Towards the use of the DISARM framework as a lever for raising awareness and protecting audiences targeted by disinformation operations.

Jean-Philippe Riant[1,*,†] and Ugo Peyre[2,*,†]

[1] *Pôle d'Excellence Cyber de Rennes, Datask, France*

[2] *Institut d'Etudes Politiques de Rennes, Datask, France*

The emergence of vocabulary previously reserved for military conflicts within the field of communication highlights how information has become a key issue in current confrontations. The increasing importance of information in these conflicts has been made possible by recent transformations in adoption, production, and dissemination practices driven by digital tools and social networks.

Democracies, where information and opinions are free, are destabilized by campaigns spreading false information or deliberate misinformation orchestrated by authoritarian regimes, for which disinformation is part of a strategy targeting adversaries.

We propose to acknowledge this ongoing information warfare and, after conducting an inventory of media literacy and awareness programs, to assess the level of protection or resistance capabilities among the audiences targeted by these disinformation campaigns. To model what is happening at different scales—strategy, moderation, influence, reception, and sharing—a parallel will be drawn with air defense systems intended to protect populations from asymmetrical saturation attacks.

Beyond this comparison, the cognitive mechanisms employed by individuals when confronted with new information on social networks will be described. Similarly, influence and propagation models on social networks will be compared to identify leverage points within individuals that could be acted upon.

Various frameworks, analysis models, and particularly the DISARM framework will be examined to determine how they could drive the development of new tools for raising awareness and protecting social network users of all ages. The potential for creating engaging scenarios or serious games for adults based on the DISARM framework will also be discussed.

[*] Corresponding author.
[†] These authors contributed equally

jp.riant@datask.fr (JP. Riant); ugopeyre42@gmail.com (U. Peyre)

1. Disinformation, manipulation of information, fake news, false truths, principles and definitions

In the *Dictionnaire de la désinformation* published in 2011 [1] , disinformation is defined as a covert action of a hostile nature aimed at causing the impotence or weakening of the opponent by scrambling their information (manipulation of information, manipulation of truth, false truths, or fake news) and disorienting their decision-making abilities. The result is an increase in the user's power relative to the decrease in the opponent's ability to act.

From the perspective of information theory, disinformation could then be seen as a mechanism for introducing and developing entropy, in other words, increasing chaos. It could be compared not to those computer viruses that gradually destroy data, but to those that imperceptibly alter initial data to create a decoy. The attack through disinformation consists in distorting the understanding of a situation.

This parallel with computer viruses highlights how the approach to combating information manipulation in the digital world initially focused on technical cybersecurity issues, particularly by seeking automated weak signals detection and response strategies.

As illustrated in France by the existence of a working group on combating information manipulation within the *Pôle d'Excellence Cyber*, the fight against disinformation is considered part of the broader "cyber" domain, which is shorthand for "cybersecurity".

In cybersecurity, the individual, or the information system user, is essential since they represent a critical entry point with high-risk potential for malicious actions. As such, many national or international regulations (GDPR [2], NIS [3], ISO 27001 [4], among others) mandate awareness initiatives for information system users. The goal is for them to adopt best practices and enhance the security of digital systems through appropriate behavior and a "resistant" attitude towards attacks, as described, for example, in the MITRE ATT&CK framework [5]. Frameworks are models for representing and analyzing disinformation or cybersecurity operations. We will later discuss, in more detail, the DISARM framework (for Disinformation Analysis and Risk Management - an open-source project by the DISARM Foundation) and the emerging DIMA framework (for Detect, Identify, Memorize, and Act - a project by the M82 association).

Here, we see the emergence of a duality in vocabulary between the military and security fields. Cybersecurity faces adversaries such as criminals in various forms, potentially state-sponsored, but still falling under common law. In the case of disinformation, defense issues are military in nature, as these destabilization operations contribute to a form of hybrid warfare. The informational aspect creates conditions for a possible victory without fighting on the real geopolitical battlefield, after weakening the adversary's convictions [6].

Regarding the fight against disinformation, the individual is a key entry point that must be addressed. However, it is the aggregation of individual behaviors that are receptive to disinformation that lays the groundwork for destabilization or the emergence of opinions that foster a form of chaos, creating a broader phenomenon that acts on and through the masses [7]. What, then, is the state of global awareness and the mindset regarding informational defence [8] that Colon advocates for [9], or that Riant envisions by aiming to create or strengthen the conditions for a public resistance against information falling from the sky like propaganda leaflets in a besieged city [10]?

2. Are we at war? Are citizens enough protected?

Heard by the French Senate inquiry committee on foreign influences, the French Minister of Europe denounced a "brutalization of international relations" and warned that "disinformation has become a real weapon of war" [11].

The same inquiry committee stated in its report, released in July 2024, that we have entered a "neo-Cold War" [12].

Many authors discuss arming institutions or citizens. Some suggest that we should "arm ourselves for cognitive warfare" [13]. Others urge us to "arm everyone in the information war" and describe an emergency situation in a French parliamentary report by the cultural committee [14].

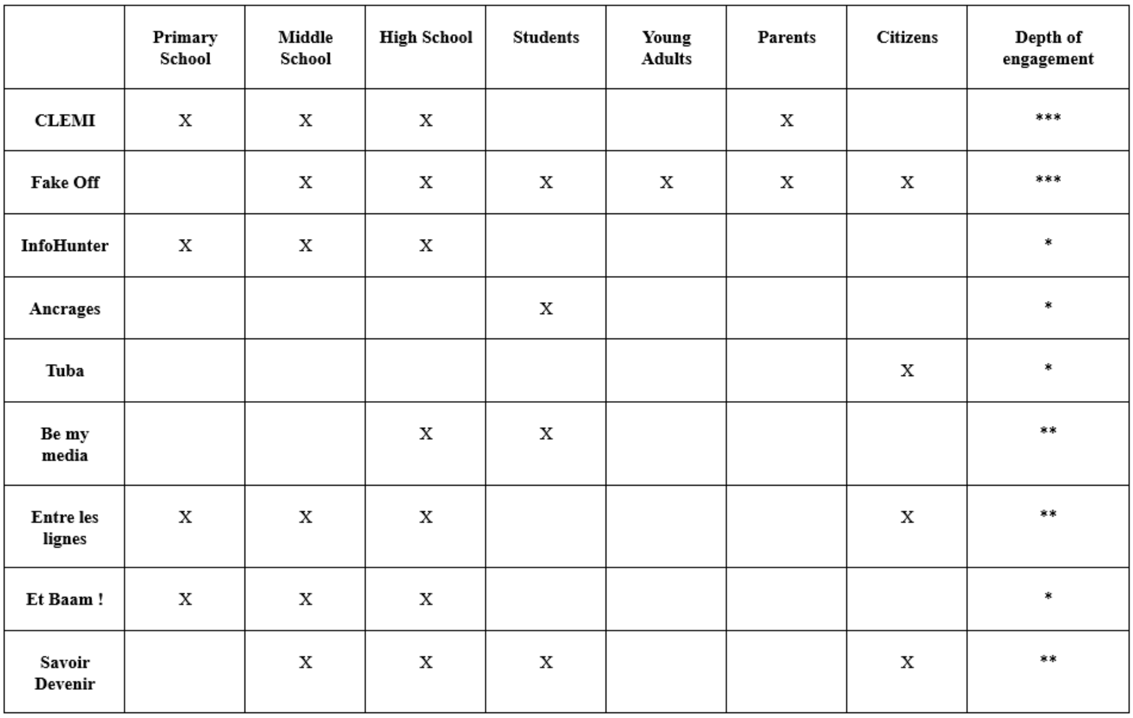
NATO, an organization at the heart of military issues, defines information warfare as "operations aimed at gaining an informational advantage over an adversary" [15] and is actively engaged in the fight against disinformation [16].

It would be too lengthy to list all the positions that use the terms war or armament in relation to the concepts of disinformation, information manipulation, or foreign interference, whether in institutional statements or in academic works.

We will assume that we are at war for the remainder of our analysis. However, it should be noted that the triggering factors necessary for every citizen to be mobilized (existential fear for their country, their democratic model, their freedoms) are not fully grasped by everyone. How can we accelerate this awareness using appropriate tools or processes so that each person becomes more vigilant or concerned about their own behavior?

What measures currently exist in France to protect individuals from this threat? Based on internet research using keywords like "fight against disinformation," "media education," and "awareness-raising," and by focusing only on organizations offering practical content coupled with workshops, we summarize in Table 1 the organizations that we have identified as providing content or awareness activities related to disinformation, media education, or media literacy. Media literacy is defined by the European Commission as "the ability to access media, critically understand and evaluate different aspects of media and its content, and create communications in various contexts" [17]. Beyond the French initiatives catalogued, the fight against disinformation and media literacy is a global issue engaging numerous organizations and initiatives internationally. For example, the EUvsDisinfo project serves as a European equivalent to VIGINUM [18], similar to the DFRLab across the Atlantic [19]. On the national level, Finland is a leading example that many European countries, including France, should emulate. Media and information literacy has been carried out by The Finnish Newspaper Association for 50 years [20]. Initiatives led by the Finnish National Audiovisual Institute, such as 'Media Literacy Week,' aim to strengthen Finnish society's resilience against informational threats, mainly from Russia [21].

It should be noted that in France, the prevention or awareness of disinformation is primarily viewed through the lens of media education, under the responsibility of the Ministry of National Education, with significant geographic disparities in effective implementation, as indicated in the Ministry of National Education's report published in 2023 [14].



	Primary School	Middle School	High School	Students	Young Adults	Parents	Citizens	Depth of engagement
CLEMI	X	X	X			X		***
Fake Off		X	X	X	X	X	X	***
InfoHunter	X	X	X					*
Ancrages				X				*
Tuba							X	*
Be my media			X	X				**
Entre les lignes	X	X	X				X	**
Et Baam !	X	X	X					*
Savoir Devenir		X	X	X			X	**

Table 1: Awareness-Raising Measures for Disinformation and Media Education in France (*low depth, **medium depth, ***high depth)[3]

The risks of opinion manipulation do not, at first glance, hold significant interest for the private or commercial sector (although the risk of political instability is highlighted by the World Economic Forum [22]). As a result, addressing disinformation is left to public or non-

[3] - **CLEMI** : Diverse offerings reaching a wide audience. Content is frequently updated. National scope.
- **Fake Off** : Broad target audience (both school and non-school environments). Numerous workshops organized. Ready-to-use educational kits.
- **InfoHunter** : Limited offerings. Few online educational resources, which are not updated.
- **Ancrages** : Recent awareness initiative (March 2024). Few resources related to media and information literacy.
- **Tuba** : Focused on a single disinformation issue. Few resources related to media and information literacy.
- **Be my media** : Many workshops organized around media and information literacy. Large quantity of educational content. Varied target audience. Content not frequently updated.
- **Entre les lignes** : Varied awareness services (with training for supervisory staff). Regularly updated content. No educational resources.
- **Et Baam** ! : Limited and varied offerings, sporadically updated content.
- **Savoir Devenir** : No awareness workshops. Numerous educational resources but infrequently updated. National scope. Training for supervisory staff.

profit actors. The limited funding relative to the scale of the issue partly explains the inadequate response compared to the ongoing and intense nature of the threat. The lack of national coordination is also noted, as highlighted by the French Senate commission on foreign interference in its 2024 report [12]).

The limited availability of measures, their weak deployment across the population, and especially their positioning far from a sense of urgency and mobilization in situations of conflict or aggression, should be considered in light of the fact that disinformation is considered the top threat to the global economy over the next two years [22]. The reasons given include the upcoming large number of democratic elections, as well as a distortion of reality likely to polarize public debate, something France has experienced since the 2017 elections and through the various crises the country has faced over the past 10 years (Macron Leaks, Yellow Vests, COVID-19 and anti-vaccine, Mali, New Caledonia, European and legislative elections…). Let us recall that, according to Ellul, "Propaganda – an action aimed at shaping the perception of the world to steer collective action in favor of the propagandist's objective – is the means to gain and maintain power" [7]. Meanwhile, as early as 1928, Bernays asserted that "Propaganda – the conscious and intelligent effort to influence the opinions and actions of the masses – is the executive arm of the invisible government" [23].

The world's top threat and the weakness of individual protection measures - paradox often observed in pandemic contexts where public responses are slow to be implemented at a meaningful and relevant scale.
To identify new avenues for individual-level efforts in combating disinformation, we first propose to take stock of what occurs at the individual level when a person is exposed to disinformation operations without necessarily being aware of it, while also potentially becoming a vector for its spread.

3. Levels of scale and types of actions or reactions

To identify new levers for individual-level countermeasures, we first propose to assess what is happening at the individual level when confronted with disinformation operations, often without being fully aware of it, while potentially serving as a vector for its spread.

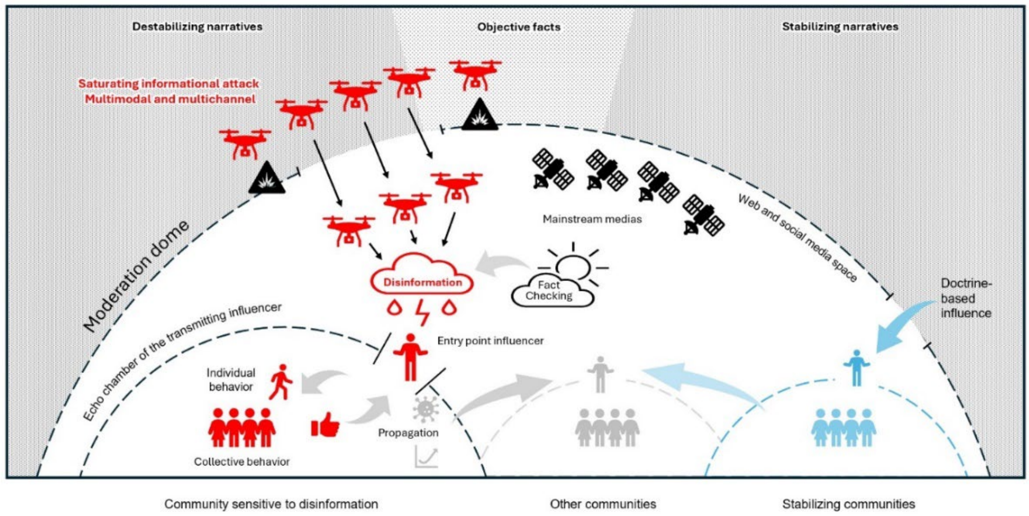


Figure 1 - Modelling of a Saturating and Coordinated Information Attack Based on the Principle of an Anti-Aircraft Assault and an Iron Dome-Type Protection System

We distinguish four levels of scale, ranging from the most global to the most individual. We begin with the strategy of global actors (states, terrorist groups, hacktivists…), followed by systemic defense mechanisms (platform moderation as early as possible in the distribution chain, removal after detection or reporting of potentially illegal or harmful content). Next, we integrate a level focused on influence (which can be analyzed from the perspective of opinion leaders' strategies, whether mercantile or related to personal branding). Finally, we direct our analysis to the individual level, where people adopt behaviors and propagation mechanisms based on individual sensitivities or protective behaviors (critical thinking) or dissemination behaviors (propagation mechanisms [24]). According to Boullier, this level is where “the individual is traversed by diverse and varied propagations that will inhabit and shape them”.

To illustrate the difficulty or lack of willingness of platforms to moderate their content, Chavalarias points out that Facebook only moderates 20% of the political ads it broadcasts on its network [25]. In the same vein, according to Brussels, Facebook and Instagram are experiencing a "proliferation of ads that pose a risk" of political manipulation – or that serve as vectors for financial scams [26]. The X network is also criticized when Elon Musk is reminded of his responsibility to moderate not only his platform but also his own statements [27].

According to the Digital Services Act [28], platforms have moderation duties, especially after content is reported. However, it should be noted that they are not held to strict outcome obligations and often struggle to meet their procedural obligations.

"Total moderation," seen as an effective defense against saturating attacks, is difficult to achieve. To draw a parallel with the Iron Dome, 75% to 96% [29] of enemy rockets are intercepted, so the system is not foolproof. The lack of total protection at a distance justifies the availability of numerous public or private shelters [30] and the strong culture of individual protection ingrained in the population [31]. This is what needs to be implemented in the digital world.

Closer to individuals, social media users tend to consume content within an echo chamber, which can be defined as an environment where an individual's opinion, political tendency, or belief on a certain subject is reinforced by repeated interactions with peers who share similar views [32]. These echo chambers can be further intensified by filter bubbles driven by content distribution algorithms. Influencers, formerly known as opinion leaders before the rise of social media, are the vectors for introducing new information within these echo chambers.

A social media user can be defined as an influencer when they have the ability to convince someone to change their opinion, attitude, or behavior [33]. Based on their activity on social media, it is possible to identify three types of influencers: [34]

- **The opinion leader**, whose influence is carried by the content they produce, can generate significant income if they maintain their influence.
- **The informational influencer** uses their position within social networks to share existing information from traditional media or journalists.
- **The activist** stands out through high levels of activity, aiming to promote a specific political opinion.

At the individual level, both cognitive and perception mechanisms, as well as more collective dynamics of propagation and virality, come into play. We detail these in the following paragraphs.

4. The mechanisms triggered by the individual when facing authentic or inauthentic information

There is a before and after in the integration of information by the individual: the awareness of the difference that the information makes for them.

As Laborde [35] describes, one can "influence with integrity", but influencing is not the same as manipulating, since manipulation is not the practice of honest people, even though it is important for them to be aware of techniques that can be used to guide behavior [36]. Therefore, a duality can be identified between influence and manipulation, shifting depending on the level of integrity that can be measured in the communicator. This integrity could be defined by assessing whether the communicator uses their power "for" serving the receiver’s interests, teaching them something, helping them better grasp objective truth, or whether they use their power "over" the receiver by guiding their behaviors according to their own interests. Power *for* or power *over*—this is a proposed evaluative distinction to judge the toxic nature of a system.

Similarly, if the difference created by the transmission of information aims to benefit the receiver, we can speak of an information process. However, if the goal is to take control over the receiver by altering their free will or using them against their own interests for a purpose beyond their understanding, we then speak of disinformation. Power *for* or power *over*, influence or manipulation.

What mechanisms influence the perception of information and, consequently, the behaviours they generate?

First, individuals tend to seek out and remember information that confirms their pre-existing beliefs (confirmation bias) [37]. This tendency is amplified when inauthentic content is sensationalist and emotionally charged. Truthful information, on the other hand, is less memorable because it seems "bland" compared to the avalanche of false but highly impactful content [38].

Added to this is the influence of social pressure: people often share information because others have shared it before them, thereby reinforcing its perceived truthfulness through mere repetition [39]. This phenomenon, characteristic of social networks, is part of the illusory truth effect, where the familiarity of information, even if false, increases its credibility. This mechanism is even more powerful because individuals do not always realize that they have already been exposed to this information [40].

In relation to the Online Misinformation Engagement Framework [41], the DIMA model proposed by Boyer [13] and the M82 association is useful in understanding the various biases individuals face when interacting with information and the expected actions upon encountering this information. Inspired by the MITRE ATT&CK and DISARM matrices, it breaks down the interaction process into four successive phases. When an individual is exposed to information, a set of cognitive mechanisms determines how this information will be perceived, processed, memorized, and potentially translated into action:

- **Detect:** The brain's selection process, when faced with a continuous flow of information, is influenced by biases such as the contrast effect or confirmation bias. These mechanisms favor content that stands out from the flow or confirms our pre-existing beliefs.
- **Inform:** After selection, the brain assigns meaning to the captured information. There is no passivity in this process; the individual reinterprets the information according to specific mental patterns like the anchoring bias (the first piece of information received serves as a reference point).
- **Memorize:** The information is then integrated into the individual's mental representations. The same content can be memorized differently depending on the narrative and emotional context in which it is introduced. Thus, confirmation bias reinforces information that aligns with pre-existing beliefs.
- **Act:** This phase involves transforming information into action. The action bias promotes the idea that acting is preferable to inaction, while the availability bias gives more weight to striking examples. As a result, the individual is driven to act based on a distorted perception of the urgency of a situation.

The neurobiological process underlying the use of social networks must also be considered. On these platforms, every like, comment, or notification trigger dopamine production. By activating this reward system, individuals are driven to seek more interactions. This dependence on social validation alters how information is perceived and processed. In the pursuit of social approval, individuals gradually lose their critical thinking ability and adopt beliefs, even if they are false [42].

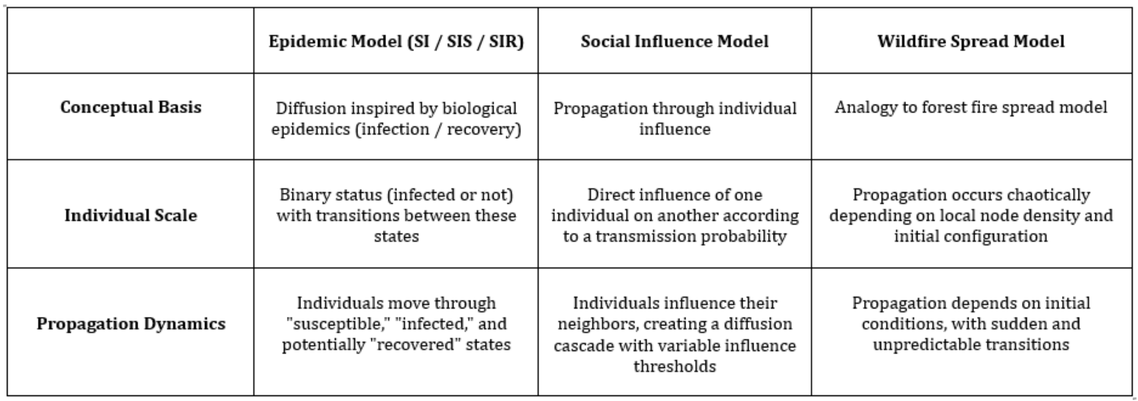
It is important to note that the DIMA framework provides an analytical framework for understanding how individuals interact with information. The final point in this analytical grid addresses action, a conative dimension that encourages reflection at a higher level of scale, focusing on the propagation or virality at play within the collective.

5. Social Networks: Different Models of Information Propagation

The conative dimension of a message (even if implicit) or a communication strategy seeks to influence the behavior or actions of the recipient, acting as an encouragement or prompt to adopt a certain behavior. We have seen that the logic of reinforcing one's social standing within a group or reward mechanisms creates the conditions for sharing and virality. These are the conditions that lead to the emergence of propagation mechanisms.

Numerous theoretical models for information propagation on social networks have been proposed. Notably, we can distinguish:

- **Epidemic Models** inspired by the spread of diseases, categorizing individuals as "infected," "susceptible," or "immune" (SI, SIS, SIR models).
- **Social Influence Models** that highlight the key role of "opinion leaders" or "influential nodes" in the diffusion of information [43].
- **The Wildfire Spread Model** inspired by the propagation of forest fires [44].



	Epidemic Model (SI / SIS / SIR)	Social Influence Model	Wildfire Spread Model
Conceptual Basis	Diffusion inspired by biological epidemics (infection / recovery)	Propagation through individual influence	Analogy to forest fire spread model
Individual Scale	Binary status (infected or not) with transitions between these states	Direct influence of one individual on another according to a transmission probability	Propagation occurs chaotically depending on local node density and initial configuration
Propagation Dynamics	Individuals move through "susceptible," "infected," and potentially "recovered" states	Individuals influence their neighbors, creating a diffusion cascade with variable influence thresholds	Propagation depends on initial conditions, with sudden and unpredictable transitions

Table 2: Summary of parameters for propagation models on social networks

These different models highlight the central role of the individual in the propagation of information on social networks. The individual functions as a node, and their interactions with others are the connections that spread information. It is disseminated through dynamics of individual influence. Thus, an active user who frequently interacts with their network plays a key role in either amplifying or hindering the spread of information [43].

6. Discussion. Awareness levers and pedagogy of resistance, opportunities offered by the Disarm framework

For an overview of disinformation operation models (referred to as frameworks in English), Cánovas López de Molina and al. identifies in their state-of-the-art review eight types of models or analytical principles, testing five of them on a real operation in Mali to identify the specificities and commonalities of these different models (DISARM, ABCDE, ALERT, BEND, SCOCTH) [45]. It should be noted that the DIMA model had not yet been published at the time of this article's release and therefore could not be included in the analysis.

Unlike Cánovas López de Molina and al. [45], the aim of our work is not to compare the models, but rather to highlight that these cross-sectional analysis tools for disinformation operations offer several advantages, making them effective tools for awareness and prevention efforts:

- They offer a comprehensive, temporal, and detailed view of an operation, helping to raise awareness of all the steps, particularly those preceding the dissemination of information, that are implemented to influence individuals and public opinion.
- These models, especially DISARM, provide a taxonomy that facilitates the understanding of tactics, techniques, or procedures by producing a shared taxonomy that is easily translatable and, most importantly, comprehensible to non-experts, as tested and validated by NATO and the Hybrid CoE [46].
- The modeling provides a synthetic and shared representation that can serve as a foundation for analysis, as well as for the creation of fictional scenarios used in training or awareness programs.

Let's focus on this last point to better understand how these frameworks offer numerous opportunities to create new tools for raising awareness and building resilience among social media users.

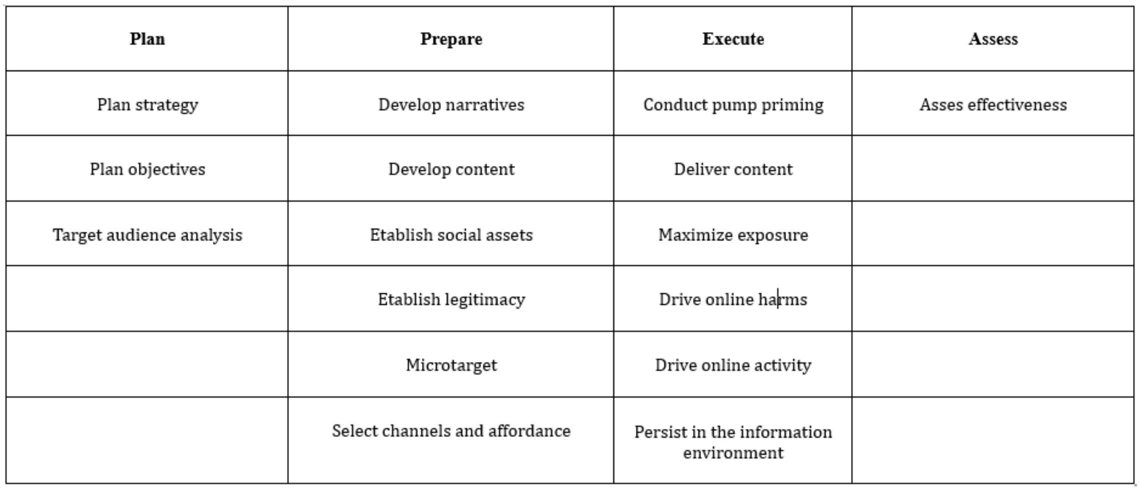
First of all, it should be noted that simple media education within the school context is not enough. Firstly, because it is not equally distributed and implemented across our territory, and secondly, because it takes place within the school environment, which has little influence compared to the time students spend on platforms. In 2023, in France, according to Diplomeo [47] :

- 18% of 16–25-year-olds report spending more than 5 hours per day on social media (+6 points compared to last year)
- 45% spend between 3 and 5 hours per day
- 28% spend between 1 and 2 hours per day
- 9% spend less than 1 hour per day

On the other hand, "youth is less a status than it is a set of challenges that force individuals to build their own experience" [48]. Therefore, we must consider broader initiatives that can take place in digital environments, allowing for unique and truly formative experiences through discovery and experimentation.

The DISARM framework offers several advantages for enabling designers to develop new awareness concepts for the public:

- Its comprehensive and temporal approach (from the oldest to the most recent, from left to right) allows for in-depth work on a "narrative arc," similar to how series writers create coherence across multiple episodes.
- Its taxonomy facilitates collaboration among professionals from different fields - such as communicators, scriptwriters, educators, and game designers - on the same topic.
- DISARM is an open model that easily accommodates the addition of new techniques, making it adaptable to evolving tactics observed in the field.
- Its red matrix provides insights into everything a malicious attacker can do to design a sophisticated scheme, offering a comprehensive and synthesized view of the chronology and multimodal complexity of a disinformation operation. It allows users to step into the attacker's shoes by understanding the stages of their strategy.
- The blue matrix provides an appropriate response to various attack possibilities. For each attack described in the red matrix, the corresponding countermeasure is given by the blue matrix
- The DISARM framework is now a reference tool used by services as an information-sharing platform among friendly and allied actors facing these attacks.



Plan	Prepare	Execute	Assess
Plan strategy	Develop narratives	Conduct pump priming	Asses effectiveness
Plan objectives	Develop content	Deliver content	
Target audience analysis	Etablish social assets	Maximize exposure	
	Etablish legitimacy	Drive online harms	
	Microtarget	Drive online activity	
	Select channels and affordance	Persist in the information environment	

Table 3. Simplified representation of process titles and tactics in the red DISARM matrix [49]

Several elements lead us to believe that adapting this framework into a game could be an interesting development avenue for awareness-raising tools targeted at different audiences - secondary school students, university students, young professionals, and parents:

- Gaming is already integrated into the blue matrix under code C00011: media education. Games to identify false information [50].
- As highlighted by the creator of the internationally successful game *Grand Theft Auto*, which allows players to embody a car thief, the designers initially envisioned a game where players were police officers. However, success came when they reversed the model and allowed players to take on the role of the thief: "Seeing law enforcement's response intensify based on the severity of one's crimes". [51]
- In the case of disinformation, designing operations from the perspective of a state or organization and imagining what would be necessary to create destabilization conditions could lead to a beneficial dissociation that raises awareness of the tactics targeting us in the real world.
- Game (even a serious game for more informed audiences) or simulation can be adapted for all audiences across different platforms—online, on mobile devices, as card games, or in simulators, like C00022: table-based simulation game [50]. These approaches have shown superior learning outcomes and a positive user experience [52] [53].

To explore mechanisms for raising awareness, building resilience, and reducing individuals' susceptibility to manipulative content, it is possible to virtually position the individual as the attacker so that they understand the mechanics of the operations in which they might be the target or a transmission vector. *Bad News* is an example of an online game that puts the player in the shoes of an instigator of a disinformation operation. It has been described as a tool for combating disinformation by the 'Information Manipulation' commission of the IHEDN [54]. *Bad News* would potentially enhance individuals' resilience against disinformation spread on social media[55].

In the next phase, based on interviews conducted with DISARM framework users and game designers, it will be necessary to translate this tool into a scenario creation engine for awareness-raising in a playful format. Further work will focus on the methodology for developing this engine and identifying stakeholders to be involved in the process.

Educational (or awareness) strategies, developed into practical tools for "all" individuals, while specifying them for each target audience, should be considered as an output: middle school students, high school students, higher education students, young adults, and finally, parents. Each target audience will have a differentiated version of the awareness program, but all will be structured based on the same red DISARM matrix. In the long run, it will be necessary to define the specific needs of each group and evaluate the proper understanding and usage of the proposed tool.

7. Conclusion

In response to the challenges posed by interference and disinformation, it is crucial to develop adapted and effective solutions. This article suggests exploring methods of countering disinformation at the individual level by evaluating opportunities to make individuals less susceptible or contagious to operations that threaten the stability of our societies.

The spread of dishonest information is a long-term process involving defined processes, tactics, and techniques. To equip individuals against disinformation, it seems necessary to expose them to the strategies they face daily. In this way, disinformation could be thwarted before it can achieve its intended impact. Conversely, taking a purely defensive stance would only aim to understand the source, technique, or tactic used after the fact - in other words - attempting to extinguish a fire once it has already spread.

Tools recognized in the cyber community, such as the DISARM framework, exist and provide a framework for designing playful programs that can be adapted to all platforms and audiences. In future work, we will propose ways to adapt and simplify this framework to make it a tool for mediation and awareness. Once this work is completed, we hope it will be at the heart of concrete initiatives in the fight against disinformation by fostering new levels of citizen responsibility and engagement.

References

[1] F. Géré, “La désinformation,” in *Dictionnaire de la désinformation*, in Dictionnaire. , Paris: Armand Colin, 2011, pp. 57–69. [Online]. Available: https://www.cairn.info/dictionnaire-de-la-desinformation--9782200257729-p-57.htm

[2] “Le règlement général sur la protection des données - RGPD.” Accessed: Aug. 23, 2024. [Online]. Available: https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[3] *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l’ensemble de l’Union*, vol. 333. 2022. Accessed: Aug. 23, 2024. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/fra

[4] 14:00-17:00, “ISO/IEC 27001:2022,” ISO. Accessed: Aug. 23, 2024. [Online]. Available: https://www.iso.org/fr/standard/27001

[5] “MITRE ATT&CK®.” Accessed: Aug. 23, 2024. [Online]. Available: https://attack.mitre.org/

[6] Sun zi, F. Wang, and S. B. Griffith, *L’art de la guerre*, Nouvelle éd. 2017, Revue et mise à jour. in Champs. Paris: Flammarion, 2017.

[7] J. Ellul, *Propagandes*. in Classiques des sciences sociales. Paris: Economica, 1990.

[8] “« La guerre de l’information » - 4 questions à David Colon,” IRIS. Accessed: Aug. 23, 2024. [Online]. Available: https://www.iris-france.org/182662-la-guerre-de-linformation-4-questions-a-david-colon/

[9] D. Colon, *La guerre de l’information: les États à la conquête de nos esprits*. in Essais. Paris: Tallandier, 2023.

[10] J-L. Gibernon (Dir.) and J-P. Riant (Dir.), “Lutte contre la manipulation de l’information, regards croisés de professionnels du secteur,” Nov. 2023. Accessed: Aug. 23, 2024.

[Online]. Available: https://www.pole-excellence-cyber.org/wp-content/uploads/2024/01/LMI_PEC_2023.pdf

[11] A. Graillot, “Ingérences étrangères : « La désinformation est devenue une véritable arme de guerre », alerte Jean-Noël Barrot,” Public Sénat. Accessed: Aug. 25, 2024. [Online]. Available: https://www.publicsenat.fr/actualites/parlementaire/ingerences-etrangeres-la-desinformation-est-devenue-une-veritable-arme-de-guerre-alerte-jean-noel-barrot

[12] D. de Legge and R. Temal, “Lutte contre les influences étrangères malveillantes, pour une mobilisation de toute la nation face à la néo-guerre froide.,” Rapport n° 739 (2023-2024), juillet 2024.

[13] B. Boyer, “S’armer pour la guerre cognitive : le modèle DIMA,” Medium. Accessed: Aug. 24, 2024. [Online]. Available: https://medium.com/@Cybart/sarmer-pour-la-guerre-cognitive-le-mod%C3%A8le-dima-4224044856c2

[14] S. Leleu-Merviel and V. Spillebout., “Armer chacun dans la guerre de l’information. Etat d’urgence.,” Assemblée Nationale, Commission des affaires culturelles et de l’éducation., 2023. [Online]. Available: https://hal.science/hal-04072759v1/document

[15] NATO Defence Education Enhancement Program, “NATO Disinformation 2 pages.” [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/05/pdf/2005-deepportal4-information-warfare-fr.PDF

[16] NATO, “L’approche de l’OTAN en matière de lutte contre la désinformation,” NATO. Accessed: Aug. 25, 2024. [Online]. Available: https://www.nato.int/cps/fr/natohq/topics_219728.htm

[17] “A European approach to media literacy in the digital environment,” CEDEFOP. Accessed: Aug. 23, 2024. [Online]. Available: https://www.cedefop.europa.eu/en/news/european-approach-media-literacy-digital-environment

[18] “EUvsDisinfo,” EUvsDisinfo. [Online]. Available: https://euvsdisinfo.eu/

[19] “DFRLab,” DFRLab. [Online]. Available: https://dfrlab.org/

[20] Rédaction, “Finlande : quelles leçons tirer de sa lutte contre la désinformation ?,” L’œil de la Maison des journalistes. [Online]. Available: https://www.oeil-maisondesjournalistes.fr/2023/04/12/finlande-quelles-lecons-tirer-de-sa-lutte-contre-la-desinformation/

[21] P. Rossi, “Educated decisions: Finnish media literacy deters disinformation,” This is Finland. [Online]. Available: https://finland.fi/life-society/educated-decisions-finnish-media-literacy-deters-disinformation/

[22] “Global Risks Report 2024,” World Economic Forum. Accessed: Aug. 23, 2024. [Online]. Available: https://www.weforum.org/publications/global-risks-report-2024/

[23] E. L. Bernays, N. Baillargeon, and O. Bonis, *Propaganda: comment manipuler l’opinion en démocratie*. Paris: Zones, 2007.

[24] D. Boullier, *Propagations: un nouveau paradigme pour les sciences sociales*. in Collection U. Malakoff: Armand Colin, 2023.

[25] France Culture, *Le Temps du débat - Ingérences étrangères : la France fait-elle face ?* [Online]. Available: https://podcasts.apple.com/fr/podcast/le-temps-du-d%C3%A9bat/id209089492

[26] “La Commission européenne prend ses distances après la mise en garde de Thierry Breton à Elon Musk,” Aug. 13, 2024. Accessed: Aug. 25, 2024. [Online]. Available: https://www.lemonde.fr/economie/article/2024/08/13/la-commission-europeenne-prend-ses-distances-avec-thierry-breton-apres-sa-mise-en-garde-a-elon-musk_6280037_3234.html

[27] “Modération des publicités : la Commission européenne ouvre une procédure formelle contre Meta,” Apr. 30, 2024. Accessed: Aug. 25, 2024. [Online]. Available: https://www.lemonde.fr/pixels/article/2024/04/30/moderation-des-publicites-la-commission-europeenne-ouvre-une-procedure-formelle-contre-meta_6230760_4408996.html

[28] *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (Texte présentant de l’intérêt pour l’EEE)*, vol. 277. 2022. Accessed: Aug. 25, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2022/2065/oj/fra

[29] P. T. O. I. STAFF, “Près de 1 100 roquettes ont été tirées de Gaza en direction d’Israël, en trois jours.” Accessed: Aug. 22, 2024. [Online]. Available: https://fr.timesofisrael.com/580-roquettes-ont-ete-tirees-de-gaza-en-direction-disrael-en-trois-jours/

[30] i24NEWS, “Israël: près de 30% de la population privée d’abris antimissiles en cas d’attaque,” i24NEWS. Accessed: Aug. 22, 2024. [Online]. Available: https://www.i24news.tv/fr/actu/israel/1596461259-israel-pas-de-refuges-antiaeriens-pour-pres-de-30-de-la-population-en-cas-d-attaque

[31] “Que faire en cas de crise ?,” La France en Israël - Ambassade de France à Tel Aviv. Accessed: Aug. 22, 2024. [Online]. Available: https://il.ambafrance.org/Que-faire-en-cas-de-crise-11108

[32] M. Cinelli, G. D. F. Morales, A. Galeazzi, W. Quattrociocchi, and M. Starnini, “Echo Chambers on Social Media: A comparative analysis,” Apr. 20, 2020, *arXiv*: arXiv:2004.09603. doi: 10.48550/arXiv.2004.09603.

[33] E. Dubois and D. Gaffney, “The Multiple Facets of Influence: Identifying Political Influentials and Opinion Leaders on Twitter,” *American Behavioral Scientist*, vol. 58, no. 10, pp. 1260–1277, Sep. 2014, doi: 10.1177/0002764214527088.

[34] F. B. Soares, R. Recuero, and G. Zago, “Influencers in Polarized Political Networks on Twitter,” in *Proceedings of the 9th International Conference on Social Media and Society*, in SMSociety ’18. New York, NY, USA: Association for Computing Machinery, Jul. 2018, pp. 168–177. doi: 10.1145/3217804.3217909.

[35] Genie. Z. Laborde, *Influencer avec intégrité: la programmation neurolinguistique dans l’entreprise*, Nouv. tirage. Paris: InterEditions, 1993.

[36] R.-V. Joule and J.-L. Beauvois, *Petit traité de manipulation à l’usage des honnêtes gens*, Éd. collector. Fontaine: PUG, 2022.

[37] A. Guess, B. Lyons, B. Nyhan, and J. Reifler, *Avoiding the echo chamber about echo chambers: Why selective exposure to like-minded political news is less prevalent than you think*. 2018.

[38] C. Martel, G. Pennycook, and D. G. Rand, “Reliance on emotion promotes belief in fake news,” *Cogn. Research*, vol. 5, no. 1, p. 47, Dec. 2020, doi: 10.1186/s41235-020-00252-3.

[39] R. Wedgwood, “The Aim Of Belief,” *Nous*, vol. 36, no. s16, pp. 267–297, Oct. 2002, doi: 10.1111/1468-0068.36.s16.10.

[40] G. Pennycook, T. D. Cannon, and D. G. Rand, “Prior exposure increases perceived accuracy of fake news.,” *Journal of Experimental Psychology: General*, vol. 147, no. 12, pp. 1865–1880, Dec. 2018, doi: 10.1037/xge0000465.

[41] M. Geers, B. Swire-Thompson, P. Lorenz-Spreen, S. M. Herzog, A. Kozyreva, and R. Hertwig, “The Online Misinformation Engagement Framework,” *Current Opinion in Psychology*, vol. 55, p. 101739, Feb. 2024, doi: 10.1016/j.copsyc.2023.101739.

[42] H. B. Macit, G. Macit, and O. Güngör, “A RESEARCH ON SOCIAL MEDIA ADDICTION AND DOPAMINE DRIVEN FEEDBACK,” *MAKU IIBFD*, vol. 5, no. 3, Art. no. 3, Dec. 2018, doi: 10.30798/makuiibf.435845.

[43] M. Li, X. Wang, K. Gao, and S. Zhang, “A Survey on Information Diffusion in Online Social Networks: Models and Methods,” *Information*, vol. 8, no. 4, Art. no. 4, Dec. 2017, doi: 10.3390/info8040118.

[44] V. Indu and S. M. Thampi, “A nature - inspired approach based on Forest Fire model for modeling rumor propagation in social networks,” *Journal of Network and Computer Applications*, vol. 125, pp. 28–41, Jan. 2019, doi: 10.1016/j.jnca.2018.10.003.

[45] G. Cánovas López de Molina, F. Sánchez González, P. Nespoli, J. Pastor Galindo, and J. A. Ruipérez Valiente, *Analyzing frameworks to model disinformation attacks in online social networks*. Universidad de Sevilla. Escuela Técnica Superior de Ingeniería Informática, 2024. [Online]. Available: https://idus.us.es/handle/11441/159640

[46] H. Newman, “Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework ‘DISARM’”.

[47] L. Diplomeo, “Réseaux sociaux : Instagram tire une nouvelle fois son épingle du jeu chez les 16-25 ans.” Accessed: Aug. 26, 2024. [Online]. Available: https://diplomeo.com/actualite-sondage_reseaux_sociaux_jeunes_2023

[48] F. Dubet, “La jeunesse est une épreuve,” *Revue de philosophie et de sciences sociales*, vol. N°5, pp. 275–291, 2004.

[49] “GitHub - DISARMFoundation/DISARMframeworks: Master copies of the DISARM frameworks, with generated files to help you explore the data.” Accessed: Aug. 28, 2024. [Online]. Available: https://github.com/DISARMFoundation/DISARMframeworks

[50] “Welcome to DISARM - Disarm Framework Explorer.” Accessed: Aug. 26, 2024. [Online]. Available: https://disarmframework.herokuapp.com/

[51] “« GTA » : comment un jeu de sales gosses est devenu un phénomène planétaire,” Aug. 12, 2024. Accessed: Aug. 24, 2024. [Online]. Available: https://www.lemonde.fr/series-d-ete/article/2024/08/12/gta-comment-un-jeu-de-sales-gosses-est-devenu-un-phenomene-planetaire_6278682_3451060.html

[52] Z. Yu, “A Meta-Analysis of Use of Serious Games in Education over a Decade,” *International Journal of Computer Games Technology*, vol. 2019, pp. 1–8, Feb. 2019, doi: 10.1155/2019/4797032.

[53] M. Roozeboom, G. van de Boer-Visschedijk, and E. Oprins, “The effectiveness of three serious games measuring generic learning features,” *British Journal of Educational Technology*, vol. 48, Oct. 2015, doi: 10.1111/bjet.12342.

[54] Commission « Manipulations de l’Information », “Benchmark des outils de lutte contre la désinformation,” Association des Auditeurs en Intelligence Economique de l’IHEDN, Sep. 2024. [Online]. Available: https://www.ie-ihedn.org/wp-content/uploads/2024/09/AAIE-IHEDN_Benchmark_Outils_-Lutte-Desinformation.pdf

[55] Gusmanson.nl, “Bad News - Play the fake news game!,” Bad News v2. [Online]. Available: https://www.getbadnews.com/books/english/