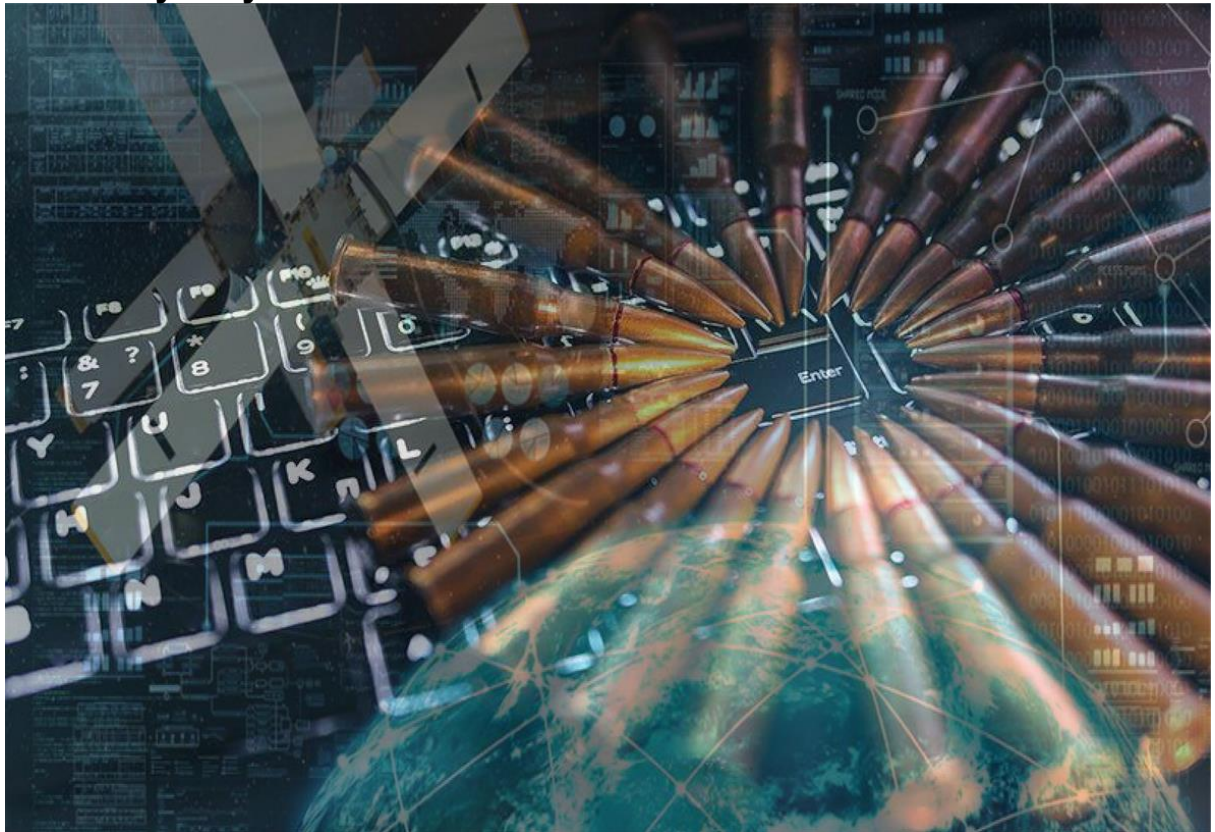# The Strategies of Digital Warfare in Changing the Face of the World

(Cyber Warfare and Visual Disinformation as a Model)

*"Imagination is more important than knowledge; with imagination we can see the future."*_ **Albert Einstein**

*"Future war will not be like conventional wars"*_ **US Defense Secretary Lloyd Austin**

رابط المقال الأصلي
Osman Ali: A researcher at Al Furat Center for Studies

Studies

Introduction

Geography, armies, and the pillars of states have become vulnerable to collapse and fall, on the media and electronic platforms before they fall on reality in conflicts, political disputes, and social unrest areas, due to the ongoing development of technology and its continuously updated generations.

Many concepts and theories of the psychology of influence, penetration and control have changed, alongside the rules of the game, the map of domination and the balances of power. Despite what the Internet and the means of communication provide for real-time communication between individuals and groups, shortening geography and time and facilitating daily life, they have become - at the same time -an exceptional destination for many recruited propaganda circles, which mobilize all their material and human energies to reshape and frame counter-public opinion.

Within the next pages, we will use the descriptive approach to study and analyze the strategies and dimensions of employing the different powers of the modern generations, from advanced technology to striking the vital targets of enemies and rivals. We will try to discern the effects resulting from all of this, at multiple levels and conclude logical explanations by relying on clear sources and authentic scientific references (Previous studies, research, reports, and television programs) to enrich the displayed content. These contents will be addressed in our research paper as following:

First: Cyber Warfare

Second: Visual Disinformation

Third: the Outcomes and Conclusion

First: Cyber Warfare

In the midst of an atmosphere full of developments and global changes, the equation of influence and control and changing the direction of the world needs to review the thinking way and dynamics of the conflict, especially with the transition from the traditional military strategy to the space strategy, in which the "Lords" of war and money are directed to employ (cyber armies, and technological capabilities). and long-range sensors), as vital arenas with complete elements, to demonstrate superiority, strength, and the ability to threaten and falsify minds, woo instincts, and guide their owners according to pre-established plans and agendas.

Cyber warfare is called on those cross-border electronic wars, which are led by electronic attacks that penetrate communication systems at an incredible speed, aiming at causing malfunctions in

technical devices and global Internet networks, and the result is catastrophic malfunctions.

New wars are often waged using the latest smart technologies, and with the support of technical research centers and psychological and sociological circles, which are invested by money owners, politicians and decision-makers, to give the popular base that supporting the ruling party or the state-for example - messages of reassurance that raise the spirit and morale, on one hand, and brighten the bad image of the practices of systems, institutions and individuals, on the other hand.

 the external front-level work also takes place; Hostilities are launched behind the borders with the aim of undermining the societal fabric and causing the greatest possible loss in vital sectors, and the minds and souls of those who find it an obstacle are being exhausted, to pass their current or future strategies and plans. Moreover, the information space filled with outrageous lies and fabricated contents in most cases. The latest technology in forgery and deception, to win the battle. Therefore, all indicators confirm that the world is going through unequal wars in terms of parity in defensive and offensive security capabilities, and it is difficult to predict the results and effects of modern wars. In this context, we will discuss the concept of **The Fifth-Generation Warfare (5G)**, the most prominent weapons used in Cyber warfare, with a statement of the repercussions and risks of this war at all levels.

The Fifth-Generation Warfare (5G)

In information wars or the 5G war, powers and states wage wars and subjugate superpowers to their powers without using a single bullet. The mechanism for controlling the beliefs of the armies and the people's thoughts has completely changed, and is being done at a speed of fewer than 1 m per second, via the electronic recruitment of spies, the use of communication networks, and drones; To cause the greatest possible damage to the various communication sectors and vital facilities, and to the point of paralyzing the movement of countries, and imposing restrictions on the aspects of life, and the whole matter depends on who owns the data and disrupts the satellites.

The American writer "John Robb" described in his book on the fifth generation wars: "It is a war of ideas, it unleashes a spiral of

violence and increases by the method of the sudden destruction of the opponent's forces, morally and psychologically, by launching a process that would spread frustration among the opponent, and its field is cyberspace."

There are those who find that the fifth generation war extends in its philosophy of economic theory (destruction and construction), by the American economist and politician "Joseph Schumpeter", which was later adopted by former US Secretary of State "Condoleezza Rice", when she launched in 2005 the term "creative chaos" to create " a new Middle East", but in general, the one who owns information and data (BIG DATA), is the strongest and most worthy of uniqueness on the scene, and he can impose his own conditions on major companies and countries. A team of programmers hired spies, and trainers will be able to perform easily the task entrusted to it, and with minimal losses and exorbitant prices.

The form No (1) - 5G warfare's' features

Moreover, the fifth generation of war is not subjected to moral or social and value constraints, and it is capable of accessing social structures and national media rules, due to its attractions and penetration factors related to immediate access to the counterparty's database via dissemination and disinformation its penetration its networks, and disrupting its vital civilian and military facilities (power stations, airports, water networks, electricity, alarm

systems, military defense mechanisms, etc..), by means of electromagnetic waves emitted from electronic cannons, causing losses of billions of dollars, through the use of malware that It encrypts opponents' electronic systems.

2) Cyber offensive weapons

The focus of the North Atlantic Treaty Organization (NATO) meetings on the danger of cyber warfare, and the stress of the heads of some major countries, such as America, Russia and the West, on the aggravation of cyber-attacks against their targets, did not come out of a vacuum, in order to be given priority on the list of their security concerns and agendas. The fifth item of "NATO", considers any threat to one of its members as "aggression" that threatens everyone, and these fears and warnings are real-time products of the extent of the development of cyber capabilities in our time, which has become a sovereign indicator to show the strength and capabilities of any country.

In the past, (hard power) constituted a backbone for managing face-to-face battlefields, but the need to reduce losses, speed up military decisiveness, and strike targets with high accuracy, prompted the human mind to take advantage of previous technical experiences, to form offensive and defensive space deterrence forces, based on accurate cyber weapons to process supported data with artificial intelligence.

Moreover, it becomes possible to identify the sources of electromagnetic energy through network systems, and early alarm devices, which identify the sources of the threat and try to assess the damage if it occurs.

In this form of emerging hypersonic cyber warfare, many high-precision cyber offensive weapons are invented, especially those based on modern directed energy, including "high-power microwave weapons (HPM), which is one of the most important new weapons in the field of cyber warfare.

For example, the United States has conducted a lot of research on the development of "microwave weapons", and called it the "knockout process", caused by shining a laser on parts of the brain that causes fear, panic, and fatigue disorders, as used by the DARPA Foundation (DARPA) in order to cause damage to heart,

destroy veins, cause auditory hallucinations, and even installing them on fighter jets and military vehicles to be used in wars.

There is a good example in this regard is when China used the "microwave" against Indian forces in their last border skirmishes, in June 2020. When China found itself unable to repel India's combat-trained military superiority, and attacks in mountainous areas, which occupied the high of Himalayas. The Chinese forces installed "microwaves" on vehicles, rays beamed on the mountaintops, the result was the Indian forces felt dizzy, sudden fatigue, vomiting, and auditory hallucinations, which made them retreat immediately, and therefore China occupied those areas easily.

3) Types of cyber warfare

Based on the enormous capabilities of offensive weapons of destruction, the endless cyberspace - in length and width - has become a modern field of conflict between states, and a terrifying indicator of the crystallization of the capabilities of states,

governments, and even individuals, to review the effectiveness of the electronic arsenal on the local or global arenas, therefore, the conflict moved from applied noise to the resounding silence. The focus was also on electronic attacks, cyber-crimes, and threatening hacking of the thought patterns of the targeted audience, with artificial intelligence becoming the most prominent title for the transition from the conflict on the ground to the conflict in the unlimited space, thus, the forging of the system of ideas and public awareness in favor of submitting to the ideology of cyber security was hundreds of times more powerful than the fourth generation of the Internet. We can cite

examples of a number of emerging electronic wars, which inflicted great losses on the conflicting parties, prompting them to review their accounts and preserve their vital facilities from any sudden electronic attack, and some of these models as the following:

1- Russian cyber-attacks; such as those carried out against the US State Department, and hacking of elections during the former US President Donald Trump, in addition to the disruption of the US oil pipelines "Colonial" for several days.

Russia also exploited cyber-attacks during its conflicts with Georgia in 2008 and Crimea in 2014, as well as destroying data and disrupting the computer systems of the Ukrainian government with a type of malicious program called a "Wiper".

2- The Iranian cyber army (affiliated with the Revolutionary Guards) hacked official accounts and vital sectors in Israel, including others belonging to Saudi "Aramco", and Qatari institutions, as well as the malicious "Stuxnet" worm that Israel employed to strike the Iranian "Natanz" nuclear facility, on 11 April of 2021.

3- Israel's use of the "PEGASUS" program to spy on the phones of journalists and its anti-activists.

4) The cyber warfare risks and its repercussions

In light of the electronic arms race resulting from the digital revolution, the international and regional powers are entering into a new conflict, based on the use of artificial intelligence (the nervous system of future alliances), aiming at faster, smarter, safer and more accurate performance in hitting targets (creation of humanoid robots) within armies, financial companies, and vital structures. Plus, rising the danger of the effects resulting from the cyber war that threatens the whole world, as the sovereignty of states and the independence of their decisions are in constant decline in favor of the escalation of the roles of cross-border technical companies, piracy, electronic espionage, organized crime networks and others, which today pose many challenges, uniting the ranks of competitors to preserve on global cyber security.

Cyber risks are also the biggest concern for companies all over the world in 2022, according to the risk scale issued by Allianz (Allianz Risk Barometer; is the company's annual report that identifies the

most important risks that companies may face in the coming months of this year).

In general, we summarize the serious risks resulting from the rise of suspicious cyber combat units as following:

_ Economic losses, billions of dollars in cybercrime, and global trade paralysis.

_ Tension in diplomatic relations amongst countries, and a decline in trust between allies.

_Decreased ability to secure confidential information against attacks by trained spies.

_ It poses a real threat to nuclear security in the world, therefore the outbreak of cyber nuclear war is no longer ruled out.

_ Disrupting the static electrons of vital facilities, starting with the threat of oil and gas companies, and ending up with cutting off electricity to the world (electricity outage in eastern states in America for a few hours).

_ Destroying civil and military defense mechanisms and posing a threat to the sensitive activities of states.

_ Major countries and international companies are being held captive to the mercy and blackmail of espionage and hacking networks, which often demand large ransoms, which were (imposed on 200 US companies previously).

_ Increasing the information and technical gap between the developed and underdeveloped countries.

_ Causing breaches of databases and agents accounts, and infringement of intellectual property and individuals' privacy.

_ Major outages of information technology, striking and disrupting electronic platforms (as happened with Meta company "Facebook previously", whose services were stopped around the world for 6 hours on the 4th of October of last year).

_ Exacerbation of security violations, and the use of cyberspace to launch and coordinate terrorist attacks against the interests of individuals and states.

As for the extent of the serious damage resulting from penetrating the safe cyber wall, in fact, the numbers seem alarming and shocking, while statistics estimated the losses of cybercrimes at about 6 trillion dollar in 2021, it is expected - according to experts - to cost the world more than 10 trillion dollar by 2025, and this is what prompted countries, such as America, China and Western powers, to strengthen its digital section, by allocating an independent budget within its annual budget, estimated at millions of dollars, to ensure cyber security and confront the risks that its vital activities and sovereign institutions are expected to be exposed to.

In the United States, there are about 879,000 cyber security professionals out of the total manpower. Globally, the gap is larger, and the labor market needs about 3.12 million jobs in this field, according to (ISC) ², it is an international non-profit organization .It offers training and certification programs in the field of cyber security.
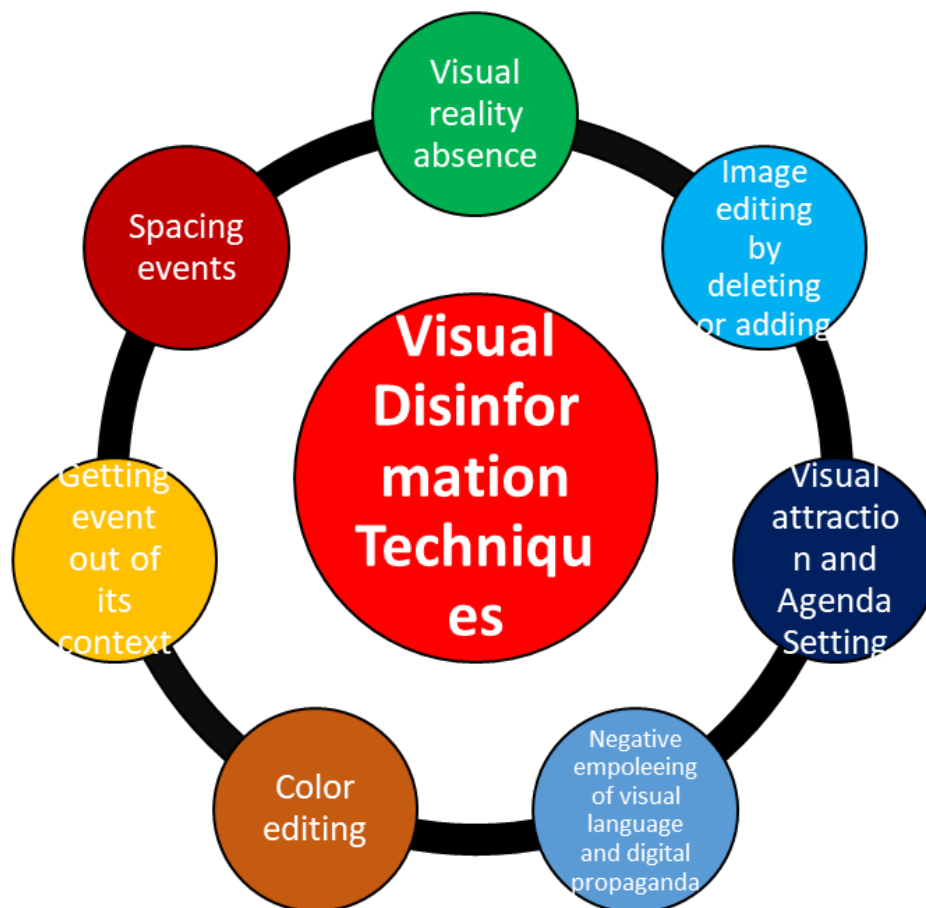
Based on what has been said, and apart from the capabilities of states armed with modern systems in cyber security, most of the Middle East countries are absent from the space armament scene, and they lack the qualifications to manage remote conflict (future conflict), with the exception of some countries, such as Iran, Israel and Gulf states that allocate independent budgets to achieve Cyber security. Briefly, the loss of any party not concerned with virtual technologies in any future battle devoid of the use of conventional weapons is a fait accompli, and it must be pointed out that modern rules of attack and revenge may leave us shocked by the surprise, as computers, care and communication systems are being malfunctioned, and applications and secured privacy are being Hacked. Subsequently, the closest and worst scenario to the targeted parties is surrender and submission to complex malware attacks, especially if terrorist and extremist organizations or those who will seek revenge because of conflicting interests and intersecting strategies run the electronic circuits.

Second: Visual Disinformation

The photo has always been an influential symbolic authority used for documentary and artistic purposes, giving the course of incidents the elements of both credibility and aesthetics, and it remained the best credible tool of persuasion and expression to

capture the detailed facts in human history. It is believed that the photo "is far better than thousands of words, and is even more expressing that speaking "in the context of enriching the visual memory of nations and peoples.

This was what could be believed - really - before the successive development of techniques of manipulating and modifying photos, emptying them of the original content, and employing them outside their natural context, as a form of misleading and visually framing the audience, within the scope of a blackout, deletion and absence, even within the frameworks of dismantling and fragmentation of the elements of the still and animated photo. This matter was further exacerbated by the latest techniques of deception in the visual photo, represented by the technique of "deep fake - realistic simulation", and the visual framing of events, in its updated form.

The form No (2) - Visual Disinformation Techniques

1) The "Deep Fakes "and "Plausible Deniability" technology

Editing photos is not a new thing, but the development of "digital graphics" tools in light of artificial intelligence, and visual persuasion have put us in front of a huge stream of modified and fabricated videos, which look real and amazing in their realism, to the extent of the transformation of old static images into videos look alive and imitate the late figures. Due to the increasing popularity of this technology, it has turned into an effective means to blackmail public opinion and manipulate its needs and plunge the victims into a climate of psychological disorder and constant threat.

In digital disinformation Media, the software is developed with automated self-learning techniques, after complex digital processing of precise visual details of composition, feature change, and sound modulation, in which it affects the digital footprint of images, and in this way, visual and audio content is created through the use of several applications (Reface, Wombo, Zao..).

The Russian-Ukrainian war was a vital arena for creating fake videos about Ukrainian President Volodymyr Zelensky. Previously, the same thing occurred with US Presidents Donald Trump, Barack Obama, and many international figures.

On the other hand, given the fears resulting from the use of the technology, the European Police Agency, "Europol", warned of the expansion of the use of "deep fake" technology in the world of crime, owing to its ability to make people appear on the Internet, saying or doing things they had not previously said or done, or impersonate entirely new characters, and it could have a devastating effect If this technology falls into the wrong hands.

Thus, the "augmented reality" technology has proven its tremendous ability to forge an identity, impersonate by professionals, and cyber criminals, and has been used to falsify everything, and this would lead to undesirable consequences, leading to:

_ Disinformation, the spread of digital crimes, fraud cases, and cyberbullying.

_ The spread of a culture of "plausible deniability", in which what is real, is confused with fake content.

_ Privacy violation and raising doubts about the credibility of matters, especially with the use of personal features in inappropriate places.

_ Identity theft and illegal gain by impersonation, hacking of phones and bank accounts.

_ Distorting the public image of important figures and community leaders, even after exposing the falsified videos.

_ Falsification of voices, which makes us lose confidence in any call or audio record.

2) "Metaverse" and "Parallel World"

We have never realized or expected, to shake hands with someone, do shopping online, or even live parties, and simulate reality digitally, but this is what has become easy to believe with the "Metaverse" technology; which is considered one of the most recent and most surprising products of the millennium to change concepts, human characteristics, and lifestyles within complex networks of interconnected digital worlds, combining physical reality and the visually shaped virtual world.

The term "Metaverse" appearance dates back to the science fiction novel "Snow Crash" by the American writer Neil Stevenson. Its events revolve around live virtual characters who meet in 3D buildings and other virtual reality settings, usually covering history, linguistics, anthropology, religion, computer science, politics and cryptography.

Moreover, changing the name of "Facebook" company to "Meta" is a series of digital arrangements in which the virtual world is being linked, represented by its multiple platforms, technology experts expect that the "Metaverse" technology is going to change the reality of digital networks (its companies and social platforms), to open new horizons and fields we have never realized, as in (commercial shopping, education, training workshops, digital currency trading, and designing surgical rooms), within an augmented digital reality, which provides various vital services to humanity through symbolic images that impersonate real forms by using augmented reality glasses, smartphones, and similar virtual tools according to the "public domain", which is directly based on

the interaction between individuals and groups, without being subject to censorship or communication obstacles.

According to what was previously said, many global electronic companies were able to take bold steps, especially during the Corona pandemic, therefore, they went to develop mechanisms for digital communication between people. At the forefront of these companies are "Microsoft", "Meta", "Apple" and "Amazon", as they transformed their tools, content and digital atmosphere into 3D, and it did not stop there, but even countries in competitive race, to simulate a virtual reality that keeps pace with their rivals and examines military strategies and visually security plans from the "parallel world" portal.

In light of these technical developments, tech scientist Luis Rosenberg expresses his concern about the repercussions of Metaverse, saying: "Users will neither feel free to choose, nor will disconnect their augmented reality system, which will put them at an unfavorable social, economic and intellectual Virtual constructs can easily be designed to amplify political and social division, ostracize certain groups, and even provoke hatred and mistrust."

In fact, it is not possible to predict or speculate much about what the "Metaverse" technology can lead to in the current circumstance because it is the result of a series of successive developments, but - like any other digital technology - it will carry positive and negative dimensions, which are difficult to do without in our digital world. In addition, it will not only be restricted to people interaction, but it is an introduction to the quantitative link between the physical reality on Earth planet and other planets throughout a series of digital media. It is another new world that will change the direction of the world upside down, and here the advanced countries - scientifically and technically - will be the pioneered, decision-makers and sovereign, along with the change of the laws of conflict and digital armament.
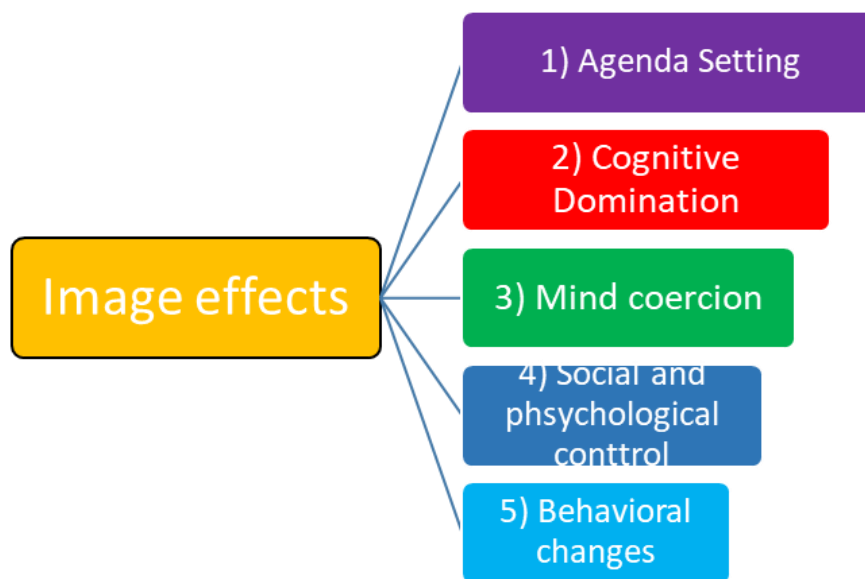
3) Visual framing of events

An image that may be captured at a particular moment, or re-updated after it was previously published in different times, geography, or events, is a product of the "media framing" theory; Which is one of the most dangerous theories of public opinion-making and its crystallization, in which events and scenes are employed within biased contexts, to the extent that the phrase "An

eyewitness is better than hearsay" is no longer sufficient to establish the credibility of the events. The importance of modern technologies in the production of picture stories is framed by the ideology of the communicator, in which some aspects are highlighted, and others are neglected and isolated (cognitive exclusion), in order to convey specific messages to public opinion.

The popular and circulated image is often more influential than the textual content, which is a natural product of the image's superior capabilities, which are high in persuasion, drawing attention, and reaping a base of sympathy and mass mobilization. The fixed or composite image itself is a universal language that eliminates illiteracy impediments, and there is no need for much knowledge, or a high level of focus, as needed in the text.

In light of the imagination dimension overshadowing, whether in terms of acquiring knowledge or making prejudgment decisions, dominating and controlling social values, generating mental submission (brainwashing) and psychological impact actor based on image deception in simulation cases, transfer from visual effects.

The Form No. (3) - Image Effects

Visual framing may also take many forms, including "contextual image disinformation" based on re-synthesizing events, weaving its details by extracting images from their temporal and spatial

origins, and re-updating them in similar places and atmospheres while employing eye-catching and attractive news headlines in terms of form and content, in order drowning the audience is in a sea of imagination, and it can focus heavily on controlling the nature of the visual content, and pushing the recipient to realize its elements, and he starts to absorb, think, and worry about it until it becomes in his list of priorities at the expense of other topics and contents, which are overlooked in favor of the communicator's agenda, and this is the essence of the theory of "the agenda-setting" advocated by "Walter Lippmann" a hundred years ago

In most cases, it may amount to fabricating events and fabricating scenes in order to mislead public opinion and to achieve its drifting to the pre-planned propaganda agenda. In this regard, we give an example of the investigation conducted by the US Associated Press - nearly three years ago - on Turkey's support for fake propaganda campaigns on Twitter and Instagram, to influence public opinion around the world regarding its military invasion of northeastern Syria. It was not satisfied with these campaigns, but also used images stolen from a foreign agency that have nothing to do with the Syrian events. For example, a recent photo was taken that supposedly shows a Turkish soldier giving a Syrian girl water, but this photo is fake, and it is from the Associated Press and was published in 2015.

A photo that went viral portrays a Syrian woman wearing a purpled dress carried by Turkish soldiers, gained a massive retweet but was in fact stolen from the Associated Press in 2010, during flood

evacuations in Pakistan.

In addition to the scenes of Turkish reinforcements aiming at launching a new military operation in the east of the Euphrates, in which images of Turkish armored vehicles and military convoys were re-circulated as preparations for the "all-out battle."

It is evident from the above model that the image is used to deceive the public in favor of supporting the Turkish narration.

The danger today, more than ever, lies in the mass of content and digital interaction, as the number of surfers on social platforms increases in the digital world, and most of the publications and content supported by fake images turn into a "trend" that invades social media platforms, and they become issues of public opinion (subjected to re-modify based on the political orientation), and it reaps high rates of followings, participation, and sympathy, and often may result in bloody acts of violence and hatred rooted in the social depth, as in (the waves of hostility of Turkish citizens towards Syrian refugees, and the western far-right against foreigners).

In line with the above-mentioned, the image that is published outside its natural context or its features and elements are being exploited (colors, personal features, geography of areas, depth, and angles), is classified under the category of "media disinformation by exclusion and systematic deception", and its internationalization is exacerbated with conflict of interests and the intensification of competition and conflict between rivals and decision-makers. As a result, the ethics and social responsibilities of practicing the profession become absent in the event of publication and the deceptive dimension of the ideology-based image and modified with a high-tech prevails.

Third: The Outcomes

Based on the above description and analysis, we can brief in a number of results:

1- Modern wars will not be like the previous ones, they will be silent and more effective than conventional wars, as the effects and risks will threaten all vital sectors (military, information security, nuclear, economic, political, health, as well as

communication and electricity networks, and everything that runs on energy).

2- The wars will no longer be organized and expected, instead it will become surprising and shocking in their tactics and strategies so that they confuse everyone's calculations, and it is not excluded that major countries will be classified among the list of victims, so it is not easy to predict the results, especially since the source of the threat might be unanimous.

3- Cyber wars may result in the rise and decline of other countries and powers, and more cases of blackmail, threats and hacks.

4- Doubt is going to be mixed with certainty and truth with imagination, privacy and confidentiality will be violated, visual dazzle will prevail over depth and analysis, and maintaining the sovereignty of states and the vitality of their facilities will become a difficult mission.

5- The rules of the security conflict and the digital arms race will change, and the "scientifically and technically" developed countries will become sovereign and decision-makers at the global level.

6- Visual disinformation techniques, led by "deep counterfeiting" will change the face of the world, and dissipate the rules of trust and credibility, so that the ratification of fake and denial of the original would become more common. Subsequently, the distinction between reality and imagination will become very difficult, and the public image of senior figures, states and governments will be distorted.

7- By having highly advanced editing techniques for visual content, it will become easier to fabricate events and empty them from the original and natural contexts, and it will be difficult to trace the fabrications and detect the deceptive dimension of still and moving images.

The Conclusion

Keeping pace with the interconnecting generations of current or future war and their strategies in influence and persuasion, and the attendant opposite change to conceptual frameworks, cultural identities, political trends, and even lifestyle, imposes on us the inevitability of quickly realizing the consequences of digital

domination and control and visual deception, and absorbing successive developments in the virtual space. In addition to the importance of strengthening the internal structure with an integrated system of rational scientific values, digital awareness, and information security. This matter needs concerted individual and collective efforts, and high levels of (technical, informational, media, security, and psychological..) coordination amongst systems, countries and companies, in order to control digital work fields, fill technical gaps, and the possibility of enacting deterrent legislation, and establish controls to reduce digital fraud, hacking, encryption extortion. In the event that those rooms and space circles are not being used by who are affiliated with countries, governments, and companies throughout issuing disinformation and the psychologies of influence and virtual projection. In these conditions, the matter will be different and it will need to internationalize the matter within international contexts to unify efforts, and correct digital paths to serve everyone, through the creation of international transparency offices and bodies, digital control rooms equipped with the latest cyber-security and monitoring technologies, in addition to detective applications for malicious programs and visual disinformation. Moreover, allocating independent budgets to support cyber security, launching platforms that support positive digital content, as well as positively employing digital technology in the fields of (medical, media, economic and social...) development to accomplish tasks quickly, with high accuracy, and with less effort and time.

In the face of greed, selfishness and conflict, all of humanity shares the same destiny, the part is linked to the whole and vice versa, and all scenarios are possible ahead of us in the "beyond the virtual" world, and the future will guarantee who will control the rules of domination and control.