Nowadays conflicts tend to become rather “wars of choice”, wherefore the problem of legitimacy, public perception and identity plays a critical part, often challenging the traditional warfare means and rules. Digitalisation of politics and de-territorialisation of hegemony and power are not for certain new trends. However, the contemporary turn of these technology driven revolutions is accentuated by the intervention of multiple non-state actors, as S. Svetoka pointed out in 2016, struggling to acquire effective instruments to conduct asymmetrical, irregular and hybrid wars. In this context, the research intends to discuss the theme of the narrative operations, used as a part of a hybrid warfare in Russia vs NATO Crimean scenario, addressing topics as: post-state security threats and weaponization of social media, patterns of pro-Russian cyber propaganda and perspectives of development for regional security landscape, under siege of digital modernity.

Keywords: social media, hybrid warfare, information strategies, narrative cyber operations, NATO, Russia.
INTRODUCTION. “WARS OF CHOICE” AND NEW EQUATIONS OF SOFT POWER

How social media has become a weapon of war stays linked to the ascent of two related processes: weaponization of culture, information and money and militarisation of globalisation. The concept of “weaponization of culture and ideas”, essential for understanding the hybrid use of new digital networks, was coined by Peter Pomerantsev and Michael Weiss in 2014, in an early attempt to frame Russia’s new 21st-century “hybrid” or “non-linear” conflict strategy. Moreover, taking into account Frank Hoffman’s ground-breaking observation, related to the “blurred character of modern wars”, tending to conceal the borders amid peace and conflict, along with the Chief of the General Staff, Valery Gerasimov, famous quote, claiming that “The role of non-military means (...) have exceeded the power of force of weapons in their effectiveness”, weaponization of culture may announce a major change within contemporary representations of security and power. Weaponization of culture, ideas, information and money have become vital processes within the Kremlin’s, and not only, new approaches upon hybrid and non-linear wars, as a result of a silent information revolution. The ascent of digitalisation, subsequent to 2010 landmark, disclosed new socialisation and association patterns, challenging the nation-states monopoles upon foreign and public affairs and fostering the autonomisation of different non-state bodies. Military lobbies, economic networks, civic platforms or malign political and ideological

---

groups are only a few of the new stakeholders entering the security arena in recent times, their influence upon domestic and foreign policies being connected to soft power formulas as propaganda, disinformation, fake news and cyber-attacks.

Militarisation of globalisation revealed among other things the tensional lines arisen amid westernisation’s cultural model and the vernacular reactions occurred at democracy’s edges. Indigenisation has come as a world-wide evolution paradox, the initial adoption on behalf of non-Western societies of western liberal thinking being followed by traditionalist, nationalist and nativist responses. Those initial cultural vulnerabilities of the ’90s were aggravated by the digital modernisation, which enabled movements as de-territorialisation of power, ingravescence of social cleavages, decline of national solidarities and not lastly, the growing power of alternative community and association vectors. Fragmentation of national audiences and radicalisation of dormant publics resulted in decay of the previous security equilibriums and pacts, the use of social media as hybrid warfare tool becoming the trade mark of present conflicts.

Since many modern conflicts are labelled as “wars of choice”, requiring high degrees of legitimacy and popular support, multiple state and non-state actors are struggling in building and acquiring new tools for fighting asymmetrical and hybrid warfare. Moreover, the global interplay between civic-based social media movements and ascension of populist policies, grafted also on digital grounds, calls for reflection. The initial optimistic expectation concerning the democratising potential of digital sphere was replaced by the spectrum of dark information operations, determining inversions of the democracy in the region and authoritarian echoes.

It is considered that targeted narrative operations can achieve results no less impressive than attacks on critical infrastructure, the weaponization of social media collocating activities and effects.

---

6 Sanda Svetoka, Social Media as Tool of Hybrid Warfare, NATO Strategic Communication Centre of Excellence, Riga, 2016, p. 10.  
7 Thomas Elkjer Nissen, Social Media’s Role in Hybrid Strategies, NATO Strategic Centre for Excellence in Communication, Riga, 2019, p. 5.  
8 Ibidem, p. 10.
as: Targeting, Intelligence Collection, Defence, Command and Control, Inform and Influence and Hybrid Operations. The increasing complexity of the narrative-oriented hybrid measures recently deployed in social media playground, shadowing gradually the traditional cyberspace measures, as the Russian-Ukrainian conflict has demonstrated, may conduct to a provocative hypothesis. Not only that the nature of contemporary conflicts has changed, gliding towards complex multi-modal operations, blending kinetic and cyber approaches, but the future of warfare may encompass a second generation of hybrid warfare. While narrative patterns tend to reshape the reality perception, political commitment, national borders and identity formations of increasingly divided audiences, the rise of the hybrid use of communication sphere may conduct in the near future towards the proliferation of new power actors. State and non-state bodies, media outlets, inland diasporic communities or ethnic enclaves may use the magnifying impact of social media in order to litigate the classical hegemons. The following sections engage in pursuit of this hypothesis, aiming to discuss the new trends and strategic orientations revealed by Russia’s cyber approach to the Crimean conflict, concentrating mostly upon the hybrid use of communication and cultural narratives.

**THE SECOND GENERATION OF HYBRID WARFARE AND THE POST-STATE SECURITY CHALLENGES**

Beyond any doubt, Russia’s invasion in Ukraine sparked vivid debates upon traditional geopolitical norms and warfare tactics, but also inaugurated a new phase into the already complicated spectrum of non-traditional conflicts. The well-known definition launched by analyst and author Frank Hoffman concerning the new versions of modern war, considers that hybrid confrontations have as distinctive feature the “blend of the lethality of state conflict with the fanatical and protracted fervour of irregular war.” Further expanded

---

9 *Ibidem*, p. 11.


12 *Ibidem*, p. 3.
definitions depict the hybrid phenomena as a new formula of warfare that reunites at least three interrelated layers: complex campaigns that combine low-level, both conventional and special operations, offensive cyber and space actions and psychological operations designed to influence popular perception and international opinion. Thereby, the new Russian informational strategy has apparently targeted a well-established class of objectives, including: the recovery of a cultural *ecumene*, in its near vicinities through the instrumentality of “Novorussia” doctrine, the limitation of EU project dominance, the control upon strategic resources and energy pipelines, and the stimulation of a divide within Western political and security pacts.

However, the startling reconversion of the global and regional landscapes under the pressure of digitalisation offered unpredictable outcomes, all the more as information revolution will continuously change the nature of borders, identities and even power actors. Digitalisation has determined important consequences as rampant modernisation of traditional and fragmented societies, political mobilisation of new social groups or revival of national, ethnic and religious identities. These background processes were translated within the security and warfare arena by tendencies as: diffusion of power from governments to non-state actors worldwide, redistribution of economic and military power, ascension of alternative global and local governance institutions and increasing mobility of large populations, fuelled by growing social inequality. Second-order effects encompassed by new informational, cultural and political trends also involved deepening of internal social fractures, contagion of social conflicts, violent extremism, nationalist and isolationist reactions.

While the changing picture of international security environment, along with power diffusions from governments to non-state actors worldwide, challenged the initial geopolitical quests of the Ukrainian secession, new subsurface evolutions began to redraw the modern and hybrid confrontation game. Considering that the borders amid state and non-state actors have become increasingly blurred,

14 *Ibidem*, p. 4.
17 *Ibidem*, p. 85.
validating the hypothesis of a hybridisation of power players, assuming from now on multiple identities and several actions means, the stake of recent conflicts began to glide towards identity and cultural strategies. Taking into account the early 2000 NATO and Russia security policies, grounded dominantly on conventional tactics and using communication operations as secondary and adjuvant propaganda tools (rather sanctioning the results of confrontations than deciding the gainer), present conflicts tend to be progressively dependent on narrative strategies.

New information environment changed the features of warfare, confrontations not ending with the conclusion of hostilities, because the results may be reversed by the intervention of narratives about “who was right/wrong or won/lost”. The need to construct interpretative structures and strategic narratives, in which audiences can identify meanings, justifications of groups and state actions or legitimacy of foreign or domestic power policies, transformed social media and digital communication in instruments of war, with similar purposes and consequences as the use of force. The mediatisation and virtualisation of politics enhanced thus the potential of hybrid conflicts, while restyling the term’s meanings. New definition attempts concerning the hybrid phenomenon emphasise the presence of two distinctive versions of hybrid confrontations. Even if hybrid conflicts are still largely characterised by “integrated deployment of multiple military and non-military means”, the increasing relevance of additional layers as disinformation, influencing, military intimidation, employment of deception, ambiguity and deniability could signalise a change into the fabric and goals of hybrid warfare.

Hybrid conflict is still understood mainly as a conflict between states, but the growing relevance of disruptive, elusive operations, difficult to assign to a certain party, may open the road for a new pattern of hybrid aggression, involving non-state contenders. The discrete autonomisation of various institutional and organisational components, acting as proxies or grey flag action groups, both under

---

19 *Ibidem*, p. 20.
20 Frans-Paul van der Putten, Minke Meijnders (eds.), *Hybrid Conflict: The Roles of Russia, North Korea and China*, Dutch National Network of Safety and Security Analysts (ANV), May 2018, p. 5.
the patronage of nation-states and beyond that, raise new questions about accountability and the future development of security policies. The transformations occurred within the strategies of major security blocs, as NATO and Russia, act as a meaningful proof for these reconfigurations of hybrid warfare, hybrid threats and mostly hybrid toolbox. It is considered that the most notable aspect of the way in which Russia has lately engaged hybrid conflicts consists in shaping public opinion\textsuperscript{21}. Moreover, Russia has apparently shifted from being offensive against Western political influence, detaching from previous isolationist discourses and assuming chameleonic and subversive measures. These discrete and efficient hybrid operations included seizing and controlling new communication platforms and networks, destabilising democratic processes and institutions in European societies, weakening the liberal values and most important, reviving vernacular affinities for populist and personalist leadership models\textsuperscript{22}. This essential change marked the transition from an insular strategy to a diffusion move. Nevertheless, the new cultural and narrative-based approaches required the creation of complex eco-systems, bringing together non-governmental organisations, economic actors, transnational networks based on ethnic, cultural, religious or political identity vectors, and most of all, establishing media outlets and social media web. By using multiple epicentres and diffusion strings, the new stage of Russia’s hybrid responses may also trigger subsidiary consequences. Many of the contractors of its hybrid campaigns are non-state bodies, claiming partial autonomy and parallel promotion of their own strategic agendas, as the populist moves supported across Europe proved, after they secured political power. It is the case of Hungary’s privileged relations with Russia, still affected by Orban regime nationalistic drifts. Another useful example may appeal Russia’s complicated alliance with Germany\textsuperscript{23}, constantly put under pressure by other competitive coalitions, as Western security partnerships.

\footnote{\textit{Ibidem}, p. 2.}
\footnote{\textit{Ibidem}.}
The second generation of hybrid threats remain hence inextricably linked to the influence of new communication environments, constantly questioning the previous patterns of identity building, association and legitimacy. New hybrid approaches, employed by Russia in Eastern and Central Europe, demonstrate the resilience of old-fashioned strategic objective (expansion of influence, control of proximal space, limitation of Western influence), but translated from this time forward in innovative patterns, difficult to counteract or to discern from actions of subsidiary power players. Altogether, the information revolution started after 2010 and reaching the zenith point after 2015, contributed to the inauguration of a post-state security order, within the bounds of hybrid approaches started to compete other traditional means in assuring, projecting and exerting hegemony and power. “Masquerade of non-involvement”24, to invoke Bachmann and Gunneriusson influential phrase, recalls for an increase use of ambiguity, making difficult, if not impossible, the attribution of responsibility or efficient counter reactions. In post-Crimea years, Russia has developed robust capacities for information operations on the Internet25, Russian cyber-methods focusing rather on perception and discursive power than on support of direct military operations. Going one step further, if initial disinformation media campaigns were started by in-house sites as Russia Today and Sputniknews26, new hybrid attacks went far beyond simple manipulation of digital media, by instrumentality of fake news, trolls farms and forged public and civic spheres. However, the contemporary developments of hybrid actions may claim that the first generation of trolls and fake-news may be close to its twilights, since increasingly sophisticated means of hybrid communication enter the scene. The long-term objective of Russian influence is to weaken and divide NATO and the UE, larger populations and audiences being targeted through traditional and new media. Still, minorities, refugees, extremists, radical nationalist and various diasporic stances are used to deepen the social, national

26 Ibidem.
and cultural divides\textsuperscript{27}, as covert agents of the new soft-influence doctrine. Half-controlled, half-autonomous, these local actors, trapped into an extensive network of allies and front organisations, engage into a conjugated effort for the “reconstruction of reality” and rewriting of public beliefs, legitimacy credos and support\textsuperscript{28}. The externalisation of the hybrid operations and the growing segmentation of Russian strategy, alternatively adapted to national and local realities, make difficult to track the changes supervened within the geopolitical and security situation, all the more that narrative approaches could evade their expected consequences. The major effort made for controlling media narratives surrounding the events in Ukraine was pictured as pre-requisite condition of the combat\textsuperscript{29}. Henceforth, subsequent hybrid clashes highlighted the ambivalence of media campaigns and their underground dynamic. For instance, Eastern and Central Europe social-media civic movements ceased under the stress of reigniting populism, while Russian propaganda sometimes nourished strong and coherent countercultures, revamping the national agendas under the auspices of modern and liberal frames. Still, the growing dependence, announced since 2014, on cyber-enabled capabilities, both in civilian and military realms, may forecast a paradigm shift. The following section investigates the evolution and patterns of Russia’s new hybrid strategy, placed under the influences of narrative approaches, which have become the epitome expression of new power confrontations.

RUSSIA AGAINST NATO. NARRATIVE-DRIVEN STRATEGIES IN THE CONTEXT OF SOCIAL MEDIA

The war days in Ukraine have demonstrated that cyberspace may play a critical role in conducting narrative-driven operations, as a part of hybrid strategy, wherein “the main targets are not the machines or networks, but the minds of the people”\textsuperscript{30}. The Internet and the social media have the ability to multiply the information at high speed

\textsuperscript{27} Geir Hågen Karlsen, Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe, Palgrave Communications, vol. 5, 2019, p. 2.


\textsuperscript{29} Ibidem.

\textsuperscript{30} Elina Lange-Ionatamishvili, Sanda Svetoka, Strategic Communication and the Social Media in the Russia Ukraine Conflict, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2018, p. 105.
and significantly lower costs, which made them available for propaganda use, information warfare or influence operations, ever since the new virtual arena of communication was established. Moreover, the concept of social cyber-attack has been brought into prominence by the growing popularity of social networks, its employment during the Ukrainian crisis demonstrating the power of highly dynamic contents and the inherent difficulties in pursuing the genuine sources of digital news. The social cyber-attacks have as general purpose the manipulation of a society perception and values, generating in the same time span disruptive behaviours, and they should be addressed in broader terms of Psychological Operations tradition. PSYOPS constitutes a classical military activity aiming to influence the perceptions, attitudes and behaviours of target populations, often consisting in civilians or foreign audiences. PSYOPS objectives were traditionally reached by the instrumentality of complex operations as the release of a master narrative, contaminating the public debates, the use of symbols or mythology landmarks and the exploitation of cultural biases and group identities.

In PSYOPS casuistry, the influence upon a certain target audience is achieved by spreading rumours, using three major manipulation patterns: hate rumours exploit the ingrained dislikes and prejudices of the target populations, fear rumours make appeal to a human tendency to validate the worst-case scenario, while hope rumours respond to the latent wishes for a favourable turn of events and conflict resolution. Nevertheless, the proposed taxonomy presents itself as reductionistic, offering yet a comprehensive image upon the main stimuli engaged in the creation and control of digital crowds, by the intervention of narrative structures. It remains important to stress that the ascent of the narrative equations of hybrid aggression was potentiated by subsidiary structural facts as the lacunar and sometimes disconnected form of textual messages (posts, status updates, #tags, memes, and comments), the trust-based experience of social networks, imitating the image of genuine like-minded groups, and the opportunity to assume false identities for network users.
and influencers\textsuperscript{34}. Following Rebecca Goolsby broad definition, social cyber-attacks involve crowd manipulation and hysteria propagation, ending in chaotic mass behaviour, escalation of rumour, confusion, panic and uncontrolled violence\textsuperscript{35}. Acting under false pretences or anonymously, the designers of the social cyber-attacks may release a new and distinctive signal into the social media environment, or could capture and distort an existing signal\textsuperscript{36}. The attacks may concern the legitimacy of a combative group (the example of the Syrian insurgency), the validation of a fatal scenario (the menace of foreign intervention and civil war in the context of social media-driven Arab Springs) or the confirmation of the presumptive winning force, within unclear and frozen conflicts situations (Transnistria remains an ideographic sample for forged or disputed combative success). Since Russia is no stranger to false flag intervention strategies in the Balkans and its near vicinity, the spreading of rumours and use of narrative covert operations was exploited long before the advent of digitalisation.

However, the social age of the Internet disclosed new strategic opportunities, mostly derived from its de-territorialised nature, non-attributable and undelayed impact, and universal meaning. The recent times social cyber-attacks were directed under narrative formulas, insomuch as actions of pro-Russian “Cyber Berkut” (КиберБеркут) or its nemesis, the Ukrainian “Cyber Hundred” (Киберсотня) demonstrated during the Crimean crisis\textsuperscript{37}. Even if the mentioned unconventional action groups were made famous by their successful attacks against the North Atlantic Treaty Organisation (NATO) and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), their core activities were linked to the narrative aggressions. The Cyber Berkut conducted a massive cyber operation during the Ukrainian parliamentary elections from October 2014, hacking electronic advertising billboards in order to promote videos depicting the important Ukrainian leaders as “war criminals”, “oligarchs”, and “traitors”\textsuperscript{38}. The structure of master narrative was in this very case

\textsuperscript{34} Ibidem.


\textsuperscript{36} Ibidem, p. 105.

\textsuperscript{37} Ibidem, p. 106.

\textsuperscript{38} Ibidem.
Social Media as Hybrid Warfare Tool  
– Putting Russia’s Informational Strategy in Context –

based on a simplification and isolation hypothesis. The audience, simply defined under the label of “Ukrainian citizens”\textsuperscript{39} (the releaser intentionally ignoring the strong ethnic, cultural and political divides), was turned against politicians, using a potpourri of stereotypes. The function of the master narrative was to engage further rumours, distortions and concerns, exploiting already deep-rotted psychological apprehensions. By invoking the “futility of elections”\textsuperscript{40}, the maleficent expression of Western influence, the endanger of chronically civil war, or the urge to action against government and deputies, the master narrative aimed to give a comprehensive answer to fear, hope and hate rumours, circulated already within its target audiences. The message was issued afterward on social media, generating strong debates, increasing audiences’ cleavages and shadowing the real setting-agenda of the electoral moment.

The cyber equation of narrative operations reiterates old-fashioned manipulation theories, but the virtual space may engage new subsidiary opportunities such as snowballing (the initial message is propagated without supplementary costs, the sources fading into the background), the majority illusion (the audiences are constantly manipulated to believe that a specific opinion and perspective constitutes the dominant social conviction) or the increasingly popular snapshot technique, where the public has the delusion of real time participation into the event.

The Ukrainian case put under debate the traditional strategic communication solutions by blending cyber-attacks, digital intelligence operations and classical narrative manipulation campaigns, the release of a supposed intercepted phone conversation between the US Assistant Secretary of State Victoria Nuland and Geoffrey Pyatt, the US Ambassador to Ukraine in early 2014, serving as a living proof for this new hybrid approach. The allegedly leaked conversation revealed a presumed Western intervention upon Ukrainian post-Yanukovych transition, highlighting also strong biases against possible successors from the Opposition\textsuperscript{41}. The apparently bugged conversation was released

\textsuperscript{39} Ibidem.
\textsuperscript{40} Ibidem.
on Youtube also referring to the growing tensions amid the EU and NATO. In defiance to the authenticity sham, on which the scenario was built, the case involves rather a narrative approach. The tailored narrative aims in this situation to appeal latent anti-Western and conspiracy rumours, acting as a catalyst for later developments of collective perception and legitimacy attribution. During the Ukrainian conflict, Russia made use of complex narrative scripts, disseminated simultaneously on traditional and new media, by the instrumentality of “breaking” and eye-witness’ accounts, these venues mutually reinforcing the connections amid older and younger audiences.

The manipulation and distribution of purported atrocities committed by the Ukrainian army had the role to alienate the general audience from the state’s institutional identity and to create a community fracture. By circulating fake news and false testimonies about tortured civilians, organ trafficking, burning crops, child soldiers and use of heavy weapons against civilians, the concerted social-media campaigns influenced for a long time span the target population behaviour and reactions.

As a fact, the Romanian reader may find some of these counterfeited stories peculiarly disturbing, as the early post-revolutionary months issued a strong resemblance and similar narrative techniques, disseminated at that time in newspapers and television. Going back to the Ukrainian scene, new coined epithets, as “ruscist” (combining the terms “fascist” and “Russian”), proved the ascent of hybrid communication aggressions in other social media cells, beyond Facebook and Vkontakte, insomuch as some analyses of Twitter posts from 2014 confirmed. Social media hoaxes passed in many cases unsanctioned, the waves of indignations and false confirmations increasing the credibleness of the master narrative. The list of rumours divulged through the instrumentality of social media during the Ukrainian conflict grew to be quite long, key narratives including the creation of concentration camps, under the direct orders of the European Union and the Kyiv government, the confiscation of private

42 Ibidem, p. 106.
44 Ibidem.
45 Russian social media networking, imitating the Facebook platform interface and structure.
property, the pressure of right-wing guerrillas, hiding into the woods, or the future nationalisation of private property. The exacerbated rumours were placed in sharp contrast with the counter-campaign of “Polite People,” supporting the Russian occupation of Crimea. The two pictures were in fact part of a layered master narrative opposing different reality translations. The complicated train of events preceding Crimea’s annexation included nevertheless the presence of a strong Russian affinity, rooted in decade-long interactions and community building processes, but the extreme polarisation of the two images was purportedly fabricated.

The development and resolution of Crimea’s case offered considerable evidences that social media was from then on extensively used to support military and influence action on the ground, the new hybrid cyber strategies employing concomitantly attacks upon infrastructures and the psychological influence of target audiences. Since the Russian-Ukrainian conflict has proved the unquestionable alteration in the structure of modern war, the lines between cyber and information offensive becoming also blurred, an important question tends to emerge. What has become the stake of post-Crimean narrative hybrid operations, engaged by Russia and not only, in the framework of a multi-polar, post-national and increasingly instable regional picture?

Psychological Warfare opportunities, means and impact have changed the dissemination of information under formulas of narrative structures in order to achieve effects such as shape, inform, manipulate, expose, diminish, promote, coerce and deter, bringing sometimes paradoxical results. The methods of influence utilised in social media sphere may be divided in two main categories: overt, implying creation of official websites, accounts, channels, forums, and covert, making use of fake identities, botnets and trolling.

---

49 Sanda Svetoka, Social media as Tool of Hybrid Warfare, p. 17.
was presented as an undisputed success. Still, the query persists. Was it meant to be? NATO does not officially foresee the use of covert or clandestine operations to influence attitudes, behaviours and engagement of civil audiences, beyond the limits of military campaigns. For NATO PSYOPS remain defined as “planned activities using methods of communication and other means directed at approved audiences to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives”\textsuperscript{50}.

Meantime, undemocratic players or simply non-state bodies make use of covert cyber operations, in order to achieve miscellaneous economic, strategic and political purposes\textsuperscript{51}. What should be NATO’s response in front of this proliferation of hybrid threats, originated in communication realm? The answer may lay at the bottom of digitalisation-globalisation phenomena. The subtle and irreversible change occurred within the nature of nation-states under the pressure of digital modernity created parallel association and community structures. The mushrooming of NGOs, the autonomisation of media outlets and the enlargement of economic transnational networks or the growing activism of diasporic stances enable them to act like proxies in favour of democratisation projects or at least to make more complicated the classical influence and manipulation operations. Even when these new emerged actors do not act in synergy with security providers and real time hegemons, their very existence may hinder the efficiency of cyber warfare, especially in its cultural and psychological equations. The enclavisation of the Eastern European youth within the bounds of former traditional and parochial societies or the reignited radical affinities in the peripheral spaces of well-established Western democracies are for sure the symptoms of a divided landscape. The decline of classical unidirectional mass communication and the rise of parallel information and communication networks stimulated furthermore an alienation process, whose beneficiaries are still cast in shadow.

\textsuperscript{51} Ibidem, p. 17.
Against this background, the ascent of non-state and post-state bodies will determine new hybrid threats in the field of cyber-attacks, so much the more technology-driven propaganda conducted to the empowerment of malign groups and individuals. It remains clear that the major security players will not ignore these tendencies, many of the new digital challengers in the field of strategic communication being already placed under the tutelage of classical power structures. In spite of that, some of the “troll armies”, “social bots” and “fake users” may originate beyond the lines of what Russian theorist Igor Panarin calls “information special forces”\(^{52}\). The externalisation of hybrid cyber operations intensifies the risks of misuse and misappropriation.

In Ukraine’s case, Russia confronted a well-structured Western offensive, grounded on clear objectives such as preservation of democracy in the region, protection of national borders and regional status quo and limitations of strategic pressures exerted against NATO. The army of proxies and subcontractors faced a common security agenda, but it may not be the case in other less polarised scenarios. Another recurrent debate topic asks if NATO should use the same unconventional panoply, giving the fact that cyber security has become a hot topic on international agenda.

The “Panarin School”\(^{53}\), built around the writings of Russian scholar Igor Panarin, claims that Western forces, including NATO security alliance, developed and implemented “information aggression” operations ever since the collapse of the Soviet Union, the “coloured revolutions” wave and the Middle East Springs being also incriminated as expressions of cultural propaganda\(^{54}\). The basic terms engaged by this perspective upon information warfare include: social control, social manoeuvring, for targeting and dividing special audiences, information manipulation, disinformation and not lastly lobbying\(^{55}\). Actually, Russian criticism against westernisation processes generated adjacent queries about setting the limits of narrative-driven operations. What should be considered as a cyber-attack, derived from PSYOPS panoply, and what should be labelled as an open campaign in favour

---


\(^{53}\) Ibidem, p. 15.

\(^{54}\) Ibidem.

\(^{55}\) Ibidem.
of a cultural credo? Can we speak about narrative operations that could evade the hybrid label? The prolongation of the Russia vs NATO informal warfare is strongly connected to the reconfiguration of power balance in Eastern Europe and the Balkans. Still, most of the analyses dedicated to Russia vs NATO hybrid confrontation stop on the fringes of the Ukrainian study case. However, later phenomena as imitating grass-roots movements using social media vector (known as “astroturfing”\(^{56}\)) or distorting communication and public consensus by releasing rumours may call for reflection. On this account, the dynamic of recent days hybrid confrontations should be addressed in the context of the multiplication of the actors involved in circulating and building influencing narratives, channelling the meanings of already complicated topics like nation, sovereignty, identity or legitimacy.

**CONCLUSIONS**

The hybrid war concept has undergone major transformation during the past decades. Originally coined in the early 2000 in order to describe the multi-modal activities carried out by a non-state actor against a traditional state body, as the Chechen struggle against Russia proved through the instrumentality of guerrilla tactics, blended with coordinate military operations\(^ {57}\), the hybrid warfare meanings have gradually evolved to extremely complex varieties. The Israeli war against Lebanon from 2006 revealed the image of a non-state actor, Hezbollah, employing successively terrorist activities and high-tech military capabilities, and measures traditionally attributed to nation-states, as extended diplomatic and communication campaigns. Hezbollah potential in imitating the behaviour and actions of a classical state-actor opened influential debates related to the future of hybrid approaches. Incrementally, the hybrid solutions were transferring from the side of non-state bodies towards classical security actors and further to the use of global hegemons. Certainly, the Ukrainian casuistry demonstrated how hybrid war became associated with state behaviour, NATO labelling the Russian methods in Crimea.

---

\(^{56}\) Sanda Svetoka, *Social Media as Tool of Hybrid Warfare*, p. 27.


\(^{58}\) *Ibidem*.
as ones of hybrid approach\textsuperscript{59}. Since then scholars and analysts consider hybrid conflicts presuming the existence of state-led activity that incorporates non-state actors and other components\textsuperscript{60}. Yet, the recent developments of hybrid challenges may disclose further evolutions of the hybrid toolkit and expansion of its gallery of purchasers. Not only that a myriad of non-state malign and benign bodies recall the use of hybrid operations, mostly targeting communication sphere, in order to achieve political, economic or strategic dominance, but the state-led security policies may be put under scrutiny. Russia new cultural propaganda and influencing measures exceed the limitations of original hybrid reactions, and at the same time offer essential autonomy to adjacent players. The reconstruction of a Russian cultural heartland may be a security objective for sure, but who will make sense by this strategic legacy is still unclear. Moreover, the hybridisation and fragmentation of state-actors remain conclusively based on the opportunities and vulnerabilities arising from the new virtual communication environments. Miscellaneous audiences could act as pressure vectors, influencing and conditioning the actions, policies and strategies of governments, while the state’s security institutions and economic organisations may also experience the revelation of autonomy. The growing distances between centres and peripheries, and the polyphony of the new rhetoric arena enhanced the internal borders and surpassed the national and physical boundaries. New equations of identity, solidarity and association were made available for the use of unanticipated diverse malign and benign actors, their empowerment raising complex questions upon further evolution of security and democracy in the region.

As Bachmann wisely concluded\textsuperscript{61}, traditional combat is here to stay, no matter what sophisticated means of actions could be provided by social networks, media outlets or political influencers. Any doubt in this matter may inflict dramatic costs, as the 2019 war timeline already proved. The growing interest manifested by terrorist groups, radical activists or separatists and anti-state forces for defence and military technologies demonstrates beyond any doubt that narrative-driven

\textsuperscript{59} Ibidem.
\textsuperscript{60} Ibidem.
\textsuperscript{61} Sascha-Dominik Bachmann, Håkan Gunneriusson, \textit{op. cit.}, p. 79.
operations are, at least for the moment, just supportive measure for war and peace. Nonetheless, contemporary culture is trapped under the siege of major changes, markets turning into conversations\textsuperscript{62}, states acting as “imagined communities”\textsuperscript{63}, image dominating the new language syntax. In light of these considerations, the new generation of digital crowds will be one of hybrid confrontations, governed by heterogeneous publics and multi-modal older and newer hegemons.

**BIBLIOGRAPHY:**


Social Media as Hybrid Warfare Tool
– Putting Russia’s Informational Strategy in Context –

17. Thomas Elkjer Nissen, *#The Weaponization Of Social Media, @Characteristics of Contemporary Conflicts*, Royal Danish Defence College, Copenhagen, 2015.