doctrine.⁷

But what is new, is the domain of cyberspace, in which fabricated news can spread fast and appears to have severe impact. Much is written on disinformation operations, about influencing people and groups via social media.⁸ But the question is how? How do influence

---

operations generate effects? Why is cyberspace, internet, or even social media inducive for influencing audiences? And why are people even susceptible to influences on social media?

The core question to be answered in this article therefore is: “how and why do influence operations generate effects via cyberspace and what is the added value of cyberspace in that context?” After this introduction, a brief overview is given on what cyberspace entails and what an influence operation is for the purpose of this article (section 2). Next an analysis is given on how and why influence operations generate effect (section 3) highlighting the notion of framing the strategic narrative, executing of cyber related activities including disinformation campaigns, and finally exploiting social media, supporting the cyber-related activities. The final section (4) provides some reflections on how cyberspace enhances influence operations.

This article holds some limitations. Firstly it focusses on State-level influence operations; secondly on influence operations below the threshold of the use of force; and thirdly cyberspace is used as a vector to generate effects in the cognitive dimension, hence outside cyberspace. Fabricated news in this article is part of a deliberately constructed informational element e.g. disinformation, within a strategic plan of a State, consequently the catch-all term ‘fake news’ which can include white lies, misinformation, manipulated political rhetoric and propaganda will not be used. The article will make use of a model of State A (influencer) and State B (target) to explain influence operations in general. Where appropriate the influence operations will be illustrated with 2020 Corona-related disinformation campaign in Italy allegedly conducted by the Russian Federation (RF).

2. Influence Operations in Cyberspace

This section will dissect cyberspace as well as influence operations. Peeling down these two topics is needed to illustrate which segments of either concept will contribute to the effectiveness of influence operations in cyberspace.

2.1. Cyberspace

Cyberspace as the ‘networked information infrastructure’, is part of the information environment we live in. The information environment can be conceptually divided into

---

9 Without precluding that influence operations can and will be used during armed conflicts or war as supporting or supported line of operations to achieve a goal; and that influence operations can have effects in cyberspace e.g. data theft, destruction of data, malware or ransom software.
12 Or as Kuehl describes it, cyberspace is global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies: Daniel T Kuehl, “From Cyberspace to Cyberpower;” in Cyberpower and National
three dimensions. The physical dimension encompasses the globe, and furthermore, every conceivable tangible object. The cognitive dimension entails our individual and collective knowledge, perception, understanding and wisdom. The virtual dimension entails where and how information is collected, processed, stored, disseminated, and protected digitally. It is the digital, imaginary reflection of the two other dimensions.

Cyberspace can be regarded as a part of the information environment, though the scope of cyberspace within the information environment depends on the perspective chosen. Virtual personas allow real persons or organisations to access cyberspace via e-mail address or accounts on social media platforms. The virtual personas enable access to the logical layer, which includes all non-tangible elements manifested in data or code (‘zeros and ones’), such as operating systems, protocols, applications, or other software and data components. The logical layer cannot function without the third, physical network layer which comprises the hardware (computers, routers, smartphones) and the physical connections between these hubs (fibre optic cables). Data is produced, transmitted, processed and stored in physical parts and information flows through physical components of various networks.

---


The three layers unique to cyberspace are: the physical network layer – hence the computers and glass fibre cables;\textsuperscript{16} the logical layer i.e. the software and the data; and the virtual persona which are the reflections of (groups of) persons in the virtual dimension.

\textit{Figure 2: Cyberspace}

The characteristics of the cyber domain can be used to influence other actors distinct from the land or sea domain. Cyberspace is, in principle, boundless and ubiquitous, and there is a low threshold of admission which empowers non-state entities. Furthermore, in cyberspace the distinction between real and virtual disappears both in persons but also regarding acts and facts.\textsuperscript{17} Finally, the social media platforms allow for communication of all to all, enhancing behaviour based on the tendency to ‘like’ the posts of people who are similar or admired, rather than on facts.\textsuperscript{18} The attributes of the virtual dimension of cyberspace are well suited to deliberately manipulate the senses in order to alter the understanding of a situation and the subsequent autonomous decision-making process.

\subsection*{2.2. Influence operations}

Influencing, related to political sciences, can be described as ‘the ability to persuade other(s) to do what one wants, or refrain from doing what one does not want’.\textsuperscript{19} More broadly the activity to convince or persuade another actor that one’s views or opinions prevails over those of others, but also to prevent that the view of the other actor will prevail.

\begin{itemize}
\item \textsuperscript{17} Cohen and Bar’el, “The Use of Cyberwarfare in Influence Operations.”
\item \textsuperscript{19} See e.g. Simon. Reich, “The Future of International Relations : A Symbiotic Realism,” in \textit{Good-Bye Hegemony}, 2018., p. 179.
\end{itemize}
Though influence operations have been described in numerous ways, the communalities are the absence of the use of force or even warfare; the focus on the cognitive dimension and the objective to change the behaviour of other actors directly or indirectly via a change in attitude. In this sense, behaviour is physical manifestation of activity of an actor in its environment, while attitude has a psychological and cognitive element related to beliefs, emotions, knowledge and psyche of an actor, society or political system, and is passive in nature.

An influence operation can be described as ‘the deployment of resources for cognitive ends that foster or change a targeted audience’s behaviour’, directly of via changing the attitude. Whilst the use of force is excluded from the definition of influence, the core forms of influence are persuasion, coercion, and manipulation as depicted in figure 3 below.

Persuasive influence operations aim to alter the autonomous decision-making of the targeted audience (state leadership, opinion leaders, mass public) by changing the weighing of the options to choose from; openly and willingly. Persuasion is to be understood as entailing an open appeal for a rational and a conscious deliberation and subsequent choice. The weight can be changed by persuading the targeted audience to alter its understanding, perception and mindset of the environment, thereby conversing the attitude of the audience. And by changing the understanding, perception and worldview (attitude), influence the decision-making of the targeted audience in a way beneficial to the
influencer, which in turn induces change in the behaviour of the targeted audience. During persuasive influence operations, the targeted audience still possesses, or perceives to possess, the ability for deliberative understanding and autonomous decisions: the targeted audience makes a willing choice to change its behaviour.32

Coercive influence operations can be explained in terms of an unwilling act, meaning that coercive operations do not provide meaningful options to the opposing audience, and limit or annihilate the decision-making options of a targeted audience.33 As there are no ‘acceptable alternatives’,34 the opponent is forced to make an unwilling choice to act.

---

32 Hollis, “The Influence of War; The War for Influence.” p. 36. A persuasive influence operation is aligned with Hollis’ influence operations which exclude coercion.
Coercive operations, in contrast to persuasive influence operations, do not aim to change the attitude\(^{36}\) of a targeted audience but aim for a change in behaviour,\(^{37}\) aligning it with the demands of the coercer.\(^{38}\) Reversing this argument, an influence operation that short-cuts or circumvents the deliberate understanding and autonomous decision-making is coercive in nature.

A targeted audience or person that is being persuaded will keep the possibility of make a free choice, while coercion ‘robs them of choice’;\(^{39}\) in both cases however the ‘capacity for conscious decision-making remains intact’\(^{40}\) This in contrast to manipulation which attempts to subvert, undermine and even take control of the targeted audience capacity to make a decision. Manipulation does not aim to influence the belief but uses psychological levers, heuristics and cognitive biases to achieve results, often in a subconscious, hidden or covert manner.

Influence operations are deliberate activities targeting the cognitive dimension with the aim to change the attitude or behaviour of the targeted audience. The dynamics of a conscious, overt persuasive and coercive influence operation might be obvious. But the more manipulative, subconscious, psychological and deceptive the influence operation is, including via disinformation campaigns, the bigger the question on how they generate effects.

3. Generating Effects

This section will analyse how influence operations can effectively change the attitude and behaviour of target audiences via cyberspace. In general, influence operations will follow the sequence of preparation, execution, and finally exploitation those activities that are successful.\(^{41}\)

3.1. Preparing the Influence Operation

Preparing a deliberate influence operation is complex and will be broken down in defining an intent, a strategic narrative and framing as the operationalising of the narrative.

---

38 Compliance can be achieved by coercion and enticement, is a short-term change in behaviour. Cragin and Gerwehr, *Dissuading Terror: Strategic Influence and the Struggle Against Terrorism*, pp. 15-20.
40 Susser, Roessler, and Nissenbaum. p. 15.
3.1.1. The Intent

Before engaging in an influence operation, State A will need to define an intent. The intent will serve the vital interests of State A, it is formulated in general political terms, and can change over time. The intent of the State is part of, or derives from, its attitude and perception of the world – based on collective cognition and knowledge of a society (history, collective memory, culture, political and geospatial context). The Russian (RF) intent when executing influence operations in Western democratic States, including Italy, could best be described as creating strategic confusion, thereby alluding the success and strength of autocratic forms of government. They also seek to undermine democracy, sow distrust in Western institutions, and destabilise societies, this with the goal to control or ensure failure of European pro-Western government and leadership and weaken NATO and the EU.

3.1.2. The strategic narrative

If State A decides to act or react based on its vital interests, its attitude and perception is transformed into behaviour. The instruments of power such as diplomacy, information, military, economy, are the embodiment of the behaviour of State A, and will be deployed to change the attitude and behaviour of State B, with the aim to further and protect State A’s national interests and values.

Influence operations in cyberspace are an exponent of the informational instrument of power. Influence operations (below the threshold of the use of force) aim to alter or undermine the deliberate understanding and autonomous decision-making of the targeted audience, using a clear strategic and calibrated narrative as the main expression of power.

Though not unique to cyberspace, the strategic narrative is a deliberate, cognitive construct to unite groups of people and generate a shared view of a collective history and desired objective for the future, examples of which are the concept of ‘American Exceptionalism’, or the Israeli notion of the ‘Promised Land’. When used in an affirmative way, narratives aim to persuading, manipulating and convincing opponents by initiating the process of altering or counterbalancing their perceptions and belief and hence the context

---

46 Without being exclusive. Other instruments of power are culture and knowledge (DIME-CK).
and weighing of the decision-making options. Related to the RF intent to create strategic confusion in Western democracies, the generic narratives used relate to ‘anti-EU/Transatlantic’ sentiments. And though Italy has a vast communist history and strong ties with Moscow, compared to other European States, the reason could be to strengthen the popular sentiments towards Moscow and away from NATO.

3.1.3. Framing

Strategic narratives do not automatically influence a targeted audience. To effectuate a narrative, it will need to be broken down into simpler structures called frames or scripts.

Framing is the operationalisation of a strategic narrative and aims to create a script which will incline the audiences to make predetermined (reflexive) decision based on their heuristics, and in line with the will of the State executing the influence operation. Therefore, framing triangulates a) the strategic narrative, b) with divisive topics of a society and c) audiences’ preferences and heuristics. This revolving around an event, such as an election, a referendum or an occurrence such as Covid-19.

![Figure 4 Framing the Narrative](image)

51 Antelava and Iacoboni, “The Influence Operation behind Russia’s Coronavirus Aid to Italy.”
Framing efforts can make use of differences between groups, accentuate feeling of rejection and neglect with minority group, fuel internal divisions over political issues or exploiting tensions between neighbouring countries. Taking in mind the headlines regarding NATO’s exercise in times of Corona as mentioned in ‘Il Manifesto’, the frames designed do not need to be true, but need to be framed as true and must ‘at least partially respond to reality, or at least accepted views’, thereby making use of preferences or cognitive and social heuristics of the targeted audience.

The Italian case, where (as in many European countries) outlets and politicians from the far-left and far-right have expressed discontent with the governmental policy on Covid-19 containment and the alleged disenfranchisement of basic right, illustrates the effect of framing. The Italian MP Mrs Cunial addressed Parliament on 14 May 2020 to amplify the known Covid-19 disinformation and conspiracy rhetoric, gaining appraisal by social media platforms tags such as ‘Noi stiamo con la Russia di Putin’, ‘Italexit’, ‘Euroexit’ and ‘No5G Milano’. Earlier the communist daily ‘Il Manifesto’ had implied that during the ‘Defender Europe 20’-exercise US and NATO forces were the source of contagion for the Covid-19 virus in Europe. An exercise, thus Il Manifesto, backed by the EU. Aftermath the headlines in Il Manifesto and the public attention the anti-NATO messages gained in Italia, Russia became involved magnifying the content via VKontante, the RF social media platform similar to Facebook.

In the Italian case the triangulation between the narrative, a divisive topic and audiences’ heuristics can be well depicted. The disinformation activities will serve both the Russian but also an Italian domestic anti-EU narrative. Revolving around Covid-19, the narrative is linked to socially divisive topics such as on the corrupt and nepotist Deep State, the alleged US or EU dominance of the Italian government, or the migrant crisis. These topics are intertwined with the heuristics of specific groups within Italy such as the communist that have an anti-US, anti-NATO and anti-establishment inclination; or far-right fascist groups that wilfully find confirmation in their desire for an independent Northern Italy; and the general socially biased sentiment that Italy’s interest are increasingly less aligned to those of the EU. The frame made, is that Covid-19 is a US-borne virus, financed by Bill

54 Rid, Active Measures: The Secret History of Disinformation and Political Warfare. pp. 4-5. Rid quotes Ladislav Bittman whom he interviewed.

55 Related to Gates, Deep State, WHO etc, see: DFRLab, “Italian MP Amplifies Debunked COVID-19 Conspiracy Theories on the Floor of Parliament.” Of note: MP Mrs Sara Cunial was elected to represent the ‘cinque stelle’ party but expelled due to her extreme stances.

56 Meaning ‘we stand with Putin’s Russia’ see also: https://www.facebook.com/1761482714098169/posts/2641809226065509

57 The director of the Rome based International Institute of Strategic Studies states that ‘Moscow is using the Covid-19 outbreak “to strengthen anti-EU feelings and to reinforce the impression that the EU is crumbling, to make propaganda gains and gather intelligence at the heart of NATO.”’ In, Antelava and Iacoboni, “The Influence Operation behind Russia’s Coronavirus Aid to Italy.”


Gates. US troops are now in Europe, spreading the virus with the consent of the EU and the WHO. Italy condones it, most likely because corrupt State official benefit from infringing the freedom of speech and demonstration. There is no causality in this frame, but also no proof that it’s not true.

Socially divisive topics vary from State to State and depend on attitude, perception and history of that State. There are inherently antagonistic dynamics within societies based on contrasting views, values and opinion of groups of humans and priors of the political leadership or population. Moreover, shared practices, ideas and values are not fixed but in a continuous state of change, such as the paradoxical trade-off between health, economy and the infringements on freedom in the age of Covid-19.

The essence of socially divisive topics, especially for democracies, is that these topics force groups in society to communicate, in order to achieve or influence a common view and shared representation, whether during election time, ad-hoc rallies or on late-night talk shows. Framing uses these natural seams caused by communication dynamics to address or inject topics that will raise discord in a society. Finding socially divisive topics will require research and in-depth knowledge of a society.

Addressing socially divisive topics is still a very conscious way of persuading an audience using arguments, logic and rationales. In the Italian case, the spread of corona was linked

---

60 DFRLab, “Italian MP Amplifies Debunked COVID-19 Conspiracy Theories on the Floor of Parliament.”

61 The 2016 UK EU Referendum also saw frames in which long-standing resentment against the EU, was somehow linked to the economic malaise and migrants issues, see also: James Ball, Post-Truth: How Bullshit Conquered the World, Biteback Publishing (London, 2017). p. 60. Another example is the Lisa-case where a girl of Russian descent was allegedly kidnapped by an Arab-looking person in Germany implying stereotyping and applying spurious causality associating Arabs people with migrants having have bad intentions; and furthermore, that Germany is not able and willing to protect Russian minorities. While little girl Lisa reappeared shortly after she was reported lost, the incident caused a political row between RF and Germany. See: Johan E. Korteling, Maaijke Duistermaat, and Alexander Toet, “Subconscious Manipulation in Psychological Warfare,” 2018, pp. 13-14; Aristides Mahairas and Mikhail Dwilyanski, “Disinformation – (Dezinformatsiya),” The Cyber Defense Review, 2018, 21–27.


65 Tansino, “Analysing Strategic Communications through Early Modern Theatre.” p. 53. Paraphrasing Moscovici who argues that there are three communicative needs within any social group: the need to make a foreign element familiar, the need to create a shared field of communication, and the need to form a common identity.

66 Tansino. p. 55.


to migrants and would have resulted in supermarket riots.\textsuperscript{69} This is a way of influencing which could eventually change the attitude of an audience. However, to generate a reflexive response to activities of influence operations and make an audience instantly receptive to alter its behaviour directly, it is required to address the subconscious cognitive processes of groups and audiences.

Cognitive and social heuristics or ‘rules of thumb’\textsuperscript{70} are psychological reflexes which set in during conditions of time constraints, or during shortage or an overload of information.\textsuperscript{71} Usually these ‘mental shortcuts’ generate acceptable outcomes, but they can also lead to suboptimal judgements or biases. Feeding these shortcuts with fabricated content will add to biased judgement and blur the common understanding of a situation. Examples of cognitive heuristics are the biases related to focus,\textsuperscript{72} conformation, anchoring, stereotyping or oversimplifying, while social heuristics rely on authority, scarcity, reciprocity and social proof.\textsuperscript{73} In the Italian case, fabricated statement alluded to existing fears regarding State control, dominance of the EU over national values, restrictive measures that limit citizens’ rights, creating faux relations between topics (anchoring), or exacerbating confirmed beliefs (e.g. regarding migrants).

Russian ‘Active Measures’ rely on heuristics in what they call reflexive control,\textsuperscript{74} i.e. ‘conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.’\textsuperscript{75} With this mechanism RF seeks to influence the target audience in a subconscious manner utilising the cognitive biases which set in due to the limitations in the available data and in the human information processing capacity.\textsuperscript{76}

The emergence of cyberspace makes it possible to target very specific groups in society.\textsuperscript{77} On the one hand because the data of these groups is available on internet and social media,

\footnotesize{\textsuperscript{69} Cristiani, “The Paradox of Russia’s Disinformation Activities in Italy.” pp. 3-4.  
\textsuperscript{72} focus on what we want to see, thereby neglect data that would otherwise have logical or rational relevance  
\textsuperscript{77} Knowledge of preferences or biases of the audiences and target groups must be obtained based on political preferences, ethnical background, NRA membership, voting behaviour, on-line consumer and social behaviour, mode of transport and so on. The data can be harvested from platforms like Facebook using tool like ‘thisisyourdigitallife’ or ‘My Personality’. During the 2016 US presidential elections, Cambridge Analytica claimed to have thousands of attributes of a large segment of American voters (50-87 Million) See also: Information Commissioner’s Office, “Investigation into the Use of Data Analytics in Political Campaigns,” 2018.pp. 16-18.}
on the other hand because big data and data science techniques make it possible to single out these groups. As a result, these audiences can receive very specific content in a language that they comprehend and via a medium on which they communicate. These micro targeting techniques can have a positive effect in mobilising groups to engage in the political or societal discourse, but can also be used to generate disengagement and polarisation.

3.2. Executing cyber related activities

Influence operations can only be effective if the audience is susceptible to the content of the operations. Therefore, after operationalising the strategic narrative, the influence operation needs to be executed via actual activities in cyberspace. The cyber-related activities which are built on the frames, range from disinformation campaign, to leaking of sensitive information, and trolling activities. These activities are not mutually exclusive and far from new. During the executing of the cyber-related activities, State A actually engaged with (the targeted audiences of) State B, whether the latter is aware of it or not. The frames made are injected in State B’s society utilising the virtual persona layer of cyberspace as a vector for relaying content making use of cyber-related activities: disinformation, leaking of sensitive information, trolling and political grooming.

Disinformation campaigns aim to sow discord among targeted audiences, by deliberate spreading of misleading, carefully constructed, verifiably false, or falsified information. Disinformation also entails leaving essential data out; conceal the true relation between fact, or create new relations; hide valuable information in an overwhelming mass of disseminated data; oversimplify events; use unclear concepts; change a national position occasionally. Disinformation is created, presented and disseminated for economic gain or

---

82 Mahairas and Dvilyanski, “Disinformation – (Dezinformatsiya).” p. 21.
ideological purposes, to intentionally deceive the public,\textsuperscript{87} and may cause public harm including threats to democratic political and policy-making processes.\textsuperscript{88} Disinformation, such as the idea that 30,000 US troops are spreading Covid-19 all over Europe, or the notion that “Planet Lockdown” is an encroachment on civil liberties\textsuperscript{89} use heuristics related to the retainment-principle, which entails that once perceived and digested information is ‘trapped’,\textsuperscript{90} and the confirmation-principle arguing people are highly susceptible for information that can be recognised and is consistent with existing belief.\textsuperscript{91}

Leaking is the revealing\textsuperscript{92} of non-public information into the public domain with the purpose to harm an individual, organisation or State.\textsuperscript{93} Leaked information is not necessarily false or manipulated.\textsuperscript{94} Leaking will sow doubt, confusion and cynicism among the targeted audience since the information was not intended for public consumption, but also since the information will be disseminated from other outlets than expected. Leaking, ‘dumping’,\textsuperscript{95} kompromat\textsuperscript{96} or white-washing operations are often preceded by a computer intrusion – a hack. Leaking operations address cognitive heuristics, most notably the focus- and the probabilistic blindness-principle which argue that our reasoning capacities are limited, flawed and error-prone.

Trolling is the deliberate act of making discriminatory, abusive or otherwise controversial remarks and threatening, inflammatory, abusive, harassing or disruptive behaviour on internet fora with the aim to harm persons, organisations or States.\textsuperscript{97} The intent of trolling

\begin{itemize}
\item \textsuperscript{87} Allcott speaks, in other words, about pecuniary or ideological motivation. Allcott and Gentzkow, “Social Media and Fake News in the 2016 Election.” p. 217.
\item \textsuperscript{90} Korteling, Duistermaat, and Toet, “Subconscious Manipulation in Psychological Warfare.” p. 19. As in the famous example ‘do not think about the pink elephant’.
\item \textsuperscript{91} Korteling, Duistermaat, and Toet. pp. 15-16.
\item \textsuperscript{93} Sander, “Democracy under the influence: paradigms of state responsibility for Cyber Influence Operations on Elections”, in CJIL, 2019, p 8,9. Whistleblowing is a sort of doxing operation.
\item \textsuperscript{94} Leaking can also be seen as a subset of disinformation. In that rationale disinformation is not merely false in content but can also be false of fabricated by using unexpected outlets or forms while the content is true.
\item \textsuperscript{95} Mueller, “Report On The Investigation Into Russian Interference In The 2016 Presidential Election.” pp. 36 ff.
\item \textsuperscript{97} Sander, “The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations.” p. 16. In some policy and academic literature trolling is seen as a species of disinformation, a rationale that will not be followed due to the deliberate abusive nature of trolling. See also: United States Senate Committee on Intelligence, “Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia’s Use of Social Media,” vol. 2, 2019. p. 18.
\end{itemize}
campaigns is to fuel extreme ideologies, hyper partisanship, or conspiratorial political ideas purporting to polarise audiences.\textsuperscript{98} Trolling can lead to intimidation, self-censorship, dissuade specific groups from casting a vote and silencing dissenting actors in a State.\textsuperscript{99} The content is deliberately fabricated, seeking to target and ridicule the moral virtues or failings of organisations, causes or people. Political trolling injects cynicism to the content stimulating disengagement, and while disinformation aims to sow discord and confusion, the result of trolling is to increase the in-group identification and hence the difference between groups in a community or society. Trolling is a diffusional technique, making use of the heuristic association-principle\textsuperscript{100} which refers to the concept that our brain looks for associative relationships, patterns and coherences of the information that is received such as stereotyping or stigmatisation. Trolling can be so extreme that they lose effectiveness or even become counterproductive.\textsuperscript{101}

Political grooming\textsuperscript{102} refers to an influence activity to discredit or favour a person of some authority,\textsuperscript{103} whether incumbent or desiring to be. Political grooming revolves around the concept of infiltrating politics by cultivation of political allies,\textsuperscript{104} and contains cyber-related techniques ranging from defamation, lobbying abroad,\textsuperscript{105} foreign political advertising, party financing, supporting or manipulating diaspora or minorities abroad on political issues.\textsuperscript{106} In the Italian case it could be possible that the RF is supporting the Italian League (Lega),\textsuperscript{107} but also pro-Kremlin far-left Communist party. The RF cultivates political extremes,\textsuperscript{108} by (financially) supporting specific left-wing and right-wing anti-establishment or anti-EU parties in Europe. Techniques used are to artificially boost the popularity or dismay of a

\textsuperscript{98} Diego A. Martin and Jacob N. Shapiro, “Trends in Online Foreign Influence Efforts,” \textit{ESOC Publications}, 2019, 64. p. 8.
\textsuperscript{102} EU vs Disinformation, “Election Meddling and Pro-Kremlin Disinformation: What You Need to Know.” p. 4.
\textsuperscript{103} Jeangene Vilmer, “Information Manipulation: A Challenge for Our Democracies.” p. 77.
\textsuperscript{104} Polyakova et al., “The Kremlin’s Trojan Horses.”, p. 3.
\textsuperscript{105} Ajir and Vailliant, “Russian Information Warfare : Implications for Deterrence Theory.” pp. 80-81.
\textsuperscript{107} Polyakova et al., “The Kremlin’s Trojan Horses.” p. 4.
\textsuperscript{108} United States Senate Committee on Foreign Relations, “Minority Report on Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security.” pp. 50 ff.
candidate, using similar (semi) automated technics to increase the followers on Twitter and Facebook.\textsuperscript{109}

The goal of cyber-related activities is executing the framed strategic narrative. In the Italian case, this means to undermine and counter the Western political narrative, the EU and trans-Atlantic institutions, to sow discord and fuel social fragmentation and polarisation, to paralyse the democratic process, but also to blur the line between fact and fiction. The Italian Covid-19 case was allegedly picked-up by RF agents as it suited the anti-US and anti-EU narrative, but was not initiated by RF.

### 3.3. Exploiting social media

Successful activities will need to be exploited. Similar to regular activities, whether military-type or marketing operations, after the thorough preparation and executed, the output and the outcome will need to be assessed and evaluated, and based on that new targets can be selected and exploited. The latter is even more relevant for influence activities in cyberspace since these often dependent on ambiguous socially divisive topics and heuristics of targeted audience and will therefore not have a predictable result\textsuperscript{110} based on causal relations.\textsuperscript{111} But the one’s that do catch on need to be exploited.

Social media can be exploited to make audience -even more- receptive to the content of a cyber-related activity in two interrelated ways: amplify and magnify messages, and create the illusion of truth.

In cyberspace, messages can be repeated almost indefinitely not limited by scarcity of resources (enough paper to print on or human capital). Communication in cyberspace is not dependent on specific outlet, government communiques or a high price of admission to broadcast. Everyone can speak up and share his opinion, views and emotion. In this context, Thomas Rid speaks about outsourcing communication,\textsuperscript{112} since not only governmental agencies but everyone with a social media account is a communicator. Not surprisingly, the message sometimes gets out of control and loses effectiveness. Apart from the human activity in creating and repeating messages, as with Italian case where RF social

\textsuperscript{109} Cockerell, “How Russian Bots Amplify Britain’s Jacob Rees-Mogg,” 2019. But political grooming can be initiated by domestic actors with the aim to coordinate with a foreign State to change the election dynamics, see: Aaltola, “Democracy’s Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling.” p. 4.

\textsuperscript{110} Rid, \textit{Active Measures: The Secret History of Disinformation and Political Warfare}. pp. 318-321. After the explosion of the Chernobyl Nuclear Power Plan in 1986, the KGB forged letters of the US Intelligence Services and leaked them to US newspapers. The latter did not pick up the story.

\textsuperscript{111} The concept that a change in attitude results in a change in behaviour is not uncontested. Ajzen and Fishbein argue that there is a causal sequence going from belief to attitude, social norm, intention and behaviour. Icek Ajzen and Martin Fishbein, \textit{Understanding Attitudes and Predicting Social Behavior}, ed. Martin. Fishbein (Upper Saddle River, N.J: Prentice-Hall, 1980). Others, like Fointaint do not believe a clear causal relation exists but urge for more research on this topics. Fointaint and Barbier, “Persuasion et Influence : Changer Les Attitudes, Changer Les Comportements. Regards de La Psychologie Sociale.” p. 1.

\textsuperscript{112} Rid, \textit{Active Measures: The Secret History of Disinformation and Political Warfare}. p. 434.
media platform VKontakte picked up the anti-NATO Corona narrative, content can be repeated and reinforced via software programmes, the so-called ‘bots’. Bots are used to generate support of politicians by amplifying and disseminating media messages on i.a. Twitter, Facebook or Instagram, exploiting political grooming of agents that reinforce the narrative.

The amplification of messages creates an illusion of proof and authority. If many agree, support or ‘like’ a person or message humans - as social being - are inclined to perceive this as being familiar, true, genuine or authoritative, addressing heuristics of the audiences. This illusionary connection, and addictive inclination, relates to the number of likes instead of the factuality, can be exploited. The frames, mentioned earlier, couple socially divisive topics to heuristics of target audiences in line with a narrative revolving around an event. But the connection created does not need to be true or involve causality. The ‘trapped’ fabricated news, - such as the spreading of the Corona virus by NATO soldiers, endorsed by the EU - can benefit from continued and consistent repetition of the message for instance with Twitter-bots, making use of the compatibility-principle. And when disinformation is shared or broadcasted at the right moment, it addresses our focus-principle which implies that countervailing information will be discarded. Using credible persons or outlets to disseminate, repeat and magnify the data, generates familiarity with the topic, and the inclination to belief that the content of message is true and real. Big data and data science can generate the illusion of predictable behaviour based on the attributes of the audiences. This illusionary element lies in connections that remain hidden but creates a fictitious causality.

4. Reflections and conclusions

The aim of influence operations is to undermine the deliberate understanding and autonomous decision-making, or even to lure audience into making biased judgements. Having biased judgements means that audiences were deflected towards using cognitive and social heuristics due to a time restraint but more likely due to specific injects of (an overwhelming amount of) framed content. Subconscious techniques which force reflexive responses based on heuristics, circumvent the deliberate understanding and autonomous decision-making all together, which also makes them coercive in nature.

---

114 Cockerell, “How Russian Bots Amplify Britain's Jacob Rees-Mogg.”
116 P.W. Singer and Emerson T. Brooking, LikeWar: The Weaponization of Social Media (Houghton Mifflin Harcourt, 2018). p. 3. According to the author, every time a message is posted or a reaction (“like”) received a burst of dopamine is released creating the need for another burst and hence another “like”, or “tweet”; Peter Pomerantsev, This Is Not Propaganda : Adventures in the War against Reality (London: Faber & Faber, 2019). p. 161.
Influence operations follow a sequence starting with preparing the operation (formulate an intent, selecting the proper strategic narrative as an instrument of power, operationalising the narrative in one of several frames); executing the operation via cyber-related activities such as disinformation or trolling campaigns; and finally exploiting successful activities via social media. But these phases, as with the Italian case used, will most likely not be executing in a linear fashion by one State or agents.

This article focused on how and why influence operations generate effects via cyberspace and what the added value of cyberspace in this context is. The question can also be restated: Why does a single white lie or some fabricated new item falls moot, while other disinformation campaigns can have severe consequences related to the deliberate understanding and autonomous decision-making of the targeted audience?

The core difference between ad-hoc and deliberate influencing campaigns is twofold. First, in a deliberate influence operation, messages will be properly framed and executed during cyber-related activities. Framing is the operational art of transforming strategic or policy aims (narrative) into actionable measures (cyber-related activities). A frame couples the strategic narrative, to divisive topics of a society and audiences’ preferences and heuristics, around a specific event such as covid-19. The frame made does not need to be true. Second, influence campaigns deliberately exploit social media to magnify and amplify those messages and cyber-related activities to which the audience is initially receptive.

Though influence operations have been around for ages, cyberspace has changed influence operations and reinforced their effectiveness. First, the characteristics of cyberspace and especially social media platforms make it possible to micro-target very specific groups in society due to data regarding the behaviour and beliefs of these groups available on social media. This, exacerbated by big data and data science techniques making it possible to single out these groups. The content of the bespoke messages the audiences obtain, can have the aim to sow discord (disinformation), exacerbate polarisation (trolling), favour or undermine actors (political grooming) or create a shock-and-awe effect by leaking non-public information in the public domain.

Second, influence operations in cyberspace deviate from traditional operations, in the sense that they are not linear. Not only is it possible that the executing and exploitation phase run in parallel, it is very likely that influence operations are executed by several independent State and non-state actors. In the Italian Covid-19 case as described in this article the framing was domestic, but exploitation was driven by the RF since Italian disinformation campaign coalesced with existing RF anti EU and anti-US and NATO narratives.

Finally, the attributes of cyberspace are well suited to magnify and amplify content. The repetitive effect is best when the message fits the form and language used within the dynamics of society, and is aligned with the preferences and subconscious biases of the audience addresses. And due to the velocity and reach of internet the exploitation of
successful cyber-related activities runs in parallel with the cyber-related activity itself reinforcing its effect. Mobilising ‘armies’ of software-governed bots is also conducive for multiplying messages and ‘likes’, creating the illusion of truth, the acme of susceptibility, to initially false and fabricated frames.

**Bibliography**


EU vs Disinformation. “Disinfo:The Coronavirus Is a Bioweapon Brought to Italy by the


Jeangene Vilmer, Jean Baptiste. “Information Manipulation: A Challenge for Our Democracies.” CAPS of the Ministry for Europe and Foreign Affairs and IRSEM of the
Ministry for the Armed Forces, 2018.


Reynolds, Anna. *Social Media As a Tool of Hybrid Warfare. NATO Strategic Communication Centre of Excellence*, 2014.


