MONOGRAPH

# Digital Communication and Hybrid Threats. Presentation

## *Comunicación digital y amenazas híbridas. Presentación*

## *Comunicação digital e ameaças híbridas. Apresentação*

**Coordinators of the issue:**

**Rubén Arcos**
*Lecturer & Researcher in Communication Sciences*
*(Rey Juan Carlos University)*
*ruben.arcos@urjc.es*
*http://orcid.org/0000-0002-9665-5874*
*Spain*

**Hanna Smith**
*Research and Analysis*
*Centre of Excellence for Countering Hybrid Threats*
*(The European Centre of Excellence for Countering Hybrid Threats)*
*hanna.smith@hybridcoe.fi*
*Finland*

**ISSUE DATA**

**Published:** 1 January 2021

**Journal editors:** Francisco García García (Professor of Audiovisual Communication and Advertising, UCM) & Manuel Gértrudix Barrio (Associate Professor of Digital Communication, URJC)

**Coordinators of the issue:** Rubén Arcos (*Lecturer & researcher in communication sciences, URJC)* & Hanna Smith (*Research and Analysis, The European Centre of Excellence for Countering Hybrid Threats)*

**To cite this article:** Arcos, R. & Smith, H. (2021). Digital Communication and Hybrid Threats. Presentation, *Icono 14*, *19*(1), 1-14. doi: 10.7195/ri14.v19i1.1662

MONOGRAPH


## Abstract

*Hybrid Threats is a concept that has entered to many states official documents and security strategies. Both the EU and NATO have taken serious measures to counter hybrid threats related activity. This special issue on digital communication and hybrid threats aims to advance our understanding of how hybrid threat actors use and can potentially exploit the information environment for targeting our democratic societies and decision-making processes at different levels for different purposes. Information and communication technologies have brought remarkable advances in the ways we obtain information and build awareness on the world and its events and interact with the others, but at the same time, these developments create opportunities for conducting information and influence operations with a hostile intent at an unprecedented scales. Political warfare, active measures, and communication-led covert actions operations are not new, and propaganda has been used throughout the history in conflict and war like situations. However, today our digital communication environment and the communication tools that we employ for legitimate purposes are also being employed by hostile authoritarian actors and/or their proxies at a scale that has interfered in our democratic processes like elections, to erode trust in our institutions, polarize and divide our societies in unhealthy ways and sow animosities between states and international partner countries. Since human beings make decisions based on their representations about the world and the information available through interpersonal symbolic interactions and through the different media, information can be deliberately utilized for a malign activity to produce cognitive, affective and behavioural effects.*


**Key Words:** *Hybrid threats; Hybrid warfare; Digital communication; Disinformation; Strategic communication; Security; Intelligence*


## Resumen

*La amenaza híbrida es un concepto que aparece en documentos oficiales y estrategias de seguridad de los estados. Tanto la UE como la OTAN han tomado medidas serias para contrarrestar la actividad relacionada con las amenazas híbridas. Este monográfico sobre comunicación digital y amenazas híbridas tiene como objetivo avanzar en la comprensión de cómo los actores de amenazas híbridas utilizan y*

*pueden potencialmente explotar el entorno de la información para atacar las sociedades democráticas y los procesos de toma de decisiones en diferentes niveles, para diferentes propósitos. Las TIC han traído avances notables en la forma en que obtenemos información y construimos conciencia sobre el mundo y sus eventos e interactuamos con los demás, pero al mismo tiempo crean oportunidades para realizar operaciones e influenciar con una intención hostil. La guerra política, las medidas activas y las acciones encubiertas dirigidas por la comunicación no son nuevas, y la propaganda se ha utilizado a lo largo de la historia en situaciones de conflicto y guerra. Estas herramientas son empleadas por actores autoritarios hostiles y/o en una escala que ha interferido en procesos democráticos como las elecciones, erosiona la confianza en las instituciones, polariza y divide las sociedades de manera malsana. Dado que los seres humanos toman decisiones basadas en sus representaciones sobre el mundo y la información disponible a través de interacciones simbólicas interpersonales y a través de los diferentes medios, la información puede ser utilizada deliberadamente para actividades malignas que produzcan efectos cognitivos, afectivos y conductuales.*

**Palabras clave:** *Amenazas híbridas; Guerra híbrida; Comunicación digital; Desinformación; Comunicación estratégica; Seguridad; Inteligencia*

## *Resumo*

*Ameaças híbridas é um conceito que entrou em documentos oficiais e estratégias de segurança de muitos estados. Tanto a UE como a OTAN tomaram medidas sérias para combater a atividade relacionada com ameaças híbridas. Esta edição especial sobre comunicação digital e ameaças híbridas tem como objetivo avançar nossa compreensão de como os atores de ameaças híbridas usam e podem explorar o ambiente de informações para direcionar nossas sociedades democráticas e processos de tomada de decisão em diferentes níveis para diferentes fins. As tecnologias de informação e comunicação trouxeram avanços notáveis nas maneiras como obtemos informações e construímos consciência sobre o mundo e seus eventos e interagimos com os outros, mas, ao mesmo tempo, esses desenvolvimentos criam oportunidades para conduzir informações e influenciar operações com uma intenção hostil em um escala sem precedentes. A guerra política, as medidas ativas e as operações de ações*

*secretas conduzidas pela comunicação não são novas, e a propaganda foi usada ao longo da história em conflitos e situações semelhantes à guerra. No entanto, hoje nosso ambiente de comunicação digital e as ferramentas de comunicação que empregamos para fins legítimos também estão sendo empregados por atores autoritários hostis e / ou seus representantes em escala que tem interferido em nossos processos democráticos como eleições, corroendo a confiança em nossas instituições, polarizando e dividindo nossas sociedades de forma prejudicial à saúde e semeiam animosidades entre Estados e países parceiros internacionais.*

**Palavras chave:** *Ameaças híbridas; Guerra híbrida; Comunicação digital; Desinformação; Comunicação estratégica; Segurança; Inteligência*

# Presentation

In 1961 John F Kennedy addressed the American Newspaper Publishers Association. He described the then security environment in the following way:

> It requires a change in outlook, a change in tactics, a change in missions – by the government, by the people, by every businessman or labor leader, and by every newspaper. For we are opposed around the world by a monolithic and ruthless conspiracy that relies primarily on covert means for expanding its sphere of influence – on infiltration instead of invasion, on subversion instead of elections, on intimidation instead of free choice, on guerrillas by night instead of armies by day. It is a system which has conscripted vast human and material resources into the building of a tightly knit, highly efficient machine that combines military, diplomatic, intelligence, economic, scientific and political operations. Its preparations are concealed, not published. Its mistakes are buried, not headlined. Its dissenters are silenced, not praised. No expenditure is questioned, no rumor is printed, no secret is revealed. (Kennedy, 1961)

Kennedy's speech highlighted the challenge the West felt then. He described the Cold War environment. Today the EU and NATO countries are facing something similar. Cold War is history today as is also the battle between socialism and capitalism, which characterized the Cold War. The concept of Hybrid Threats is born out of the need to be able to describe today's security environment. As Frank Hoffmann, often

seen as the father of the term hybrid warfare, has said; "New language and new terms aids us in thinking differently and characterizing what is truly new, hopefully without overlooking what is enduring in war. A new lexicon captures the changes better than hanging on to old terms with new meanings" (Hoffmann, 2010).

Today the Hybrid threats is a concept that describes current security challenges. It has entered to many states' official documents and security strategies. Both the EU and NATO have taken serious measures to counter hybrid threats related activity. For the EU, "the concept aims to capture 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". (European Commission 2016: 2) As stated in NATO Secretary General's Annual Report, hostile adversaries "do not have to take to the battlefield to inflict damage on their adversaries" but foreign powers "can make political and strategic gains in other ways, such as spreading disinformation, launching cyber- attacks, and using deception and sabotage" (NATO, 2019: 29). These activities challenge not only the traditional distinctions between peace and war but also our understanding of what is peace and what is war. Hybrid Threats put civilians and the different departments of public administrations in affected countries –not only those with security and defence mandates– at the forefront of security as potential targets of hostile actors that scan for existing vulnerabilities or latent social, political, economic or historical cleavages to be exploited, while also seeking opportunities to create new vulnerabilities. This is a change, not perhaps so much from the Cold War, but from the post-Cold War world.

Internal and external security have started to mix in a new way. The challenge is not coming from outside but from within but initiated by an outside actor. Hybrid threat actors can target vulnerabilities of a state and specific societies in different domains through a combination of activities in multiple domains and in different phases. The conceptual model jointly developed by the European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre of the European Commission identifies thirteen domains (infrastructure, cyber, space, economy, military and defence, culture, social, public administration, legal, intel-

ligence, diplomacy, political, and the information domain) three phases (priming, destabilization, and coercion) and four activities across a spectrum (interference, influence, operations/campaigns, and warfare). Accordingly, interference and influence belong to the first phase of priming while influence and operations correspond to the destabilization phase. Operations and warfare are features of the coercion phase (Giannopoulos, Smith and Theocharidou 2020). From this perspective and framework, disinformation campaigns affect multiple domains including the information domain, but also other closely linked domains such as the cyber, social, political, intelligence, administration and cultural domains among others.

This special issue on digital communication and hybrid threats aims to advance our understanding of how hybrid threat actors use and can potentially exploit the information environment for targeting our democratic societies and decision-making processes at different levels and for different purposes. Information and communication technologies have brought remarkable advances in the ways we obtain information and build awareness on the world and its events and interact with the others, but at the same time these developments create opportunities for conducting information and influence operations with a hostile intent at an unprecedented scale.

Malicious activities in the information domain by state, non-state, and state-backed actors are an essential part of hybrid threat relating action. The EU's Council conclusions December 2019 used the concept "manipulative interference" to describe the activity that has been detected in the information domain and assessed as harmful as well as undermining democratic state systems. Political warfare, active measures, and communication-led covert actions operations are not new, and propaganda has been used throughout history in conflict and war like situations. However, today our digital communication environment and the communication tools that we employ for legitimate purposes are also being employed by hostile authoritarian actors and/or their proxies at a scale that has interfered in our democratic processes like elections, erode trust in our institutions, polarize and divide our societies in unhealthy ways and sow animosities between states and international partner countries. Since human beings make decisions based on their representations about the world and the information available through interpersonal symbolic interactions and through the different media, information

can be deliberately utilized for a malign activity to produce cognitive, affective and behavioural effects. Disinformation generated in a digital environment undermines more than traditional media (printed press and TV) the capacity of human beings to acquire a correct representation of events, institutions, and social processes, and make informed decisions affecting their communities and their own lives. At the same time, information can be disseminated in a deliberate way through multiple different channels, including social media networks, for perception management purposes so that a target state and their political leaders make decisions that benefit in some way or the other the goals of the hostile actors. Today's disinformation also hinders the ability of intelligence collection and analysis systems to provide analysis and assessments on a number of security issues. The volume, channels and speed information has, is unprecedented, challenging the intelligence cycles. Multi-domain activities and attacks are likely to be supported by the employment of information influencing activities that may seeks to increase uncertainty by introducing noise against intelligence production systems or by conducting activities in unattributable ways to covert sponsors. ICT and digital communication tools and channels with Artificial Intelligence added into the picture provide unique opportunities for conducting coordinated hostile activities that exploit the vulnerabilities of our democratic societies in targeted campaigns against individuals, institutions, and societies by the means of information and decision-making influencing.

While the communication content of symbolic interactions in social media platforms has varying degrees of visibility, coordinated inauthentic behaviours and the use of cyber-proxies challenge detection and attribution. The "weaponization" of information by hybrid threat actors can adopt multiple forms and raises the question of how to prevent, counter, and respond to it without undermining the democratic rights and liberties of our societies and how to detect the real threats from the polarization that always exist in democratic societies. Advancing the knowledge and understanding of hybrid threats through research and analysis is a prerequisite for developing effective policies and taking actions aimed at countering them. In these endeavours the role and awareness civil society and individuals is key, particularly when it comes to developing resilience societies against disinformation campaigns and hostile information influencing.

The special issue addresses this challenge of furthering hybrid threats from the information, cyber and digital communication perspective. It is important to understand the strengths of our digital ecosystems and societies as well as the systemic vulnerabilities of democratic societies. Equally important is to understand hybrid threats; the processes, methods, and tools by which hybrid threats target in coordinated campaigns and activities of democratic states.

The role of academic research becomes even more important than before to be able to show patterns and thinking behind Hybrid Threats. There is a need to understand better the phenomenon, those behind the activity and its changing nature. In this picture equally important become the collaboration between academia and practitioners. The academic research needs to be connected to practitioner experience and hand-on knowledge. Notes should be compared. The key in countering Hybrid Threats is the framework of whole-of-government and whole-of-society responses. This is central when it comes to detecting, countering and attributing malign disinformation. When designing the Call for papers for this special issue, we advanced the following list of research questions and potential themes and topics for a hybrid threats research agenda from a digital communication perspective.

## Topics

- Generative medias and Deepfakes
- Reflexive control and active measures in the cyberspace
- Policies and strategies to counter digital Information operations
- Inauthentic behavior and amplification
- Early identification, detection, and attribution of coordinated activities by threat actors
- Disinformation, divisive topic themes, and conspiracy theories in digital and traditional media
- Technology and Digital communication trends

- Awareness, digital society resilience to disinformation, and deterrence
- Open-source information and fact-checking
- Measurement and evaluation of disinformation effects
- Education and training to combat disinformation and communication-led hostile activities

## Research Questions

- What opportunities for malicious information influencing do the digital media ecosystem provide?
- Who are the main hybrid threat actors and how can they exploit the existing vulnerabilities of our societies?
- What technological developments like AI and automation are likely to be exploited in hostile strategic communication activities?
- How technologies can be used to detect and counter hybrid threats in the information domain?

While non a single special issue could realistically aspire to entirely address such a broad list of topics, the contributions of international scholars from Estonia, Norway, Romania, Spain, Sweden, the United Kingdom, United States, included in the present issue of Icono 14 offer good coverage of research articles on many of the topics above.

All the articles in this issue highlight the fact that today's security environment is very complex and multidimensional whether we are talking about theoretical approach, describing case-studies or looking at it from a practitioners' perspective. This character is inherent to hybrid threats too, which makes it difficult conceptualize and contextualize. This complexity requires similar conceptual tools and frameworks than multidisciplinary approaches. The multiple domains that can be potentially be targeted and affected means that without the multidisciplinary approach something will be missing in the analysis. This is highlighted in the ar-

ticles too; the role of gender and intersectionality for understanding how hybrid threats operate, the role of cyber, how old strategic culture traditions like Soviet reflexive control concept is still alive today, how psychological aspects need to be understood and used to build a defence, how we can trace narratives but how difficult they are to attribute, what needs to be taken into consideration about strategic communication and so on. Together the articles paint a picture of a very complex information landscape where new and old are mixed, where new tools are in use, where targets vary according to the purpose and where those not part of defence and security establishments are an important part of both resilience and being targeted.

The articles of this special issue are being organized according to an internal logic that first present conceptual and theoretical contributions, followed by case studies, and finally contributing articles focused on responses to disinformation as part of hybrid threats.

Firstly, Håkan Gunneriusson's contributing article "Hybrid warfare: development, historical context, challenges and interpretations" examines the emergence of the term hybrid warfare and its evolution as empirical situations evolved challenging initial conceptual elaborations and argues on the significance of Russia's strategy of reflexive control against the West highlighting the importance of the cyber domain with this regard. Gunneriussons outlook is not very positive for the future. In his view, the advances that both Russia and China have made can in the worst case challenge the whole international system unpredictable consequences. He makes some comparisons to the Cold War but sees that today's ideological battle is between the democratic states and authoritarian. The slow awakening of the West has been due to the globalized economy. In Gunneriusson article it is highlighted well how historical knowledge is important, analogies should not be taken always as one to one and how strategic interests can also hinder responses and /or threat perceptions.

Gunhild Hoogensen Gjørv in her article "Identity, stability, Hybrid Threats and Disinformation" adopts a concepts-oriented approach and argues on the relevance of and target civilians through disinformation with the aim of destabilizing soci-

eties, fueling polarization, and unrest and conflict. She shows how important an understanding of different concepts is when trying to make sense of our security environment. Hoogensen- Gjørv's argument is that when examining the ways in which men and women may engage in hybrid threats/ warfare differently, and how they might be targeted differently, allows us to think about different levels and strategies of resilience and resistance. Her claim is that we could expect that societies which were more gender equal might be more resilient to the hybrid threat activity which involves weaponizing social divisions to create civil conflict.

Ivo Jurvee's and Uku Arold's article shows the ways our security environment has changed through cyber and how we should be thinking about psychological defence from today's perspective. They show how Estonia has tackled the new security realm with a comprehensive national defence that is built upon understanding that the society itself is object of security and should provide appropriate safeguards and responses. Estonian conceptualisations of national cybersecurity, psychological defence, and strategic communications are elaborated in the light of actual seminal threat situations. In this context system-centric cyber-defence and value-centric psychological defence complement each other. In Jurvee's and Arold's article not only the case of Estonia becomes clear but also the multidisciplinary approach that is needed to counter Hybrid Threats.

Julian Richards' article shows how disinformation takes dominance in the British information space before the Scottish independence and Brexit referendum as well as in and around some other events. He highlights how difficult it is to differentiate between manipulative interference in the sense that is typical to Hybrid Threat activity and locally generated opinions. According to Richards "it cannot be denied that some degree of organised disinformation, a significant proportion of it conducted at the hands of the IRA in St Petersburg, has been going on". This highlights also the importance of open source academic research's role when learning more about actors behind Hybrid Threat activity. He concludes that the purpose of the activities is to "create a general fog of uncertainty and division in Western societies which can, in the longer term, have a strategic effect on politics and its evolution. Such developments also cause a generally destabilising effect in Western polities, whereby more extreme political expressions start to challenge

normative, mainstream views. These are issues not to be taken lightly". This is a strong recommendation to continue tracking activities through research but also actively taking action to counter it as well as build long term resilience against such activities.

Ellery G Cushman and Kiril Avramov analyze in their article sexuality and gender-based narratives in Russian and pro-Russian disinformation. By surveying the disinfo cases database of the Strategic Communication and Information Analysis Division of the European External Action Service (EEAS) from 2015 to 2020, Cushman and Avramov identify 25 specific narratives and seven broad metanarratives in the collected sample (N=185). The broad metanarratives that emerged from disinformation stories in their analysis include: "Western perversion of traditional morals and resulting collapse," "Disintegration of traditional gender norms in the West," "Western subversion via 'gender based ideology'," "Russia as the savior of traditional Christendom," "Sexual predation by an 'Other'," the "Complicity of Western elites, media, and judicial systems," and the "Extreme tolerance in the West". They conclude that "Russian and pro-Russian outlets utilize sexuality and gender-based narratives in disinformation operations because of their extremely potent emotionally based content and their ability to reuse storylines and narratives in different cultural contexts with only minor corrections" and include the recommendation of conducting further research on the ways these sexualities and gender-based narratives are being modified and tailored to target the specific features of national cultures.

Ileana Surdu, Mihaela Teodor Cristina Ivan and Irena Chiru bring in the practitioners approach. They present the results of an empirical sociological study within the CRESCEnt project (Mind the gap in media coverage and strategic communication in case of security threats) that aims to identify elements of enhancing critical thinking, responsible communication, and accountable behaviour. Three European states were targeted by the study: Romania, Spain, and Greece, while 28 practitioners in communication, intelligence and security and law enforcement contributed to the research with significant input on topics related to ethical, successful, and strategic communication characteristics. They explain the importance of ethical strategic communication and conclude with some guidelines for

the practitioners like "an institutional spokesperson or a journalist while conducting press releases or press conferences, or reporting to the public, must be able to establish and increase trust, cooperation, and awareness of the public, to develop a sincere and equitable relationship with the media". This highlights the fact that the way information is delivered counts perhaps more in today's media environment than the substance or facts.

Finally, Alba García-Ortega and José Alberto García-Aviles, "explore the potential of five newsgames designed to educate users against disinformation". Their article employs a qualitative matrix as a methodological tool for analysing a sample of newsgames that includes the newsgames Guerra a la mentira (RTVE Lab, 2017), iReporter (BBC, 2018), #Hacked (Al Jazeera News, 2016), Factitious (The American University Game Lab, 2017), and Bad News (DROG, 2018). The authors conclude that newsgames can be useful devices to raise awareness on fake news and counter disinformation on public issues.

The seven articles of this special issue give us insights to the role of digital communications and hybrid threats, both 21st-century phenomena that has challenged our societies, in today's security environment. Hybrid Threats present us a security puzzle, which we are still learning to respond to. The articles show how our information environment can be used against us but also how it can be our strength. There is still more to be discovered, but it's clear that academic research has a very important place in enhancing understanding, building resilience and finding ways to counter the Hybrid Threats. For the comprehensive understanding of the changes that have occurred theorization and conceptualization of different terms and concepts is needed, they need to be validated and examined in case-studies and then the results need to be connected to the practitioners and private sector. Three of the articles in this special issue are produced inside the framework of the EU-HYBNET Horizon 2020 project funded by the European Commission (No. 883054). The EU-HYBNET is a pan-European network of practitioners, stakeholders, academics, industry players and SME actors. The networks, that bring different actors together, are needed to find new innovative and creative solutions to the challenge Hybrid Threats present.

MONOGRAPH

# References

Council of the European Union (2019). Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions (Brussels, 10 December 2019). https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf

European Commission (2016). Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats: a European Union response JOIN/2016/018 final. https://bit.ly/3pi30b4

Giannopoulos, G., Smith, H., Theocharidou, M. The Landscape of Hybrid Threats: A Conceptual Model, European Commission, Ispra, 2020, JRC11728

Hoffman, Frank G. 2010. "'Hybrid Threats': Neither Omnipotent Nor Unbeatable." *Orbis 54*(3): 441–55.

John F. Kennedy, Address before the American Newspaper Publishers Association, 27 April 1961, jfklibrary.org/Research/Research-Aids/JFK-Speeches/American-Newspaper-Publish- ers-Association_19610427.aspx

NATO (2020). The Secretary General's Annual Report 2019. 19 March 2020 https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf