H-ermes. Journal of Communication
H-ermes, J. Comm. 25 (2023), 167-184
ISSN 2284-0753, DOI 10.1285/i22840753n25p167
http://siba-ese.unisalento.it

Ontological insecurity and cognitive threats: emerging security challenges in the Information Age

Arcangelo Leone de Castris, The Alan Turing Institute

Ontological insecurity and cognitive threats: emerging security challenges in the Information Age. *Over the past two decades, digital communication and information technologies have enabled new avenues of conflict. Information has historically been used as a medium for projecting power, but the scale and speed at which it can be disseminated today have led to new ways in which power can be acquired and exercised. As a result, a reassessment of the security challenges brought about by emerging information and communication technologies has started in Western strategic thinking. To contribute to a better understanding of the ways in which information can be used for strategic, adversarial purposes, this paper traces the genealogy of the category of 'hybrid threats' and reflects on the novel concept of 'cognitive threat' as a new type of hybrid security challenge that is characteristic of the digital age.*

Keywords: hybrid warfare, information age, disinformation, ontological security.

Introduction

"The old world is dying, and the new world cannot be born: in this time of interregnum, morbid symptoms arise." With this sentence, Antonio Gramsci captured the displacing and disorienting feeling that spread across Italian society between the two major wars of the 1900s. For Gramsci, World War I marked the end of an epoch – Modernity. Its remnants, however, were so engrained in the sentiment of society that the transition towards the next historical could not be fully realised. This historical hiatus is what Gramsci called "interregnum"; a time of crisis.

Today we are, once again, living in a time of "interregnum". A prolonged one, commenced with the onset of the Information Age in the 1970s. As noted by one of the main theorists of the Information Age,

> We live in confusing times, as is often the case in periods of historical transition between different forms of society. This is because the intellectual categories that we use to understand what happens around us have been coined in different circumstances, and can hardly grasp what is new by referring to the past (Castells 2010, p. XVI).

The Information Age is marked by the advent of information technologies as vehicles to project power. Information technologies have turned the world into a single, interconnected environment, transforming the ways in which we communicate, behave and even think. Their diffusion bore promises of unprecedented societal evolution, unmatched wealth and universal access to knowledge. After almost thirty years since the Internet has gone global, however, we are confronted by a different reality. The version of the Information Age we live in is one of great human divides, inequalities, wars, and existential crises.

The "morbid symptoms" of the current interregnum are the withering of our ability to understand the informational complexity of the world in which we operate and, as a result, the spread of an incapacitating sense of existential insecurity. This paper analyzes some of these symptoms with the objective of contributing to the scholarly conversation about how Western democracies can address related policy concerns. The main argument of this paper is that a new type of threat, here called "cognitive threat", deserves formal recognition as a subcategory of the broader concept of "hybrid threats". In today's information environment, digital communication technologies afford us the capability to target and influence human cognitive processes with highly consequential results. Cognition, as a result, has become a potential "theatre" of conflict and shall be considered a strategic domain when States develop security policies for the contemporary Information Age.

The paper starts by discussing how information has been conceptualised and employed for the purposes of power and conflict. With time, the concept of information has expanded from its classical connotation as an instrument of national power to a strategic domain in its own right. This qualitative shift in the understanding of information carries substantial consequences in terms of policy response. The fact that information is understood as a domain within which conflict can be waged implies that its design, the actors operating therein and the rules underpinning its functioning acquire relevance from a public security perspective. Building on these considerations, the paper traces a genealogy of "hybrid threats" – a category that has deeply shaped contemporary strategic

thinking and whose rationale roots in the recognition that contemporary information technologies have caused deep transformations in the modes in which power is projected. Finally, the paper proposes an operation of theoretical specification and update of the hybrid threat category focusing on the relation between human cognition and the information environment and arguing that a new sub-category of hybrid threats – "cognitive threats" – is emerging. Before moving further, it is important to highlight that, while the focus of this paper is limited to the impact that the internet revolution had on the modes of conflict, the rise of hybrid threats is the result of a combination of different factors. Some of the most important include the geopolitical multipolarity of today's world, the complex inter-state economic dependencies caused by globalisation, and the democratisation of access to technologies (Monaghan 2019).

The ascent of information warfare and the cyberspace

Information has long been considered one of the most important instruments of power[1] and has been employed as such since ancient times.[2] In modern strategic thinking, information has been linked to military operations and conceptualized under different labels, each one offering relative definitional variations depending on the context to which it was applied (Nemeth 2002).

Some examples include "influence operations" (Pijpers 2023), "PSYOPs" (Narula 2008), and even political propaganda (Bernays 1928). All fall under the broader umbrella of "strategic communications" and can be brought back to unity by considering the conceptual premise on which they are construed: that information is both a source and an instrument of power. In fact, if possessing relevant information equals having a strategic advantage over the adversary, controlling the mediums through which information flows or being able to shape them equals controlling the messages they convey.

The force multiplier potential of information increased exponentially following major turning points in the evolution of communication technologies. The type

[1] The DIME (Diplomacy, Information, Military, Economics) model developed by the US Department of Defence includes information among the four main instruments of State power.

[2] E.g., the notorious stratagem employed by Genghis Khan, who sent messengers ahead of his army's advance to warn those about to be conquered about their imminent fate in order to scare them away, is a classic examples of information used as an instrument of power.

machine, the telegraph, the telephone, the radio and the television, in fact, have revolutionized the modes and scale of conflict, allowing information to be exchanged at unprecedented speed and in new formats. However, new communication technologies have not only shaped the structural, phenomenal features of the battles for power but also transformed the way conflict is perceived by the public and how war and politics are experienced by the citizens, ultimately enabling the engineering of those experiences.[3]

Coupled with progress in fields such as predictive behaviour and psychological modelling, new information and communication technologies made it possible to access a domain which had long been sought after by political power: the individuals' psychological domain. In 1944, Robert D. Leigh, the former Director of the U.S. Foreign Broadcast Intelligence Service, stated at a Congress hearing that:

> Around the world at this hour and every hour of the 24, there is a constant battle on the ether waves for the possession of man's thoughts, emotions, and attitudes – influencing his will to fight, to stop fighting, to work hard, to stop working, to resist and sabotage, to doubt, to grumble, to stand fast in faith and loyalty (…) we estimate that by short wave alone, you as a citizen of this radio world are being assailed by 2.000 words per minute in 40-45 different languages and dialects (Leigh 1944).

Psychological warfare, intended as the planned use of propaganda (Lasswell, 1927) and other psychological operations to influence the opinions, emotions, attitudes, and behaviour of opposition groups, became an integral part of all modern military strategies starting from the Second World War.[4] The object of psychological warfare as theorized in the 1950s was twofold: on the one hand to demoralize the enemy, break down his actual convictions and begin a process of indoctrination to lower its offensive and defensive capacity; on the other, to "remoralize" the allies and more broadly all individuals that were sympathetic to

[3] As famously stated by J. Goebbels, "it would not have been possible for us to take power and to use it in the ways we have without the radio" (Goebbels, 1933).

[4] The two main techniques of psychological warfare employed during WWII were the use of radio and the distribution of informational leaflets. It is estimated that during the war Western Allies, Russia excluded, dropped at least 8 billions leaflets.

the cause of war, including those behind the enemy lines included (Crossman 1952).

This power competition for the individuals' "hearts and minds" continued throughout the second half of the XX Century. It was largely used in Vietnam, Korea and, most notably, in the Cold War's theatre. Russia, in fact, developed its own version of psychological warfare – called 'reflexive control theory' – which was conceptualized "as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" (Thomas 2004, p. 237).

Despite their diffusion, however, the effectiveness of these techniques was contested. It was not easy, in fact, to assess the effect that they had on behaviours and beliefs. And, in addition to that, their integration within broader military strategies often happened to be more cumbersome than expected, sometimes engendering unanticipated, negative effects. Indeed, different case studies suggest inconsistent results.[5] This difficulty in streamlining psychological techniques into military operations, coupled with the widespread perception that the world order was about to find a seemingly permanent balance, led the momentum of psychological warfare to fade away – at least in Western strategic thinking.

All of this changed with the advent of the internet. If previous communication technologies allowed remote one-to-one or one-to-many communications, the internet enabled multiple users to communicate with each other in real-time. For the first time, people could create and access decentralized digital "spaces". Information technology changed the very own structure of communications; as a consequence, the way in which we do business, administrate a country, educate our children and interact with each other changed.

The way in which we compete for power did so too. Not only had the internet revolution enabled qualitatively new forms of threats such as cyberattacks. It soon became evident that it had deeper structural implications. Information started to be

[5] An example of propaganda commonly assessed as ineffective was the U.S. leaflet-dropping in the context of the Vietnam war, where the population famously 'detourned' them into toilet paper. On the contrary, successful beyond expectations was the 'V for Victory' propaganda campaign launched by the BBC durin World War Two.

conceptualized not only as an instrument of power but as a strategic realm of its own kind – just like land, sea, air and space – where strategic operations could be performed.[6]

These theoretical premises spurred the coining of a new concept – "information warfare" – which was used to indicate "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions" (U.S. Department of the Air Force 1995, p. 10). Information warfare is an asymmetrical conflict technique. Most notably, it applies to all levels of conflict as well as to peacetime and, thanks to the increasing availability and accessibility of information technologies, can be used by a plethora of different actors, including non-state actors – e.g. Hezbollah and ISIS (Clarke 2021).

The insight from which the discussion around information as a new strategic environment arose proved fruitful for it led Western military doctrine to expand the traditional model of operational domains – until then comprised of land, sea, air and space. This process, however, did not include the full spectrum of the theoretical model built around information warfare. In effect, the fifth operational domain was narrowed down to the infrastructural and logical dimensions of the information environment. It was called 'cyberspace'. According to the definition provided by the US Department of Defence (DoD), cyberspace is:

> A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (US Department of Defence 2021).

In 2011, the DoD officially included cyberspace among the formal operational domains (US Department of Defence 2011), and so did NATO (Warsaw Summit

[6] The US Joint Chiefs of Staff, JP3-13 Information Operations, 27 November 2012, p. I-1 defines the Information Environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three, interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information."

Communiqué 2016). While this sealed a major and much-needed evolution in Western strategic thinking – while the nature of national security threats remained the same, "cyberspace provides a new delivery mechanism that can increase the speed, diffusion, and power of an attack, and ensure anonymity and undetectability" (Giannopoulos 2021, p. 28) – the accent posed by the idea of information warfare on how information can be weaponized to interfere with the targets' perception and decision-making for subversive purposes was put aside. An accent that, this paper argues, needs to be brought back into focus by the contemporary public security discourse.

'Hybrid Threats': a new category to understand contemporary modes of conflict

The exploitation of the information domain is arguably the most prominent characteristic of modern-day "hybrid threats" – for instance, what made the 2014 Ukrainian crisis stand out is precisely the primary role that the strategic use of information played in securing the success of Russia's operations (StratCom 2014). In fact, even the Russo-Ukrainian conflict that started in 2022 has been at least partially ignited by information operations orchestrated by Russia as part of its hybrid strategy (Bachmann et al., 2023; Giles, 2023).

The concept of "hybridity" was first employed in the context of security studies in the early 2000s, as a way to describe the emerging and increasingly interconnected features of contemporary warfare (Mattis & Hoffman 2005). Specifically, it referred to new modes of military conflict where regular and irregular means of war are integrated and deployed simultaneously within the same battlespace; where strategic operations play around the formal threshold of warfare, making it increasingly difficult to differentiate clearly between war and peacetime; where non-state and non-military actors are capable of exerting unprecedented influence; and where the traditional features of Western strategic culture – based on hard, physical power – are turned into vulnerabilities and exploited as such (Mattis & Hoffman 2005). In other words, the category of hybrid warfare born out of the necessity to conceptualize the increasingly blatant

blending of war and peace, combatant's and non-combatants, and the prominence gained by non-kinetic means of war.

The combination of regular and irregular means of warfare had, in hindsight, already been noticed by several authors before Hoffman. "Fourth generation warfare" (Lind at al. 2001), "unrestricted warfare" (Liang & Xiangsui 1999), "compound war" (Huber 1996) are some of the most renowned examples in this sense. Yet, despite their conceptual relevance in describing the changing face of military confrontation at the onset of the 21st Century, these theories have at times been criticized because they arguably disregarded the many historical precedents where more or less traditional means of conflict had been combined for the purposes of military operations. In other words, their scholarly contribution was at least partially dismissed on the basis of their presumed redundancy and lack of an historical awareness (Echevarria 2005). In effect, following this logic, the use of irregular means of war is a strategy as old as the practice of war itself (Hoffman 2009). Hoffman's contribution, however, had the merit of systematizing and rationalizing the theoretical framework developed by earlier theorists of irregular conflict, testing it against the backdrop provided by the new challenges that came with information technology and the globalized economy.

Furthermore, particularly interesting for the purposes of this paper is Hoffman's intuition that the changing context of war shall be interpreted by factoring in the structural features of the "Information Age". In his seminal book "Conflict in the 21st Century" he, in fact, contends that

> while the U.S. military has demonstrated capacity to use technology and computer software, its performance in Iraq suggests it failed to master the opportunities presented by the Information Age. At the strategic level, the American government has not excelled at employing information effectively in today's Long War against Islamist extremism. Some of this can be attributed to a mis-conceptualization of the information dimension or battlespace centred on technology and computer networks instead of human software and culture (Hoffman 2007, p. 52).

Albeit conceived in the context of a specific military culture and inspired by circumstantial events, Hoffman's considerations soon proved to be of much wider applicability. The emphasis posed on the multi-modal character of contemporary

conflicts, in fact, offered a much-needed theoretical framework to bring into focus the 2014 Russian operations in Ukraine as well as the propaganda and information operations carried out by Da'esh. In fact, on the one hand, the hybrid offensive deployed by Russia – which succeeded in annexing the territory of Crimea without a formal military intervention – took many by surprise, sowing confusion and preventing the EU and NATO from intervening in a meaningful way. On the other hand, the phenomenon of 'foreign fighters' raised much alarm due to the radicalization of many young Europeans who had been moved by Islamist propaganda on social media and to the threat posed by their eventual return to Europe (European External Action Service 2013). These events represented a turning point for the European security environment, playing an essential role in cementing the concept of 'hybridity' into both EU's and NATO's institutional terminology (Renz & Smith 2016).

Since then, "hybrid threats" has become a buzzword of Western security jargon. In effect, both the EU and NATO have proposed their own tentative definitions of the concept. NATO's original definition of "hybrid threats" is to be found in a Capstone Concept published in 2010, which defined hybrid threats as:

> those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives (NATO 2010).

Consistent with NATO's nature of military organization, its approach to countering hybrid threats is first and foremost strategic and tactical. Hybrid threats, from the perspective of NATO, pose a problem for they constitute a type of attack that, other than being hardly detectable, challenges the application of the collective defence clause provided for in Article 5 of the North Atlantic Treaty. Therefore, for the Alliance the scope of "hybrid threats" is modelled against and limited to scenarios of war. The definition given by the EU, instead, is broader and more nuanced, reflecting the Union's intrinsic focus on soft power and its limited competence in the area of defence. Despite the initial use of the wording "hybrid warfare" – inspired by NATO terminology – the EU notion of "hybrid threats" is more plastic and it encompasses:

> the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. (EU High Representative of the Union for Foreign Affairs and Security Policy 2016, p.2)

The difference in nuance between the two definitions, however, not only reflects the specificities of the mandate and instruments typical of the two organizations but epitomizes the difficulty – if not the impossibility – to agree on how to consistently define a category encompassing phenomena as diverse as Russia's cyberattacks in Ukraine and the online recruitment propaganda of Da'esh. "Hybrid threats" have proven resistant to rigid conceptual systematizations, in a sense transposing into the semantic domain the same element of ambiguity that characterizes the phenomena they aim at describing. As a result, the different existing definitions often vary in terms of attribution requirements, capabilities, means, and actors involved.[7] Choosing only one definition as the definitive one, however, is not the solution in this case. On the contrary, considering the mutant nature of hybrid threats, the result would be the rapid obsolescence of the formal category, outpaced by the rate at which technology and the world at large evolve today. Therefore, while it is important to preserve consistency, the semantic plasticity of the term "hybrid threats" allows enough flexibility to pick and choose on the basis of the circumstances and can evolve together with the empirical phenomena it intends to address. If this has represented an obstacle to operationalise an encompassing response to "hybrid threats", it has also turned hybrid threats into a category able to capture the complexities of the contemporary world, weighting in the interconnected nature of challenges, the multiplicity of actors involved, and the variety of means they employ.

[7] For another definition of "hybrid threats" see The European Centre of Excellence for Countering Hybrid Threats, 'Hybrid threats as a concept' January 14, 2018, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/: "The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution."

A step forward in the development of a functional systematisation of hybrid threats has been the publication of a joint study by the Hybrid CoE of Helsinki and the European Commission's Joint Research Centre in February 2021. The study proposed a conceptual model of hybrid threats that can be adapted to both operational and strategic thinking at the EU, NATO and Member State levels. Here hybrid threats are defined as deliberately synchronised and combined actions targeting democratic societies' systemic vulnerabilities by:

> using multiple synchronised tools (in principle, non-military) to create linear and non-linear effects; creating ambiguity (covert and plausible deniability) and hiding real intent; exhibiting deliberate thresholds manipulation when it comes to detection and response; exploiting the seams of democratic society as well as between different jurisdictions; often including a distraction element, such as action in one place, and a target somewhere else (Giannopoulos et al. 2021, p. 11).

The model's classification of the domains that are conducive to hybrid activity includes, in addition to cyberspace, the information domain. In effect, information is considered the cornerstone of hybrid threats inasmuch as "it is used to undermine the perception of the security of the people by pitting political, social and cultural identities against each other" (Ibid., p. 32). As explained below, recognising that the information environment is comprised of both human/cognitive and technical/infrastructural components and that they are equally relevant from a strategic point of view is a fundamental advancement to rationalise and respond to contemporary and future forms of conflict.

"Cognitive Threats" as a subcategory of hybrid threats

The rapid success of the concept of hybrid threats tells of how much scholars and policymakers needed a new theoretical framework through which they could interpret the features of a changing security environment. As a conceptual category, in fact, hybrid threats bear the quality of conveying the impact that the current state of societal evolution has on the ways in which conflict is waged.

By so doing, hybrid threats have filled an important gap and substantively shaped contemporary strategic thinking. As noted, however, with the passing of time, hybrid threats have come to encompass an increasingly diverse range of

phenomena. In this sense, from a theoretical perspective, it would be correct to look at hybrid threats as a category rather than as a concept – i.e. as a conceptualization characterized by a higher order of abstraction. As a category, hybrid threats have proved valuable in providing a theoretical framework that informed not only the production of new scientific knowledge but also several policy reforms both at the national, EU and international levels (Pawlak 2017). However, in order to properly focus the security policy debate on how to counter threats designed to influence the information domain, it would be useful to adopt a more granular and centred approach.

The concept of information warfare is too narrow to encompass the cross-sectoral security problems addressed in this paper. Its scope, in fact, remains confined to the military realm and to a more classical understanding of conflict. A purely military-centric approach to hybrid threats would fail to provide a full account of the range of social and political challenges that we currently face. Nevertheless, the debate that framed information in terms of strategic domain remains pivotal to understanding cognitive threats and the security policy implications that they pose. Even if the idea of information as a strategic domain was conceptualized with a reference to the cyberspace, the conversation around it opened the way to reflect on the risks related to the interaction between information, human cognition and modern information technologies. Both the US DoD and NATO, in fact, refer to the operational domain of cyberspace as a component of the wider 'information environment', formally comprised also of a cognitive dimension.

Information has been considered a key instrument of power long before the advent of digital information technologies. These, however, have changed the modes and the extent to which information is produced, processed, diffused and consumed. Matched with the more recent developments in the fields of, *inter alia*, artificial intelligence, data analysis and computing, they have brought information conflicts to a whole new level. Today, technology allows for an unprecedented ability to understand and influence human cognition. Our attention can be targeted and directed, doubts can be instilled, ideas purposefully constructed and turned

into belief systems, and trust between citizens as well as in public institutions disrupted.

These trends have led some scholars to contemplate the opportunity to expand the formal classification of strategic domains. Adding up to land, sea, air, space and cyberspace, they contend that a sixth domain, the cognitive domain, also deserves systematic recognition (Hartley & Jobson 2021). An intuition that is also at least in part validated by institutional strategic thinking, although still in an unstructured form.[8] Whether the cognitive realm deserves recognition as a domain of its own kind or as a new component of the cyber domain is debatable and represents a question that will need to be answered by military strategists in the coming years. In either case, be it the extension of an already established domain or the creation of a new one, a revision of current strategic models will be required.

If it is true that human cognition has become yet another dimension through which power can be projected and exercised, an informed and effective security policy shall begin by assessing threats that are specific to that domain. In this sense, the concept of cognitive threats can support thinking through new forms of hybrid challenges. Cognitive threats can be thought of as a sub-category of hybrid threats. They specify the conceptual components of the hybrid threat category by emphasising their relation and relevance to cognitive processes. In particular, by influencing cognitive processes, cognitive threats can harm the ontological security of target individuals. When an individual's ontological security is harmed, his/her rational agency withers. The intensity of such disruption may vary. If brought to its extreme consequences, however, individuals lose the ability to agree on a shared representation of the world as they perceive it. As a result, any form of large-scale social organisation loses its existential tenets.

[8] E.g. NATO, *Allied Joint Doctrine for Cyberspace Operations*, AJP-3.20, January 2020, p.1 states that: "The Alliance finds itself operating in increasingly interconnected environments, in particular, cyberspace and the information environment (IE) [see IE definition above, p 15]. The free flow of data and seamless functioning of networks have become critical for functions and services for civil society and for military forces. State and non-state actors seek to exploit vulnerabilities in military and non-military information systems to exfiltrate, corrupt or destroy data or to gain prestige, political or military advantage or profit. Digital networks and systems, therefore, need to be safeguarded against information denial by disruption, degradation or destruction, and manipulation and exfiltration. In an interconnected world where military success may depend as much on the ability to control one's narrative as the ability to create physical effects, freedom of action in cyberspace may be as important as control over land, air and space, or sea." As mentioned in Section 3.1.

As a sub-category of hybrid threats, cognitive threats are also comprised of a range of manifestations. What follows is a non-exhaustive, open-ended list of cases that could be addressed by policymakers as threats to cognitive security:

Disinformation and Misinformation. Disinformation is understood as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm" (European Commission 2016, p. 3). Misinformation, instead, relates to the unintentional spread of "verifiably false or misleading information" (European Commission 2016, p. 3). As observed also by the European Commission, new technologies have increased the scale, targeting precision and speed at which false information can be spread to unprecedented levels, fostering the emergence of powerful echo chambers and strengthening the potential of disinformation campaigns. Unlike propaganda, which is purposefully designed to achieve a shift of political gravity, disinformation often does not communicate any explicit political cause or message. In many cases, it is used to sow confusion, discord and distrust in existing practices/ideas.

Computational Propaganda. Computing power has brought traditional propaganda on a whole new level. If compared to disinformation, "propaganda is usually associated with tactics and strategies that are designed to disseminate messages and views in support of a particular political cause, ideology or interest" (Fiott & Parkes 2019, p. 35). Thanks to the combination of automation and big data analysis, control over narratives online, especially on social media, can be greatly effective (Woolley & Howard 2019).

Foreign influence efforts. Defined as coordinated campaigns that a State conducts with the objective of influencing one or more aspects of the political functioning of another State by producing and disseminating content designed to appear as genuine and indigenous to the target state (Martin et al. 2020).

Conclusion

Manipulating the information environment to influence human cognitive processes is becoming an increasingly viable strategy for projecting power – be it for political or economic purposes. As a result, a reassessment of the challenges

brought about by new information and communication technologies is needed. Proposing a modest contribution to this goal, this paper reflects on the concept of "cognitive threats", i.e. threats to the ontological security of individuals and to the security of the social organizations in which they partake. The by-product of "cognitive threats", regardless of their effectiveness in achieving their stated goal, is a degradation of the rational agency of individuals and of the soundness of the institutions regulating their lives. Without the formal recognition that public security policies need to explicitly recognize and address the psychological domain as a strategic domain, cognitive insecurity is set to become an ever more threatening prospect.

Bibliography

Bachmann, S.D. D., Putter, D. and Duczynski, G., 2023, 'Hybrid warfare and disinformation: A Ukraine war perspective.' *Global Policy*, vol. 0, pp. 1-12.

Castells, M., 2010, 'Preface to the 2010 Edition of The Rise of the Network Society', in Castells, M., *The Rise of the Network Society*, Chichester, Wiley-Blackwell, 2nd.

Clarke, C.P., 2017, 'How Hezbollah Came to Dominate Information Warfare', *RAND*, accessed 01/04/2021, https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html.

Crossman, R.H., 1952, 'Psychological Warfare', *The Journal of the Royal United Service Institution*, vol. XCVII, no.587.

Echevarria, J., 2005, 'Fourth Generation War and other myths', *Strategic Studies Institute*, pp. 1-10.

European Commission and the High Representative of the Union for foreign affairs and security policy, 2016, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats: a European Union response*.

European Commission/High Representative of the Union for Foreign Affairs and Security Policy, 2016, *Joint Framework on Countering Hybrid Threats*.

European External Action Service, 2015, *Countering Hybrid Threats*.

Hoffman, F.G., 2009, 'Hybrid Warfare and Challenges', *JFQ*, vol. 52, no. 1.

Hoffman, F.G., 2007, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, Potomac Institute for Policy Studies.

Giannopoulos, G., Smith, H. and Theocharidou, M., 2021, 'The Landscape of Hybrid Threats: A conceptual model', *Publications Office of the European Union*.

Giles, K., 2023, 'Humour in online information warfare: Case study on Russia's war on Ukraine.' *Hybrid CoE Working Papers*, no. 26.

Hartley, D.S. and Jobson, K.O., 2021, *Cognitive Superiority: Information to Power*, Cham, Springer Nature.

Howard, N.P., 2020, *Lie Machines: How to Save Democracy from Toll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*, New Haven, Yale University Press.

Huber, T., 1996, *Compound Warfare: The Fatal Knot*, Fort Leavenworth, Command and General Staff College.

Lasswell, H.D., 1927, 'The Theory of Political Propaganda.' *The American Political Science Review*, vol. 21, no. 3, pp. 627-631.

Liang, Q. and Xiangsui, W., 1999, *Unrestricted Warfare*, Beijing, PLA Literature and Arts Publishing House.

Lind, W.S., Nightengale, K., Schmitt, J. and Wilson, I.G., 2001, 'The Changing Face of War: Into the Fourth Generation', *Marine Corps Gazette*, November 2001.

Margot, P., 2003, 'Any good news in soft news? The impact of soft news preference on political knowledge', *Political Communication*, vol. 20, no. 2, pp. 149-171.

Martin, D.A., Shapiro, J.N. and Ilhardt, J.G., 2020, 'Trends in Online Influence Efforts, *Empirical Studies of Conflict Project*.

Mattis, J.N. and Hoffman, F.G., 2005, 'Future Warfare: The Rise of Hybrid Warfare', *U.S. Naval Institute Proceedings*.

Monaghan, S., 2019, 'Countering Hybrid Warfare: So What for the Future Joint Force?.' *Prism*, vol. 8, no. 2, pp. 82-99.

Narula, S., 2004, 'Psychological operations (PSYOPs): A conceptual overview.' *Strategic Analysis*, vol. 28, no. 1, pp. 177-192.

NATO, 2010, 'BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats'.

Nemeth, W.J., 2002, *Future War and Chechnya: A Case for Hybrid Warfare*. Naval Postgraduate School.

Pawlak, P., 2017, 'Countering hybrid threats: EU-NATO cooperation', *European Parliamentary Research Service*, accessed 25/04/2021.

Pijpers, P.M.J., 2023, *Influence Operations in Cyberspace and the Applicability of International Law*. Elgar International Law and Technology series.

Renz, B., and H. Smith, 2016, 'Russia and Hybrid Warfare – Going beyond the Label', *Aleksanteri Papers*, no. 1, accessed 20 February 2021, https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_wa.

StratCom CoE, 2014, *Analysis of Russia's Information Campaign Against Ukraine*.

Thomas, T. L., 2004, 'Russia's Reflexive Control Theory and the Military', *Journal of Slavic Military Studies*, vol. 17, pp. 237–256.

U.S. Department of the Air Force, Cornerstones of Information Warfare, Washington, National government publication. 1995, p. 10.

US Department of Defence, Department of Defence Strategy for Operating in Cyberspace, July 2011, p. 5.

US Department of Defence, DOD Dictionary of Military and Associated Terms, January 2021.

Woolley, S.C. and Howard, P.N., 2017, 'Computational Propaganda Worldwide: Executive Summary', *Oxford Internet Institute*, Working Paper No. 11.