INTERNATIONAL RELATIONS GRADUATION PROJECT

Social Media as an Emerging Cyber-Threat in IR

AUTHOR: Pedro Vicente Esteban Orellana

TUTOR: Jesús Alfonso Soto Pineda

GLOBAL BACHELOR'S DEGREE IN INTERNATIONAL RELATIONS

Academic Year: 2020/2021

FACULTY OF SOCIAL SCIENCES AND COMMUNICATION

UNIVERSIDAD EUROPEA DE MADRID

ABSTRACT

The purpose of this dissertation is to assess the current impact of SNS[1] as a destabilization factor in the framework of IR[2] within the theory of Structural Realism.

The thesis analyses how SNS are currently being used as an asymmetrical tool by states to ensure their national security both offensively and defensively. Simultaneously, it also assesses how SNS may be weaponized in the cyber-space to wage war against other states. The paper covers the security dilemma derived from a technological arms race in cyberspace and its implications to the current International World order. Similarly, the thesis analyses the role of MNCs[3] in this environment and ponders the impacts of SNS to current liberal democracies and individual freedoms.

Lastly, the paper proposes courses of action both to deescalate the security dilemma and improve democracy health by modifying the framework in which SNS operate currently.

Wordcount: 15,087

Keywords: SNS, Cyber-weapons, Influence, Information, National Security, Cyber-threat, IR, Psy-ops

[1] Social Networking Service hereafter referred as SNS. *Ibid* - Table of Acronyms and Abbreviations
[2] International Relations, hereafter referred as IR. *Ibid* - Table of Acronyms and Abbreviations
[3] Multinational Corporations hereafter referred as MNCs. *Ibid* - Table of Acronyms and Abbreviations

TABLE OF FIGURES

LIST OF TABLES

TABLE OF ACRONYMS AND ABBREVIATIONS

ACRONYM	DEFINITION
AI	Artificial Intelligence
APA	American Psychology Association
API	Application Programming Interface
AUDINT	Audible Intelligence
AWS	Amazon Web Services
BBI	Brain to Brain Interface
BBS	Bulletin Board System
BCI	Brain to Computer Interface
C2	Command and Control
CNA	Computer Network Attack
CCP	Chinese Communist Party
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
CNN	Cable News Network
CoG	Centre of Gravity
COMINT	Communications Intelligence
CYBERCOM	United States Cyber Command
DAESH	Islamic State of Iraq and the Levant (الدولة الإسلامية في العراق والشام)
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
FB	Facebook
FBI	Federal Bureau of Investigation
FP	Foreign Policy
GPS	Global Positioning System
HQ	Headquarters
HUMINT	Human Intelligence
INFOOPS	Information Operations
IR	International Relations
IRC	Internet Relay Chat
ISPs	Internet Service Providers
IT	Information Technology
KGB	Committee for the State Security (Комитет государственной безопасности)
MIT	Massachusetts Institute of Technology
MNC	Multinational Corporation
MP	Member of Parliament
NATO	North Atlantic Treaty Organization
NEURINT	Neuro-cognitive Intelligence
OSINT	Open Source Intelligence

OSOME	Observatory on Social Media
POV	Poinf ot View
PSYOPS	Psychological Operations
RT	Russia Today
SIGINT	Signals Intelligence
SNS	Social Network Sites
UK	United Kingdom
URL	Uniform Resource Locator
US	United States of America
UW	Unconventional Warfare
VPN	Virtual Private Network
WMD	Weapons of Math Destruction

TABLE OF TECHNICAL DEFINITIONS

NAME	DEFINITION
Algorithm	A finite sequence of computer instructions crafted to solve a problem and put together by a human
Artificial Intelligence	A synthetic and static human-mimicking intelligence aiming to establish a successful decision making path to find an optimal solution to a problem
Astroturfing	To create an illusion of a genuine grassroots movement by trying to mask its creators
Backdoor	A covert method to bypass authentication typically hidden from regular users and either known or left there on purpose by its creators
Big Data	The discipline that analyses, structures and extracts tangible information from great variety of data, in increasing volumes at a higher rate velocity
Big Tech	Refers to biggest players in the tech industry: FB, AWS, Alphabet, Apple and Microsoft. It may also extend to regional Tech clusters like Baidu, Wechat, VK, Yandex, etc.
Black Ops	Secret covert operations usually carried by government agencies
Botnet	Internet connected devices running one or more bots controlled by an owner
Butterfly attack	A SNS attack aimed at imposters mimicking behavior of a social group to insert divisive rhetoric or disinformation

Centre of Gravity	A Clausewitzian term describing the point at which all military force must be directed so to destabilize an enemy with peak efficiency
Clickbait	A text or thumbnail link designed to attract attention of users to follow a link and read, view, or listen to the linked piece of online content with a defining characteristic of being deceptive, typically sensationalized or misleading
Command and Control (C2)	A set of organizational and technical attributes and processes employing human, physical, and information resources to solve problems and accomplish missions
Cookie	Text files with small pieces of data that are used to identify your computer or persona as you make use of a site
Cyberspace	The virtual computer world that is used to facilitate online communication typically involving a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol
Cyborg	A bot-assisted human targeted at deceiving real SNS users by mimicking human behaviour escaping AI
Data Exhaust	Trail of raw data typically left after online user activity
Deep Web	Parts of the World Wide Web whose contents are not indexed by standard web search-engines
Follow Train	In SNS, a chain reaction of follow requests upon an action or set of actions

Gerasimov Doctrine	A military doctrine featuring the use of state machinery on all fronts to wage asymmetric warfare
Hacker	A person skilled in computer systems with the ability of an all-round knowledge that allows it to understand, see flaws, and find creative ways around them
Hacktivist	Civil disobedience by means of computer-based techniques generally, falling under the category of the grey hat hacking community
Honey trap	Setting up a resource with the objective of trapping people attempting to use it.
Hybrid Warfare	A military strategy which employs political warfare and blends conventional warfare, irregular warfare, and cyberwarfare; with other influencing methods, such as fake news, diplomacy, lawfare and foreign electoral intervention
Infosphere	A metaphysical realm of information, data, knowledge, and communication
Keyword Squatting	To craft a hashtag or SNS account to favour SEO results
Machine Learning	Artificial Intelligence aimed at the self-improvement of AI algorithms without human input or mediation
Media Outlet	A publication or broadcast program that provides news and feature stories to the public through various distribution channels

Meme	An artifact of communication on the Internet with a symbolic meaning around a person, thing, or event
Metadata	Data aimed at fingerprinting other data
Millennial generation	Generation born in between the early mid 80's to the mid late 90's
Muddy the waters	Distribution of conflicting information to cloud public perception of an individual, group, or topic, making the target subject to more complex or confusing information
Netizen	Citizen of the net or Internet user
Phishing	Fraudulently posing as a trustworthy entity in a malicious attempt to access confidential information.
Psy-Ops	Psychological operations within the framework of Psychological warfare
Security Dilemma	A spiral model that produces increasing tensions originating from defence moves that can potentially derive in conflict
Sock Puppet	A false online organic identity used for deception purposes
Strategic Narrative	How a state openly portrays to others in the International Arena
Swarming	When loosely organized online groups come together for specific objectives or campaigns
Sybil	Another definition for a robot or bot account

Trolling	Engaging in inflammatory, divisive, or distracting behaviour in an online community with the goal of provoking readers or viewers into an emotional response
Web Scrapping	Automated processes to extract data from websites
Zero-day exploit	A computer-software vulnerability that is unknown to those who should be interested in mitigating the vulnerability

TABLE OF CONTENTS

1. INTRODUCTION

SNS are a powerful vehicle to influence society. Conceived originally to connect people in a cheaper and more efficient way, they have been the main agents impelling Internet growth. As such, they have both intentionally, and unintentionally become powerful psychological apparatuses within cyberspace for which to inform and influence masses. To states and non-state actors, they have become strong tools to re-affirm and project power within the anarchic international arena; for which this working paper analyses the problems this represents in the existing IR framework.

Within this first section, the paper formulates in section: 1.1 Research Question;
two Research Questions on which section 3: Research; and section 4:

Conclusions responds to. Similarly, section 1.2: Research Objectives; formulates the objectives the body of this works aims to give answers to. Lastly, section 1.3: Methodologies; gathers the actions taken in this paper to research this topic using the Theoretical framework described in the adjacent section 2.

1.1 RESEARCH QUESTION

Since the inception of the Internet, a chain reaction of revolutions has burst in the realm of media and communications. While media was already experiencing important changes during the 80's affecting its influence capabilities in different realms of politics (Piers, 2005), the gradual interconnectivity of personal computers has allowed for new ways to connect people as well as knowledge (Hey & Papay, 2014).

Media has successfully adapted to the possibilities the Internet had to offer, and, in this process, a new set of challenges have arisen as it has reached its maturity stage[4] (Muzellec, Ronteau, & Lambkin, 2015). Perhaps the greatest precedent in history dates back to the chaos created by the printing press revolution in the XV century (Eisenstein, 1980). Characterised by a sudden leap in terms of information feeding to the masses, this milestone marked the essential foundations for a system of checks and balances in mass communication (Herman & Chomsky, 1988). Its consequences in information spread, shaped drastically the course of Europe´s statecraft in the upcoming centuries (Fergusson, 2009).

Today, society is affected by an ever-detrimental phenomenon. The Internet at its current capacity allows for new forms of communication[5] approximately every six months (Connor & Weatherall, 2019). Algorithms in SNS often favour virality leading

[4] See **FIGURE *6*: A GRAPHICAL DEPICTION OF THE WEB EVOLUTION. SOURCE: (SEGALLER, 1998)**

[5] Referring to platforms or media outlets

to misinformation[6] rather than veracity by capitalizing on attention (O'Neil & Schutt, 2015). There are different tactics from which actors in IR can gain or lose within this ecosystem. Hence, the research question to be analysed is: *"In what ways does SNS act as a destabilization factor to the existing IR framework?"*

Due to the transcendental role of states in IR, a derived research question to be considered is: *"To what extent is national security compromised by the absolute freedom of use in social media?"*

1.2 Research Objectives

The main objectives of the dissertation are as follows:

- To identify the ecosystem crafted around SNS' architecture and the effects in its users[7].
- To research how SNS can influence psychological behaviour and how can it be used as a weapon in the anarchic IR arena.
- To translate existing theories in IR to the cyber-space IR realm.
- To study the security dilemma in terms of a cyber-arms race.

Secondary objectives in this dissertation are:

- The application of artificial intelligence as seen in SNS to craft cyber-warfare.
- A brief economic study of the role of the fractional reserve system and its impact to SNS.
- A forecast in the future of liberal democracies.

[6] I.e.: Clickbait, links designed to attract attention featuring deceptive and misleading content (Munger, 2020)
[7] Also known as netizens, citizens of the net (Hauben, 1997)

1.3 METHODOLOGIES

This dissertation is an analytical research based on a qualitative content analysis taking for the most part, literature review[8] to support the validity of its statements. Given the quantitative nature of some of these studies, the research may also be classified as a meta-analysis; or extraordinarily, a statistical analysis. Due to the tech-prone nature of social media and complimenting the literature review previously mentioned; the dissertation also engages slightly in active research by using a range of technical IT tools transparent to the paper itself. The purpose of these are to verify the validity and veracity of the qualitative content of previous authors present in the

Bibliography section.

The research uses the assistance of technical tools in conjunction to determine possible anomalies in algorithms based on machine learning, both present in SNS discussions (Ferrara, 2017). According to (Ferrara, Varol, Davis, Menczer, & Flammini, 2016), it is necessary to compliment these tools with qualitative resources of this nature so to induce accurate results in a research alike. This is the case when dealing with social engineering understanding (Bennett, Segerberg, & Knüpfer, 2018). For instance, bots, a recurrent actor in SNS, are known to regularly use a host to mimic human behaviour[9]. Though this makes a bot sometimes unrecognizable, it would still be possible to reverse engineer the social process in order to discard a “false positive” (Aguilera Diaz & Seisdedos, 2020).

[8] *Ibid - 11 -* Bibliography

[9] This is often known as a hybrid bot or cyborg (Bennett et al., 2018)

2. THEORETICAL FRAMEWORK

The dissertation considers the following theories, classified in the social sciences realm, to formulate its conclusions to the research questions and research objectives.

- In International Relations:
  - Use of the *security dilemma offense-defence* theory and the intensity scenarios described by Jervis (Jervis, 1978).
  - Extensive use of *structural realism* as a way to understand how states behave both in the physical, and by extension, cybernetic world (Mearsheimer, 2001).
  - Liberalism theories such as *Democracy Theory* (Doyle, 1986) and *the End of History* (Fukuyama, 2015) to pinpoint the present and future of liberal democracies from a structural realism POV.
  - John Ikenberry's social theory and liberal international order (Deudney & Ikenberry, 1999) to establish a co-relation between SNS actors and the liberal order.
  - Use of Carl von Clausewitz's theories on war (Clausewitz, 2008) adapted to modern warfare and cyber-warfare scenarios (Maurer, 2017).
  - Use of P.W. Singer and Nissen theoretical frameworks on the Weaponization of SNS (Singer, 2018) (Nissen, 2015).
- In Political Theory
  - Use of the Iron's *Law of Oligarchy* (Michels, 2019) to explain the metamorphosis of SNS and MNCs; and how it has changed the balance of political power against the nation-state they belong.

- Use of the *Manufacturing Consent* theory (Herman & Chomsky, 1988) to criticize and assess the evolution of inter-relation between power elites and media ownership.

- In Economic Theory
  - Austrian School of Economics' theories to explain the cause-effect of the current monetary-market capitalist economy and its effects in states, corporations and liberal democracies (Huerta de Soto, 1998).

Additionally, the paper also elaborates arguments to the research objectives on an existing framework[10] elaborated by (Qi, Monod, Fang, & Deng, 2018) using four archetypical philosophical theories ranging from individualistic to collectivistic; to depict Social Media's user behaviour as seen in **FIGURE *1***:

- Goffman's *Symbolic Interactionism* (Goffman, 2016)
  - Social media is understood as a performance where people play its role, often times separated from their own personal life "backstage". Influence and persuasion are key motives in this game and as a player, it is about finding your adversary's next move before you fall prey to them.
- Bourdieu's *Theory of Practice* (Bourdieu, 2018)
  - The main goal of an individual joining SNS is to build up *social capital* (Bourdieu, 2018). Sometimes, this may lead to economic capital in the hopes of doing so. Online social capital in this sense, can be considered, even more powerful than its social offline counterpart. Each social media post is, hence, subject to a careful evaluation by the netizen so to

[10] Qi, J., Monod, E., Fang, B., & Deng, S. (2018). Theories of Social Media: Philosophical Foundations. *Engineering*, *4*(1), 94–102. https://doi.org/10.1016/j.eng.2018.02.009

maximize these premises. SNS posts must be seen as collective because they are influenced by the existing social structure.

- Sartre's *Existentialism* (Sartre, Cohen-Solal, & Elkaïm-Sartre, 2007)
  - While immersed in SNS, netizens see themselves from the point of view of how others look at them in that same cyberspace realm. Relationships are seen as a by-product of how your contacts look at you. Reality is heavily distorted and forged on the basis of how your cyberspace life is presented in SNS. Hence, the concept of your existential project may be understood from the grand total of posts uploaded to SNS.
- Heidegger's *Phenomenology* (Heidegger, 1993)
  - The world contributes to the defining of who I am as a person. The existence of other actors also defines the person. How this is showed in SNS reflects how you care for others, because they are essential to your defining. Without them, human existence is at peril. This is key on understanding the real person behind those posts.

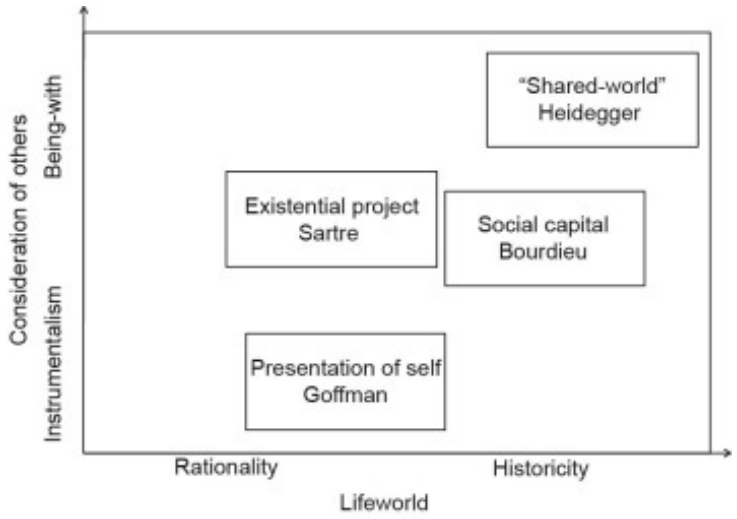

FIGURE 1: ARCHETYPICAL THEORIES IN SOCIAL MEDIA (QI, MONOD, FANG, & DENG, 2018)

3. RESEARCH

The following sections cover how SNS have amassed power so far, how SNS can be politicized in an IR framework, how that politization influences FP[11] making and ultimately, how it affects society in general. The first section covers the evolution and compares SNS to traditional media by using the *Information Gap* and *Dunning-Kruger* effects as indicators of power yield. It also elaborates on the malleable and fragile psychological human condition. The second section covers on the potential for SNS to be weaponized either for political purposes, or to wage war. It also gives insights in technical aspects of cyberspace. The third section focuses on how does this weaponization influences IR by applying structural realism in cyberspace and its geo-cyber politics implications. The fourth section covers how SNS menace the integrity of liberal democracies due to the double bind paradigm immerse in the curtail of individual freedoms. The latter is explained more in depth in the last section and final

[11] Foreign Policy, hereafter FP. *Ibid* -Table of Acronyms and Abbreviations

Conclusions answering the Research Questions.

3.1 THE RISE OF SNS AND ITS IMPACT TO IR

In IR, traditional theories[12] commonly focus on states as the main actor. IT[13] as an agent of societal change, has had no relevant place within the IR realm despite its increasing gains in political power (Fritsch, 2011). It usually ends up disguising as a non-state actor in the MNCs category. In reality, it is something part of a bigger picture, IR theories have failed to portray yet.

The *Information Gap* concept, described by Baum & Potter, describes how media has acted as a modulator between political leaders and the public realm (Baum & Potter, 2019). As **FIGURE *2*** shows, for years, there used to be a massive gap between these two actors. With politicians being able to freely do an undo policies without feeling accountable for any of their actions. Eventually with time, the gap closed as information became public or declassified. The main actor in charge of this sensible action has been before the mid 2000's, public and private media outlets.

[12] Understanding these as realism and liberalism (and its sub-categories), and to a lesser extent, constructivism

[13] Information Technologies, hereafter IT. *Ibid* -Table of Acronyms and Abbreviations

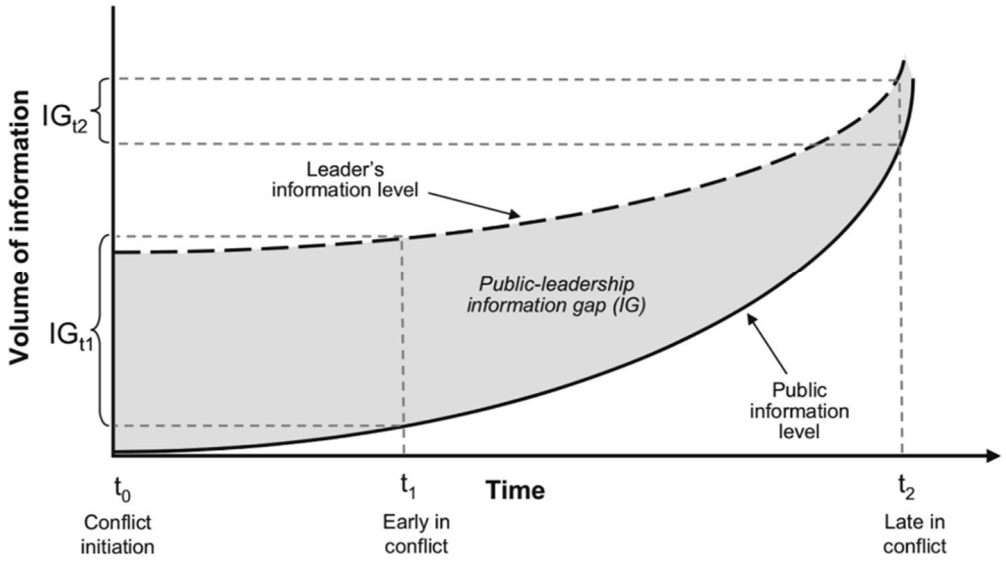

FIGURE 2: THE INFORMATION GAP (BAUM & POTTER, 2019)

Before this period, the gap was shrunken considerably by *the CNN effect* in the late 80's (Piers, 2005), taking place mostly with sensitization of the American public towards issues that aligned with FP making[14]. *The Information Gap* phenomena had two effects: (i) it cut the freedom of FP making in Washington and, (ii) it brought the private media sector closer to policy burocrats. While citizens had now a better-quality information at their disposal, it also gave private media huge amounts of power in the steering of public opinion, and less privacy to politicians to discuss sensible matters[15].

Seeing how profitable this business was, soon more private actors jumped in to cover a different spectrum of political ideology. The result was a preamble of what we see today in SNS; a gradual conflict of interests while steering public opinion between the media leviathans and the masses they endorse (Hetherington & Husser, 2012). Powerful states have also reacted to this by sponsoring their own media abroad, the most notable examples being RT[16] and Aljazeera. In doing so, they can afford a

[14] See the cases of Somalia and the Rwandan Genocide in the early 1990s (Moore, 1998)
[15] This trend is continued until today were information is weaponized and most sensible topics are left exposed voluntarily by party rivals to harm their counterparts (Singer, 2018)
[16] Russia Today, hereafter RT. *Ibid* -Table of Acronyms and Abbreviations

multilateral FP approach, in which media may be targeted at creating havoc abroad while the state's FP is aimed towards diplomacy (Suchkov, 2021). These are also used to portray a heightened image of their country abroad with an enhanced strategic narrative more difficult to read in between lines.

Many of the implicit matters absorbed in the *Information Gap* were for the most part, national security affairs (Almond, 1956). These would typically include: (i) conflict casualties, (ii) elite discord, (iii) unknown political consensus, (iv) classified documents, (v) diplomatic negotiations and (vi) military transfers, among others. Because of the intrinsic nature of policymaking[17], its exercise is never aimed at satisfying the whole of the population.

The "*Information Gap*" had a reason to be there in the first place. Policies require intrinsic privacy between the different parties while being crafted. Early theorists in journalism like Walter Lippmann saw public opinion as a true threat to democracy implying "*Truth and news cannot be the same thing"* (Lippmann, 2017). Both views of Lippmann and Almond in journalism cross paths[18] but with the arousal of the *CNN effect*, these views backfired in favour of reality. The *CNN Effect* certainly brought more transparency but with it, a new paradox in ideology fragmentation.

Cognitive biases leading to overconfidence like the *Dunning-Kruger Effect* (Kruger & Dunning, 1999) explain in part the tragedy in public opinion's polarization seen today with SNS. As seen in **FIGURE *3***, people who are less competent, fail to correctly assess their own level of skill and, in fact, for the most part they overestimate it. Moreover, they also tend to underestimate the level of their peers and fail to recognize their own

[17] Understanding this nature with Clausewitz definition: "*War is politics by other means"* (Clausewitz, 2008)
[18] See the Almond–Lippmann consensus (Holsti, 1992)

errors leading to an overconfidence cognitive bias (Heuer, 1999). This behaviour is amplified progressively since the baby-boomer generation and consistently augmented with the maturity of the Internet and the now adult millennial generation (Kumar, 2019).

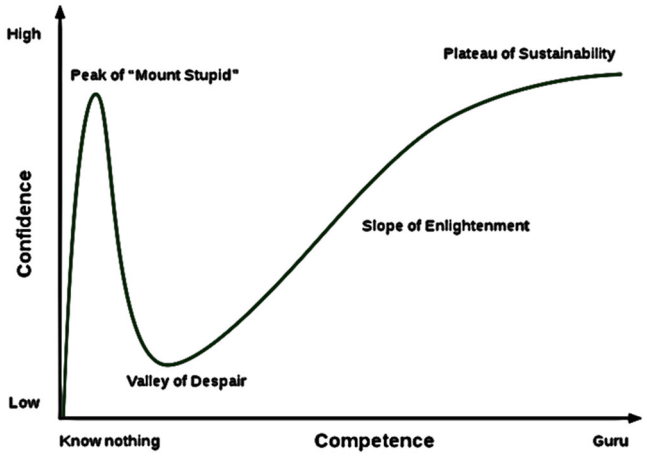

FIGURE 3: THE DUNNING-KRUGER EFFECT (KRUGER & DUNNING, 1999)

The *Dunning-Kruger effect* affects the whole of the population and the only way to challenge it, is by increasing experience over time. The effect may be extrapolated even to genuine experts in a particular area to another in which they are less familiar. Though experts tend to be more realistic about their competence levels, often times they underestimate their real level of knowledge[19]. In an era of overstimulation of the senses and information bombardment (Rocamora, 2011), the *Dunning-Kruger effect* is more likely to occur, particularly in those segments of population with lower education levels. SNS being almost of universal access, encourage confrontation by means of its algorithms desperately looking to exploit psychological attention and virality. Such traits do not help dissipate this effect but rather enlarge it even more.

[19] This is usually seen in the latest stage known as the plateau of sustainability (Kruger & Dunning, 1999)

When extrapolated to political psychology, the *Dunning-Kruger effect* leaves room to steer public opinion (Sears, Huddy, & Jervis, 2003), and to this end, gives massive dividends in power to media conglomerates and political planners. This may induce in the manipulation of masses in a chaotic fashion described by Sigmund Freud (Bowman, Freud, & Riviere, 1928) in Group Psychology and the Analysis of the Ego: "*When the Id, responsible for our human animal instincts is able to override the ego, the rational part, then manipulation has been accomplished*" (Bowman et al., 1928).

Private media[20] after the *CNN effect* must be seen as an intermediary between the state, an information provider, and the final consumer, the citizens. In this scheme, the state no longer has the full control of the *Information Gap* (Baum & Potter, 2019), but it rather collaborates directly between the private entities facilitating the information they deem adequate (See **FIGURE *4***). However, because private media is a business, they fall prey of the supply and demand laws in which consumers are taken into consideration as a part of their business model. In this sense, side collateral effects of modern capitalism align with Nietzsche's views of the press in the late XIX century when he mentioned: *"Sick are they always, they seek deception over truth"* (Nietzsche, 1977).

As seen in **FIGURE *4***, prior to the *CNN effect*, with state media, the flow of information tended to be unidirectional having fewer key stakeholders. The *CNN effect* was disruptive in the sense it introduced a constant 24/7 newscast feeding an artificial demand for information regardless of whether there were quality-news[21] available or not.

[20] Understood as traditional media before SNS arrival
[21] Also known as *hard news* (Stacks, 2004)

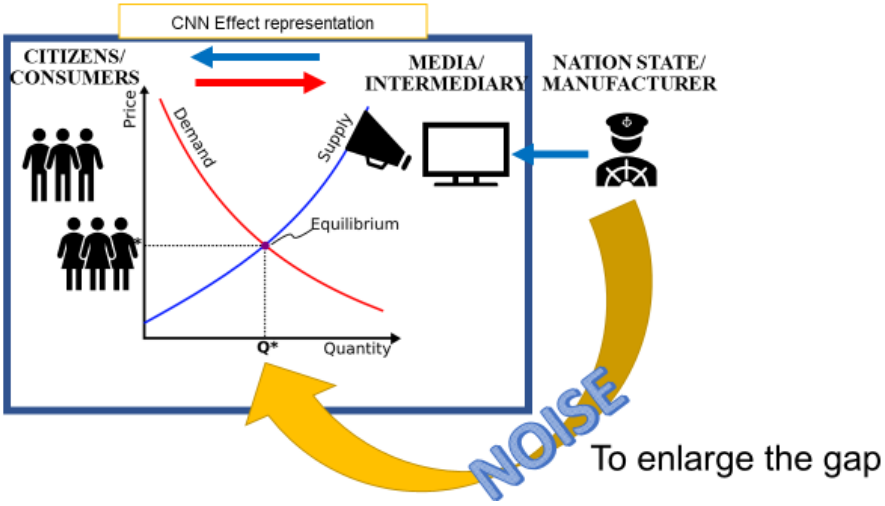

FIGURE 4: THE CNN EFFECT REPRESENTATION. OWN MADE GRAPHIC

In this model, if the state wants to enlarge the *Information Gap* as it was previously accustomed, it has two options: (i) introduce *noise* leading to confusion in the supply and demand curve leaving private media the task of investigating and broadcasting it[22]; or, (ii) allying with private media to broadcast a tailored message together (Herman & Chomsky, 1988). None of these options favour democracy's health and fell prey of free market externalities (Grauwe, 2017). It can be considered effectively a double bind product of freedom of press and speech (Bateson, 2000).

Alternatively, private media in an effort to gain political power, may ignore the state as the main facilitator of information and attempt to steer public opinion by untapping secret matters and broadcasting these to the masses (Piers, 2005). This phenomenon must be considered the predecessor of the Internet's hyper-fragmentation stage we are currently experiencing. As soon as private media was drought to independently broadcast news undermining those policies established by a democratic government, the market drought them to find a niche audience and aimed to capitalize on them by matching a defined political ideology (Piers, 2005).

[22] Notice this model assumes the introduction of noise is done using the many broadcast channels the state has at its disposal

This fed a vicious circle in which more private actors were progressively draught in to attract a segment of the political market aligned with the content broadcasted. While this could not be considered misinformation, it was definitely aimed at improving the market-share. Citizens that had no time to contrast information[23], simply fell victims of the *Dunning-Kruger effect* seen in **FIGURE *3***. This is the methodology behind the coinage of *Fourth Estate* as described by Carlyle in XIX century Britain (Carlyle, 1901).

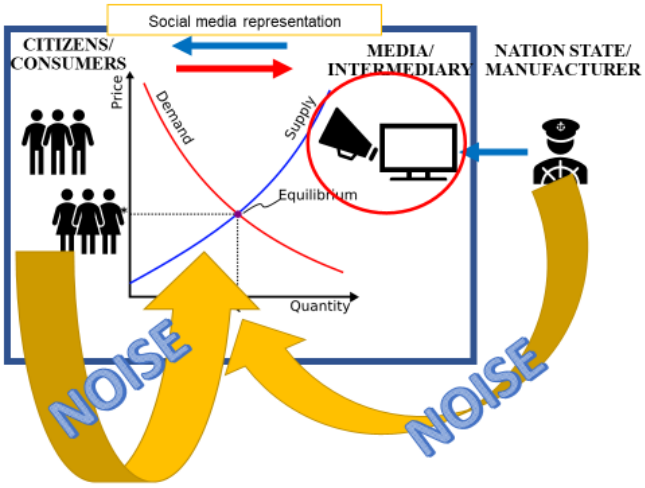

FIGURE 5: SOCIAL MEDIA REPRESENTATION. OWN MADE GRAPHIC

With SNS and the Internet, this model changes one more time. As seen in **FIGURE *5***, now consumers are entitled and encouraged by platforms to show their own opinions with the added ability to influence others[24] resembling what private media had been doing so far. This information environment allows for users to engage in discussions with peers synchronised ideologically without necessarily engaging in debate and contrasting opinions[25], each following a distorted version of reality. It

[23] By information, the paper focuses on political information for which identifies the majority of citizens do not care actively in getting accurate and contrasted information, but rather choose an easy option (Delli Carpini, 2005)
[24] See (Qi et al., 2018), (Sartre et al., 2007), and (Bourdieu, 2018)
[25] Debate does happen but it tends to be highly toxic, with phenomena such as *trolling, muddy the waters,* and *butterfly effects* common in SNS discussions (Harvard, 2020) *Ibid* -

ACRONYM	DEFINITION
AI	Artificial Intelligence

APA	American Psychology Association
API	Application Programming Interface
AUDINT	Audible Intelligence
AWS	Amazon Web Services
BBI	Brain to Brain Interface
BBS	Bulletin Board System
BCI	Brain to Computer Interface
C2	Command and Control
CNA	Computer Network Attack
CCP	Chinese Communist Party
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
CNN	Cable News Network
CoG	Centre of Gravity
COMINT	Communications Intelligence
CYBERCOM	United States Cyber Command
DAESH	Islamic State of Iraq and the Levant (الدولة الإسلامية في العراق والشام)
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
FB	Facebook
FBI	Federal Bureau of Investigation
FP	Foreign Policy
GPS	Global Positioning System
HQ	Headquarters
HUMINT	Human Intelligence
INFOOPS	Information Operations
IR	International Relations
IRC	Internet Relay Chat
ISPs	Internet Service Providers
IT	Information Technology
KGB	Committee for the State Security (Комитет государственной безопасности)
MIT	Massachusetts Institute of Technology
MNC	Multinational Corporation
MP	Member of Parliament
NATO	North Atlantic Treaty Organization
NEURINT	Neuro-cognitive Intelligence
OSINT	Open Source Intelligence
OSOME	Observatory on Social Media
POV	Poinf ot View

exploits the *Dunning-Kruger effect* as a basis for capitalization in user activity and traffic in the platform disregarding the content of information broadcasted in all layers of cyberspace as seen in **FIGURE *7***.

SNS act as a bridge between the consumers and today fully bypasses traditional media outlets in some audience groups. The business model is now shifted towards attention by means of an algorithm (Hadnagy, 2010). The level of hard news now plummets even more as noise[26] is introduced in a bi-directional fashion both from the state (to enlarge the gap) and from the consumers (to seek influence[27]).

All SNS have learnt successfully how to capitalize attention in a way the market rewards it best, seen by means of the algorithm used (O'Neil, 2017). The effects of such policies, sponsored similarly across the *Big Tech* spectrum go in correlation with the *Dunning*-Kruger effect and exploit the peak of "*Mount Stupid*" (See **FIGURE *3***) to the greatest extent possible[28] allowing for an illusion of being informed (Schäfer, 2020) in an ever-increasing labyrinth overflow of highly-biased and uncertain information. This phenomena transfers the *Fourh Estate* from conventional media outlets to Big

PSYOPS	Psychological Operations
RT	Russia Today
SIGINT	Signals Intelligence
SNS	Social Network Sites
UK	United Kingdom
URL	Uniform Resource Locator
US	United States of America
UW	Unconventional Warfare
VPN	Virtual Private Network
WMD	Weapons of Math Destruction

Table of Technical Definitions

[26] The noise effect is known in SNS as Muddying the Waters. *Ibid* - Table of Technical Definitions

[27] See **FIGURE *5***

[28] See (Donovan & boyd, 2021)

Tech conglomerates while enlarging a potential and very dangerous *manipulation gap* open to third agents in the IR arena also present in the cyberspace dimension (Carlini, 2018).

As the *millennial* and *zoom* generations are attracted to this new model (Prensky, 2001), traditional media outlets have been left behind, often times pushing soft-news featuring sensationalism as a desperate attempt to redefine a business model so to compete for attention leftovers (Lazer et al., 2018). Democracy is left in multiple double-binds between freedoms and new technologies poisoning political leaders' ability to persuade their audience effectively (Piers, 2005).

3.2 WEAPONIZATION AND SECURITIZATION OF SNS

The Internet revolution made communications and information access simpler by improving on directionality[29], as seen in **FIGURE *6***. While the IT revolutions have had positive points, it must be pointed out the instruments embedded in cyberspace with each revision, are in no way simple nor easy to grasp, and to this end, subject to heavy manipulation[30].

Today, SNS represents many different things in the cyberspace[31] realm. They are not only mere tools for communication, but also entertainment, informative, pedagogic, and above all, powerful psychological apparatuses (Nissen, 2015). The trend is widening ever since their inception for these reasons (van Dijck, 2013), blurring the

[29] Previously, communication was merely unidirectional being this a milestone with the Internet 2.0 and later, allowing for communication multi-directionality (Singer, 2018)
[30] Technicalities include the TCP/IP, HTTP/S, DNS, and Social associated technologies. They resemble to a great extent financial instruments, stock markets and market economic complexity (N. F. Johnson, 2003)
[31] Defined as: Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures - General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, US.

line between informing and what is considered, to induce or influence behaviours (Taylor, 1995).

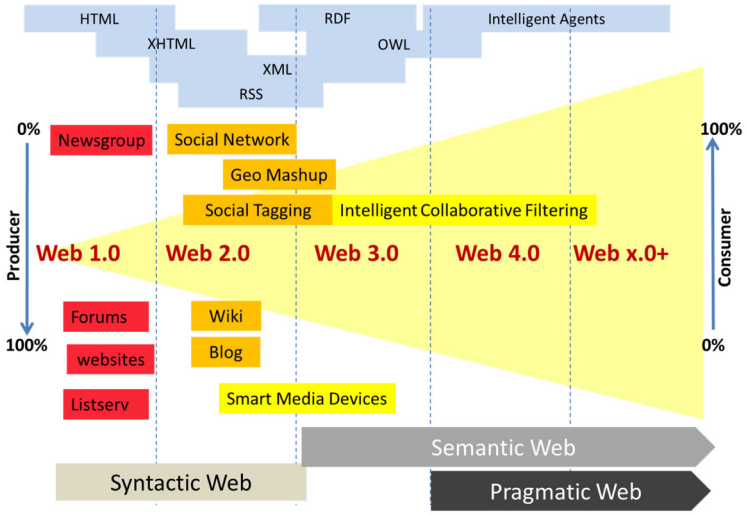

FIGURE 6: A GRAPHICAL DEPICTION OF THE WEB EVOLUTION. SOURCE: (SEGALLER, 1998)

States, and SNS upon its success burst, tend to conform a natural synergy displacing traditional media as seen in **FIGURE *4***. This synergy had greater incentives to materialize as it could potentially allow the state to harden its control over its population at all levels as seen in **FIGURE *7***. Amplifying the state realm in the three layers of cyberspace (M. Libicki, 2011): (i) physical, (ii) synthetic and (iii) semantic[32]; would allow the state to regain back, some of the freedom lost to the *CNN effect* and the *Information Gap* (Baum & Potter, 2019). This however, enters in contradiction with the major individual freedoms and is covered in sections: 3.4 SNS, Economy and Future of Liberal Democracies and 3.5 SNS Maturity and Individual Freedoms.

[32] Niessen and Libicki have similar definitions of the three layers identifiable in **FIGURE *7***: ***The Information Environment*** (Nissen, 2015)

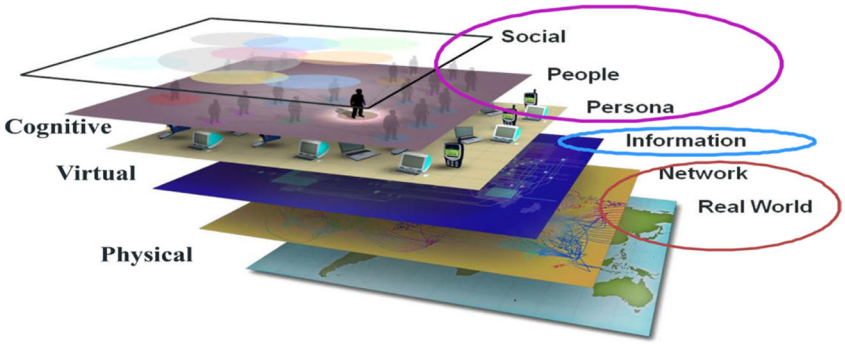

FIGURE 7: THE INFORMATION ENVIRONMENT. SOURCE : (NIESSEN, 2015)

As military analyst Thomas Elkjer Nissen notes (Nissen, 2015), SNS surpasses the civil sphere the moment it starts to be useful in the shaping of politics and global conflicts. This moment starts precisely, as seen in **FIGURE *6***, after the Web 2.0 with social media in the growth phase and the introduction of the *semantic web*[33]. This "*weaponization of social media"*, as Niessen puts it, starts with a few platforms[34] controlling the spread of ideas and opinions in the cyberspace realm contributing to a *Big Brother* setup similar to Orwell's 1984 dystopia (Orwell, 1949).

This is highly disruptive since it allows an oligopoly of companies to have full control of a highly demanded segment of cyberspace, and, what is more important, its information traffic. This control, as Niessen observes, is not only effective in the virtual layer but to a great extent also trespasses in the cognitive and physical spaces as noted in **FIGURE *7***. None of this was feasible before with the printing press, radio[35], telegraph or telephone technologies (Singer, 2018). For this reason, war, and national security strategies today, integrate increasingly sophisticated IT warfare tactics that often times situate SNS at its core. This, in conjunction with psy-ops and black-ops[36]

[33] The semantic web would correspond to Niessen's cognitive layer seen also in **FIGURE *7***
[34] These can be considered today SNS among Nasdaq's Big Tech: Twitter, FB, Alphabet and AWS but also regional ones including the Ant group, Wechat, and VK.
[35] Singer notices how in the Russo-Japanese war both sides used Marconi radios, for which its inventor hold no control over communications
[36] Refer to *Ibid*-Table of Technical Definitions

as seen in **FIGURE *8***, make SNS understanding and control essential, so to secure C2.[37]

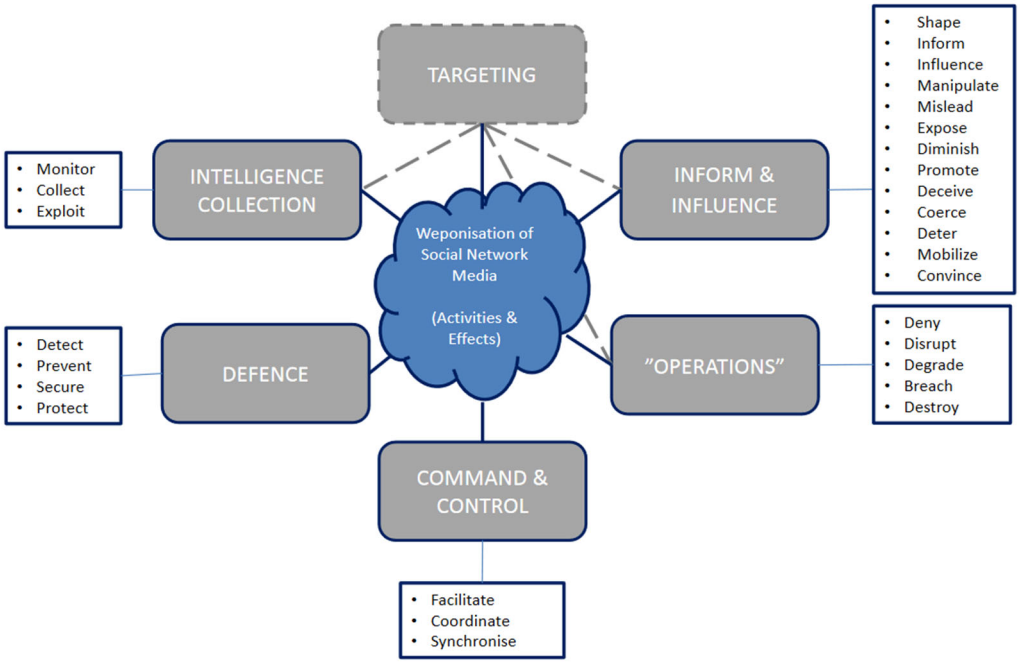

FIGURE 8: ACTIVITIES AND EFFECTS FRAMEWORK. SOURCE: (NISSEN, 2015)

Weaponizing SNS is in part, a natural evolution from an intelligence perspective. In the Cold War, no governmental agency would have dared to make sensible information publicly available for their rivals to dig in without attempting to mislead their counterpart in the process. The KGB, CIA and associated diplomats abroad had meticulously trained personnel investigating its enemy's footsteps with all means available[38], a process now done at a fraction of cost and risk. SNS democratized all

[37] Command and Control hereafter referred as C2. *Ibid* - Table of Acronyms and Abbreviations. In a Cyberwarfare IT context C2 might also be used together with C3 referred as: Communications, Command and Control

[38] This would include bugging rooms, interfering communications, subscribing to magazines, infiltration in academia, etc.

vital influential processes[39] by introducing the term "*disintermediation[40]"* in society and equalizing everybody to the role of key stakeholders[41] competing now for attention.

From an intelligence perspective, the result undermines society and state integrity. This may be understood best from Aristotle's definition of democracy were involving all masses in decision-making, works against the concept of political efficiency (Winthrop, 2019). As a result, this leaves governments[42] exposed to a level of national unrest and foreign meddling never seen before in history (Nichols, 2005).

On the other hand, intelligence agencies now have it easier to conduct much of its collection and operations as seen in **FIGURE *8***. Most HUMINT[43] missions have been displaced by its less risky, and cheaper counterpart, OSINT[44] based to a great extent in SNS[45] derivatives. While open sources used to be a deceptive source of intelligence in the past, now they are often the only available method to gain access in a space that it is exclusively virtual (Nato, 2001). This space happens also to be public and again, allows civil society, with accruable knowledge on how SNS works, to expose government actions using crowdsourcing methodology to operate at an agency level[46] (Higgins, 2021).

The actors involved in the shaping of SNS influential processes, have also blurred the line separating the *testis* and the *superstes[47]*. Where media was before a mere

[39] Most vital and strategic instruments of influence in society include: political, psychological, economic and social (Nissen, 2015)
[40] Understood as the process of cutting intermediaries, a trend seen in the transition between Internet 2.0 and 3.0 with services like Uber, Tinder, BlaBlaCar, etc. Conversely, it may also be argued it created new virtual intermediaries instead
[41] See Heidegger's shared world theory in Social Media Philosophical Foundations (Qi et al., 2018)
[42] Nichols notices western democracies are notably more exposed and harmed
[43] Human Intelligence hereafter referred as HUMINT. *Ibid* - Table of Acronyms and Abbreviations
[44] Open Source Intelligence hereafter referred as OSINT. *Ibid* - Table of Acronyms and Abbreviations
[45] SNS-based OSINT is also known as SIGINT/COMINT, and at the same time in CNE and CNA.
[46] See the case of Eliot Higgins' blog, Brown Moses and Bellingcat projects based on OSINT techniques
[47] Understood as witness and victim respectively

and exclusive intermediary between the centre of action and the public, now anybody can jump in as seen above in **FIGURE *5***. Moreover, what makes the *testis* and *superstes* often indistinguishable is the fact SNS netizens often override the original story by constructing a brand-new tale from different sources originating in SNS while sited in front of a computer (Higgins, 2021).This interexchange of role's actions then transcends to the cognitive and physical layers as seen in **FIGURE *7***,**FIGURE *7*** where it becomes increasingly difficult to identify the veracity and integrity of the original messages.

An effectively weaponized SNS is aimed at creating effects on the adversary by means of espionage, sabotage, disruption, exploitation or all of the latter combined so to influence the target's beliefs to align with yours (Rid, 2013), as noted in **FIGURE *8***. In Clausewitz 's terms, this set of actions must be aimed at disrupting the opponent's *centre of gravity* by targeting in this case, the psychological morale of those netizens and effectively achieving war by all means (Clausewitz, 2008). This is done by carefully studying the *strategic narrative* of the *opponent*[48] in social media, for which SNS prove once again, the best vehicle.

Once successfully reverse-engineered the *social construction* and s*trategic narrative* of an opponent, Clausewitzian strategies may also be formulated at creating *fog*[49] and *friction*[50]. Examples of these are clearly seen in the *Gerasimov Doctrine* (Galeotti, 2019) and Chinese military strategies consisting in asymmetric warfare (Liang & Wang, 2002). These rely heavily in SNS to structure their C2 processes so

[48] Notice the *opponent* refers to a state's population and the narrative may be official if it comes from a state, or socially constructed if we refer to the society as a whole
[49] Understood as *uncertainty* (Clausewitz, 2008)
[50] Understood as *unexpected consequences* while at war (Clausewitz, 2008)

to gain substantial leverage against bigger military budget opponents as seen once again in **FIGURE *8***.

In the case of states, it must be noted the *strategic narrative* consists of two sub-concepts: (i) *institutional narratives* and (ii) *theatre narratives*. The first can be described as the modern equivalent of the *raison d'etat* in FP making (Butterfield, 1975). The *theatre narrative* on the other hand, should be understood from Sartre's existentialism philosophical foundation (Sartre et al., 2007)[51] which, at the same time, varies depending on the social construction of the opponent. This might be a complex thematic to study as plenty of cognitive biases are added on top of the SNS ecosystem and the three layers previously seen. All elements must be correctly decoded so to learn relevant intelligence concerning the opponent (Heuer, 1999).

The *theatre narrative* when used by a state in SNS, is meant to act as a façade of apparently friendly and diplomatic intentions that must be read in between lines so to gain access to its *institutional* and *strategic narratives* (Nissen, 2015). Simultaneously, *theatre narratives* are present in citizen's lives because they themselves are part of the structure the state has assisted to create. Hence, the importance of Sartre's existentialism theories and Heuer's cognitive biases so to understand states' strategic narratives in the SNS frameworks.

One clear example of *SNS weaponization* is Tik Tok. Owned by ByteDance, a privately held company with HQ in Beijing, it raises distrust among other states when it profiles its nationals by leaving *backdoors* opened for the CCP to monitor this data. Effectively, with this move, the CCP is implanting its surveillance model out of its borders (Gutmann, 2010). This collection of information is considered by many a

[51] See *Ibid - 4 -* (Qi et al., 2018)

breach of sovereignty in cyberspace because of the ongoing cooperation enforcement the CCP applies to all technological corporations based in mainland China[52] (Moloney, 2020). This is particularly worrying as it leaves raw information at the mercy of an opponent which can then gain access to both the *social construction* and *strategic narratives* previously mentioned. It furthermore, aligns with both China's National Security Strategy (Bolt & Gray, 2007) and the *Made in China 2025* initiative (Li, 2018) allowing for potential use of *SNS weaponization* in acquiring technological advantages and leapfrogging unfairly[53]. Much like the *Gerasimov Doctrine,* the Chinese acknowledge this as *Unrestricted Warfare*[54] (Liang & Wang, 2002).

Other examples of *SNS weaponization* are based on understanding the algorithms in such platforms and its effects on the three layers of the information environment as seen in **FIGURE *7***. Understanding the *theatre's narrative* reactiveness and how a society is affected *culturally* by SNS, it is possible to steer public opinion by exploiting vulnerabilities associated to a culture. An example are *sock puppets* and *bot armies* (Ferrara et al., 2016), aimed at influencing (See **FIGURE *8***) previously targeted population more affected by the *Dunning-Kruger effect*. This was the case of Cambridge Analytica interference in the US election and BREXIT among other political events according to C. Wylie(Wylie, 2019).

The opposite trend, *securitization of SNS*, is also prominent in IR. States, although most do not hold direct control over SNS, they constrain the reach, availability, and

[52] See China's Cybersecurity Law and Export Rules, Nov 2018: *"…requirement of Chinese companies to cooperate with government intelligence operations if so requested and may allow the Chinese government access to user data collected by any company doing business in China*"

[53] One example of this is the ongoing battle to secure Quantum computing technologies and their key role in the Industry 4.0, see (Kania & Costello, 2017)

[54] Notice the same degree of hesitation and rejection is expressed by Chinese and Russian officials about American *weaponized SNS* operating in their territory. This is the reason why Russia's SORM (Ermoshina, Loveluck, & Musiani, 2021) and most famously, China's Golden Shield Project censor or prohibit actively American SNS in their territories. It is also what fuels the cyber arms-race

privacy of SNS users in favour of enhanced security policies that respond to the anarchic IR arena and the delicate *balance of power*. In this case, there are two notable examples on how to proceed with a national defence strategy: (i) By gaining leverage on censorship and (ii) by capitalizing on privacy.

In the first case, it can be noted how states claim back sovereignty over cyberspace as another realm. This is typically the case of states governed *de facto* by a unique party or semi-authoritarian regime. The goal of *securitization* is to protect the *strategic narrative* by means of securing citizen's data within their borders denying any possible foreign interference at the expense of press and speech freedoms (Baños, 2017). The most notable examples are China and Russia[55]; with the first exporting its technology to Middle Eastern and Central Asian states[56].

Were countries fall behind in budget to secure their cybersecurity, their last resource is found in outsourcing[57] it abroad (Schneier, 2018). This represents another twist in International Relations similar to buying physical weapons and securing alliances in a Bandwagoning move (Schweller, 1994). It also allows this market to develop creating dependence, not relieving the security dilemma, but rather, enlarging it even more by making bi-lateral and multi-lateral alliances the rule, not the exception.

The second defence strategy is carried out at the expense of user's privacy rights and freedoms. This is typically the strategy followed after 9/11 by western liberal democracies conducted notoriously by the NSA with the XKEYSCORE and PRISM

[55] See Russia's Internet model and the ban of LinkedIn (Maréchal, 2017)
[56] See Michaela Flemming's Trojan Horse for a more detailed view on China's exporting surveillance hardware and software to periphery states (Flemming, 2020)
[57] Some companies specialized in cybersecurity: FinFisher, the Gamma Group, Cyberbit, VAStech and the NSO group. Most belong to the EU and Israel with the exception of South Africa.

programs[58], and outsourced to allies[59] for SIGINT[60] collection (Baños, 2020). The core of the defence strategy was initially aimed at preventing terrorist attacks that could have an impact in the national security of a state by collecting and storing data that could incriminate potential terrorists (Véliz, 2019). This defence strategy relies on passive data collection[61] and apparent preservation of civil liberties while not being so assertive in claiming a realm of cyberspace linked to the state in the physical layer (M. Libicki, 2011). It is effectively a modern day cyber-trojan horse

However, both liberal democracies and one-party states hold similarities in terms of they are both *de facto* claiming sovereignty over a significant portion of cyberspace with increasing restrictions in content and physical locations. This is seen obvious with ISP service restrictions and active monitoring of traffic (Khattak, Javed, Khayam, Uzmi, & Paxson, 2014) that renders anonymity, a historical milestone pre-Internet 2.0 (see **FIGURE *6***).

Censoring or actively controlling social media though, has been something liberal democracies have been very reluctant to implement in an attempt to postpone a cut in civil liberties. In IR however, much as everything subject to militarization, the weaponization of SNS must be treated as a matter of dissuasion (Huth, 1999). Western liberal democracies have remained passive actors outsourcing this task to the private sector while SNS businesses capitalized on the handling of personal information with disregard to ethical values (Véliz, 2019). While the US passed some regulation[62] to gradually take back control lost to *surveillance capitalism* (Zuboff,

[58] Disclosed programs post-Snowden, ongoing programs include BULLRUN, MAINWAY, ECHELON, DCSN and MYSTIC among others (Aid, 2009)
[59] See the Five Eyes Intelligence alliance and surveillance programs associated (Patman & Southgate, 2016)
[60] Signals Intelligence hereafter referred as SIGINT. *Ibid* - Table of Acronyms and Abbreviations
[61] See the Cloud Act, 2017 (Mulligan, 2018)
[62] See how US regulation changed after 9/11 (Kurra, 2011)

2019), this was mostly an exercise of buck-passing (Mearsheimer, 2014) without actually crippling the ability of SNS over cyber-power accumulation.

Not every move was passive in this security dilemma (Herz, 1951). As seen before, the US post 9-11 became highly active in both espionage and attack via the NSA and the targeting terrorist sponsors (Schneier, 2018). According to Schneier, the US indirectly encouraged the development of an insecure commercial pool from which it could later benefit from[63]. It undermined the premises of citizen privacy hoping to use private technological giants to its advantage in conducting FP. As this became public, it eventually led to an escalation of the *security dilemma* in the cyberspace realm, where attack was more cost-effective than defence[64].

SNS have demonstrated outstanding performance within states and non-states actors. Conversely, the latter have been using SNS offensively: (i) Hacktivists, and (ii) terrorists[65]. Information by itself is in many ways is a source of power in IR. While in the past it was costly to obtain, arguably only available to state apparatuses; the electromagnetic spectrum has allowed for economies of scale and scope in a new arms race to obtain the latest element of power, cyberpower. Besides allowing almost every stakeholder in society to freely enter in this race, cyberpower allowed also for IR theory redefinition in an even more chaotic fashion.

Some recent examples on this dynamic are listed in the

[63] Presumably via *zero day* exploits and *backdoors*
[64] Examples include: *Moonlight Maze* (Loeb, 2001)*, Titan Rain*(Gutmann, 2010)*, Buckshot Yankee* (Burt, 2010)*, Stuxnet* (Lindsay, 2013)*,* and *Wannacry* (Adams, 2018) from the most famous cyberattacks
[65] See the examples of Julian Assange, Anonymous and Al Qaeda among others (Wojtasik, 2017)

Annex section at the end of this paper. With a wide array of influence means such as: manipulation, recruitment capabilities, exposure of facts/ personalities, mobilization of masses, deceiving, coercing, diminishing, creating misinformation, promoting of figures, and intelligence collection; cyberpower in IR can completely redefine power dynamics. In the next section,

3.3 SNS and IR , the paper discusses how SNS shall be used in a persistent anarchic environment and how it shapes power and politics today.

3.3 SNS AND IR THEORY APPLIED TO CYBERSPACE

SNS and media are closely linked in as long as both seek to both inform and exert influence. SNS, as seen in section

3.2 Weaponization and Securitization of SNS, has great potential to be weaponized making it possible to establish a connection between SNS and structural realism (Mearsheimer, 2001). Taking Robert Dahl's[66] definition of power: *"A has power over B, to the extent that he can get B, to do something that B would not otherwise do"*; and crossing it with Adam Liff's cyberwarfare definition[67], it can be extracted that if A strikes first over B, it will have a set of significant advantages.

A first advantage is claimed in the surprise factor which may create uncertainty and chaos fractures that could result in a societal crisis and fracture a state[68]. The second advantage has to do with the defence mechanisms that must be created to either mitigate or deter any coercive attacks[69] (K. C. Yang et al., 2019). Both advantages in this case, give place to a *not intense security dilemma* (Jervis, 1978), and a

[66] Robert Dahl, 'The Concept of Power', Behavioural Science 2(1957): 201-215, 201f.
[67] "*A deliberate hostile, cost-inducing use of CNA against an adversary's critical, civilian or military infrastructure with coercive intent or to extract political concessions (…) in order to frame another actor for strategic purposes"* (Liff, 2012)
[68] Assuming A has correctly decoded the *strategic narrative* of B.
[69] Part of offensive counter-intelligence disciplines (Barnea, 2017)

subsequent *Arms Race* in cyberspace, were an offence move always holds an advantage.

Nevertheless, cyber-space is a massive non-physical space built on social constructions and hence, with blurry lines in the limits of sovereignty which makes it equally chaotic if not worse than the IR arena. This makes it effectively, a multipolar space not exclusive to states, yet they remain as the main actors for which an *intense security dilemma* could also be plausible (Jervis, 1978). In this case and according to Jervis, a defence move should have an advantage. This view is also shared by Martin C. Libicki in **FIGURE *9***, where he classifies contemporary cyber-combat in the defence category of the deter-disarm-defence triangle (M. C. Libicki, 2009).

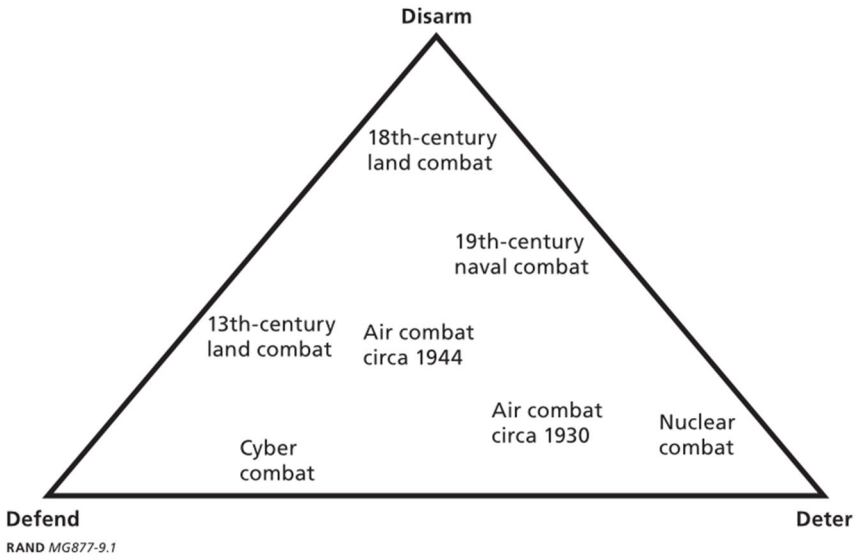

FIGURE 9: VARIOUS FORMS OF COMBAT IN THE DETER-DISARM-DEFEND TRIANGLE. SOURCE: (M. C. LIBICKI, 2009)

However, Jervis' security dilemma is subject to criticism from a structural realist perspective, because as Mearsheimer notes, states, are mostly power maximisers due to the uncertainty context (Mearsheimer, 2014). Moreover, Jervis does not consider the difference in character of cyberweapons and the role of non-state actors in his security dilemma equation. Taking into consideration the potential for *SNS*

Weaponization seen in the theoretical frameworks of P.W. Singer and Nissen, it may be concluded an offence move so far is a guarantor for national security and state perpetuity[70] (Nissen, 2015).

As the Internet economy gains momentum with the development of the industry 4.0, society is likely to follow suit (Mazali & Mazali, 2018). States regard this as a key indicator to secure, and hence SNS are vital in this new equation. Humans are social animals by nature, and it is sociability precisely, the factor SNS capitalize on. States besides seeking power also pursue survival over time (Pashakhanlou, 2017). For this to happen, they must exert a certain degree of social control avoiding sudden unforeseen changes in short timespans within the mass of their population. The same uncertainty force that drags states to pursue power in the anarchic IR system, is transposed in its political system by means of population control. Individual and collective behaviour to this end, must be secured in a predictable and controlled fashion. SNS and Big Tech[71], to this end, are facilitators of the social engineering required in exploiting human's fragile psyche condition. This is done today in SNS by means of machine learning, AI, and algorithms alike (Wright, 2018).

When a modern nation-state is faced against a non-state actor of higher scale and scope that could menace its monopoly in control over identity, it is natural for the state to treat such actor as a key element to secure its national strategy. SNS for now have only permeated in the social sphere, and this arms race remains exclusively psychological. However, as FB[72] and peers keep innovating, it is likely to see SNS permeating in the sovereignty sphere of the state in areas like monetary policy, culture,

[70] Using a Structural Realism mindset. Liberals hold an opposite stance advocating for defence and proliferation of information among states to deter any attack by a rogue agent out of the *pax consensus*
[71] Big Tech here applies also to regional SNS like Baidu, Wechat, VK and Yandex for instance
[72] See Facebook's Libra virtual currency project (Brühl, 2020)

and even political institutions. States seeking to secure power, must not only seek to partner up with SNS behemoths, but also start looking at its cyberspace counterpart, as another space within borders in which the four properties defining a nation-state persistently apply: (i) sovereignty, (ii) population, (iii) territory and (iv) government.

Attempting to redefine how cyberspace is treated from a realist scope is ambiguous due to the utopian nature of the Internet in its early days and predominance of non-state actors. Treating the Internet and cyberspace from the scope of Vernon's product lifecycle (Vernon, 1979), it can be appreciated that in the Internet early days, users were much more idealist in constructing a common space of knowledge with mutual trust being a common denominator among netizens (Refer to **FIGURE *6***). As Internet reached maturity in its many revolutions, trust was further lost, and what idealists once coined as an *e-wonderland*, now has become more of an *e-wasteland* (Ogunseitan, Schoenung, Saphores, & Shapiro, 2009).

From a structural realist perspective, states cannot be trusted because of a lack of transparency in intentions[73] due to an existing international anarchic environment (Mearsheimer, 2014). This effectively renders cyberspace in the image of its physical counterpart, an electronic wasteland; where self-interest imposes over ideologies resembling classical realism (Baylis, Smith, & Owens, 2020). Classical realism plays a bigger role in cyberspace IR, because it helps explain human nature as the main driver for conflict (Donnelly, 2000). Since states, as mentioned earlier, are no longer the exclusive protagonists, classical realism helps explain the sources of anarchy in cyberspace, and hence, cyberconflict among state and non-state actors.

[73] This is the importance of successfully understanding the *strategic narrative* and its sub-products, the *institutional* and *theatre narratives*

Nevertheless, states are ultimately responsible for structure in detriment of agency. This is reflected in how cyberspace has been conceived and its development. States have provided an existing social construction in which technology, though abstract in principle, is not exempt by any means from political and economic leanings (Корыбко & Савин, 2021). Hence, any society emerging from cyberspace is likely to be anarchic in nature due to the structural concerns in how technology was shaped to begin with. As ongoing social construction in cyberspace starts to transpire to the cognitive and physical layers (See **FIGURE *7***) of the information environment (Nissen, 2015), netizens eventually collide with the existing physical barriers of the state they live in. This at the same time, echoes to the existing strategic narrative of a state and its role in IR.

The phenomenon of globalization reaches also SNS and by extension, netizens, and states. As seen in **FIGURE *6***, the early days of the Internet were characterised by a liberal[74] attitude inwards this environment. This trend continued after the dissolution of the USSR and the end of the Cold War for which a netizen could not effectively be classified as a citizen of an x state. This is a phenomenon for which the state had initially a lack of proper mechanisms to secure its ties on identity. The concept of *imagined communities* (Anderson, 2006) started to adopt a new meaning in cyberspace, for which a brand-new social construction had started to conform both globally and virtually.

As years passed, states realised how states discretely waging *asymmetric warfare* (Giles, 2020) were exploiting the Internet and globalization capabilities. The anarchic nature of the international system was replicated in SNS, having both rival states and

[74] Understanding liberal from an American perspective

non-state actors, exploiting the *e-wonderland* ecosystem to their advantage[75]. Liberal democracies are arguably, the most affected by *asymmetric warfare* because it exploits the core of their freedoms. This is presented in the next section of the paper, 3.4 SNS, Economy and Future of Liberal Democracies.

3.4 SNS, Economy and Future of Liberal Democracies

Some western liberal democracies, as seen in the prior section, have been hesitant in both *weaponizing* and *securitizing* SNS, as if information embedded in their innards was second to their elements of national power. This is a fatal miscalculation for national security, as information is arguably the source from which many facets of power are derived. While democracies spent time harmonizing the equilibrium between freedoms and the Internet, adversary states positioned in a head start as their means to wage *asymmetric warfare* (Thornton, 2007). Having seen the role media played in the most recent past as traditional information brokers, it seems almost as if democratic states were forgetting recent lessons from the past.

From democracies to autocracies, information is a valuable resource that is getting increasingly difficult to control in a SNS environment. This is not because SNS is not subject to the rule of law or the status apparatus, but rather, because of the social construction that remains free and is present in the semantic or cognitive layer (M. Libicki, 2011). In this line and as Nissen notes, SNS enabled more routines for defection, identity exchange, loyalty marketplaces, diplomatic dogfights, and overall,

[75] Notice this category is broad enough to include all sorts of industrial espionage, political activism, early versions of the Deep Web (Frediani, 2016), scams and most notoriously, the enabling of terrorist communications as seen with 9/11

a sense of illiteracy to journalism standards (Nissen, 2015). This array of dangerous routines affect both governmental systems equally.

At this point, it is worth to highlight once again General Gerasimov's remarks: "*The very rules of war have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness"* (Schnaufer, 2017). Gerasimov's approach, both realist and Clausewitzian, has allowed for an effective use of Nissen's above-mentioned routines in the leveraging of an *asymmetric* strategy against western democracies.

A noticeable example is Russia's active use of botnets, hackers, media, and dissemination of deceptive information in SNS, also known as non-linear warfare (Schnaufer, 2017). The latter, has come to the point to be the preferred way of winning a conflict before resorting to military tactics[76] echoing back to Sun Tzu's 13 principles of war (Tzu, 2012). Gerasimov's framework facilitates Russia's geopolitical agenda in creating transcended unrest from one layer of the information environment to the remaining two as seen in **FIGURE *7***.

How is this only affecting mostly western liberal democracies? There is a number of underlying reasons worth highlighting from an economical perspective. Statistically, states identified with this form of government have enjoyed of unprecedented levels of socio-economic welfare derived from free market economies. This has been achieved in part, due to a fractional reserve monetary banking system that induces the fallacy of unlimited growth (Ferguson, 2010). Financial crises appear as a result of it, featuring a misuse of monetary theory (Menger, 1892) yielding towards monetary

[76] In practice, both military and non-military tactics (hybrid warfare) have been implemented by Russia in the Abkhazian and Donbass conflicts. See (Jasper, 2020)

nominalism, and confusion about the nature of fiat money; ultimately leading to the squandering of capital (Lachmann, 1978).

Market Capitalism has degenerated in a vicious spiral of products and services that may allow for faster growth but which often times, do not offer anything tangible nor contribute to a healthy economy. This is the case of the majority of financial products like derivatives, options, bonds, or shares. Each of them owes its being to the fractional reserve system predominant in liberal democracies. Everyone subject to them is left adrift to conducts such as speculation, consumerism[77], corruption, a lack of ethics, unemployment, and, as a direct consequence, heavier reliance on the state. This dystopian reality is then transduced to citizens by means of the actors involved in this ecosystem, among them, SNS. The result can be seen as a *tragedy of the commons* at a social scale (Hardin, 2009).

How does this materialize in weakening democracies? The progress of society cannot be set by politicians[78], but rather, by financiers who determine the speed of technological advance in an artificial monetary market economy with disregard to human capital nor capital of any sort as it is completely misinterpreted (Von Mises, 2012). State burocrats have better quality incentives adapting to the conditions imposed by these economic agents. The rules of this game alter human kindness and transform it into an aggressive player at all levels left at the mercy of a powerful oligarchy that does not align with the concept of brilliance necessarily (Hayek, 2001). With increasing levels of inequality, the social contract gets gradually eroded (Butlin, Rousseau, Tozer, & Bosanquet, 1895).

[77] In detriment to savings
[78] Or any materialization of the general will

In contemporary times, SNS has been known to engage in what has come to be known as *surveillance capitalism* (Zuboff, 2019). This is the latest materialization of growth at the expense of user privacy (Véliz, 2019), marking a new low in ethics in favour of business. With Big Tech now attempting to redefine the Iron Law of Oligarchy (Michels, 2019), we are now observing what once was a dystopia (Huxley, 2014), is potentially becoming a reality in the form of a new re-branded world order (Schwab & Malleret, 2020). This phenomenon will be explained more in detail in 3.5 SNS Maturity and Individual Freedoms.

This oligarchical aberration comes as a part of the liberal package because sadly, democratic states often overlook people's interests as both political parties in democracies and economical hegemons end up converging interests at some point (Newman, 2019). Unfortunately, the liberal democracies have not risen to the occasion to counterbalance this phenomenon. This has been a provocation to chiliastic agents endogenous to the system aiming to capitalize on power, and the result has been translated mainly in different interpretations of discontent within the local population.

The economics vs politics question is always a fundamental question to watch. The shift is left palpable in SNS with two big fronts, corporate lobbyists, and state burocrats. The two align for personal gains rather than empowering citizens (Levitsky & Ziblatt, 2018). As businessmen attempt to bypass national sovereignty onto politics, this leaves the mass of the population undefended against political and psychological manipulation of exogenous agents via SNS[79].

[79] Notice former President Obama, once an advocate, has recalled in the last 4 years, the Internet as the single most dangerous threat to democracy (Goldberg, 2020)

This struggle may be local among party politics disputes, or as a form of foreign meddling[80] taking advantage of the first. Both eventually lead towards polarization and discord (Bennett et al., 2018). The same *strategic narrative* states used among each other in an IR context, is also used in party politics. Adversary states noticing turmoil at an internal level attempt to capitalize on this by polarizing segments of the population or boosting existing independent movements (J. K. Lee, Choi, Kim, & Kim, 2014). What is more, field experiments suggest SNS integrated algorithms often times give this task already consummated to state opponents due to its addictive nature in promoting biased content to prolong organic use on the platform (Levy, 2021).

Liberal democracies weakest of all points is seen in elections. The four main threats are: (i) misinformation Campaigns, (ii) propaganda, (iii) voter suppression and (iv), societal discord. Notice all four of them are exclusive to SNS as the delivery vehicle[81]. In the first and second case, this can be done with the use of bots, AI, and cyborgs to spread all of disinformation tactics as seen in **FIGURE *8*** (Luceri, Deb, Giordano, & Ferrara, 2019). These two tactics exploit the virtual layer of the information by means of deciphering the algorithm language in SNS. Examples of this can be seen with Cambridge Analytica's business model (Wylie, 2019), or more recently, with the outcome of Taiwan's elections (Han, 2007). Voter suppression and societal discord exploit mostly the cognitive, and to a lesser extent, the physical layer. This is done by altering in the *theatre narrative* of the targeted netizens in an attempt to influence a direct action on the person in the *physical layer*[82].

[80] Leveraging on local politics unrest
[81] Libicki uses an analogy between missiles and cyber-weapons in terms both consist of: (i) a delivery vehicle, (ii) a navigation system, and (iii) a payload (M. C. Libicki, 2009)
[82] Notice the reverse trend is also possible and SNS have been used for instance, in Ghana, for positive political action (Agbozo & Spassov, 2019)

Psychologist Jonathan Haidt suggests in his *Beehive Hypothesis* the need for humans to belong to a group (Haidt, 2012). Once again, this in another point at which SNS excel. Haidt highlights the fanatism unfolded traditionally over religion and sports, now also extending into politics. For states in IR, it has not taken them long to figure out this same logic can be applied into politics and more specifically, in democracies with multiple representations in parliaments. SNS are a good vehicle to target party advocates at the opposite ends of the political spectrum. Once these masses are agitated, it is a vicious circle eager to replicate at a local scale as seen with parties[83] like: *AFD* in Germany, *Rassemblement National* in France, *Podemos* in Spain (Sampedro, 2014). *Fidesz* in Hungary; or the *Five Stars Movement* in Italy (Vittori, 2020).

Unrestricted Warfare in IR politics is consummated the moment the narrative at a local level is no longer aimed at discussing facts or finding consensus, but rather delegitimize one another in a skirmish for political power (Orriols & Balcells, 2012). This coupled with heavily distorted facts boosted by algorithms designed for meeting shareholder's objectives rather than for displaying true facts, leaves democracies completely exposed (Levitsky & Ziblatt, 2018).

The CCP acknowledges these weaknesses directly in *Document Number 9*[84] which provides for information on how China sees the West liberal democracies and their complete rejection to this model of government. In this document, the CCP explicitly rejects the separation of powers, universal rights, and freedom of press

[83] Most parties in democracies are now dragged to use SNS strategies as a part of their competitive advantage to reach out to their masses and potential new voters
[84] Leaked CCP document also known as *"Briefing on the Current Situation in the Ideological Realm"* - (CCP, 2013)

identifying these as potential threats to the party theoretical foundations and its long-term strategies (CCP, 2013).

Democracy concerns over the health of its norms and institutions has intensified in recent years resulting in increasing polarization (Levitsky & Ziblatt, 2018). There may no longer be a consensus on what is to constitute a democracy[85]. Political actors are increasingly appealing to emotions rather than facts (Iyengar, Sood, & Lelkes, 2012). This could lead to citizens at both ends of the political spectrum to advocate for a fairer system tailored to their definition of a social contract with disastrous consequences. It is a clear sign of fatigue in the liberal democratic model (Doyle, 1986), and it should act as a red line so to start amending the core problems in it. It is precisely, as Bauman describes it, an effective divorce between politics and power were politicians only aim at building careers rather than crafting policies[86] (Bauman, 2013).

Liberal academics say democracy has been the victim of its own success (IKENBERRY, 2020). On the other hand, the combination of liberal democracy and free market economics, has allowed for social values that undermine the same human condition. Liberalism in this framework has backfired in part because it relied heavily on an unchecked capitalism[87]. The two combined produced serious market inefficiencies for which, democracy was not able to provide answers. Populism and other movements that undermine the integrity of democracy have been triggered in part by a by-product of liberalism, media[88].

[85] See the Hard-Core Sport fan phenomenon in Trumpism (Devlin & Brown, 2021)
[86] Bauman notes a certain dose of political sacrifice in the golden age of democracies as explained by Fukuyama (Fukuyama, 2006)
[87] Both the state and its citizens fell prey to the underlying framework of monetary fiscal policy (Klein, 2011)
[88] Notice that media was also partially responsible for the export of liberal democracy as a form of government with the Washington Consensus as the main creed (Birdsall, De La Torre, & Caicedo, 2012)

This in itself is a double bind paradox, as media, and particularly, private media and SNS; is a product of capitalism and freedom of speech in its purest form[89]. Orthodox states[90] have at the same time, capitalized on this and created political strategies to delegitimize such freedoms while attempting to redefine democracy to their convenience (Tolstoy & McCaffray, 2015).

It is worth to highlight how SNS also affect to a lesser extent autocracies and one party-states. A recent example of this is Alexander Navalny, him being accused of attempting to ignite a colour revolution in Russia triggered and sponsored by the West (M. Johnson, 2021). Russian sock puppets and state media have been fighting this recent phenomenon hard[91], showing distressing signs that SNS interference could also interfere in their present form of government, hence posing a threat to their national security. This effectively puts SNS as a both valuable and strategic asset across different forms of government as **FIGURE *10*** shows.

[89] See the manufactured consent (Herman & Chomsky, 1988)
[90] See Russia Today, hybrid warfare strategies (Orttung & Nelson, 2019) and Russian propaganda apparatuses deployed abroad in disguise (Shlapentokh, 2019)
[91] An example of one of many blog entries posted by the Embassy of Russia in Spain and distributed via the "*Geoestrategia"* Telegram channel can be seen here (Geoestrategia, 2021)

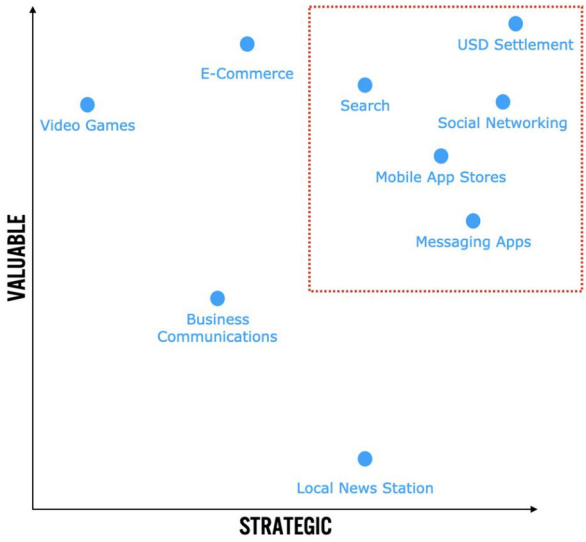

FIGURE 10: STRATEGIC VS VALUABLE SECTORS. SOURCE: THE CHINA STRATEGY GROUP

While Russia and China have strict policies for the dissemination of information on the physical and cognitive layer, this control will soon be extending as explained above, progressively onto the virtual layer. As a part of the cyber arms-race, the question is whether this control over Internet freedom will permeate also into liberal democracies. The paper treats this topic more in depth in the next section: 3.5 SNS Maturity and Individual Freedoms.

3.5 SNS Maturity and Individual Freedoms

Many Internet based businesses started to emerge from the remaining's of the Internet 2.0 post-dot com bubble (World Bank, 2005). Investors readjusted expectations after this economic meltdown, in advance of a new player waiting to redefine the Internet business as we know it today. This player was Google, and their business model came to challenge advertisement on demand based on customer's

personal data[92]. All Internet companies followed suit and soon transforming netizen's privacy in a raw material with massive power yields (Véliz, 2019).

In section 3.4 SNS, Economy and Future of Liberal Democracies, the paper attributed this result to the fractional reserve monetary system model implanted worldwide. Market economies came up with a good product to give a solution to expensive, lengthy, cross-border communications. SNS came to fill a market gap with huge demand in the market[93]. This business model however, was hard to monetize without recurring to ads, the trend in the Internet 2.0 era (Clemons, 2009). Because of constant growth constrains, this problem was soon turned around by redefining the business model in selling user's data in exchange of a free innocuous services like SNS[94].

What SNS were doing in reality was monetizing user's personal data in the virtual layer by developing a series of technologies aimed at capturing and processing massive amounts of data into pattern behaviour linked to a user(Gleich, 2011). This would be ultimately sold to third party data brokers[95], as seen in **FIGURE *11***. In the midst of this business strategy, netizens are at the core, who are not only the extraction source, but also the end client.

[92] A milestone coined as *Surveillance Capitalism* (Zuboff, 2019)
[93] It started first with email services in 1971, later with BBS, the Usenet, IRC, Yahoo, Google, "The Facebook", and most lately Amazon.
[94] See Google's history and their relation with investors (Vise, 2007)
[95] Some of the largest data brokers world wide as in 2021 are: Oracle, Acxiom, and Verisk

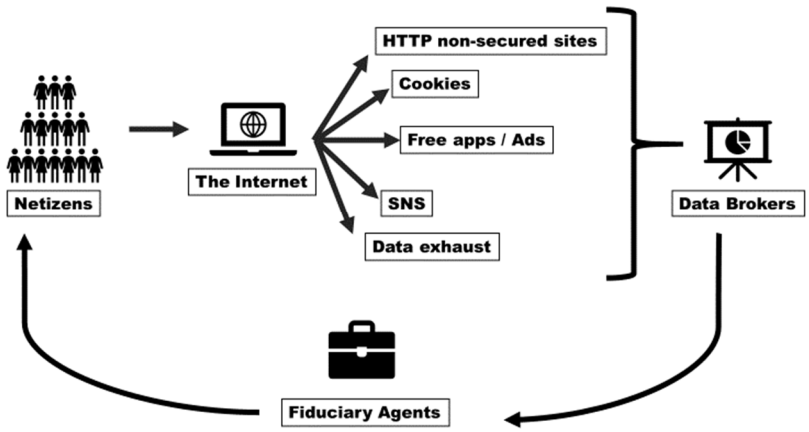

FIGURE 11: SURVEILLANCE CAPITALISM BUSINESS CYCLE. OWN MADE GRAPHIC

. For SNS, a big business competence, it is to make the platform as appealing to the end user so to harvest as much data as possible with disregard to above-described adverse effects nor a sustainable economy. The paper described in section 3.2 Weaponization and Securitization of SNS, how these are most effectively used as psychological apparatuses. User engagement is, to this end, another exploitation of the human psyche, often times the weakest link in the business cycle represented above (Sears et al., 2003).

In cybersecurity, the human is always the target as the cognitive layer in the information space is deemed equally, the weakest link of all three layers (Denno, 2016). For this reason, hackers[96] at both side of the spectrum[97] always put the netizen at the top of the pyramid as their main exploit target. States however, as seen in 3.3 SNS and IR Theory Applied to Cyberspace, due to IR anarchic arena constrains, tend to place national security in a first place (Patman & Southgate, 2016), leaving netizens exposed. SNS platforms, capitalize on this business advantage closing a highly toxic

[96] For purposes of this work, a hacker is a person who fully understands how a system works and acknowledges its vulnerabilities leaving up to his/her ethical standards the choice of whether to exploit these or not for personal gains.
[97] The spectrum refers to ethical constrains: *White hat hackers* are also known as ethical hackers whereas *black hat hackers* are known for illegal activities.

spiral that not only harvests and sells data; but also renders Big Tech the single most powerful social engineer (Hadnagy, 2010). This is particularly visible when such companies are allowed to self-regulate their content censoring what they consider goes against their definition of ethical standards (Nurik, 2019). It is also visible with the four philosophic foundations in understanding SNS seen at the beginning of this paper in **FIGURE *1*** (Qi et al., 2018).

The public not only has embraced this new way of communicating, but it has come to be an essential part in their lives (Beyens, Frison, & Eggermont, 2016) often not being aware of the privacy risks SNS entail. To some even, it is the only part of the Internet[98] they know and access on a regular basis. This user behaviour is in part fuelled by other agents in the economy where *disintermediation* has taken place. For instance, smartphones in conjunction with SNS have allowed the creation of new businesses that gradually have displaced traditional companies and shaped society to be SNS-friendly and dependent (van Dijck, 2013).

The threat to netizen's privacy and individual freedoms is implicit when their information is put for sale to the highest bidder (Schneier, 2015). SNS collect via algorithms, AI, and machine learning personal information within the three layers of the information environment: cognitive, virtual and physical (Nissen, 2015) as seen in the examples of **TABLE *1***. States in this scheme, may limit the capacity to who this information is sold and impose cooperation with their agencies by means of leaving *backdoors* opened or *zero-day* exploits untapped (Schneier, 2018). This again does not benefit the netizen nor democracy, but rather the SNS platforms and the state in a tacit deal to preserve the current social contract stability with the existing blueprints

[98] Notice how the Internet is commonly known to have a visible, invisible and "deep" part (Frediani, 2016)

in power and economic dynamics. The most representative example of this is 9-11. It transformed privacy perceptions and triggered a synchronization between public and private realms in an attempt to shield national security in the US.

COGNITIVE	VIRTUAL	PHYSICAL	PERSONAL IDENTIFICATORS
Listening habits	Cookies	Address	E-mail
Buying preferences	App data	Social circle	IMEI
Content uploaded	Metadata	GPS location patterns	Device Fingerprint
Socializing habits	IP address	Health and Fitness	IMSI
Ad interactions	Browsing history	Financial information	MAC address
Suggestions accepted	Quick sign-ins	Biometrics	UUID

TABLE 1: SNS DATA COLLECTION EXAMPLES. SOURCE: OWN MADE

Notice netizen's privacy is being bartered at the same time, in exchange of securing the *strategic narrative* of the state, while attempting to compromise other states in an international power skirmish. This has its effects in the free market, allowing for cybersecurity MNCs to enter into an offensive arms race, giving place to the security dilemma seen in 3.3 SNS and IR Theory Applied to Cyberspace. With the Web 3.0, privacy started to see a sudden decline, and with it, political[99], social and economic stability of the international community (Carlini, 2018).

Core technologies in SNS like AI and machine learning are curiously bringing liberal democracies and autocracies closer than ever before in the curtailing of individual freedoms. This is not a coincidence. Governments empowered with these

[99] Both autocracies and democracies are affected, regardless of the political system

technologies can understand their citizens and control them better while also forecasting patters of problematic behaviour (Wright, 2018). Here again is worth highlighting the example of China. She recognizes this implicitly in its *2017 AI Development Plan*, acknowledging the new opportunities AI brings in social construction, prediction, and control, at reasonable costs (Hoffman, 2018). When this model is not only implanted in Beijing, but also seeking clients where to export it abroad, it leaves the floor opened for a Neo-Cold-War struggle confronting once again two social systems.

By contrast, in the West, were free markets and liberal democracies are present, the debate is deeply controversial as it enters in direct confrontation with the definition of freedom. While one party and authoritarian states have a clear position in who should control the flow of information and social engineering, in the west, as seen in section 3.4 SNS, Economy and Future of Liberal Democracies; the debate is present between SNS, MNCs and the government. Furthermore, as the Industrial Revolution 4.0 settles, it is not yet clear whether a central planned AI enhanced economy, will have something new to offer in an ecosystem leaded by connected machines (Huang, Rust, & Maksimovic, 2019).

SNS maturity has so far been tackled with outdated regulation often struggling to catch up with the advances of technologies. Because of that, society has embarked in a one-way street trapped by the demons of growth, competitiveness, and efficiency. It is not yet clear regulation provides the best answers without engaging in a dystopia, by-product of a double bind between security, productivity, and social progress (Kass, 2001). Yet, under current forms of governance, it is clear AI must be constrained by all means to avoid it to escape human control (Nilsson, 2009). This path unfortunately leaves fewer choices for citizens willing to live in modern societies harmoniously.

4. CONCLUSIONS

While social engineering has traditionally been shaped using inherent human psychological flaws, the possibilities SNS has to offer in this area represent a qualitative milestone in terms of scope. Information has proved to be useful in disseminating ideas and boosting inventions, but in the wrong hands, it is also a dangerous asset to look after. There has been precedents in history that signal democratization of information does not necessarily lead to a better society, but rather, to its quick demise.

After this research, the paper has found that contemporary conflicts have an increasing IT component embedded as a result of an incapacity to control the spread of information over SNS. Available regulation models enters in contradiction with traditional freedoms of speech and press in liberal democracies. Members in society are double victims of a struggle between the social engineers facilitating the SNS platform, the state they belong to, and the foreign meddling done by third entities.

While democracies spend time and monetary resources figuring out a solution, other international actors use those very same SNS to create a foggy scenario that can unbalance the centre of gravity of the opponent in a divide and rule fashion. In such a scenario, this research finds the possibility of a clash in consolidated democracies very likely, particularly after the welfare state is slowly dismantled by higher levels of inequality.

A clear path to defend against SNS attacks is to anticipate them via intelligence collection. This nevertheless exploits the same weaknesses of social media and it paradoxically, achieves defence with offence moves as seen in section 3.2 Weaponization and Securitization of SNS. Entering this vicious spiral derives in a

security dilemma in the virtual layer; one that can also transcend to the cognitive and physical layers providing appropriate psy-ops exploit the strategic narrative of a state and its peoples.

The renaissance of communism-based ideologies as well as nationalistic parties all around Europe and the US is particularly worrying. People are embracing dogmas that seemed to be once and for all abandoned under new chiliastic rebranded mottos. Cyberspace being open to everyone, is the materialized utopia of a world without tangible borders where anyone, can push and shape an ideology creating turmoil to the core existence of a consolidated society. Like the Matrix, rulers and people with power, must admit utopias are not a possibility in this world and that the human nature is unequivocally chaotic.

Pragmatic regulation is the only viable path for now. The lack of action from governments to regulate on this issue accordingly, has left essentially SNS with the ability to be their own judges in a *de facto* monopoly service for political communication. This has derived in netizen's ambitions to flourish in a toxic environmental platform biased towards attention where bots and artificial technologies are the protagonists of human demise.

Cyberwar is both cheap and stealthy. The technology needed to launch a disinformation campaign evolves at a much faster pace than those technologies aimed at preventing it, hence the *arms race* dilemma. A few years ago, *sybil* armies were causing havoc among SNS users prior to an election. At the time of this research, *deep fakes* are the leading edge in impersonation technology with a vast influence potential in steering public opinion with SNS as their delivery vehicle.

The issues described in the body of this work are all considered a cyberthreat to national security. They undermine the basis of true democracy by spreading mass messages of disinformation as well as induce in manipulative practices. Consumers have little protection against these acts because often times, they do not seek the best quality information but rather the most easily available and tailored to their preferences. The responsibility is a shared burden between democratic governments not caring about empowering their citizens with freedom of knowledge, and the citizens themselves for believing the state's narrative. Nevertheless, the states have been victims at the same time of the fractional monetary system structure that governs us all.

Rogue states finding this theatre narrative loophole can exploit such vulnerabilities almost without limits. The Chinese have been aware of SNS advantages but played its cards slightly different. Considering Nissen's framework in **FIGURE *7***, China has limited utopian cyberspace globalization and halted Western SNS by acknowledging the dystopian harvesting of their citizen's data, another legitimate part of state sovereignty in their eyes. This, on the other hand, has not stopped the country from implementing heavy surveillance by sponsoring their own SNS and business conglomerates. Here, SNS pose another threat to democracies as Chinese core technologies, may also be weaponised and exported to expand influence and create dependence in a technological arms race towards the Industry 4.0.

The US acknowledges China as an asymmetric competitor and recognizes the current trajectory not being favourable to US interests[100]. Particularly, the US sees

[100] See leaked document: China Strategy. (2020). Assymetric Competition: A Strategy for China and Technology. Retrieved from https://assets.documentcloud.org/documents/20463382/final-memo-china-strategy-group-axios-1.pdf

China as attempting to supplant US technological dominance. While China is still dependent on the US, the question is how long will this advantage last at the current pace? With an increasing digital future, it seems likely the clash between the US and China will be taking place within the virtual realm, as seen in **FIGURE *10***.

As economic forecasts become a reality regarding Chinese economy, there are good reasons to think war is inevitable. The problem with globalization lies within the transition from periphery to core, and the danger it represents to the established hegemon in the form of the *Thucydides Trap*. With China actively avoiding the *middle-income trap*, this can be potentially dangerous to the current market-economy as it tends to disrupt the job market of developed economies, triggering a brain-drain that could eventually result in the stagnation of technological advances in traditional powers.

As a final conclusion to this research, the two research questions are now briefly responded bellow:

RQ1: In what ways does SNS act as a destabilization factor to the existing IR framework?

SNS are used actively as a psychological weapon within the cyberspace realm by a variety of actors non-exclusive to states. Since SNS are subject to be weaponized, governments consider them in their national security strategies which at the same time, impacts directly in the elaboration of FP and IR. While IR is anarchic, SNS operates within a free-market context lacking for the most part international regulation. Some states have already created specific policies expanding their sovereignty to the cyberspace realm including SNS. Other states are leaving this space unregulated and subject to MNCs acceptable use policies. This move leaves societies and

governments subject to foreign interference and the destabilization of consolidated democracies. The alternative is a hyper-vigilant state empowered with AI and machine learning algorithms derivated from SNS, that could menace traditional freedoms and potentially shape a new world order.

RQ2: To what extent is national security compromised by the absolute freedom of use in social media?"

Similar to what happened with the printing press revolution, the full democratization of information at all layers in society could spark a sudden change with potential disastrous consequences for a society. Individuals seeking profit derived from influence, can use SNS to manipulate others becoming new age mercenaries. Like media conglomerates in the past, newer actors have learnt how to modulate the message to their audience seeking their attention over information quality.

The seek for truth has become a hunt not worth the effort for the average citizen. In advanced highly specialized economies, citizens are constantly bombarded with information and constrained by time. Their competitive advantage does not allow them to contrast information and seek the freedom to think for themselves. SNS have effectively exploited the human condition and the social structure, which compromises accordingly the national security of a state if left unchecked.

States have not found a balanced option. This research can extract as a final conclusion, that it will be the tipping point for the state to maximize its realms cutting down individual liberties in favour of national security. In other words, assuring the state and its elites remain for as long as possible without detriment of what is to happen to the mass of its society.

Exploring possible recommendations to avoid entering a point of no return, there is an existing debate between advocates for regulation of SNS and others that would ban them entirely. On a personal note, societies that strive are well educated and empowered to know how to discriminate between good and bad information. This model passes by abandoning party politics and caring for actual society progress displaying above all transparency. For this to work, democracy needs to be redefined radically by reshaping personal incentives together with the checks and balances between the three powers.

Solving the political problem, it would be the turn for the economic incentives. SNS as companies, its primary objective is to make profit. Selling user's privacy to other companies that sell their products and services back to the users is a model that harms the creativity and capacity to think freely. Furthermore, *the economics of popularity* seen in SNS allow for a user competition in attention within the SNS cyberspace. This is canalized in a format previously agreed upon by these same platforms which of course does not favour freedom of thought as such. The economic problem unfortunately, is something that would require macroeconomic adjustment at an international scale.

The last solution concerns ethics. SNS should be bound to state its political leaning to its users as a simple way for them to make an informed decision when signing up for a particular platform. This would allow to break the whole ecosystem of massive SNS oligopolies and for smaller competitors to jump in. Breaking these modern day Silicon Valley *zaibatsus* would also break the popularity incentives and allow for a healthier cyberspace. With this, foreign interference would also be harder to achieve as the pool of users would be diversified in different chambers without the ability to echo one another.

5. BIBLIOGRAPHY

Adams, C. (2018). Learning the lessons of WannaCry. *Computer Fraud & Security*, *2018*(9), 6–9. https://doi.org/10.1016/S1361-3723(18)30084-8

Agbozo, E., & Spassov, K. (2019). Social media as a trigger for positive political action: The case of Ghana's fight against illegal small-scale mining (Galamsey). *African Journal of Science, Technology, Innovation and Development*, *11*(5), 611–617. https://doi.org/10.1080/20421338.2018.1557369

Aguilera Diaz, V., & Seisdedos, C. (2020). *Open Source INTelligence (OSINT): Investigar personas e Identidades en Internet*. Oxword.

Aid, M. M. (2009). *The secret sentry: The untold history of the National Security Agency*. Bloomsbury Publishing USA.

Almond, G. A. (1956). Comparative Political Systems. *The Journal of Politics*. https://doi.org/10.2307/2127255

Anderson, B. R. O. (Benedict R. O. (2006). *Imagined communities : reflections on the origin and spread of nationalism* (Rev. ed.). London ; New York ; Verso.

Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society*, *54*(2), 138–149.

Baños, P. (2017, December 13). Ciberespionaje, influencia política y desinformación (I) - El Orden Mundial - EOM. *El Orden Mundial*. Retrieved from https://elordenmundial.com/ciberespionaje-influencia-politica-y-desinformacion-i/

Baños, P. (2020). *El Dominio Mental*. Ariel.

Barnea, A. (2017). Counterintelligence: stepson of the intelligence discipline. *Israel Affairs*, *23*(4), 715–726. https://doi.org/10.1080/13537121.2017.1333725

Bateson, G. (2000). *Steps to an ecology of mind* (University). Chicago: Chicago : University of Chicago Press.

Baum, M. A., & Potter, P. B. K. (2019). Media, public opinion, and foreign policy in the age of social media. *Journal of Politics*. https://doi.org/10.1086/702233

Bauman, Z. (2013). Europe is trapped between power and politics. *Roadmap to a Social Europe*, 14.

Baylis, J., Smith, S., & Owens, P. (2020). *The globalization of world politics : an introduction to international relations.* (Eighth edi). Oxford University Press.

Bennett, W. L., Segerberg, A., & Knüpfer, C. B. (2018). The democratic interface: technology, political organization, and diverging patterns of electoral representation. *Information Communication and Society*, *21*(11), 1655–1680. https://doi.org/10.1080/1369118X.2017.1348533

Beyens, I., Frison, E., & Eggermont, S. (2016). "I don't want to miss a thing": Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress. *Computers in Human Behavior*, *64*, 1–8.

Birdsall, N., De La Torre, A., & Caicedo, F. V. (2012). The Washington Consensus: Assessing A "damaged Brand." In *The Oxford Handbook of Latin American Economics*. https://doi.org/10.1093/oxfordhb/9780199571048.013.0004

Bolt, P. J., & Gray, A. K. (2007). *CHINA'S NATIONAL SECURITY STRATEGY*.

Bourdieu, P. (2018). The forms of capital. In *The Sociology of Economic Life, Third Edition*. https://doi.org/10.4324/9780429494338

Bowman, K. M., Freud, S., & Riviere, J. (1928). The Ego and the Id. *The American Journal of Psychology*. https://doi.org/10.2307/1414355

Brühl, V. (2020). Libra — A Differentiated View on Facebook's Virtual Currency Project. *Inter Economics*, *55*(1), 54–61. https://doi.org/10.1007/s10272-020-0869-1

Burt, A. (2010). Taking cyber action: Operation Buckshot Yankee Spurred Creation of CYBERCOM. *Inside the Pentagon's inside the Navy*, *23*(35), 3.

Butlin, F. M., Rousseau, J. J., Tozer, H. J., & Bosanquet, B. (1895). The Social Contract on Principles of Political Right. *The Economic Journal*. https://doi.org/10.2307/2956638

Butterfield, H. (1975). *Raison d'etat : the relations between morality and government*. Brighton]: University of Sussex.

Buzan, B. (2018). How and How Not to Develop IR Theory: Lessons from Core and Periphery. *The Chinese Journal of International Politics*, *11*(4), 391–414.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, *17*, 22.

Cai, F. (2012). Is There a ″Middle-income Trap″? Theories, Experiences and Relevance to China. *China & World Economy*, *20*(1), 49–61.

Carlini, A. (2018). Las redes sociales como factor de desestabiización. *Instituto Español de Estudios Estratégicos*, *79*.

Carlyle, T. (1901). *On heroes, hero-worship and the heroic in history.* (H. D. (Henry D. Traill, Ed.). New York : C. Scribner's Sons.

CCP. (2013). Document 9: A ChinaFile Translation | ChinaFile. Retrieved January 20, 2021, from https://www.chinafile.com/document-9-chinafile-translation

Clausewitz, C. von. (2008). *On War.* Princeton: Princeton University Press.

Clemons, E. K. (2009). The complex problem of monetizing virtual electronic social networks. *Decision Support Systems*, *48*(1), 46–56.

CN-CERT. (2019). Disinformation in Cyberspace. *National Cryptologic Centre*, *Buenas Pra*(13), 33. Retrieved from https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3561-ccn-cert-bp-13-disinformation-in-cyberspace-1/file.html

Connor, C. O., & Weatherall, J. O. (2019). Why we trust lies: The most effective misinformation starts with seeds of truth. *Scientific American*.

Delli Carpini, M. X. (2005). An overview of the state of citizens' knowledge about politics. *Departmental Papers (ASC)*, 53.

Denno, J. (2016). *Attacking the human-the weakest link in cybersecurity*. Utica College.

Deudney, D., & Ikenberry, G. J. (1999). The nature and sources of liberal international order. *Review of International Studies*. https://doi.org/10.1017/S0260210599001795

Devlin, M., & Brown, N. (2021). Voters are starting to act like hard-core sports fans –

with dangerous repercussions for democracy. Retrieved March 21, 2021, from The Conversation website: https://theconversation.com/voters-are-starting-to-act-like-hard-core-sports-fans-with-dangerous-repercussions-for-democracy-153175

Donnelly, J. (2000). *Realism and international relations*. Cambridge University Press.

Donovan, J., & boyd, danah. (2021). Stop the Presses? Moving From Strategic Silence to Strategic Amplification in a Networked Media Ecosystem. *American Behavioral Scientist*, *65*(2), 333–350. https://doi.org/10.1177/0002764219878229

Doyle, M. W. (1986). Liberalism and world politics. *American Political Science Review*. https://doi.org/10.1017/S0003055400185041

Eisenstein, E. L. (1980). The Printing Press as an Agent of Change. In *The Printing Press as an Agent of Change*. https://doi.org/10.1017/cbo9781107049963

Engesser, S., Ernst, N., Esser, F., & Büchel, F. (2017). Populism and social media: how politicians spread a fragmented ideology. *Information, Communication & Society*, *20*(8), 1109–1126. https://doi.org/10.1080/1369118X.2016.1207697

Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*. https://doi.org/10.1080/19331681.2021.1905972

Ferguson, N. (2010). Why the West Rules-for Now: The Patterns of History, and What They Reveal About the Future. *Foreign Affairs*, *89*(6), 197.

Fergusson, N. (2009). *The ascent of money: A financial history of the world*. https://doi.org/10.1007/bf03395689

Ferrara, E. (2017). *DISINFORMATION AND SOCIAL BOT OPERATIONS IN THE RUN UP TO THE 2017 FRENCH PRESIDENTIAL ELECTION*.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96–104. https://doi.org/10.1145/2818717

Flemming, M. (2020). The Tech Trojan Horse. China's Strategic Export of the Surveillance State. *The Project on International Peace and Security*, *12*(3). Retrieved from https://www.wm.edu/offices/global-research/research-labs/pips/white_papers/2019-2020/flemming-final.pdf

Frediani, C. (2016). *Deep Web, going beneath the surface*.

Fritsch, S. (2011). Technology and Global Affairs. *International Studies Perspectives*, *12*(1), 27–45.

Fukuyama, F. (2006). *The end of history and the last man* (1st Free P). New York: Free Press ;

Fukuyama, F. (2015). The end of history? In *Conflict After the Cold War: Arguments on Causes of War and Peace*. https://doi.org/10.5840/tpm20022019

Galeotti, M. (2019). The mythical 'Gerasimov Doctrine' and the language of threat. *Critical Studies on Security*, *7*(2), 157–161. https://doi.org/10.1080/21624887.2018.1441623

Geoestrategia. (2021). La UE y EE.UU. imponen sus ridículas sanciones contra Rusia por el caso de Alexéi Navalny. Moscú responde a EEUU: "No juegues con fuego."

Retrieved May 2, 2021, from El Espia Digital website: http://www.geoestrategia.es/index.php/noticias/historico-de-noticias/33223-2021-03-03-12-05-10

Giles, A. (2020). *"Valery Gerasimov's Doctrine."* https://doi.org/10.13140/RG.2.2.10944.35848

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Gleich, J. (2011). How Google Dominates Us. *New York Review of Books*.

Goffman, E. (2016). The presentation of self in everyday life. In *Social Theory Re-Wired: New Connections to Classical and Contemporary Perspectives: Second Edition*. https://doi.org/10.4324/9781315775357

Goldberg, J. (2020, November). Why Obama Fears for Our Democracy - The Atlantic. Retrieved April 30, 2021, from The Atlantic website: https://www.theatlantic.com/ideas/archive/2020/11/why-obama-fears-for-our-democracy/617087/

Grauwe, P. de. (2017). *The limits of the market : the pendulum between government and market* (First edit).

Gutmann, E. (2010). HACKER NATION: China's Cyber Assault. *World Affairs (Washington)*, *173*(1), 70–79. https://doi.org/10.3200/WAFS.173.1.70-80

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. *The Art of Human Hacking*.

Haidt, J. (2012). *The righteous mind: Why good people are divided by politics and religion*. Vintage.

Han, G. (2007). Mainland China frames Taiwan: How China's news websites covered Taiwan's 2004 presidential election. *Asian Journal of Communication*, *17*(1), 40–57.

Hardin, G. (2009). The tragedy of the commons. *Journal of Natural Resources Policy Research*. https://doi.org/10.1080/19390450903037302

Harvard. (2020). *The Media Manipulation Casebook Code Book*.

Hauben, M. (1997). *Netizens : on the history and impact of usenet and the internet*. Los Alamitos, Calif.: IEEE Computer Society Press.

Hayek, F. A. von (Friedrich A. (2001). *The road to serfdom*.

Heidegger, M. (1993). Basic writings : from Being and time (1927) to The task of thinking (1964). *His Works*.

Herman, E. S., & Chomsky, N. (1988). Manufacturing consent: A propaganda model. *Manufacturing Consent*.

Herz, J. H. (1951). *Political realism and political idealism : a study in theory and realities*. Chicago: Chicago : Chicago University Press.

Hetherington, M. J., & Husser, J. A. (2012). How Trust Matters: The Changing Political Relevance of Political Trust. *American Journal of Political Science*. https://doi.org/10.1111/j.1540-5907.2011.00548.x

Heuer, R. J. (1999). Psycology Intelligence Analysis. In *Centre for the Study of Intelligence*.

Hey, T., & Papay, G. (2014). Licklider's Intergalactic Computer Network. In *The Computing Universe*. https://doi.org/10.1017/cbo9781139032643.013

Higgins, E. (2021). *We Are Bellingcat: An Intelligence Agency for the People* (1st ed.). Bloomsbury.

Hoffman, S. (2018). Managing the state: Social credit, surveillance and the CCP's plan for China. *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative*, 42.

Holsti, O. R. (1992). Public Opinion and Foreign Policy: Challenges to the Almond-Lippmann Consensus. *International Studies Quarterly*.

Huang, M.-H., Rust, R., & Maksimovic, V. (2019). The feeling economy: Managing in the next generation of artificial intelligence (AI). *California Management Review*, *61*(4), 43–65.

Huerta de Soto, J. (1998). Dinero, Crédito Bancario y Ciclos Económicos. In *Revista de Economía Aplicada*.

Huth, P. K. (1999). DETERRENCE AND INTERNATIONAL CONFLICT: Empirical Findings and Theoretical Debates. *Annual Review of Political Science*, *2*(1), 25–48. https://doi.org/10.1146/annurev.polisci.2.1.25

Huxley, A. (2014). *Brave new world*.

IKENBERRY, G. J. (2020). A World Safe for Democracy: Liberal Internationalism and the Crises of Global Order. In *A World Safe for Democracy*. New Haven: Yale University Press.

Iyengar, S., Sood, G., & Lelkes, Y. (2012). Affect, not ideologya social identity perspective on polarization. *Public Opinion Quarterly*, *76*(3), 405–431.

Jasper, S. (2020). *Russian Cyber Operations: Coding the Boundaries of Conflict*. Georgetown University Press.

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics*, *30*(2), 167–214. https://doi.org/10.2307/2009958

Johnson, M. (2021, February 24). Cognitive Breakdown: The Navalny Hoax, American Imperialism and Media Censorship | Katehon think tank. Geopolitics & Tradition. Retrieved May 2, 2021, from Katehon website: https://katehon.com/en/article/cognitive-breakdown-navalny-hoax-american-imperialism-and-media-censorship

Johnson, N. F. (2003). *Financial market complexity*. Oxford: Oxford University Press.

Kania, E. B., & Costello, J. K. (2017). Quantum technologies, US-China strategic competition, and future dynamics of cyber stability. *2017 International Conference on Cyber Conflict (CyCon US)*, 89–96. IEEE.

Kass, L. (2001). Preventing a brave new world. *The New Republic*, *5*(01), 1–17.

Khattak, S., Javed, M., Khayam, S. A., Uzmi, Z. A., & Paxson, V. (2014). A look at the consequences of internet censorship through an isp lens. *Proceedings of the 2014 Conference on Internet Measurement Conference*, 271–284.

Klein, E. (2011). The dangers of misinterpreting Keynes. *The Washington Post*.

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, *77*(6), 1121–1134.

https://doi.org/10.1037/0022-3514.77.6.1121

Kumar, V. D. (2019). Beyond Dunning–Kruger Effect: Undermining the Biases Which Would Lead to Flawed Self-assessment Among Students. *Medical Science Educator*, *29*(4), 1155–1156. https://doi.org/10.1007/s40670-019-00806-1

Kurra, B. (2011, September 11). How 9/11 Completely Changed Surveillance in U.S. | WIRED. Retrieved March 29, 2021, from Wired website: https://www.wired.com/2011/09/911-surveillance/

Lachmann, L. M. (Ludwig M. (1978). *Capital and its structure*. Kansas City: S. Andrews and McMeel.

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., … Zittrain, J. L. (2018). The science of fake news: Addressing fake news requires a multidisciplinary effort. *Science*, *359*(6380), 1094–1096. https://doi.org/10.1126/science.aao2998

Lee, J. (2019). Did Thucydides Believe in Thucydides' Trap? The History of the Peloponnesian War and Its Relevance to U.S.-China Relations. *Chinese Journal of Political Science*, *24*(1), 67–86.

Lee, J. K., Choi, J., Kim, C., & Kim, Y. (2014). Social media, network heterogeneity, and opinion polarization. *Journal of Communication*, *64*(4), 702–722.

Levitsky, S., & Ziblatt, D. (2018). *How Democracies Die*. New York: Crown.

Levy, R. (2021). Social media, news consumption, and polarization: Evidence from a field experiment. *American Economic Review*, *111*(3), 831–870.

Li, L. (2018). China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0." *Technological Forecasting & Social Change*, *135*, 66–74.

Liang, Q., & Wang, X. (2002). *Unrestricted Warfare: China's Master Plan to Destroy America*. Newsmax.com.

Libicki, M. (2011). The Nature of Strategic Instability in Cyberspace. *The Brown Journal of World Affairs*, *18*(1), 71–79.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND corporation.

Liff, A. P. (2012). Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, *35*(3), 401–428.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lippmann, W. (2017). Public opinion. In *Public Opinion*. https://doi.org/10.4324/9781315127736

Loeb, V. (2001). NSA Adviser Says Cyber-Assaults On Pentagon Persist With Few Clues: FINAL Edition. *The Washington Post*.

López-Pujalte, C., & Nuño-Moral, M. V. (2020). La "infodemia" en la crisis del coronavirus: Análisis de desinformaciones en España y Latinoamérica. *Revista Española de Documentación Científica*. https://doi.org/10.3989/redc.2020.3.1807

Luceri, L., Deb, A., Giordano, S., & Ferrara, E. (2019). Evolution of bot and human behavior during elections. *First Monday*. https://doi.org/10.5210/fm.v24i9.10213

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29–41.

Maurer, D. (2017). *ADVANCING STRATEGIC THOUGHT SERIES The Clash of the Trinities: A New Theoretical Analysis of the General Nature of War*. Retrieved from https://tjaglcspublic.army.mil/documents/27431/1942420/MAJ+Dan+Mauerer+PUB1365+Clash+of+the++Trinities.pdf/39a51dd9-56c9-4e89-8c0d-1f3ce77c5718

Mazali, T., & Mazali, T. (2018). From industry 4.0 to society 4.0, there and back. *AI & Society*, *33*(3), 405–411. https://doi.org/10.1007/s00146-017-0792-6

Mearsheimer, J. J. (2001). Anarchy and the Struggle for Power. *The Tragedy of Great Power Politics*.

Mearsheimer, J. J. (2014). *The tragedy of great power politics* (Updated ed).

Menger, K. (1892). On the Origin of Money. *The Economic Journal*, 239–255. https://doi.org/10.2307/2956146

Michels, R. (2019). The iron law of oligarchy. In *Power in Modern Societies*. https://doi.org/10.4324/9780429302824-13

Moloney, P. (2020). *TikTok: Technology Overview and Issues*. Retrieved from https://crsreports.congress.gov

Moore, J. (1998). Hard choices: moral dilemmas in humanitarian intervention. In *Hard choices*. Lanham, MD: The Rowman & Littlefield Publishing Group.

Mulligan, S. P. (2018). *Cross-border data sharing under the CLOUD Act*. Congressional Research Service.

Munger, K. (2020). All the News That's Fit to Click: The Economics of Clickbait Media. *Political Communication*, *37*(3), 376–397.

Muzellec, L., Ronteau, S., & Lambkin, M. (2015). Two-sided Internet platforms: A business model lifecycle perspective. *Industrial Marketing Management*, *45*, 139–150. https://doi.org/10.1016/j.indmarman.2015.02.012

Nato. (2001). Nato Open Source Intelligence Handbook. *Skeletal Radiology*.

Newman, P. (2019). Taking Government Out of Politics: Murray Rothbard on Political and Local Reform During the Progressive Era. *Quarterly Journal of Austrian Economics*, *22*(1), 49–67.

Nichols, J. (2005). *Tragedy and farce : how the American media sell wars, spin elections, and destroy democracy*. New York: New Press : Distributed by W.W. Norton.

Nietzsche, F. W. (1977). *Thus spoke Zarathustra : a book for everyone and no one* (R. J. Hollingdale, Ed.). Harmondsworth, England: Harmondsworth, England.

Nilsson, N. J. (2009). *The quest for artificial intelligence*. Cambridge University Press.

Nissen, T. E. (2015). The Weaponization Of Social Media - Characteristics of Contemporary Conflicts. In *Royal Danish Defence College*.

Nurik, C. (2019). "Men Are Scum": Self-Regulation, Hate Speech, and Gender-Based Censorship on Facebook. *International Journal of Communication*, *13*, 21.

O'Neil, C. (2017). How can we stop algorithms telling lies? *The Guardian*.

O'Neil, C., & Schutt, R. (2015). Doing Data Science: Straight Talk from the Frontline.

In *The effects of brief mindfulness intervention on acute pain experience: An examination of individual difference*.

Ogunseitan, O. A., Schoenung, J. M., Saphores, J.-D. M., & Shapiro, A. A. (2009). The Electronics Revolution: From E-Wonderland to E-Wasteland. *Science (American Association for the Advancement of Science)*, *326*(5953), 670–671. https://doi.org/10.1126/science.1176929

Orriols, L., & Balcells, L. (2012). Party polarisation and spatial voting in Spain. *South European Society and Politics*, *17*(3), 393–409.

Orttung, R. W., & Nelson, E. (2019). Russia Today's strategy and effectiveness on YouTube. *Post-Soviet Affairs*, *35*(2), 77–92.

Orwell, G. (1949). *1984.*

Parello-Plesner, J. (2018). China's LinkedIn Honey Traps. Retrieved April 13, 2021, from Hudson Institute website: https://www.hudson.org/research/14637-china-s-linked-in-honey-traps

Pashakhanlou, A. H. (2017). *Realism and fear in international relations : Morgenthau, Waltz and Mearsheimer reconsidered*.

Patman, R. G., & Southgate, L. (2016). National security and surveillance: the public impact of the GCSB Amendment Bill and the Snowden revelations in New Zealand. *Intelligence and National Security*, *31*(6), 871–887.

Piers, R. (2005). The CNN effect: The myth of news, foreign policy and intervention. In *The CNN Effect: The Myth of News, Foreign Policy and Intervention*. https://doi.org/10.4324/9780203995037

Prensky, M. (2001). *Digital Natives, Digital Immigrants* (Vol. 9). MCB University Press.

Priebe, M., Rooney, B., Beauchamp-Mustafaga, N., Martini, J., & Pezard, S. (2021). *Implementing Restraint: Changes in U.S. Regional Security Policies to Operationalize a Realist Grand Strategy of Restraint*. https://doi.org/10.7249/RRA739-1

Qi, J., Monod, E., Fang, B., & Deng, S. (2018). Theories of Social Media: Philosophical Foundations. *Engineering*, *4*(1), 94–102. https://doi.org/10.1016/j.eng.2018.02.009

Rid, T. (2013). *Cyber war will not take place*. London: Hurst.

Rocamora, P. (2011). *Psicología de la sugestión en Freud. Un análisis de poder y el sometimiento*. Madrid: Manuscritos.

Sampedro, V. (2014). Podemos, de la invisibilidad a la sobre-exposición. *Teknocultura*, *12*(1). Retrieved from https://revistas.ucm.es/index.php/TEKN/article/view/48890/45616

Sartre, J. P., Cohen-Solal, A., & Elkaïm-Sartre, A. (2007). Existentialism is a humanism. In *Existentialism Is a Humanism*. https://doi.org/10.2307/j.ctv15vwkgx.5

Schäfer, S. (2020). Illusion of knowledge through Facebook news? Effects of snack news in a news feed on perceived knowledge, attitude strength, and willingness for discussions. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2019.08.031

Schnaufer, T. A. (2017). Redefining hybrid warfare: Russia's non-linear war against

the West. *Journal of Strategic Security*, *10*(1), 17–31.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Schneier, B. (2018). *Click here to kill everybody : security and survival in a hyper-connected world* (First edit).

Schwab, K., & Malleret, T. (2020). The Great Reset. *World Economic Forum, Geneva*.

Schweller, R. L. (1994). Schweller, Randall. *International Security*.

Scot Tanner, M. (2017). Beijing's New National Intelligence Law: From Defense to Offense. Retrieved April 13, 2021, from Lawfare website: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

Sears, D. O., Huddy, L., & Jervis, R. L. (2003). The psychologies underlying political psychology. *The Oxford Handbook of Political Psychology*.

Segaller, S. (1998). *Nerds 2.0.1 : a brief history of the internet*. New York: New York : TV Books.

Shlapentokh, D. (2019). The Time of Troubles in Alexander Dugin's Narrative. *European Review (Chichester, England)*, *27*(1), 143–157.

Singer, P. . (2018). *LikeWar: The Weaponization of Social Media | P.W. Singer, Emerson T. Brooking | download* (Hardcover). Retrieved from https://1lib.eu/book/3604497/844f44

Stacks, J. F. (2004). Hard Times for Hard News: A Clinical Look at U.s. Foreign Coverage. *World Policy Journal*, *20*(4), 12–21.

Suchkov, M. A. (2021). Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice. *Small Wars & Insurgencies*, 1–26.

Taylor, P. M. (1995). *Munitions of the mind : a history of propaganda from the ancient world to the present day*. Manchester: Manchester : Manchester University Press.

Thornton, R. (2007). *Asymmetric warfare: Threat and response in the 21st century*. Polity.

Tolstoy, A., & McCaffray, E. (2015). MIND GAMES: Alexander Dugin and Russia's War of Ideas. *World Affairs (Washington)*, *177*(6), 25–30.

Torres-Lugo, C., Yang, K.-C., & Menczer, F. (2020). *The Manufacture of Political Echo Chambers by Follow Train Abuse on Twitter*. Retrieved from http://arxiv.org/abs/2010.13691

Tzu, S. (2012). *Sun Tzu Art of War*. Vij Books India Pvt Ltd.

van Dijck, J. (2013). The Culture of Connectivity: A Critical History of Social Media. In *The Culture of Connectivity*. New York: Oxford University Press.

Véliz, C. (2019). The internet and privacy. In *Ethics and the Contemporary World*. https://doi.org/10.4324/9781315107752-12

Vernon, R. (1979). The product cycle hypothesis in a new international environment. *Oxford Bulletin of Economics and Statistics*, *41*(4), 255–267.

Vise, D. (2007). The google story. *Strategic Direction*.

Vittori, D. (2020). Membership and members' participation in new digital parties: Bring back the people? *Comparative European Politics*, *18*(4), 609–629. https://doi.org/10.1057/s41295-019-00201-5

Von Mises, L. (2012). The theory of money and credit. In *The Theory of Money and Credit*. https://doi.org/10.2307/2607539

Winthrop, D. (2019). *Aristotle, democracy and political science*.

Wojtasik, K. (2017). How and Why Do Terrorist Organizations Use the Internet? *Polish Political Science*, *46*(2), 105–117. https://doi.org/10.15804/ppsy2017207

World Bank. (2005). *The Dot-Com Bubble, The Bush Deficits, And The U.S. Current Account*. World Bank.

Wright, N. (2018, July 10). How Artificial Intelligence Will Reshape the Global Order. Retrieved April 29, 2021, from Foreign Affairs website: https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order

Wylie, C. (2019). *Mindf*ck : Cambridge Analytica and the Plot to Break America*. Retrieved from http://ezproxy.universidadeuropea.es/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2212276&lang=es&site=ehost-live&scope=site

Yang, K.-C., Torres-Lugo, C., & Menczer, F. (2020). Prevalence of low-credibility information on twitter during the covid-19 outbreak. *ArXiv Preprint ArXiv:2004.14484*.

Yang, K. C., Varol, O., Davis, C. A., Ferrara, E., Flammini, A., & Menczer, F. (2019). Arming the public with artificial intelligence to counter social bots. *Human Behavior and Emerging Technologies*, *1*(1), 48–61. https://doi.org/10.1002/hbe2.115

Zuboff, S. (2019). *The Age of Surveillance Capitalism*.

Корыбко, Э., & Савин, Л. (2021). THE END OF PAX AMERICANA AND THE RISE OF MULTIPOLARITY. *Сравнительная Политика*, *12*(1), 167–173.

6. ANNEX: WEAPONIZATION OF SNS, EXAMPLES

China's LinkedIn Honey Traps: Designed to target westerners with high profiles in key strategic industries with highly attractive packages to serve CCP's interests effectively turning them in spies with or without their implicit knowledge (Parello-Plesner, 2018).

COVID-19 disinformation campaigns and echo chambers: Creation of low credibility content in Twitter regarding COVID in different states with the intention of politicizing the pandemic and increase polarization. Content is first manufactured and then spread at a massive scale with the use of bots (K.-C. Yang, Torres-Lugo, & Menczer, 2020) (López-Pujalte & Nuño-Moral, 2020).

Elections and SNS campaigning: Manufacturing of political echo chambers in SNS before, during and after the campaign to seize the intention to vote for a particular candidate (Torres-Lugo, Yang, & Menczer, 2020) (Engesser, Ernst, Esser, & Büchel, 2017).

Tik-Tok ban in India: Chinese national intelligence law (Scot Tanner, 2017) holds Chinese SNS enterprises accountable for providing access, cooperation and support with Chinese intelligence if required. This allows for possible back doors and zero-day attacks that could potentially clash between the sovereignty of China over Indian citizens.

Isis cyber-extremism and recruitment via SNS: The example of a non-state actor and its success in using SNS to spread propaganda and ideology from the virtual layer, to the cognitive and physical spaces worldwide (Awan, 2017).

The Macron leaks case in the French presidential election and the use of black market reusable political bots: Disinformation campaigns originated out of France

with an alternative-right theme. Coordinated by a mix of bots and organic behaviour in an attempt to legitimate the account as a human user so to manipulate public opinion redirecting it to alternative or fabricated sources (Ferrara, 2017).

Cambridge Analytica and Brexit: Collection of personal information from FB profiles via *thisisyourdigitallife* app engineered in collaboration with Cambridge Analytica to engineer the most successful political campaign accordingly (Cadwalladr & Graham-Harrison, 2018).