Posted on the CEEEP website

Date: August 4, 2022

Social Media, Geopolitics and Power

Gonzalo Javier Rubio Piñeiro

This article has been initially published in the ***Revista Seguridad y Poder Terrestre***
Vol. 1 N.° 1 (2022): July – September
DOI: https://doi.org/10.56221/spt.v1i1.6

Abstract

Cyberspace is presented as a virtual area practically free of restrictions, gaining relevance for both leisure and work, not to mention the increase in cybercrime. Unfortunately, areas such as poverty, malnutrition and insecurity are not relevant to geopolitical analyses of the countries that fight for hegemony, but power and influence are. Geopolitical relationship and social networks are framed in the need to exert influence and project the power of state actors of international weight, such as the United States, the People's Republic of China and Russia. This situation makes it clear that States continue to be significant actors in world politics, mainly those that have developed important capacities and tools for the protection of their interests, among which is the Information War.

Keywords: Social networks, geopolitics, disinformation, platforms, power.

Introduction

Social Media is constantly growing along with technologies which work as platforms. These processes tend to change not only the way people communicate but also the pre-existing communication paradigms, aspects that are present in the strategies of developed countries. In this sense, this article analyzes the relationship between social media, geopolitics and power, taking as a case study the accession of Crimea to Russia, and examining the impact of the pandemic caused by the SARS-COV2 virus as an accelerator of processes. In addition, it infers on the intensification of the use of social media and virtual reality, as well as analyzing the relationship between the United States and the People's Republic of China (PRC) within what would be the beginning of a New Cold War.

Social Media

A study by the NYU Stern Center for Business and Human Rights, entitled "Combatting Russian Disinformation: The Case for Stepping Up the Fight Online," lists the enormous benefits of democratizing Internet information. However, it also demonstrates that social media and Internet search platforms are vulnerable to political misinformation.[1] The latter situation was evidenced during Crimea's accession to Russia, where Russian intelligence used social media to influence various target audiences (politicians, military and civilians, both Russian and

Ukrainian) in order to gain a tangible advantage on the battlefield.[2] To do so, the Russians operated through a variety of platforms, taking advantage of the multiplier effect of social media and trolls, who operate from facilities known as troll factories or troll farms.[3]

For the British-American political geographer John Agnew, in the modern geopolitical imagination, power has been narrowly defined as the ability to compel others to do something that a person or state wants, increasingly relating to territorial states, at least since the 19th century.[4] In this context, the model that fits the "contemporary societies-social media" relationship is the Integrated World Society,[5] where the nodes are the social groupings.[6] In this humanistic and utopian ideal in which priority is given to communication on a global scale - based on social media between diverse actors - there is the possibility of directing public opinion in pursuit of state and non-state needs, with spontaneous responses. Therefore, it can be said that any social actor - taking advantage of the properties of a more interconnected world - can use virtual spaces to influence the decisions of others to achieve their own interests.

Accession of Crimea to Russia

While Crimea may have been the battleground between Ukraine and Russia, the dispute also played out in cyberspace, where both governments stepped up their covert operations during the contest.[7] On the one hand, Russian operations in Ukraine coincided with the development of actions by pro-Russian factions under the hashtag #OpRussia. On the other hand, a counter faction promoted its cause with the hashtag #OpUkraine. Both sides hacked each other's websites, forums, and government sites to disrupt the other side's ability to wage conflict, while Russian rebels engaged Ukrainian forces in a conventional manner.[8]

Over the past decade, Russia forcibly annexed the Crimea region and backed pro-Russian separatist insurgents in eastern Ukraine. These bold actions were accompanied by disinformation spread through Facebook and its Russian equivalent VKontakte. As a precursor to interference in Western Europe and the United States, agents of the Russian Military Intelligence Agency, known as the GRU, created fake social media accounts to simulate popular Ukrainian hostility toward the pro-Western government in Kiev. Likewise, pro-Russian hackers attacked Ukrainian election computers in an attempt to prevent a far-right fringe party from winning the presidency.[9]

Apparently, mankind has changed the way interpersonal relationships are practiced. Human beings have exposed their intimacies into social media, becoming members of an authentic digital "Big Brother", where they encounter mirrors of their own selves.[10] However, the current global commerce is practically a war with other media because the global viral power causes deaths and refugees as if it were a real world war.[11] In this regard, while the European Union rejected the condition requested by Ukrainian President Viktor Yanukovych to sign the Association Agreement (that he be granted $27 billion in aid), Russia seized the opportunity and rewarded Yanukovych's last-minute change,

establishing an agreement in which Russia would buy Ukrainian government bonds worth $15 billion, while offering a 33% reduction in gas price. In this way, Kiev's urgencies were alleviated in short term, and it was shown to the world that the Kremlin was not willing to abandon Ukraine.[12] This move was viralized in traditional and non-traditional Mass Media (MMC), as part of the Russian communicational maneuver.

Today, with the Made in China 2025 plan, the Asian giant aims to become the world's leading technological power. Since Xi Jinping came to power, in parallel, with the growing economic role, the PRC has moved from a passive to a more active role in international relations. This strategy is materialized in projects of international impact, such as the New Silk Road, 5G technology - Huawei or the creation of the Asian Infrastructure Investment Bank, presenting themselves as alternative multilateral configurations to those led by the United States[13]. This situation expands the relationship between social media, its platforms and economic sectors with an appetite for controlling the narrative.

SpaceX and Starlink projects

In 2018, the U.S. Federal Communications Commission granted permission to Space Exploration Technologies Corp (known as SpaceX) and Starlink to deploy several low-orbit satellites in five orbital layers. By 2024, the Starlink system will consist of 12,000 satellites, almost twice as many as it has been launched since the beginning of the space age in 1957 (about 7,000). Without a doubt, satellite broadband is one of the most booming markets in the space communication sector worldwide. In this way, it highlights the undeniable opportunity for any state to put an end to the problem of the digital gap, showing how satellite is the ideal technology to reach isolated places or places with poor connectivity.[14]

In this sense, the prospects for the future of the satellite have been complementary with the rest of the technologies. In other words, it does not displace fiber optics, but complements it, definitively, extending connectivity. Satellite communication has unique advantages that differentiate it from other technologies, for example:[15] (1) with a single satellite footprint, vast extensions are covered, from countries to continents; (2) ground infrastructure deployments are not necessary; (3) the service is immediately available to the entire surface at the same time, allowing for immediate network deployment; (4) coverage is not dependent on population density or orography, so connectivity can be provided in rugged, hard-to-reach or sparsely populated environments that would never have terrestrial structures, mainly due to cost;(5) it is the only solution for mobility services such as ships and airplanes.[16]

The pandemic as a catalyst for change

Cyberspace presents itself as a virtual area free of restrictions, gaining relevance for leisure and work, not to mention the increase in cybercrime. Unfortunately, areas such as poverty, malnutrition and insecurity are not relevant to the geopolitical analyses of countries fighting for hegemony, but power and

influence.[17] To this end, they use all possible means to achieve their objectives, especially political, economic, diplomatic and communicational means, including - including the latter - social media, and, traditional and non-traditional CMMs.

In the last decade, the tension between the PRC and the United States for global leadership has become more evident. The White House has accused Beijing of lack of transparency in data related to the coronavirus, and for breaches of the trade agreement signed in early 2020. On its side, the PRC, from March to May 2020 and at the height of the virus global spread, sent medical supplies – as an aid - to the most affected countries by the pandemic.

The COVID-19 pandemic has not only highlighted the human cost of inequality and the need to strengthen national health systems, the universal and free access to basic medical services and the equitable distribution assurance of vital resources, but also the need to reformulate international organizations, especially the United Nations and its subsidiary, the World Health Organization. It also became evident that the vaccine distribution program has a dual purpose: the altruistic one of equitable distribution and the self-sustaining one of the multilateral organization. Therefore, the deficient action of these international organizations favored and expanded the PRC's zone of influence, mobilizing by means of the emergency and supporting European and Latin American countries with products to meet certain health needs.

Geopolitics Perspective: Agnew's Critique

In this context, John Agnew proposes an explanation of the changing geopolitical foundations based on three eras in which the modern geopolitical imagination has exhibited characteristic features and practices: civilizational geopolitics (1815-1875), naturalizing geopolitics (1875-1945), and ideological geopolitics (1945-1990).[18] The third of these eras - in force during the Cold War - was ideological geopolitics, based on the world division on the basis of a diversity of ideas on how best to organize political and economic life ("socialism" versus "capitalism," etc.). Since the end of the Cold War, the "Three Worlds" concept has lost much of its compeling.[19] In addition, the growing inequalities in the economic development of Third World countries have made it quite problematic to use this concept without mentioning the other two.[20]

Currently, the advancement of the PRC's influence towards the three types of worlds -defined by Agnew- is perceived by the US authorities as a threat to their hegemony, which has caused the US to shift from a strategy in which it has tried to accommodate China to the international order, to one in which its main objective is to contain the influence of the Asian country.[21] In this regard, in March 2018, President Donald Trump's administration launched a trade war against the Asian giant, which was partly bounded to the containment of Chinese technological development in pursuit of maintaining U.S. supremacy. The fact that the Asian power has led the development of a disruptive technology such as 5G means that the PRC will be the one dictating its

international standards and norms. The key is that this technology could be the skeleton of the fourth industrial revolution, which is why companies such as Huawei, a leader in the sector, are the focus of US attacks. It could also be the beginning of global control of all information transmission methods.[22]

Social media, coronavirus and non-state actors

During the COVID-19 pandemic, different non-state actors (violent and non-violent) have maliciously used social media to spread conspiracy theories and fake news about the virus origin. Conspiracy narratives often attribute the origin of the virus to governments, religious or ethnic groups, secret media, companies or entrepreneurs who, according to these interpretations, are trying to push secret agendas such as reducing the world's population, controlling the world or generating economic revenue by selling vaccines and drug treatments.

On the one hand, in the case of violent non-state actors, according to a report by the United Nations Interregional Crime and Justice Research Institute (UNICIRI), it is established that the messages are customized to match the ideological tendency of the audience.[23] For example: (1) "extreme right-wing groups"[24] have spread conspiracy theories blaming immigrants and foreigners as responsible for the spread of the virus, (2) "groups associated with Islamic terrorism"[25] have also spread conspiracy theories claiming that the virus is a "soldier of Allah" who is punishing unbelievers and enemies who have harmed Muslims in recent years, and (3) "illegal armed groups related to organized crime"[26] have disseminated images and videos providing social services taking advantage of the fragile socio-economic situation caused by the crisis.

In the cases presented, the actors claim to have "real" knowledge about the origin of the SARS-COV2 virus and prophesy that this virus will accelerate the self-destructive tendencies of the existing governmental system, causing its collapse and the creation of a new society in which its enemies will be eliminated. Discursively, disinformation responds to the following strategic objectives: (1) undermine trust in government, (2) reinforce extremist narratives and recruitment strategies, (3) increase the motivation of self-radicalized terrorists, and (4) change the negative image of criminal organizations, portraying them as a replacement for ineffective state institutions. To achieve these goals, they take advantage of the functions and services provided by social media platforms to upload communications tailored to each platform and to expand their own network and find new contacts based on criteria such as mutual friends, work and education.

Some groups are also trying to avoid control measures on major social media, avoiding the use of certain words or symbols that can be easily identified as part of "extremist language" and even trying to appear legitimate to a large audience. Likewise, various groups have shown resilience by spreading disinformation even after their accounts were deleted. To this end, one possible tactic is to reproduce the same content by creating new accounts, while another tactic is to redirect followers and visitors to less controlled and encrypted

channels (external links), such as Telegram, VK, Gab or websites. Another important aspect is the malicious use of "social bots" or "chatbots."[27]

On the other hand, in the case of non-state and non-violent actors, the massive use of social media opened up possibilities in places that had been closed due to isolation and social distancing. However, it brought with it a series of risks of various kinds, both in the private, personal and professional spheres. According to the report on "Good practices in social media" by the Incident Response Team of the National Cryptologic Center (CCN-CERT), in general terms, actors who use social media as a gateway for cyberattacks and infringe the security of users, take advantage of three types of vulnerabilities implicit in the "social architecture" of media: overexposure of personal information, information highways and mass use.[28]

Among the various malicious actions that can be developed are social engineering, identity theft, cyberbullying, sexting, grooming, reputational damage, misleading advertising, crime in the physical world, malware distribution, phishing, pharming, malicious links, promising videos and scams. Therefore, malicious use would imply the use of any kind of content disclosed on social media to obtain an illicit and/or illegal benefit, generally to the detriment of third parties or directly to produce harm to those third parties.[29]

Conclusion

The geopolitical relationship and social media are framed by the need to exert influence and project the power of state actors of international weight, such as the United States, the PRC and Russia. This situation makes it clear that States continue to be significant actors in world politics, mainly those that have developed important capabilities and tools for the protection of their interests, which is the Information War. The New Cold War between the United States and the PRC is part of this competition for hegemony, accelerated by the COVID-19 pandemic.

From the technological point of view, we can visualize a race to acquire significant advances and insert them in the international market, obtaining not only economic but also cultural and social benefits, by opening new areas of dominance primarily for the PRC. On the one hand, the world has been experiencing moments of change in satellite communications and these new technological developments will allow the growth and access to services and areas previously inaccessible for economic or technological reasons. On the other hand, the satellite is no longer an isolated platform from the rest of the telecommunications options but is an integral part of connectivity and service capacity, becoming a key element in the development and implementation of 5G technology.

However, Satarlink's self-financing leaves its owner, Elon Musk, in a position of power vis-à-vis the States. Although there are still no signs of strategic relations between the entrepreneur and the States, Supranational entities or Non-

Governmental Organizations, on the contrary, his status and power refer to a personal superiority. It should be noted that it is necessary to understand the importance of space and its relationship with the sovereignty of countries. It is therefore necessary to remember that cyberspace is the fifth domain of warfare, which complements the four classic dimensions or domains (land, sea, air and space). When the Satarlink system is fully operational (in 2024), Elon Musk will have a very important partial influence on all these domains.

During the pandemic, cyberspace -particularly social media - became a fundamental tool for society, as human beings established a place to interact, trade products and services, teach, educate, as well as, engage in politics, religion, among others. However, its malicious use was also the order of the day, generating risks for companies and institutions as well as for individuals. In this context, it has become evident that the importance and influence of CMMs (traditional and non-traditional) varies according to society stratum. However, the results of the communicational maneuvers also depend on the analysis of the target public, its sectioning, and the establishment of goals and themes for each one.

About the author:

Gonzalo Javier Rubio Piñeiro is retired Major of Argentine Army. Holds a Master degree in National Defense and a specialist in operational strategy and joint military planning, as well as in senior leadership of joint military organizations. He holds a Bachelor degree in both institutional communication and Administration. He has completed the Staff Officer and Joint Planning Course at the Joint Warfare School of the Argentine Army. Currently, he is a professor in Geopolitics and Strategic Analysis, in National Defense and in Institutions and Regimes of Defense and International Security, at the National University of Lanús (UNLA).

Endnotes:

[1] Paul M. Barrett, Tara Wadhwa y Dorothée Baumann-Pauly, "Combating Russian Disinformation: The Case for Stepping Up the Fight Online" *NYU Stern - Center for Business and Human Rights* (New York: 2018).

[2] Gonzalo Javier Rubio Piñeiro, "Capacidades del Sistema de Inteligencia ruso: Caso adhesión de Crimea a Rusia entre medidas activas, hombrecitos verdes, fuerzas especiales, ciberactivistas y espías", Ciudad Autónoma de Buenos Aires: Autores de Argentina (Argentina: 2021).

[3] Ibid.

[4] John Agnew, "Geopolítica: una re-visión de la política mundial" *Editorial Titivillus* (Madrid: 1998).

[5] Ibid, el autor en 1998 estableció que aún estaba en etapa de formación.

[6] Ibid.

[7] Gonzalo Javier Rubio Piñeiro (2021). Capacidades del Sistema de Inteligencia ruso: Caso adhesión de Crimea a Rusia…".

[8] Anderson Talon, "Adapting Unconventional Warfare Doctrine to Cyberspace Operations: An Examination of Hacktivist Based Insurgencies", *Fort Leavenworth - U.S. Army Command and General Staff College* (Kansas: 2015).

[9] Paul M. Barrett, Tara Wadhwa y Dorothée Baumann-Pauly, "Combating Russian Disinformation: The Case for Stepping Up the Fight Online".

[10] Han Byung-Chul, "La agonía del Eros" Editorial Herder (Barcelona: 2014).

[11] Han Byung-Chul, "La expulsión de lo distinto" Editorial Herder (Barcelona: 2017).

[12] Gonzalo Javier Rubio Piñeiro, "Capacidades del Sistema de Inteligencia ruso: Caso adhesión de Crimea a Rusia…".

[13] Juan Vázquez Rojo, "Estados Unidos y China pugnan por la hegemonía mundial (y no solo en economía)", *Inter Press Service - IPS - Periodismo y comunicación para el cambio global* (November 23, 2020), https://ipsnoticias.net/2020/11/estados-unidos-china-pugnan-la-hegemonia-mundial-no-solo-economia// (Cited December 1, 2021).

[14] Cristina Albarrán, "Satélite: comunicaciones desde el espacio hasta el último rincón de la Tierra", *Redes & Telecom* (January 7, 2022), https://www.redestelecom.es/comunicaciones/especiales/1130561000303/satelite-comunicaciones-espacio-hasta-ultimo-rincon-de-tierra.1.html (Cited January 18, 2022).

[15] Ibid.

[16] Ana Sánchez Arjona, "Fernando Ojeda: 'Internet es clave para frenar la despoblación porque supone una garantía de supervivencia'", *El nuevo lunes* (January 23, 2021), https://elnuevolunes.es/entrevistas/fernando-ojeda-internet-es-clave-para-frenar-la-despoblacion-porque-supone-una-garantia-de-supervivencia/ (Cited January 18, 2022).

[17] Gonzalo Javier Rubio Piñeiro, "Geopolítica pos-pandemia", *Centro de Estudios Estratégicos del Ejército del Perú* (April 22, 2021), https://ceeep.mil.pe/wp-content/uploads/2021/04/CEEEP-2021-Geopolitica-pos-pandemia.pdf (Cited November 30, 2021).

[18] The three discourses or modes of representation that are presented are called civilizational geopolitics, naturalized geopolitics, and ideological geopolitics, respectively. See John Agnew, "Geopolitics: A Revision of World Politics."

[19] The three worlds of development as defined in the Cold War: the First World of modern capitalist states, the Second World of modern but communist states and the Third World to which the other two tried to extend their influence in open rivalry. See John Agnew, "Geopolitics: A Revision of World Politics."

[20] John Agnew, "Geopolítica: una re-visión de la política mundial".

[21] Juan Vázquez Rojo, "Estados Unidos y China pugnan por la hegemonía mundial (y no solo en economía)".

[22] Ibid.

[23] "Stop the virus of disinformation - the risk of malicious use of social media during COVID-19 and the technology options to fight it", *Torino United Nations Interregional Crime and Justice Research Institute UNICRI* (Italy: 2020).

[24] Among them: The New Jersey European Heritage Association (NJEHA), Eco-Fascist Central, Corona Chan News, Corona Waffen, Atomwaffen Division (AWD), Feuerkrieg Division, Sonnenkrieg Division, AWD Deutschland y the Northern Order.

[25] Among them: ISIS y Al-Qaeda.

[26] Among them: El Cartel Jalisco Nueva Generación (CJNG), Cartel del Golfo, Cartel de Sinaloa, La Nueva Familia Michoacana y Los Granados.

[27] A social bot is a computer algorithm that automatically produces content and interacts with humans on social networks, trying to influence their opinion and behavior. Social bots are increasingly becoming an essential tool for large-scale disinformation campaigns orchestrated on social media. (*United Nations Interregional Crime and Justice Research Institute* -UNICRI, 2020).

[28] Equipo de Respuesta a incidentes del Centro Criptológico Nacional (CCN–CERT). (2021). Buenas Prácticas en Redes Sociales. Madrid: Centro Criptológico Nacional

[29] Ibid.