


Information Influence in Hybrid Environment: Reflexive Control as an Analytical Tool for Understanding Warfare in Social Media

Aki-Mauri Huhtinen, National Defence University, Helsinki, Finland

Noora Kotilainen, University of Helsinki, Helsinki, Finland

 <https://orcid.org/0000-0001-7047-754X>

Saara Särmä, Finnish National Defence University, Helsinki, Finland

Mikko Streng, Finnish National Defence University, Helsinki, Finland

ABSTRACT

The traditional government-military-public relationship to the public driver's relationship is moving to the government and military. Conflicts are increasingly asymmetrical, networked, urbanized and open to the global publicities because of internet global connections and especially global access to the social media. The public-driven network-based global possibility to online communication means threats and the nature of conflict to become "hybrid." "Hybrid warfare" challenges the standard way of waging military operations. Military and security organizations have to combat new technologies of their adversaries. This article sets out to discuss the phenomena of hybrid warfare in contemporary rhizomatic society and a hybrid media environment. Furthermore, this research considers how reflexive control functions can provide a historical perspective to ahistorical accounts of hybrid warfare and thus help us to better understand the contemporary challenges and threats of hybrid warfare, particularly coming from Russia.

KEYWORDS

Hybrid Warfare, Hybridity, Reflexive Control, Rhizomatic Thinking, Social Media

DOI: 10.4018/IJCWT.2019070101

INTRODUCTION

According to Mangat (2018), the securitization of the networked information society and publicity has increasingly become a competition to win the hearts and minds of citizens and to shape public opinion online, especially through the use of social media. This trend also changes both national and global security. Information technology facilitates the weaponization of societies, traversing political, economic, security and state boundaries. Information technology is also an integral part of how hybrid threats are created and circulated. As Singer and Brooking argue, “as the [social media] feed became more personal, it became more political” (Singer & Brooking, 2018). Broadly speaking, we can see that the West is waging a new kind of war, fought with the rustle of money, the mantras of propagandists and the invisible leakers and information spies (Galeotti 2019).

Hybrid is a buzzword much used in academia of late. It appears in various social-scientific disciplines from media studies to military studies, and from organization studies to feminist peace research, so much so that it can even be seen as an interdisciplinary trend (Benkrel et al., 2018). While the term hybrid has its origins in the animal kingdom and in biology, in contemporary use it refers to culture, the media, warfare, organizations, and leadership, among others. Formulating a systematic definition or concept of hybridity in this context would be an undertaking beyond the scope of this article. During the last five years, the inability to define and understand the Kremlin’s perspectives regarding the concept has led to academic confusion and wasted efforts and has produced a misinformed policy debate in the West (Galeotti, 2019). Fridman (2018) provides a critical assessment of the concept, explaining that today’s “obsession” with “hybrid warfare” is more to do with politics and international power than conceptual novelty. In this article, we focus on two of the contemporary usages, namely the hybrid media environment and hybrid warfare, and the ways in which the two intertwine.

Hybrid points to a mixing of things of different origins, a coming together of distinct entities, in a way that creates something new and rhizome-like, which nevertheless has continuity with the old (Chadwick, 2013; Sumiala et al., 2018). Despite the extensive contemporary references to “hybrid”, the term is problematic in many ways; it may well be elusive and nebulous, and calling things hybrid may even be misleading, as it presupposes the existence of clear, clean and non-mixed forms. According to Wigell (2019), if we adapt this term to describe the transformation of threats, we involuntarily base our argument on the idea of pure and harmonized zero-points, which in the new chaotic information age are now mutating and polluting our self-understanding of a paradisiacal world. Suggesting that hybrid is something completely new is a historically deluded argument when it comes to both media technology and warfare. War has always been hybrid in nature, foggy and chaotic, and the media and communication have always relied on mixed forms throughout history. Moreover, the hybridity of (new) media technology and the waging of war are not new phenomena. Ten years ago, James Der Derian used the term “hybrid” as a military-

industrial-media-entertainment network (MIMENET) to describe how human history, experience, intuition and all other human traits are addicted to and contaminated by technology-scripted strategies (Der Derian 2009).

However, as the term is used so extensively in numerous academic fields today, it functions as a useful anchor for this article. Indeed, the article is the product of an interdisciplinary collaboration, drawing on both media and military studies, and aiming at enhanced conceptual clarity between the particular uses of hybridity in these two fields. More specifically, the article focuses on hybrid warfare and how the concept of *Reflexive Control* (Orenstein 2019) can be a useful analytical tool for understanding the contemporary challenges military organizations face when encountering the hybrid media environment. Strategy can be described as the art of creating power. In the cyber domain, the use of social media in particular as a tool of international politics has become a new strategy in the international competition arena (Jensen et al., 2019).

On the one hand, social media and so-called new media technologies have brought the term hybrid into focus in media studies. This is particularly the case in the context of political communication, which has been seen to change fundamentally in this new media environment (Chadwick, 2013; Sumiala et al., 2018). On the other hand, the term has been extensively applied in military studies, especially since the war in Ukraine in 2014 (Ahmer & Starbird, 2018; Starbird, 2018). Hybridity is seen to pose new challenges for the ways in which military operations are conducted. Furthermore, the label “hybrid warfare” is being used in cases that have very little to do with military operations, such as Russian attempts to influence the US presidential election in 2016 (Wigell, 2019; Galeotti 2019). The Kremlin considers itself a target of Western hybrid aggression, rather than the perpetrator (Galeotti, 2019).

Conspiracy theories since 9/11 2001 have increased due to the populist narrative of politics supported by spreading useful stories in social media in order to highlight the populist theory of power and the elite block. Social media is a highly effective tool for fueling a potential conspiracy atmosphere, such as the classic dichotomy of ‘East’ versus ‘West’ (Hotchkiss, 2019; Orenstein, 2019). The cyber espionage that targets public interest groups is one of the key tools in distributing propaganda using social media (Jensen et al. 2019). It has been argued that the Kremlin has had no detailed plan for waging hybrid operations, but that its motivation has been to divide, demoralize and distract the West to the point where it will no longer be able to prevent Russia from becoming a serious player in international politics once again (Galeotti, 2019).

Yet hybrid not only poses new challenges for contemporary military thinking, it is also seen to offer new opportunities through an increased understanding of the hybrid media environment. Particularly in the case of communications operations, for example, the practice of military *strategic communication* (*StratCom*) can benefit from hybrid thinking. Strategic communication can be seen as a concept or a process that offers a long-term goal for an organization (see Galeotti, 2019). From a historical perspective, *StratCom* is analogous with the concept of political warfare. The importance of *StratCom* has grown during the last ten years along with and due to the evolution of the internet and social media. However, the idea that *StratCom* harmonizes and centralizes

the key messages in order to control a global audience and public opinion is also a paradox in democracies, as it may also contribute to radicalization in the information age (Benkler et al., 2018). The US-dominated liberal and free economic world order has been neither neutral nor apolitical. We are experiencing the return of intensified international tension, rising dictatorships, increasing disinformation and sophisticated artificial intelligence-driven weapon systems (Kagan, 2018). Furthermore, there is a tendency towards the criminalization and weaponization of journalism (Fowler, 2018).

Contemporary hybrid warfare may not represent a new type of war, but it is serving a new kind of world and environment. Hybrid war may be understood as increasingly political warfare, with the added possibility of employing kinetic military power (Galeotti, 2019). The hybrid media environment both poses challenges and offers opportunities for StratCom. From the point of view of militaries, StratCom is used in order to avoid potential communication chaos in the hybrid media environment. The aim of StratCom is to attempt to influence key leaders and the general public, as well as key organizations, all concurrently, in order to achieve harmonized messages through various channels: mass media, social media, press conferences, academic departments, protests and demonstrations (Hallahan et al., 2007).

In this paper, we set out to discuss the phenomenon of hybrid warfare in contemporary rhizomatic society and the hybrid media environment. Furthermore, we consider how Reflexive Control functions as a central idea in Russian strategic thinking. Thus, the concept of Reflexive Control can provide a historical perspective for often ahistorical accounts of hybrid warfare, and hence aid better understanding of the contemporary challenges and threats of hybrid warfare, particularly emanating from Russia.

HYBRID WARFARE OR WAR IN A NEW ENVIRONMENT

Hybrid threats are unconventional, fast, multiple and often unclear. For example, it is difficult to identify whether the source of disinformation is a single actor, non-governmental actor or a nation state. Moreover, contemporary threats do not respect boundaries, either between national and local authorities or different levels of decision-making. Such threats often pose unprecedented problems for security agencies and political decision-makers. Policymakers still expect precise control of security and military forces during operations to prevent unexpected casualties. National security and military doctrinal manuals serve to standardize security and military action by performing clearly defined functions and tasks, shared language and methodology. Military technologies and practices together support the vision of centrally controlled weapon systems, sensors and communication lines. Thus, hybridity is seen to pose new challenges for the ways in which military operations are conducted, yet it is also seen to offer new opportunities for communications operations, such as practising military strategic communication (StratCom). Little wonder then that the future of warfare is being discussed in the West, particularly by the US and NATO.

There is always the risk that governments will spend billions preparing for the wrong war. Hybrid threats are transboundary in nature and thus require different behaviour from states in responding to them than conventional security threats have required (Eriksson & Rhinard, 2009; Jokela & Katajamäki, 2018). Conventionally, security thinking has been based on a clear division between external and internal threats, whereby militaries are prepared to respond to external threats, namely those coming from outside of the state's borders. Today, there are fewer and fewer boundaries between political, economic, social and military functions in the information networked world. Moreover, in this environment there are no boundaries between civilians and combatants. There is a demand to use whatever means necessary to succeed (Galeotti, 2019).

The term hybrid can also be useful for describing how, in the last decade, Western international security politics and the operations of the military coalition led by US have been increasingly ideological in nature, rather than territorial. International conflicts are almost always based on competition between nation states and their status in the global economy, as well as rivalry over natural resources, such as clean water, fossil fuels or valuable minerals. These resources are not contained within state borders. Groups like al-Qaeda, ISIS or Boko Haram can attack wherever they want without borders and recruit fighters from beyond state borders. Importantly, social media provides them with a global reach and audience (Mangat, 2018).

Concepts like cyber warfare are not used in Russia, because security planners in Russia group different types of warfare under the same umbrella. For example, electronic and psychological operations are integrated together with the concept of information warfare. Every act or instrument that includes information content will serve the same goal without Western-style categorization (Galeotti, 2019). The main difference between Western and Russian-style military planning is the precision of categorization and systematization of security phenomenon. The main problem for both sides is creating a holistic approach to security concepts in order to integrate new information-age phenomena, such as artificial intelligence, robotics, drones and social media into the traditional instruments of a nation- state's military strategy and security organizations, and traditional equipment and arms, such as tanks, artillery, rifles and frontal aviation.

From a military studies standpoint, hybrid warfare can be seen as a combination of both an overarching theory as well as an operational perspective (McCulloh & Johnson, 2013). As an operational perspective, hybrid warfare challenges the way military operations have conventionally been conducted. Hybrid threats are unconventional, fast, multiple and often unclear. The threats are not contained within boundaries, either between national and local authorities or different levels of decision-making. One of the challenges that social media poses to military organizations is the transformation from one-way communication to two-way communication. The public and citizens can easily monitor global conflicts and distribute information (through images, YouTube videos, tweets and so on) online without the possibility of control by government or security organizations. (Mangat, 2018). It is revealing that during the last decade, one

of the most rapidly growing areas vis-à-vis security and military organisations are public affairs branches, spokespersons and social media departments. Today, militaries have to communicate interactively with the public, or the public will draw its own conclusions from the consequences of military operations.

THE PROBLEM OF WARFARE SYSTEMATIZATION IN THE WEST

When we look at the classical Western military or police doctrinal manuals, they are still developed to indicate mechanistic power within a systematically controlled environment, and an illusion of scientific systematic progress (Paparone, 2017). In practice, in countries like Afghanistan, Iraq and Syria, Western military operations do not seem to work well. There are many reasons for this, among them tight political control of military operations and attempts to achieve military victory swiftly and cheaply. The main problem in classical doctrinal thinking lies in viewing reality too mechanistically. In hybrid environments, strength amounts to more than the number of physical troops or weapon systems. Due to their lack of high-tech weapon systems, opponents of the West spread their strong and alternative ideology online through social media. In democratic countries, winning wars and battles depends on rallying the support of the public behind the military and the government. In actual fact, the internet has moved the center of gravity of the battle from physical power to public support. Information-age warfare is increasingly waged in the public domain and open to various discussions, views and comments online. Moreover, it is virtually impossible for governmental and security organizations to control the anonymous public in the information age. The virtual public sphere exists in a privately-owned virtual space (Mangat, 2018).

During crises or war in particular, there is no specific system of conflict, but rather a persistent lack of information, the ambiguity of the behaviour of different kinds of actors, couple with purposefully created disinformation. Social media in particular offers an environment for chaotic engagement in various crisis situations. Politicians and security authorities try to plan systematic security operations, but when things start to happen at the practical level, there are already scores of people at the ready to post all manner of messages on social media. Social media is the most cost-effective and swift arena for the global mass media to pick up the most shocking pieces of amateur news about crises and to distribute them to global audiences. In democratic Western countries, the general public influences the feedback into the political decision-making process.

War does not sit well with systemic thinking. The meanings of war and conflicts are often too unstable and problematic to clearly define. War does not consist merely of unambiguous facts, and nor is it a naturally occurring phenomenon. Rather, war also always involves human judgement, intuition-based actions and propaganda (Mansfield, 2008). Furthermore, many concepts and attributes of warfare, such as strategy, have lost their original meanings. The morphological process affecting the meaning of concepts seems to be anchored in the development of theories of action through multifaceted

contextualizations and recontextualizations of how and what to do when faced with important, novel situations. This morphological process of concepts has become more manifest in the phenomenon of disinformation, especially on social media platforms. When the meanings of concepts are in constant flux and rapidly changing, so-called epistemological frustration follows because we cannot find the ontological home of the concepts (Paparone, 2013).

Belief in ever-evolving progress and scientific development as a solution to all problems is characteristic of modern Western thinking. The root of this confidence lies in the progress and improvement in natural science and system theoretical thinking stemming from the experiences of the two World Wars. There was a collective understanding that military, political, economic and scientific agencies had formed a new alliance that could bring warfare under the control of technological, organizational and economic mobilization. Today, warfare cannot isolate or separate itself from the other functions of societal activities, such as social media. After the Second World War and the beginning of the Nuclear Age, the integration process of the military, modern science, engineering and production was realized. President Eisenhower called this integration process the ‘military-industrial complex’ whereby warfare was transformed into an integral part of the arsenal of peace itself (Costea & Amiridis, 2017). Carl von Clausewitz’s classic and often-cited statement that “War is a mere continuation of policy by other means” (Clausewitz, 1968) had turned into the model described by Foucault, namely that “war is the logic of social life itself” (Mansfield, 2008). The citation from Foucault is relevant when we think about the role of social media in global crises.

Contemporary threats often pose unprecedented problems for security agencies and political decision-makers. Policymakers may still expect precise control of a military force during military operations in order to prevent unexpected casualties. Military doctrinal manuals serve to standardize military action by performing clearly defined functions and tasks. Together, military technologies and practices support the vision of centrally controlled weapon systems, sensors and communication lines. Yet is this approach still valid in the hybrid media environment and against networked information threats? During recent international conflicts and wars, nation-state military forces and their adversaries – militants and terrorist groups – have fought multiple “Twitter wars” in front of a global audience. Governments and armed forces have begun generating information operations and war propaganda that have co-existed alongside the internet’s infinite supply of memes and videos (Singer and Brooking, 2018).

Security in general and warfare in particular have become increasingly complex due to the growing number and diversity of parties involved and the increase in the flow of information that follows. Conflicts no longer remain local; instead, they increasingly attract external parties, such as non-governmental actors, private companies, paramilitary units and citizens on the internet. Generally, military security, policing, and all kinds of governmental intelligence bodies are also reaching out beyond national territorial limits via global surveillance systems, which are created to monitor the world’s aviation, maritime, trade, finance and communications systems.

Consequently, contemporary warfare takes place in supermarkets, tower blocks, subway tunnels, sport stadiums, industrial districts, and rock concerts rather than open fields, jungles or deserts (Graham, 2010). As Singer and Brooking (2018) aptly point out: “The decentralized technology thus allows any individual to ignite the cycle of violence”.

Mattis and Hoffman (2005) have suggested that the enemy or adversary in the hybrid environment is a human being with the capacity to act by using rules and creative methods that take us by surprise. The enemies and adversaries in hybrid environments do not follow our ways of behaving. They can use political, social, military and criminal actions in multiple ways. They may use unexpected technological solutions (social media) together with traditional kinetic influence (terrorism or sabotage, for example).

In particular, the hybrid concept underlines the meaning of knowledge and information as weapons. From the academic perspective, knowledge can be defined as a justified true belief, and hence the function of information can be seen to lead to knowledge. Yet not all information leads to knowledge. Without trust in information we lose the pathway to knowledge. Our traditional trust in information is based on documents, but communication has become less and less directly connected to specific documents or authors (Buckland, 2017). When we watch a war being waged on TV or monitor it on the internet, are we physically part of the war? Obviously not. The logic of war is to destroy and consume the same materials and energy that a peaceful society produces to create a secure environment. This used to be counter-intuitive to economic thinking, but now that almost everything is ready-made in the material sector of human life, the logic of war has integrated more into the economic way of life. Similarly, destroying information is the only way to give rise to the production of information. Hybrid warfare resists the formation of centralized power. This is why viewing the information flow through the model of a rhizome network is so useful when describing the weaponizing process of information (Mansfield, 2008).

The global discussion that has been ongoing for the past twenty years about the evolution of information has largely been an optimistic one. When the Soviet Union collapsed more than 25 years ago, the West believed that freedom and equality had been achieved. At the same time, the internet started its victory march into our Western value lives (see Singer & Brooking, 2018). Freedom, democracy and equality increased in pace with the growth in information technology. Information technology and the internet became a metaphor in the West that rapidly contributed to bolstering support for a market economy, among other things. Information has traditionally been seen as a neutral means of enabling not only political and economic integration, but also military integration.

The nature of the discussion changed rapidly during 2014, however, and experts and decision-makers are now increasingly emphasizing the threats implicit in the information network and within communications. In this respect, the Kremlin’s policies and the events in Ukraine have generated discussion on the dangers of information, especially as disseminated through social media. A case in point was the last US presidential campaign, where Donald Trump’s triumph aroused global concern over the concept of truth (Huhtinen, 2016). The crossover between military and civilian

applications of advanced technology is now an everyday occurrence. As Leetaru (2019) has pointed out, in our globalized Web, the censorship powers gained by one government are the censorship powers gained by all governments. In other words: if the EU succeeds in restricting what citizens can say and see, Russia, China, Iran and North Korea, along with other potentially restrictive and undemocratic countries, will gain similar rights to control their citizens over the net. Looking more closely at the powers demanded by the EU, in the hands of a nation like Russia they offer an almost perfect blueprint for the future of disinformation and foreign influence.

We are used to living with surveillance and information control in the urbanized West. Everyone can be a target or a threat in the war against drugs, crime, terror, and insecurity itself (Huhtinen, 2016). The internet is not only fiber-optic cables and servers. It is also a galaxy of billions of good and bad ideas, proliferating through social media platforms (Singer & Brooking, 2018).

HYBRIDIZATION BREEDS THE RHIZOMATIC NATURE OF THE INFORMATION ENVIRONMENT

Societal security can be usefully considered in terms of the botanic model of the rhizome. It is evident that the global information environment, especially the internet, has become increasingly rhizomatic and has created more hybrid threats. The rhizome is a metaphor for an ontological form, an organism that is constantly in flux, never ceasing to develop, always becoming. It has no static existence and any point of a rhizome can be connected to any other (Deleuze and Guattari, 1980). For example, “social media algorithms work by drawing attention to content that trends on their networks, even (and especially) when people are outraged by it” (Singer and Brooking, 2018). Social media acts as a prime example of the rhizomatic nature of networks that can create opposite effects to those that were intended.

A rhizome works with planar and trans-species connections, while the traditional tree model works with vertical and linear connections. The rhizome resists the organizational structure of the root-tree system, which charts causality along chronological lines, looks for the original source of ‘things’, and looks towards the end-state or conclusion of those ‘things.’ The rhizome presents history and culture as a flat map without a hierarchy, and which has to produce and construct continuously (Robinson and McGuire, 2010). The rhizome has no beginning or end; it is always in the middle, between things. All nodes can connect to each other or be fragmented. The Western tradition of organizing is based on the idea of arboreal permanence and stability, as portrayed in the Old Testament. The mathematically based natural sciences try to find the first and ultimate point of tree trunks or concentrate on the beginning or end of something (Chia, 1999). The rhizomatic nature of information networks can best be seen in the increasing quantity of different kinds of tools for mapping, surfing, and analysing social media data on the internet. The platform applications have a plateau or surface (rhizome) environment, where people can communicate without any tree-like hierarchy (see Rogers, 2019).

The functional architecture of social media is a prime example of the rhizomatic behaviour. Social media ensures that we can always find others who share our ideas, however incorrect and ill-informed they are. The main idea of social media is not the content of message but the number of “friends” who share the message first. This phenomenon is known as “homophily”, meaning “love of the same.” The homophily process is set in motion if one shares something that is subsequently shared by someone else. Most people don’t think very deeply before clicking “share.” The most important actors are the key nodes in the network, who already have plenty of followers when they click “share”. They are the “supersenders” (Singer and Brooking, 2018).

The people in rhizome networks are still the centre of gravity, however. Only by providing them with security – mostly based on feelings – and by earning their trust and confidence can security prevail. Threats not only emanate from kinetic power. Human security is also threatened by dysfunctional governance, corruption, and the abuse of institutional power. Targeting the threats is not only about targeting individuals, but whole networks. In rhizomatic networks, the best way is to foster lasting solutions. This requires concentrated effort through consulting and building different kinds of relationships. The authorities have to communicate honestly, but it is individuals themselves who must decide which argument is the most attractive. Yet knowing is not enough; the authorities also have to find a rhizomatic way to communicate. They have to understand the people and see things through their eyes.

For example, in 2007 the websites of Estonian organizations, including the Estonian parliament, banks, ministries, newspapers and broadcasters were targeted by cyberattacks. Behind the attacks was the disagreement with Russia about the relocation of the Bronze Soldier of Tallinn. The incident provoked huge international discussion, especially in NATO, about cybersecurity and the role and responsibilities of the nation state, prompting Western governments to implement measures to safeguard citizens’ virtual security more effectively.

It is clear that the authorities must get the people involved as active participants. The truth has to be adapted to local conditions. First, the authorities have to build trust and after that resolve the problems. The truth is nothing without winning the arguments. In a rhizomatic society, it is important to plan for civil emergencies with joint situational awareness in order to respond to hybrid threats. All parts of society are responsible for preparing themselves for a crisis, especially for information warfare in social media.

As Singer and Brooking (2018,) argue, “On Twitter, popularity is a function of followers, “likes”, and retweets” ... On Google, popularity is a function of hyperlinks and keywords; the better trafficked and more relevant a particular website, the higher it ranks in Google search results. On Facebook, popularity is determined by “likes” from friends and the updates that you choose to share. The intent is to keep users emotionally grafted to the network. Bombard your friends with silly, salacious news stories and you’ll find yourself receiving less and less attention; describe a big personal moment (a wedding engagement or professional milestone) and you may dominate your local social network for days”.

Typically, a strong and masculine military leadership culture believes that it is important to resolve problems, and the main task of high-ranking officers is to resolve big problems. But in the rhizomatic information environment you cannot resolve problems, you can only manage them by monitoring, becoming aware of constantly changing options, testing and planning parallels – and mostly by doing things without 100% certainty (Hill and Watson, 2019).

We can see the rhizomatic character of situations when the internet allows the government to track the public spirit and attitudes, but at the same time the internet opens up the possibility of public responses and interpretations online. Social media in particular may stimulate public participation, but also allows the public to actively demand the accountability of governments and security organizations (Mangat, 2018). Rhizomatic tendencies can clearly be seen in this paradoxical situation. The notion of the public implies universality, openness, sharing reality, objectivity, and rationality, but the opinion of a single person as part of the public implies flux, subjectivity, and uncertainty (Mangat, 2018). This is the reason why anonymous polling is no longer a valid tool in estimating an individual person's attitudes and behaviour in social media. A loud voice and wide distribution in social media do not mean that the like-minded are as educated as expert voices. Most of us just repeat information without spending enough time to express our own augmented opinion on a matter (Mangat, 2018).

The rhizomatic nature of communication also changes the words from text and letters to more metaphorical expressions. Visuality, visual communication and hybrid forms of visual images and textual messages have become a new norm, and the status of such hybrid, metaphorical communication has increased in the social media age significantly. In particular, a meme is a phenomenon that closely resembles a rhizome. Memes can become increasingly self-referential and complex by swapping clusters of new memes. Memes can also disappear if humans no longer recognize their meaning. Memes can proliferate across the chaotic, emerging network of websites and forum boards in a rhizomatic manner (Singer & Brooking, 2018).

In conclusion, during the occupation of Crimea, the Kremlin demonstrated how to use information warfare together with tanks and artillery in a rhizomatic way. The West did not understand what was going on because the result was a violent, confusing and socially paralyzing mess. The Kremlin's whole aim was to introduce divisions into Ukrainian society. To this end, the Kremlin uses the so-called four Ds – namely dismiss, distort, distract, and dismay— when disseminating propaganda (Singer & Brooking, 2018).

REFLEXIVE CONTROL – A USEFUL TOOL FOR ANALYSING HYBRID WARFARE

The contemporary discussion on information warfare and hybrid war often lacks a historical perspective. Hybridity is thus often framed in such discussions as something novel, a phenomenon descriptive of the contemporary military environment and warfare (Mansfield, 2008). Likewise, many discussions on the hybridity of the media also often

take an ahistorical perspective, which disregards the mixed form and interaction of previous times (Paparone, 2017). While social media may be a new facet of hybridity for both media environments and warfare, both fields have always consisted of multiple elements that have come together in hybrid forms.

From the military point of view, the hybrid media environment is seen as a communications battlespace or a narrative battlefield, where both new understandings and new modes of warfare are needed if battles are to be won (Giese, 2015; Holmstrom, 2015). For example, Jeff Giese (2015) argues for the need to develop memetic warfare conceptually and to embrace it fully. He defines memetic warfare as “competition over narrative, ideas, and social control in a social-media battlefield”. However, while social media may seem like a brand-new environment needing completely new tools operationally, theoretically memetic or narrative warfare is nothing new.

The concept of Reflexive Control is capturing the interest of various Western analysts because Russia has apparently used Reflexive Control extensively in Ukraine (Thomas, 2015). Along with the concept of cognitive weapons, it is seen as a ‘home-grown concept’ (as opposed to concepts adopted from the West). Thomas locates Reflexive Control as a subcategory of information warfare, or as one of its tools (Thomas, 2015). We, however, argue that Reflexive Control is more than that. It is an underlying principle and an operational technique of information warfare, and social media offers a prime opportunity to exploit it. As Singer and Brooking (2018) argue, “But as the world has come to be ruled by the whims of virality and the attention economy, plenty of people seek to cheat their way to fame and influence. Plenty more happily sell them the tools to do so”.

We consider Reflexive Control – a Russian theoretically based concept commonly defined as “conveying to a partner or an opponent specially prepared information to incline him to voluntarily make a predetermined decision” (Chotikul, 1986; Thomas, 2004) – as a historical example of the use of information in warfare, as well as an operational technique in pursuit of perception management. The concept of Reflexive Control illuminates how the information environment and media technology have been exploited by military and governmental actors in previous years and decades as well.

Russian warfare thinkers, particularly during the Soviet time, believed that warfare could be systematic and determined with precision by mathematical laws. This is the reason why Russia also adds the systematic deception facet to all military operations, and Reflexive Control is part of the deception (see Galeotti 2019). Reflexive Control is also an important way to balance between costs and benefits in international politics. Its use allows the Kremlin to hide its activities before achieving desired outcomes (King, 2018). The ultimate goal of Reflexive Control is that the object of control will not be aware of the manipulation. During the Soviet era, the cybernetic and research project to automatize the decision-making process in the 1950s was strongly rooted in the concept of Reflexive Control, which entailed attaching the context to the object, where it could logically deduce its own solution, predetermined by the opposing party. The beginning of the Reflexive Control process is to manipulate the perception of the situation, how it is perceived by the opponent. The reason why Reflexive Control is

so useful is because a rational actor has the tendency to select quite a clear solution to resolve the problem at hand. The clear doctrine offers the possibility to integrate Reflexive Control as a hidden part of decision-making processes. The rhizomatic and exponential growth of the information network may hinder the usefulness of Reflexive Control in the future, as hybrid connections and shared and decentralized decision-making processes are posing more complex challenges (King, 2018).

In Reflexive Control theory, desirable effects are achieved by deliberately influencing the information environment of the selected target audience. The means and methods of influence are selected in a way that reflects the target's own cultural and psychological behaviour patterns and ways of reasoning. In essence, reflexive control seeks to exploit the orientation of the target audience (Thomas, 2004; Chotikul, 1986). Disinformation, deception, pressurization and creating division are common and widely mentioned methods of reflexive control (Thomas, 2004; Leonenko, 1995; Komov, 1997; Reid, 1987).

According to Chotikul (1986) and Thomas (2004; Turko & Modestov, 1996; Leonenko, 1995), the primary targets of Reflexive Control can be seen as decision-making processes and the decision-makers themselves. The approach to these targets, however, is usually indirect, and achieved by using different audiences or platforms. Chotikul (1986) presents "the cultural complex within which decisions are embedded" as a third primary target for reflexive control. This need for an indirect approach and a focus on the "cultural complex" can highlight social media as a highly useful tool for applying reflexive control. This has been acknowledged in Western academia in works concerning hybrid and information warfare (e.g. Giles et al., 2018).

According to Timothy Thomas (2015) Reflexive Control is an intrinsic part of Russian information warfare today. He argues that Russian information warfare has geopolitical goals and that it needs to be understood in Russian terms rather than by imposing Western terms on the phenomena. Reflexive Control is arguably "a method for achieving geopolitical superiority and a means for arms control negotiations" (ibid.). When a militarized organization uses social media, it is both a risk and an opportunity for the unity of the organization (Magnat 2018). In the networked age, all organizations need diversity but also a tool with which they can control their identity and security. A broad audience and two-way communication increases the richness of ideas in an organization, but it also incurs the risk of losing hierarchies and classical control at the same time. Perception management is a key consideration for all organizations, especially Western military organizations in democratic countries, where maintaining one's reputation in the public sphere is crucial (Canel & Luoma-aho, 2019). In Russia, the Kremlin tries to maintain its reputation in the opposite way, namely by increasing Reflexive Control over its own citizens, because the media and especially the internet has few restrictions (Magnat 2018). By using fake news and trolling, the Kremlin tries to be proactive by telling its own version of a particular story, and President Putin has become a major factor in personalizing the narrative of a post-superpower in the global international area.

Reflexive Control theory has its origins in Soviet studies on influencing systematic decision-making processes in cybernetics (Reid, 1987). Since the end of the Cold War, Reflexive Control has also been intensively developed in the psychological and social fields (Thomas, 2004). Today, Reflexive Control is defined more comprehensively in terms of “perception management” (Giles et al., 2018). Moreover, according to Chotikul (1986), the concept of Reflexive Control is also deeply embedded historically in the Russian and Soviet culture (Chotikul, 1986). Chotikul (1986) suggests that from a historical perspective, the principles of Reflexive Control were applied to psychologically coerce the Soviet population and culture to build and uphold support for the Soviet regime. In this way, Reflexive Control is connected to, and embedded in, classic Soviet cultural traits such as the cognitive concept of truth being malleable, and the concept of double-think as a part of the social realm (Chotikul, 1986). Through psychological approaches, emotions are also an important part of Reflexive Control in practice.

In the hybrid media and internet environment, when we do not know enough, we tend to substitute emotions for thought (Singer & Brooking, 2018). Trolling is a way to arouse as much anger as possible in an audience. Anger is the fuel of madness, and anger is also addictive. In a digital environment suffused with liars and fakes, anger feels raw and real in a way that other emotions often do not. Trolls exert power by being able to provoke anger in the toxic swamp of the rhizome. Indeed, anger is easily to spread from person to person as a means of Reflexive Control (Singer and Brooking, 2018).

The ways in which Reflexive Control is applied can be extremely hard to pinpoint in the larger context. Reflexive Control is elusive, and usually has a multi-method presence at different levels at the same time (Giles et al., 2018). Social media, or any other platform, should not be seen as the only tool for Reflexive Control. Moreover, not all social media influence is a part of Reflexive Control (Giles et al., 2018). Jaitner and Kantola (2016) and Giles et al. (2018) conclude that Reflexive Control is a concept for long-term influence, which in its very nature combines different means, platforms and approaches. According to Jaitner and Kantola (2016), Reflexive Control theory can be applied by combining both information warfare and cyber warfare methods. According to Giles et al. (2018), social media is one of the prime platforms for Russian Reflexive Control operations. Social media can be easily accessed and exploited, and captures a large audience (Giles et al., 2018).

According to the NATO STRATCOM COE report ‘Social Media as a Tool of Hybrid Warfare’ (2016), Reflexive Control is also a part of Russian information warfare methods used in social media, with both external and internal audiences. Social influence techniques used in the context of the Ukrainian conflict, for instance, can be viewed through the principal methods of Reflexive Control (Social Media as A Tool of Hybrid Warfare, 2016, Annex 2). Moreover, according to Thomas (2015), Reflexive Control was a recognizable and extensive Russian means of influence in the Ukraine conflict. According to the STRATCOM COE report (ibid.), the platforms for Reflexive Control today include mass media and social media used either individually

or in conjunction with each other. On a larger scale, Giles, Sherr and Seaboyer (2018) have recognized numerous means and methods through which social media has been or is being used in Reflexive Control. Fake followers and “likes” are easy to produce by using a dummy email address and social media account (Singer & Brooking, 2018). What is more, information influencers can use so-called “click farms” and bots. Bots are rhizome-like in their complexity. They can be convincing “chatbots” that conduct conversations using natural language and selecting from millions of preprogrammed responses, or they can be devilishly simple, pushing out the same hashtag repeatedly (Singer & Brooking, 2018).

The concept of Reflexive Control provides fascinating insights into the Russian concept of Information Operations and warfare in general. Globalization and digitalization have opened up new avenues and platforms for employing the psychological and social aspects of Reflexive Control theory in particular (Giles et al., 2018). The Russian approach to information warfare can be described as flexible, and it can readily be combined with other means of warfare as a part of the hybrid approach (Giles, 2016). On this broader strategic scale, the Russian way of combining means and methods of symmetrical and asymmetrical warfare in pursuit of its goals differs from the classical Western strategic culture. This can lead to misinterpretations and a lack of perspective in viewing actions interpreted as hybrid (Covington, 2016). In this context, awareness of the concept and theory of Reflexive Control can provide some tools for understanding and analyzing the logic and phenomena of hybrid warfare in the contemporary hybridized media environment.

CONCLUSION

In this paper, we have argued that in order to effectively face the new challenges that the hybridization of warfare and the media sphere pose for security organizations, military organizations need to move away from systemic thinking towards rhizomatic thinking. We duly highlighted that in social media, two-way communication is a way for military organizations to build community involvement and ownership of information influence. We showed how both the historical perspective and new tools for understanding contemporary challenges, viewed through the concept of Reflexive Control, provide a means to better understand and get a better grip on the logics and phenomena of contemporary hybrid warfare. In the future, conflicts will be more ideological, and influencing audiences in social media environments will no longer be confined within geopolitical and territorial (physical) boundaries.

The hybrid combination of agencies, civilian and military, public and private, and mobilized across the internet expresses global willingness – especially in the secure environment of bourgeois liberalism and modernity – for the transformation of power into all of society’s domains. All vital functions of society can integrate their capacity for the rapid development of a large scientific (system theoretical) program, in order to achieve constant experimentation with reality. To this end, the global information safety and security environment may increasingly be in need of centralized organization.

As opposed to the Western yearning for a harmonized and comfortable life supported by technology and science, other parts of the world (for example China, India, African countries, Russia, and the Middle East) have been influenced by a traditionalist culture that is at odds with the trendy search for utilitarian ethics, and pursuit of social justice and equality for all. Such goals were never achieved by scientific will or reason in the Western sense of the words. Thus, faith has not been replaced by precise scientific measurement. Many non-Westerners intuitively understand that they have no place in the 'liberal, modern and individual' world. In addition, the challenges and problems surrounding the neoliberal economic and post-industrial process increase the aggressive attitude towards Western values. This is why marginalized populations have to seek alternative fundamentals for their lives, which is something that politicians and authorities know and make use of.

For contemporary militaries, the hybrid media environment in general and social media in particular resemble narrative battlefields or communications battlespaces where hybrid means of waging military operations are needed. However, as we have argued in this paper, the contemporary discussion on information warfare and hybrid war often lacks a historical perspective. While social media may be a new facet of hybridity for both media environments and warfare, both fields have always consisted of multiple elements that have come together in hybrid forms.

Moreover, we have argued that the concept of Reflexive Control can bring a historical perspective and provide fascinating insights, particularly into Russian understandings of information operations and warfare in general. Furthermore, we have suggested that a general shift from systematic thinking to a rhizomatic understanding of societies and warfare would be useful for Western militaries and other security actors. In this context, awareness of the concept and theory of Reflexive Control can provide some tools for understanding and analyzing the logic and the phenomenon of hybrid warfare. However, further theorization and empirical research is needed in order to fully utilize the concept of Reflexive Control in the contemporary hybrid security environment.

REFERENCES

- Ahmer, A. L. G., & Starbird, S. and K. (2018) Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse. *Proceedings of the ACM on Human-Computer Interaction* (Vol. 2). New York: ACM. doi:10.1145/3274289
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda. Manipulation, Disinformation, and Radicalization in American Politics*. U.K.: Oxford University Press.
- Buckland, M. (2017). *Information and Society*. London: The MIT Press. doi:10.7551/mitpress/10922.001.0001
- Canel, M.-J., & Luoma-aho, V. (2019). *Public Sector Communication. Closing Gaps Between Citizens and Public Organizations*. USA: Wiley Blackwell.
- Chadwick, A. (2013). *The Hybrid Media System: Politics and Power*. Oxford, UK: Oxford University Press. doi:10.1093/acprof:oso/9780199759477.001.0001
- Chia, R. (1999). A “rhizomic” model of organizational change and transformation: Perspective from a metaphysics of change. *British Journal of Management*, 10(3), 214. doi:10.1111/1467-8551.00128
- Chotikul, D. (1986). *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study*. Monterey, CA: Naval Postgraduate School. doi:10.21236/ADA170613
- Costea, B., & Amiridis, K. (2017). Ernst Jünger, total mobilization and the work of war. *Organization*, 24(4), 475–490. doi:10.1177/1350508417699619
- Covington, S. R. (2016). *The Culture of Strategic Thought Behind Russia’s Modern Approaches to Warfare*. Cambridge: Harvard Kennedy School.
- Deleuze, G., & Guattari, F. (1980). *A thousand plateaus: Capitalism and schizophrenia*. London, New York: Continuum.
- Der Derian, J. (2009). *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network* (2nd ed.). New York: Routledge. doi:10.4324/9780203881538
- Eriksson, J., & Rhinard, M. (2009). The Internal-External Security Nexus. Notes on an emerging research agenda. *Cooperation and Conflict*, 44(3), 243–267. doi:10.1177/0010836709106215
- Fowler, A. (2018). *Shooting the Messenger. Criminalising Journalism*. London: Routledge. doi:10.4324/9781315099927
- Fridman, O. (2018). *Russian ‘Hybrid Warfare’. Resurgence and Politicisation*. Oxford University Press. doi:10.1093/oso/9780190877378.001.0001

- Galeotti, M. (2019). *Russian Political War. Moving Beyond the Hybrid*. London: Routledge. doi:10.4324/9780429443442
- Giese, J. (2015). It's time to embrace Memetic warfare. *Defence Strategic Communications*, 1(1), 67–75.
- Giles, K. (2016). *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence.
- Giles, K., Sherr, J., & Seaboyer, J. (2018). *Russian Reflexive Control*. Ontario: Royal Military College of Canada, Department of Political Science.
- Graham, S. (2010). *Cities under Siege. The New Military Urbanism*. Verso.
- Hallahan, K., Holtzhausen, D., Van Ruler, B., Veri, D., & Sriramesh, K. (2007). Defining strategic communication. *International Journal of Strategic Communication*, 1(1), 3–35. doi:10.1080/15531180701285244
- Hill, A., & Watson, D. (2019). The Competitive Environment. In *Strategic Leadership: Primer for Senior Leaders* (4th ed., Ch. 2, pp. 13-24). Carlisle, PA: Army War College. Retrieved from <https://publications.armywarcollege.edu/pubs/3689.pdf>
- Holmstrom, M. (2015). The narrative and social media. *Defence Strategic Communications*, 1(1), 118–132. doi:10.30966/2018.riga.1.7
- Hotchkiss, M. (2019). Russian Information Warfare and 9/11 Conspiracism: When Fake News Meets False Prophecy. In M. Sarfraz (Eds.), *Developments in Information Security and Cybernetic Wars* (Ch. 10, pp. 230-259). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-8304-2.ch010
- Huhtinen, A.-M. (2016). 'The Baltic Sea Region (BSR) as a hinge between the information rhizome of Russia and the West'. In A. Makarychev & A. Yatsyk (Eds.), *Suturing the ruptures: seams and stitches in the Baltic Sea Region* (pp. 53–80). Palgrave.
- Jaitner, M. L., & Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations. *Journal of Information Warfare*, 15(4), 27–38.
- Jensen, B., Valeriano, B., & Maness, R. (2019). 'Fancy bears and digital trolls: Cyber strategy with a Russian twist'. *The Journal of Strategic Studies*, 42(2), 212–234. doi:10.1080/01402390.2018.1559152
- Jokela, M., & Katajamäki, E. (2018). Hybridiuhat hämmäntävät jakoa sisäiseen ja ulkoiseen turvallisuuteen. *Politiikasta*. Retrieved from <https://politiikasta.fi/hybridiuhat-hammentavat-jakoa-sisaiseen-ja-ulkoiseen-turvallisuuteen/>
- Kagan, R. (2018). *The Jungle Grows Back. America and Our Imperiled World*. New York: Alfred A. Knopf.

- King, F. (2018). Reflexive Control and Disinformation in Putin's Wars [Master's thesis]. University of Colorado. Retrieved from https://scholar.colorado.edu/gssl_gradetds/27
- Leetaru, K. (2019). The EU's 'Right To Be Forgotten' Is A Blueprint For The Future Of Disinformation. *Forbes*. Retrieved from <https://www.forbes.com/sites/kalevleetaru/2019/06/07/the-eus-right-to-be-forgotten-is-a-blueprint-for-the-future-of-disinformation/#46bb22755d0f>
- Mangat, R. (2018). Tweeting Generals: Making the Case for Increased Public-Military Engagement through Social Media. In *Communication and Conflict in Multiple Settings* (Ch. 8, pp. 205-231). Leiden: Brill. Retrieved from <https://brill.com/view/book/edcoll/9789004373679/BP000013.xml?lang=en>
- Mansfield, N. (2008). *Theorizing War. From Hobbes to Badiou*. Palgrave.
- Mattis, J. N., & Hoffman, F. (2005). *Future Warfare: The Rise of Hybrid Wars*. United States Naval Institute. Retrieved from <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>
- McCulloh, T., & Johnson, R. (2013). *Hybrid Warfare JSOU Report 13-4*. Florida MacDill Airforce Base: The JSOU Press.
- Orenstein, M. A. (2019). *The Lands in Between. Russia vs. the West and the New Politics of Hybrid War*. Oxford University Press.
- Paparone, C. (2013, June 24). Resurrection is Emancipation: Exploring "Strategy" as a Dead Metaphor. *Small Wars Journal*. Retrieved from <http://smallwarsjournal.com/jrnl/art/resurrection-is-emancipation-exploring-%E2%80%9Cstrategy%E2%80%9D-as-a-dead-metaphor>
- Paparone, C. (2017). How we fight: A Critical exploration of US military doctrine. *Organization*, 24(4), 516–533. doi:10.1177/1350508417693853
- Reid, C. (1987). Reflexive Control in Soviet Military Planning. In B.D Bailey & P.J. Parker (Eds.), *Soviet Strategic Deception* (pp. 293-313). Lexington, MA: Lexington Books.
- Reynolds, A. (2016). Social Media as a Tool of Hybrid Warfare. NATO Strategic Communications Centre of Excellence.
- Robinson, L., & McGuire, M. (2010). The rhizome and the tree: Changing metaphors for information organisation. *The Journal of Documentation*, 66(4), 604–613. doi:10.1108/00220411011052975
- Rogers, R. (2019). *Doing Digital Methods*. London: SAGE.
- Singer, P. W. and Brooking, E. T. (2018) *Like War. The Weaponization of Social Media*. New York: An Eamon Dolan Book. Houghton Mifflin Harcourt.

Starbird, S. K. (2018) The Surprising Nuance Behind the Russian Troll Strategy. *Medium*. Retrieved from <https://medium.com/s/story/the-trolls-within-how-russian-information-operations-infiltrated-online-communities-691fb969b9e4>

Sumiala, J., Valaskivi, K., Tikka, M., & Huhtamäki, J. (2018). *Hybrid Media Events: The Charlie Hebdo Attacks and Global Circulation of Terrorist Violence*. Emerald. doi:10.1108/9781787148512

Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. Article in publication. *Journal of Slavic Military Studies*, 17(2), 237–256. doi:10.1080/13518040490450529

Thomas, T. (2015). Russia's 21st Century Information War: Working to undermine and destabilize populations. *Defence Strategic Communications*, 1(1), 10–26.

von Clausewitz, C. (1968). *On Wars* (J. J. Graham, Trans.). London: Penguins Book.

Wigell, M. (2019). Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. *International Affairs*, 95(2), 255–275. doi:10.1093/ia/iiz018

Aki-Mauri Huhtinen, (LTC (GS), PhD) is a military professor at the Finnish National Defence University in the Department of Leadership and Military Pedagogy. His areas of expertise are military leadership, command and control, the philosophy of science in military organizational research and the philosophy of war. He has published peer-reviewed journal articles, a book chapter and books on information warfare and non-kinetic influence in the battle space.

Noora Kotilainen (PhD) is a social science historian and political scientist specializing especially in visual communication, international relations, humanitarian studies, media studies and global politics. Her research interests include (visual media) representations of conflict, crisis and violence, global mobility, the refugee situation as well as terrorism, humanitarianism and human rights in global politics, strategic communication and visual communication. She defended her PhD in political history at the university of Helsinki in 2016. She has formerly worked as a research fellow at the Finnish Institute of International affairs, global security research program, as well as a post-doctoral fellow at the University of Helsinki faculty of Social Sciences, Political History. Currently she is affiliated at the Finnish National Defense University in an academy of Finland research project Hybrid Terrorizing (HYTE) - Developing a New Model for the Study of Global Media Events of Terrorist Violence.

Saara Särmä (PhD) is a feminist, an activist, an artist and a researcher. She is the creator of "Congrats, you have an all-male panel!" and has worked as a project researcher at Finnish National Defence University and University of Tampere. She's interested in politics of visibility and image circulation, art-based methods, and laughter in world politics.

Mikko Streng serves as a teacher in the Department of Leadership and Military Pedagogy at the Finnish National Defence University.