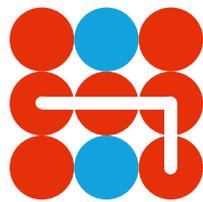

Strategic Analysis October 2018

**Post-event analysis of the
hybrid threat security
environment: assessment of
influence communication
operations**

RUBÉN ARCOS



Hybrid CoE

Post-event analysis of the hybrid threat security environment: assessment of influence communication operations

Besides the attribution challenges posed by covert influence actions, there is a need to develop effective frameworks for assessing and evaluating the effectiveness of overt and covert persuasive communications employed in the hybrid threat security environment, writes Rubén Arcos, lecturer in communication sciences at Rey Juan Carlos University in Madrid.

A key question for hybrid threat post-event assessment is who said what on behalf of whom, and why. In this context, the information in the hands of social networking companies might become indispensable for traceability and attribution. Besides the attribution challenges posed by covert influence actions, there is a need to develop effective frameworks for assessing and evaluating the effectiveness of overt and covert persuasive communications employed in the hybrid threat security environment; in other words, for analysing the cognitive, affective, and behavioural effects produced in targeted audiences and societies through the dissemination of disinformation content.

In the same way that **the dissemination of genuine information and sound judgments does not guarantee in itself that the message will be received and accepted, nor the propagation of fake news and biased opinions for influence purposes per se, such messages are likely to produce the intended influencing effects in the target publics that are exposed to them.** Hence, understanding the dynamics of information influencing is key when developing counter-measures and building resistance.

As Zimbardo and Leippe have pointed out, advertisers and agencies know full well that when they put their messages out there, it does not necessarily follow that the general public, and specifically their target audience, will see their ads. The more people watch a TV programme or follow a specific Twitter account, the more likely they are to be exposed to persuasive messages. However, the exposure of target audiences to persuasive communications does not guarantee an effective influence on attitudes and behaviour.

According to McGuire, from a processual perspective, in order to be influenced, the recipients of persuasive communications “must make the preliminary responses of paying attention to the message, comprehending its contents, accepting the conclusions advocated, and rehearsing this acceptance sufficiently to permit later expression of the induced change”. **Target audience segmentation and preliminary research and analysis for developing insights into targeted publics is a prerequisite for key message design and effective persuasion in influence campaigns.**



Existing research on alleged external interference tends to highlight the issue of whether such interference has occurred, but there is also a need for more research focused on the effects produced.

We need more evaluative research through the use of social research techniques to be able to provide findings on the cognitive/informational aspects (message exposure, understanding, and retention), attitude objectives (attitude creation, modification, and reinforcement), and behavioural effects (creation, change, and reinforcement) of overt and covert disinformation and propaganda campaigns. It is one thing to attempt to influence, but quite another to achieve such an outcome in practice. Effective influencing requires understanding the deeper characteristics of a country or region.¹ Moreover, if we better understand the effects, we might obtain a more nuanced picture of hostile actors' motives for their actions.

External meddling and the illegal Catalan referendum

The illegal Catalan referendum of 1 October 2017 is a case in point where the focus of the analysis has largely been to prove that there was outside interference. In this case, the allegations of external meddling point to Russia. According to

the 'EU versus Disinformation' portal, run by the European External Action Service East StratCom Task Force, "Pro-Kremlin accounts promoted Catalanian independence on social media, but on a smaller scale than was the case in the US".²

An unclassified May 2018 report by the Spanish National Cryptologic Centre (CCN) asserted that "the presence of activists sponsored by Russian institutions seems to be proven in the media coverage of the conflict ... in Catalonia during 2017".³ On 14 May 2018, the Spanish news agency EFE reported that Hans-Georg Maassen, president of the BfV (the domestic intelligence service of the Federal Republic of Germany), asserted during a speech at a symposium organized in Berlin to address the issue of hybrid threats that "the Russian government supported Catalan separatism with a disinformation campaign in the days leading up to the referendum".⁴ According to the newspaper *El País*, Maassen later clarified that they do not have "first-hand information; however, based on the sources we have examined it sounds very plausible and convincing and we are concerned".⁵ Earlier, on 23 September 2017, during the days leading up to the illegal Catalanian referendum, *El País* published a piece under the headline "La propaganda rusa sacude el 'procés'", later

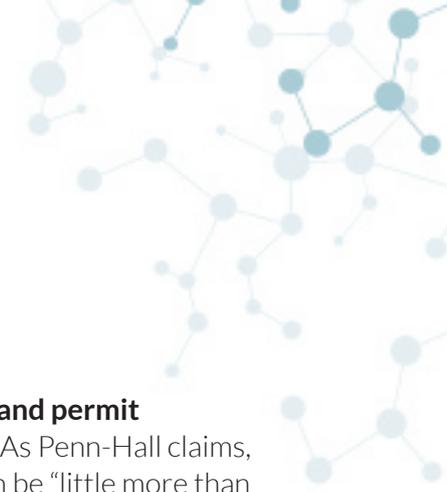
1 José-Miguel Palacios, former Head of the Analysis Division in the EU INT-CEN. Email interview with the author, 13 March 2018.

2 'Russian election meddling in the US and Beyond', 24 September 2018. Available at: <https://euvsdisinfo.eu/russian-election-meddling-in-the-us-and-beyond/>.

3 Translated by the author from the original Spanish and included as a footnote in the report 'Ciberamenazas y Tendencias 2018': "parece demostrada la presencia de activistas patrocinados por instituciones rusas en la expresión mediática del conflicto derivado de la situación creada en Cataluña durante 2017, como consecuencia del alejamiento de la legalidad constitucional vigente de ciertas instituciones autonómicas catalanas". Report available at: <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-edicion-2018-1/file.html>. Last accessed 24 September, 2018.

4 Translated from the original EFE's news story in Spanish. See <https://www.efe.com/efe/espana/portada/la-inteligencia-alemana-africa-que-rusia-apoyo-al-independentismo-catalan/10010-3615117>. Last accessed 23 September, 2018.

5 Translated from the original news story published by *El País*, 14 May 2018. See https://elpais.com/politica/2018/05/14/actualidad/1526297741_890840.html. Last accessed: 23 September, 2018.



translated into English as “Russian meddling machine sets sights on Catalonia”, stating that “The network of fake-news producers that Russia has employed to weaken the United States and the European Union is now operating at full speed on Catalonia, according to detailed analyses of pro-Kremlin websites and social media profiles by this newspaper”.⁶

Nor does the list of allegations implying that there was meddling in the information space prior to the referendum end there. **In some cases a clear and direct link to the Russian state is made.** For example, the July 2018 Interim Report of the UK House of Commons Committee on Disinformation and ‘fake news’ concluded that “Russia had a special interest in discrediting the Spanish democratic system, through Russian state-affiliated TV organizations spreading propaganda that benefitted those wanting independence in Catalonia”.

In other cases, bot armies that work to further the interests of the highest bidder for profit, basically mercenaries working for whoever is willing to contract their services, be they companies engaged in digital marketing or governments, have been mentioned. **By using proxies – groups separated from state governments but empowered to act on their behalf – it is possible to conceal the identity of the sponsor, obscure the**

nature of the threat, and permit plausible deniability. As Penn-Hall claims, sometimes proxies can be “little more than thinly veiled organs of a state’s security apparatus, while others are completely separate and autonomous organizations that function almost like contractors”.

The stories that are fed into the information space also use social media networks like Twitter⁸ to escalate existing tensions. Maldita.es, a Spanish portal member of the International Fact Checking Network, has collected cases of fake news related to Catalonia, including a tweet by the Catalan online newspaper El nacional.cat, “L’exèrcit de espanyol mou blindats a Catalunya bit.ly/2w2VshM” (The Spanish Army moves armoured vehicles in Catalonia).⁹ In the days leading up to 1 October, Twitter accounts disseminated fake stories about bogus statements by European leaders, such as the Prime Minister of Estonia, on the recognition of Catalonia’s right to decide its own future.¹⁰ The amplification of these kinds of stories through the use of fake accounts and social network bots may have the effect of giving them an aura of credibility in the eyes of uncritical users.

Furthermore, historian Jordi Canal has highlighted the key role played in the procés by “parainstitutional” organizations like the Catalan National Assembly (ANC) and Òmnium Cultural.

6 El País, 28 September 2017. See https://elpais.com/elpais/2017/09/26/inenglish/1506413477_994601.html

7 ‘No son bots rusos, es Capitalismo 3.0 reventando el debate político online’. El Diario.es, 20 November 2017. Available at: https://www.eldiario.es/politica/bots-rusos-cyborgs-mercenarios_0_708680008.html

8 <https://twitter.com/ActualidadRT/status/924108566935547904>

9 See: <https://maldita.es/bulo/no-el-ejercito-no-ha-mandado-ni-movido-blindados-en-cataluna/> Last accessed 23 September, 2018.

10 For example, as documented at Maldita.es, on 15 September 2017 the Twitter account @ElinaStig disseminated the following tweet, attracting more than a thousand retweets and a similar number of likes: “ARA MATEIX, 1er min. Estònia: @ratasjuri: “Catalunya té dret a decidir el seu futur, nosaltres ho vam fer un dia, perquè s’ho hem de negar?” (RIGHT NOW, 1st Minister Estonia: @ratasjuri: Catalonia has the right to decide its future; we did it once, so why should we deny it?) See: <https://maldita.es/bulo/no-el-gobierno-de-estonia-no-ha-apoyado-la-autodeterminacion-de-cataluna/>. According to Maldito Bulo, the account is owned by a person from Gavá (Barcelona): <https://maldita.es/bulo/no-el-gobierno-de-estonia-no-ha-apoyado-la-autodeterminacion-de-cataluna/>.



For some experts, the secessionist communicative strategy was effective and counted with the media broadcasters of the Catalan Broadcasting Corporation, particularly TV3 and Catalunya Radio, while the communication strategy of the Government of Spain was poor and reactive, if not non-existent.¹¹ It seems clear that the independentist narrative and its strategic communication activities were targeting international publics to weaken the Spanish position before the European Union.

It is unlikely that the effects of external information influencing have been decisive in the case of Catalonia. Rather, the evolution of events has responded to pre-existing internal logics in which the dissemination of inaccurate, biased, purposely deceitful, or partial information, either by external or internal actors, has had the effect of reinforcing pre-existing biased beliefs and attitudes, igniting existing tensions, causing confusion in international audiences, and obstructing the development of a prudent democratic debate. **It is worth noting that external actors have paved the way for hybrid influencing operations by seeking out those inciting tensions and testing the waters, so that they can use the target societies' weak spots to disrupt, incapacitate, and exert harmful effects on the targeted actor when needed for the benefit of the agent's interests and goals.**

A model for post-event analysis and assessment of information campaigns as a part of hybrid threat influence operations

Developing indicators and metrics for impact evaluation is key to understanding and assessing overt and covert communication activities in the hybrid threat security environment. Lasswell's

construct (and its variations) remains a relevant conceptual tool for describing the act of communication. The most famous version of this model is, "Who says what, in which channel, to whom, with what effect?" A modified version of Lasswell's construct, in one of his variations, provides a structured framework for addressing the post-event analysis and assessment of information campaigns as a part of hybrid threat influence operations:

Who says what?

On behalf of whom (or on its own behalf)?

With what intentions?

In what situations?

With what assets?

Using what strategies (key messages and channels)?

To which audiences?

Producing what kind of effects?

The model captures the structure of the communication process and considers the information (or disinformation) and opinion source, its capabilities and intentions, and effects produced (cognitive, affective, and behavioural impacts, as well as outcomes) by disseminating specific communication content (key messages) to targeted audiences. **A systematic examination of the communication process by answering the key questions posed by the model drives critical thinking in the consumption of information, provides exposure to the elements involved, and unveils the patterns and dynamics of persuasion through the use of communication (symbolic and behavioural). This is key for providing an understanding of the influencing attempts, and for developing strategies and tactics for counteracting the effects of influence operations.**

¹¹ Joan Antón, Professor of Political Science at the University of Barcelona. Email interview with the author, 17 March 2018.

Psychological research on resistance to persuasive communication has shown that by being forewarned about an imminent persuasive attack, the receiver of the message will develop resistance to the attack once it has taken place and, as a consequence, will be less persuaded if the topic has direct personal relevance inasmuch as the targeted audience will generate counter-arguments. However, as pointed out by Sagarin and Wood, “before the attack takes place, forewarning causes resistance for personally involving issues, but anticipatory agreement for less involving issues”. This is why instilling critical thinking in the consumption of information, and awareness campaigns about hybrid threats have become so important.

The importance of separating persuasion from hybrid influencing

Social influence is all-pervasive; as individuals we engage in social interaction processes with family, friends, and professional peers, and play a dual role as (1) targets of influence attempts by others, and (2) agents attempting to influence our target’s thoughts, attitudes, and behaviours. **Bearing this in mind, it is important to underline that persuasion and influence are not inherently toxic, and do not constitute a threat *per se*.**

When we talk about impeding threats in the context of influence operations, we are referring to operations that are not open or have not been attributed. Both aspects challenge the traditional countermeasures and hinder alliance building. Active measures (*aktivnyye meropriyatiya*) and covert action operations, seen as a part of the Kremlin’s playbook with their origin in Soviet KGB strategic thinking, have traditionally involved disinformation, covert propaganda, front organizations, or the use of paramilitary

organizations for political influence purposes. **Traditional state-sponsored covert influence operations aim to influence the events, developments, people, and decisions of targeted foreign entities in support of the foreign policy goals and objectives of the covert sponsor.** They are by definition difficult to attribute, and finding direct tangible evidence (operation planning documents, for example) might be an extremely difficult task.

States that are surreptitiously involved in covert action operations seek to plausibly deny sponsorship in ongoing events and past events. However, as argued by Cormac and Aldrich, the act in itself might be clearly visible or leave trails, and sometimes a deliberately calculated degree of exposure by the perpetrator can serve to put pressure on the target. What this implies is that **if a careful post-event analysis and assessment is not conducted, we might end up doing the adversary’s work ourselves if our counter-actions are based on too hastily drawn conclusions about the effects.**

Author

Dr. Rubén Arcos, PhD, is a lecturer in communication sciences at Rey Juan Carlos University in Madrid. He is founding co-director of IntelHub, a joint initiative between the American Public University System, the University of Leicester in the UK, and Rey Juan Carlos University in Spain. He is a freelance contributor to Jane's Intelligence Review and deputy editor of The International Journal of Intelligence, Security, and Public Affairs. He has served for almost 10 years as instructor and coordinating director of the first ever Master's degree in Intelligence Analysis in Spain. Dr. Arcos has published extensively on intelligence studies, strategic communications, and experiential learning in intelligence through simulations and games. He has been appointed national member of NATO Task Group SAS-114 on 'Assessment and Communication of Uncertainty in Intelligence to Support Decision-Making'. His latest publications include the books Intelligence Communication in the Digital Era: Transforming Security, Defence and Business (co-edited with Randolph H. Pherson) and The Art of Intelligence: Simulations, Exercises, and Games (co-edited with William J. Lahneman).

Literature:

Canal, Jordi (2018). Con permiso de Kafka: el proceso independentista en Cataluña. Barcelona: Península.

Centro Criptológico Nacional (2018). CCN-CERT IA 09/18 - Ciberamenas y tendencias 2018. Madrid: Gobierno de España. Available at: <https://www.ccn-cert.cni.es/en/reports/public/2835-ccn-cert-ia-09-18-ciberamenas-y-tendencias-edicion-2018-1/file.html>

Cormac, Rory and Richard J. Aldrich (2018). 'Grey is the new black: covert action and implausible deniability', International Affairs 94 (3): 477-494.

Coombs, W. Timothy and Sherry J. Holladay (2007). It's Not Just PR: Public Relations in Society. Oxford: Blackwell.



Harjanne, Atte, Muilu, Eetu, Pääkkönen, Jekaterina, and Hanna Smith (2018). Helsinki in the era of hybrid threats – Hybrid influencing and the city. City of Helsinki, publications of the Central Administration.
Available at: <https://www.hybridcoe.fi/publication-tags/reports/>

Hayes, Darrell C., Hendrix, Jerry A., and Pallavi D. Kumar (2013). Public relations cases, 9th edition. Boston: Wadsworth.

House of Commons Digital, Culture, Media and Sport Committee (2018). Disinformation and 'fake news': Interim Report. Fifth Report of Session 2017–19. Report, together with formal minutes relating to the report, ordered by the House of Commons, printed 24 July 2018.

Lasswell, Harold D. (1948). 'The structure and function of communication in society'. In *The Communication of Ideas*, edited by Lyman Bryson. New York and London: Institute for Religious and Social Studies, 37–51.

Lasswell, Harold D. (1968). 'The uses of content analysis data in studying social change', *Social Science Information* 7(1), 57–70.

McGuire, William J. (1966). 'Order of presentation as a factor in "conditioning" persuasiveness'. In Hovland, Carl I. (ed.) *The order of presentation in persuasion*. New Haven and London: Yale University Press, 98–114.

Penn-Hall, Luke (2016). 'The problem with proxies', *The Cipher Brief*, July 21, 2016. <https://www.thecipherbrief.com/the-problem-with-proxies>.

Sagarin, Brad J. and Sarah E. Wood (2007). 'Resistance to influence'. In *The science of social influence: advances and future progress*, edited by Anthony R. Pratkanis. New York and Hove: Psychology Press, 321–340.

Sapienza, Zachary S., Narayanan, Iyer, and Aaron S. Veenstra (2015). 'Reading Lasswell's Model of Communication Backward: Three Scholarly Misconceptions', *Mass Communication and Society*, 18(5), 599–622.

Treverton, Gregory F., Thvedt, Andrew, Chen, Alicia R. Lee, Lee, Kathy, and Madeleine McCue (2018). *Addressing Hybrid Threats*. Bromma: Swedish Defence University.

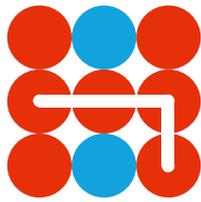
Zimbardo, Philip G. and Michael R. Leippe (1991). *The psychology of attitude change and social influence*. Boston: McGraw-Hill.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi @HybridCoE

ISBN: 978-952-7282-12-0

Hybrid CoE is an international hub for practitioners and experts, building member states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

The responsibility for the views expressed ultimately rests with the authors.



Hybrid CoE