Péter Balogh

COMPLEX CHALLENGE OF COMPLEX SOCIETIES: HYBRID THREATS OF THE NEW MILLENNIUM

ABSTRACT: *The paper outlines some remarks concerning the conceptual background of hybrid warfare. Focusing on the wider societal aspect of the phenomenon it suggests that legitimacy can be considered a key element of hybrid conflicts and proposes that such concepts as channels and embeddedness may be fruitful to interpret the processes and patterns on which hybrid threats are based. This section also introduces a kind of network approach. These elements of the presentation may contribute to a better illustration and comprehension of certain characteristics of hybrid warfare in complex societies. After briefly outlining the methodology of the empirical research, the second part of the paper introduces some of the results of case studies. It covers a wide scope of the research problem, so the processes and patterns introduced in the first section are demonstrated using various examples. That is, in the case studies the hybrid operation potential of both interest-driven states and ideologically motivated non-state actors is outlined. The case studies have a specific focus on contemporary cyber operations and the informational and cognitive dimensions of influence operations. The empirical examples cover relevant elements concerning Europe, and imply that hybrid actors can find several ways to enforce their will. Finally, the outcomes and research results are summarized, also addressing the problem of employing non-military and military approaches in light of the complexity of hybrid conflicts.*

KEYWORDS: *hybrid warfare theories and concepts, influence, embeddedness, network*

ABOUT THE AUTHOR:
Dr Péter Balogh is a lecturer at the University of Szeged, Department of Sociology; baloghp@socio.u-szeged.hu

INTRODUCTION – HYBRID WARFARE

The concept of hybrid warfare has become a rather important and widely employed model since the notion appeared in the scientific sphere in 2002. Besides that, the theory of hybrid warfare represents a rather complex, multi-faceted phenomenon of the New Millennium. A further notable feature of the concept is a single scholarly interpretation for it does not exist. That is, the concept itself is a subject of debate: in light of the efforts of military scientists Somodi and Kiss[1] to systematize the different international approaches of hybrid warfare, four different directions of interpretation can be explored. Based on their literature review the authors argue that some consider hybrid warfare a (1) completely new phenomenon. In this sense hybrid warfare seems to be a rather flexible form of applying and integrating methods and operations in order to achieve the objectives of the hybrid actor, with

[1] Kiss, Á. P. – Somodi, Z. "A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban". Honvédségi Szemle, 2019, 147 (6), 22–28.

a strategic advantage that stems from uncertainty and the delayed and/or improper reaction of the attacked country.[2] The second – partially different – approach considers hybrid warfare (2) not entirely new, but still it has certain novelties. This perspective argues that certain elements connected to the 21st century form of hybrid warfare can be found in earlier conflicts and wars throughout history, however, in certain aspects hybrid warfare proves to be unique. On the one hand the purposeful and rather effective coordination of several different methods and activities in various domains characterizes hybrid warfare, on the other hand the important role of the cyber sphere can be recognized as a novel feature.[3] Another interpretation emphasizes that the concept of hybrid warfare characterizes much more those who employ it to describe and understand the activities of the adversary (in this case dominantly the Russian Federation), rather than being useful to better comprehend the real picture. Accordingly, this third type of interpretation expresses that (3) hybrid warfare has not got any novelties.[4] In contrast, the fourth group of interpretation can be linked to the scholars of Russian military science and argues that hybrid warfare can be considered as (4) the strategy of the Western states against Russia. In this sense, hybrid warfare can be a new and effective method to destabilize and weaken the Russian Federation[5] – of which the objective is a significant element of the Russian threat perception.[6] The authors emphasize that in the case of the first interpretation – hybrid warfare as a completely new phenomenon – the clashes of narratives prove to be a significant element of hybrid warfare, however – in a somewhat contradictory manner – the concept of hybrid warfare itself also seems to be embedded in a kind of narrative contest.

This specific kind of conflict can be characterized with a high level of complexity: different conceptual sources identify and highlight several sectors or domains that can become affected in the case of a hybrid conflict.

Kiss[7] describes a concept of hybrid warfare in order to illustrate the distinct relevant areas of operation and also highlights the importance of coordination and synchronization of action among these sectors. The model nominates six different segments which represent the system of the society attacked by hybrid operation: the military, political, economic, social, the information and infrastructural areas can be distinguished and utilized in order to illustrate and understand the complex procedures hybrid operators can carry out. The interpretation proves to be rather useful as it differentiates between the direct and indirect effects of an attack, and highlights that certain additional, indirect effects can cross actual segments.

In their model Bekkers, Meessen and Lassche[8] employ a similar approach with an emphasis on the need of synchronization among a total of five different sectors. When investigating the areas of horizontal and vertical escalation, the concept employs DIMEL model

---

2 Somodi – Kiss "A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban". 22–23.

3 Somodi – Kiss "A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban". 24.

4 Somodi – Kiss "A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban". 25.

5 Somodi – Kiss "A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban". 26.

6 In this regard it seems worth to be mentioned, that when characterising the second form of interpretation – hybrid warfare is not novel, but still it is –, the authors also add, that NATO has employed a similar, hybrid-like approach in Iraq and Afghanistan with a coordination of complex methods in different domains (Somodi – Kiss 2019, 24), which indicates that the allied forces could have capabilities, competences and experience in hybrid-like multi-domain approach.

7 Kiss Á. P. "A hibrid hadviselés természetrajza". Honvédségi Szemle, 2019, 147 (4), 17–37.

8 Bekkers, F. et al. "Hybrid Conflicts: The New Normal?" The Hague Centre for Strategic Studies, 2018.

which extends the classical DIME[9] (diplomatic, informational, military, economic instruments) by incorporating the legal (L) segment. They contrast the intentional and perceptional dimensions of hybrid operations and accordingly highlight the role of terminology, narratives, and even the transformation of the interpretation of an actual event in light of the evolution of the situation.

Complexity of hybrid warfare can also be illustrated if we consider the several possible dimensions of attack Richterová[10] introduces. The concept integrates privatized power, terrorist, cyber, diplomatic power to military, political and economic power. Furthermore, it argues that civil power and media power can also be utilized against the national, governmental, international domains, critical infrastructure, financial market, media, the research and scientific sector, education and civil society – a total number of nine particular spheres.

However, the rather multi-faceted and complex conceptual model of hybrid warfare[11] introduces 40 tools that can be applied when trying to organize a hybrid operation against thirteen different possible domains. In this case, the military and defence sector is supplemented with infrastructure, cyber sphere, space, economy, culture, social or societal segment, public administration, legal sphere, intelligence, political domain, diplomacy, and information.

The theoretical frameworks, conceptualisations and models of hybrid warfare briefly introduced above illustrate that the military can be regarded a significant domain of the operations in a hybrid context, but it is not the most important or even the dominant sector when the problem of defence evolves. Before introducing the interpretation applied in our investigation it seems fruitful to highlight the concept and arguments about the role of the military in hybrid warfare by Schmid.[12] The author brings several reasons towards a shift of the perception on hybrid warfare when defining the main characteristics of the phenomena. According to the empirical experience based on the Ukrainian events since 2014, the researcher explores three characteristics of hybrid warfare: (1) a wide range of methods and means of the military domain can be applied in this specific type of conflict, however, the focus of the activities is based on primarily non-military ones – politics, morale, legitimacy. Military forms of power represent essential methods to facilitate and support the non-military domains to succeed. The primacy of non-military activities in the decision of a hybrid war can also be confirmed by the argument that (2) hybrid warfare exists and operates in a transitional space between war and peace, taking advantage of activities in the gray zone and vulnerabilities of combinations of internal and external factors. Therefore, hybrid warfare becomes a highly refined, versatile and integrated form of conflict when (3) applying both civilian and open forms of fighting, and military or covert methods in a coordinated way at the same time. Accordingly, this revised concept of hybrid warfare illustrates an approach that emphasizes the need to move away from a military-centric perception towards a concept of hybrid warfare that is dominantly based on non-military

[9] For a reconstruction and interpretation of hybrid warfare from a DIME perspective see Lowe, D. – Pitinanondha, T. "Conceptualisation of Hybrid Warfare". Defence Science and Technology Group, Australia, 2015.

[10] Richterová, J. "NATO and Hybrid Threats". Prague Students Summit, Background report. Asociace pro mezinárodní otázky (AMO), Prague, 2015.

[11] Giannopoulos, G. et al. "The Landscape of Hybrid Threats: A conceptual model". EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021.

[12] Schmid, J. "Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence". Journal on Baltic Security, 2019, 5(1): 5–15.

aspects,[13] also involving the replacement of a hierarchical perspective with a more composite and multi-related structure (Figure 1).

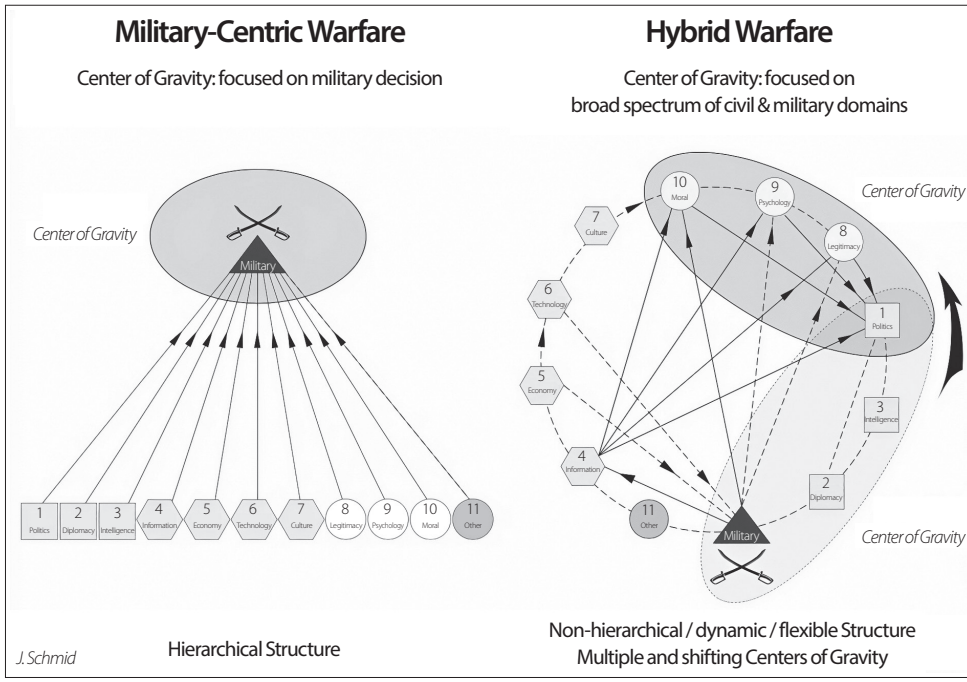


Figure 1 *The difference between Military-Centric Warfare and Hybrid Warfare (1: Politics, 2: Diplomacy, 3: Intelligence, 4: Information, 5: Economy, 6: Technology, 7: Culture, 8: Legitimacy, 9: Psychology, 10: Moral, 11: Other)*
Source: *Schmid 2015, 15.*[14]

APPROACH OF THE INVESTIGATION

In order to introduce the conceptual approach our study has been based on, it is useful to start with the widely known thought from Clausewitz,[15] that war is a continuation of politics with different measures. Conversely, in this aspect we could also argue that politics is the *continuation of war* using different methods. In this regard, the connection between warfare and politics might direct our attention towards the notion of legitimacy, which can be considered a central element of the problem.

[13] Regarding the number of different sectors relevant from the perspective of hybrid operations, this concept proves to be an intermediate one as it describes eleven domains – besides military politics, diplomacy, intelligence, information, economy, technology, culture, legitimacy, psychology, moral are included, supplemented with category other as well (Schmid, J. "Hybrid warfare on the Ukrainian battlefield". 15.).

[14] Schmid, J. "Hybrid warfare on the Ukrainian battlefield". 15.

[15] Clausewitz, C. v. "A háborúról". Zrínyi Kiadó, Budapest, 2016.

As classical social scientific arguments point out,[16] an actor can reach his or her objective by using physical pressure or the threat thereof, in order to make others behave according to his will – even against the will of others. This is the case of *power,* which might be related to warfare regarding the possibility of threatening or applying physical pressure or violent methods to make others comply with the actor's will. The other possibility is *authority,* in which case the actor's will is coupled with the acceptance of others regarding the actor's control. *Legitimacy* offers obedience of the ones controlled, which might be based on various factors.[17]

Accordingly, in this investigation we propose that hybrid threats or hybrid warfare might be interpreted as a specific form of attempt by various actors to impose their will: they seek to act – at least seemingly – legitimately and try to appear as actors that have a certain level of authority regarding the ones they wish to control. Similarly, hybrid operations can be considered as measures that *enable the actors to reach their objectives reinforced with authority,* instead of methods based on power.[18] In some cases these operations might even cause the weakening of the actually legitimate actor. At this point, it should be emphasized, that legitimacy and the chance to become an – at least partially or seemingly – authorized actor stem from the population sought to be controlled. This raises the question of how a population can be convinced and encouraged to accept an actor's will.

One possible option is to make the population familiar with the values, objectives, methods etc. offered by the actor and make them feel that these values and objectives are desirable, acceptable, and worth following. At this stage emerges the problem of *influence*.

In order to illustrate the problem of influence in this context, it can be fruitful to invoke the concept of complex security, consisting of six different sectors of security.[19] Hybrid operations enable their initiators to influence the population planned to be controlled by penetrating certain security sectors. By addressing the economic sector with a direct measure – for example with development and investment programs – a possible indirect effect can be reached towards the political sector (see Figure 2).

In our research project we propose to refer to these direct impacts as possible *entry points,* and argue that if certain entry points prove to be functional and effective, then certain kind of *channels of influence* might emerge or be created. In this way, hybrid operations could be interpreted as efforts made by an actor to channel its will towards others to enable control.

We can complement or exceed this static model on the one hand (1) if we suppose, that a certain channel – after some time – can result in changes that *offer further entry points* and create *potential channels* (Figure 3). In this way, an actor can reach more security sectors as well, and might become more and more *embedded* in the targeted society.

On the other hand, if there are (2) multiple channels available, their operation and effects can be organized, coordinated and synchronized in a way that the impacts reinforce each other and multiply the potential of control and influence (see Figure 4).

---

[16] Weber, Max. "Gazdaság és társadalom. A megértő szociológia alapvonalai I". Közgazdasági és Jogi Könyvkiadó, Budapest, 1987.

[17] Weber, M. "Gazdaság és társadalom". 77., 221–225.; see also Farkas, Z. "A hatalom és az uralom fogalma". Politikatudományi Szemle, 2011, XX/2, 31–49.

[18] Note that all conceptual frames introduced above identify political sphere as a specific domain of hybrid warfare, furthermore several models contain legal domain as a relevant one (see for example Bekkers – Meessen – Lassche. "Hybrid Conflicts: The New Normal?", Giannopoulos – Smith – Theocharidou. "The Landscape of Hybrid Threats".).

[19] Buzan, B. et al. "A biztonsági elemzés új keretei". In Póti, L. (ed.) Nemzetközi biztonsági tanulmányok. Zrínyi Kiadó, Budapest, 2006, 53–112.

Another possible case worth mentioning can emerge when (3) other actors appear in the scene, and the actual legitimate governing actor needs to consider several possible challengers with several possible networks of influence channels (see Figure 5).

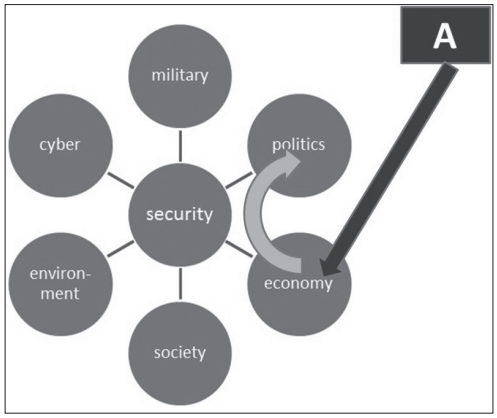


Figure 2 *Direct and indirect effects by Actor (A) in the security sector of a society (Edited by the author)*

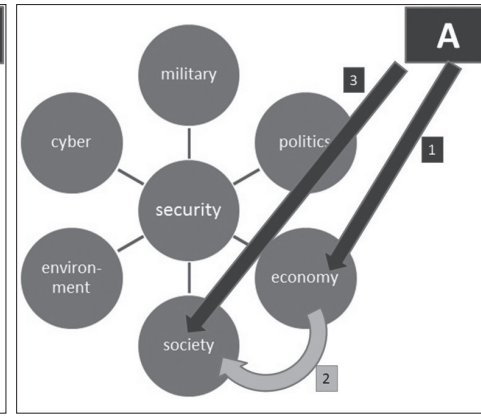


Figure 3 *Direct and indirect effects by Actor (A) to create further entry point (Edited by the author)*

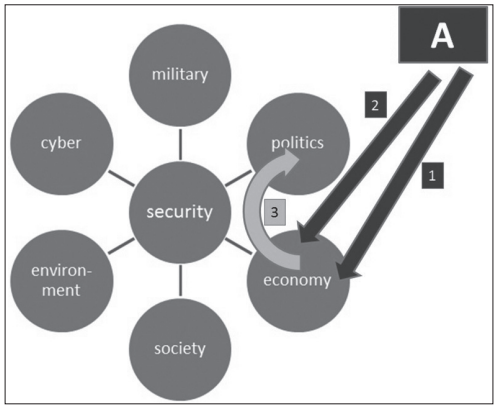


Figure 4 *Multiple coordinated direct effects by Actor (A) to increase influence potential (Edited by the author)*

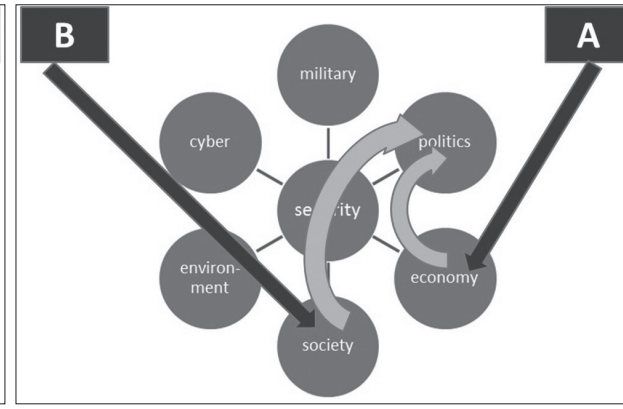


Figure 5 *Multiple actors (A, B) initiating direct and indirect effects (Edited by the author)*

The cases introduced above illustrate different possible forms of channels, effects, and influence. However, other cases can also be described. Furthermore, under realistic conditions these forms can be combined and coordinated by the initiators, leading to rather complex channels of influence adapted to the actual circumstances. It should also be emphasized, that a similar kind of channels can not only be *intentionally created* by a hybrid threat actor, but might also *emerge* due to different social processes, and the latter ones may also play significant roles and have important effects.[20]

[20] In the empirical investigations we make efforts to illustrate this rather interesting pattern.

Accordingly, we suppose that this *process of channelling control* and the *patterns of embeddedness* seem to be both important and interesting aspects of hybrid threats, and worth investigating in order to better comprehend the challenge they pose. In the next section, we investigate the topic with empirical case studies. Our empirical case studies are based on a quantitative approach supplemented with network analysis methods: we reconstruct control channels and patterns of embeddedness based on two basic, directed dyadic relations: A initiates an action (X) that is directed toward a certain security sector of B, which serves as an intermediary (see Figure 6).

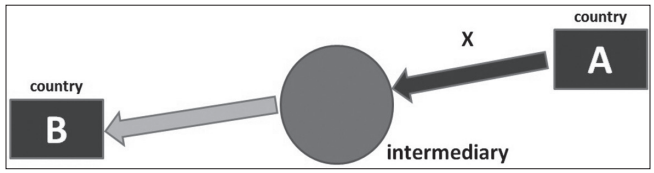


Figure 6 *Basic model of control channels in two-actor relation (Edited by the author)*

METHODOLOGICAL REMARKS

During the methodological design and preparation of the investigation we made efforts to explore possible data sources and gather data to elaborate quantitative case studies. The sources included academic publications, policy papers, registers available online, official data and statistics, as well as research outputs of other academic and policy research organizations. Based on this information complex datasets were assembled regarding the four case studies.

The case studies included two state actors, and two non-state actors were also investigated. Besides China and Russia as the two potential challengers of Western dominance and primarily the United States, a global inclusive social development movement aiming to facilitate equity and fairness towards discriminated minority groups, finally a jihadist extremist networks were also addressed. The latter ones are to illustrate the importance of the social aspects and that the activities of certain non-state actors might also be relevant in regards to the channelling issue, and may even have – an unintended – effect on the security structure of societies.

The case studies have a focus on, but not limited to, the European Union and NATO countries.

RESEARCH RESULTS – CASE STUDIES (CS)

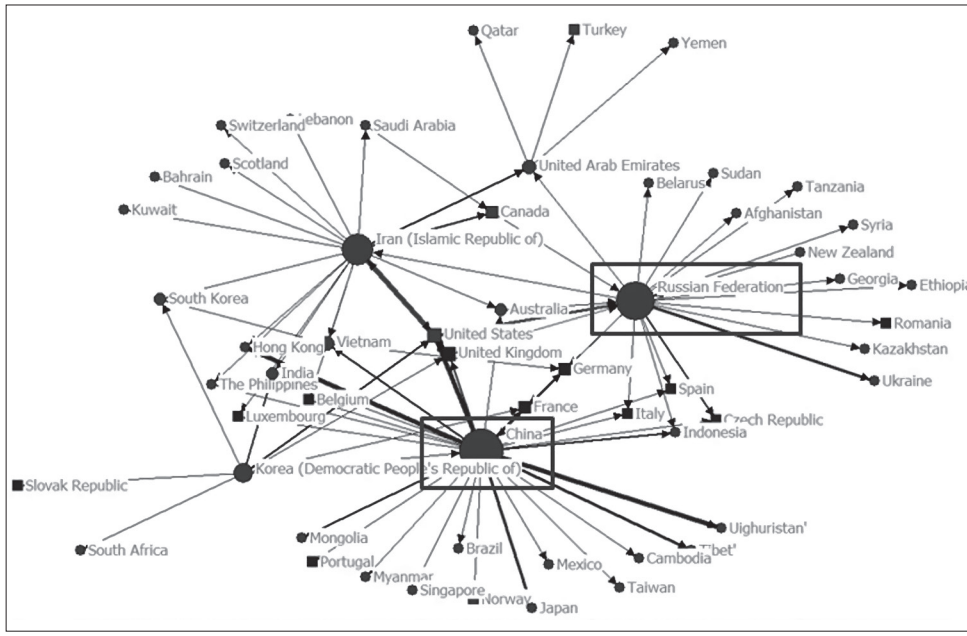
CS1 and CS2 – China and Russia

Considering global firepower, defence budget values and ranks, it proves to be indisputable that the United States of America is the most significant and powerful state in the global sphere.[21] However, China and Russia seem to be the two main challengers of the US and

[21] See for example: https://www.statista.com/chart/20418/most-powerful-militaries/, https://www.iiss.org/blogs/military-balance/2019/02/european-nato-defence-spending-up and https://twitter.com/iiss_org/status/1396793354143289348

the recent status quo, with a presumable intent and urge to catch up with and reduce the dominance of the US.

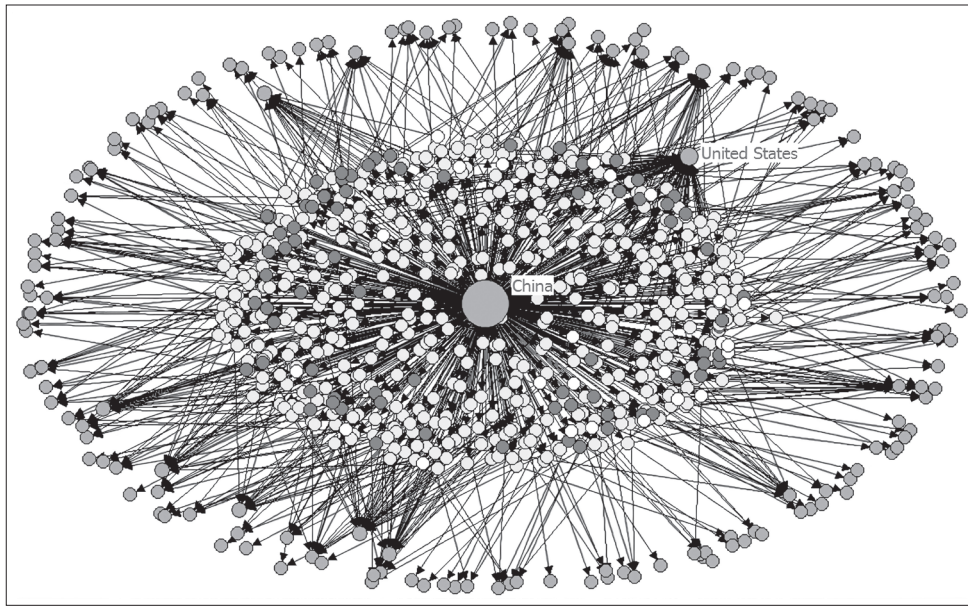
However, China and Russia seem to compensate their relative disadvantage not only in hard power: the non-kinetic domain of cyber activities proves to be a potential area to build capacities and carry out operations without possessing the most advanced physical requisites – for example warships or tanks – of hard power. This can be corroborated if we consider a recent network of state-sponsored cyber operations (see Graph 1), where China and Russia prove to be the first and second most notable actors in a triplet with Iran.



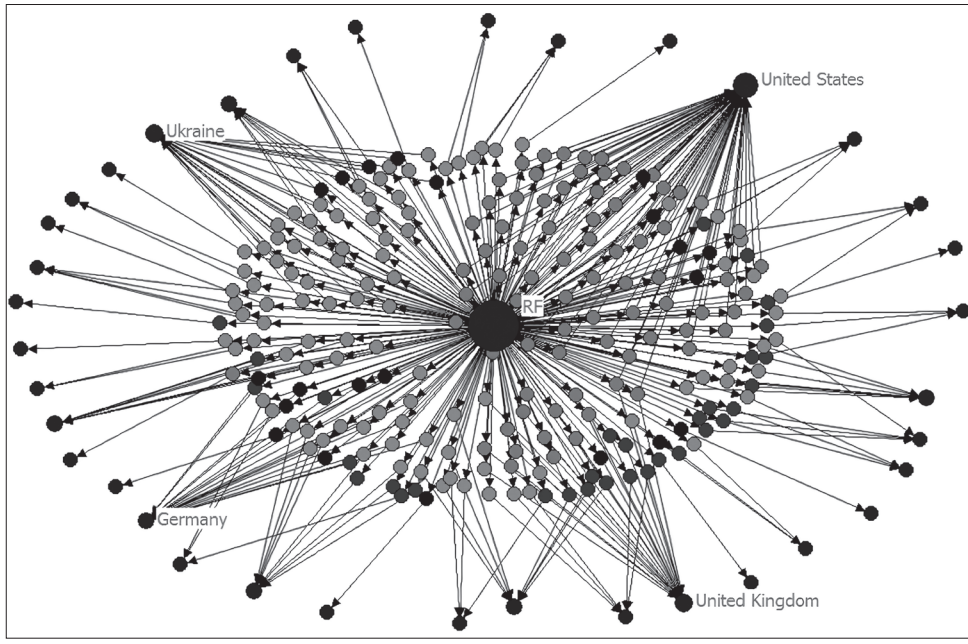
Graph 1 *Network of state-sponsored cyber operations (2019)*
(Edited by the author based on complex database)

Accordingly, in the first case study we made efforts to collect extensive data about possible entry points and channels regarding China. Based on the present results, three types of intermediaries could be mapped: the above mentioned (1) cyber operations, (2) cultural institutes as a form of soft power or cultural diplomacy, and (3) economic investment and development projects. These links and channels create a rather large-scale network of influence potential reaching several countries globally – latter ones can be found in the outer circle on the graph.

Some *multiplex relations* can be explored in the former case of China as well, however, the case study about Russia illustrates better this specific kind of tie, when more types of channels are present in a country – with the potential to multiply influence. This can be seen in the examples of Ukraine or the United States, and might be explained as there can be explored four types of channels in the network of the Russian case: besides (1) cultural institutions and (2) cyber operations, (3) extremist political formations and (4) internet trolls can also be identified as potential mediators between the investigated countries. These characteristics result in a smaller but more structured network in this case.



Graph 2 *Network of China illustrating three channel types*
(Edited by the author based on complex database)



Graph 3 *Network of the Russian Federation illustrating four channel types*
(Edited by the author based on complex database)

Although the data sources and data coverage are not standardised between the case studies of China and Russia – therefore a direct and rigorous comparison cannot be carried out, it is only an illustrative pattern – it might be mentioned that from a network analysis perspective the Russian case proves to be both a *denser* and *more centralised* network as it is shown in density and centralization values (see Table 1). It can also be concluded, that both cases illustrate an orientation towards NATO member states: higher average level of ties can be measured, especially in the Chinese case, and it can also be noted, that there seems to be a difference regarding the ties towards EU-member countries: the distribution of the links implies that in the Russian case a higher focus can be observed towards non-EU-member European countries.

Table 1 *Descriptive statistics of the networks from CS1 and CS2*
(The lower values indicated with bold letter type. Calculations by the author)

	China	**Russia**
	Network characteristics	
Density (matrix average)	**0,0020**	0,0065
Network Centralization (InDegree)	**10,923**	25,198
Country groups	**Network embeddedness (average InDegree)**	
Non EU member	**3,6**	9,4
EU member	6,0	**4,9**
Non NATO member	**2,9**	**4,0**
NATO member	9,0	7,6
Total	**4,0**	**6,4**

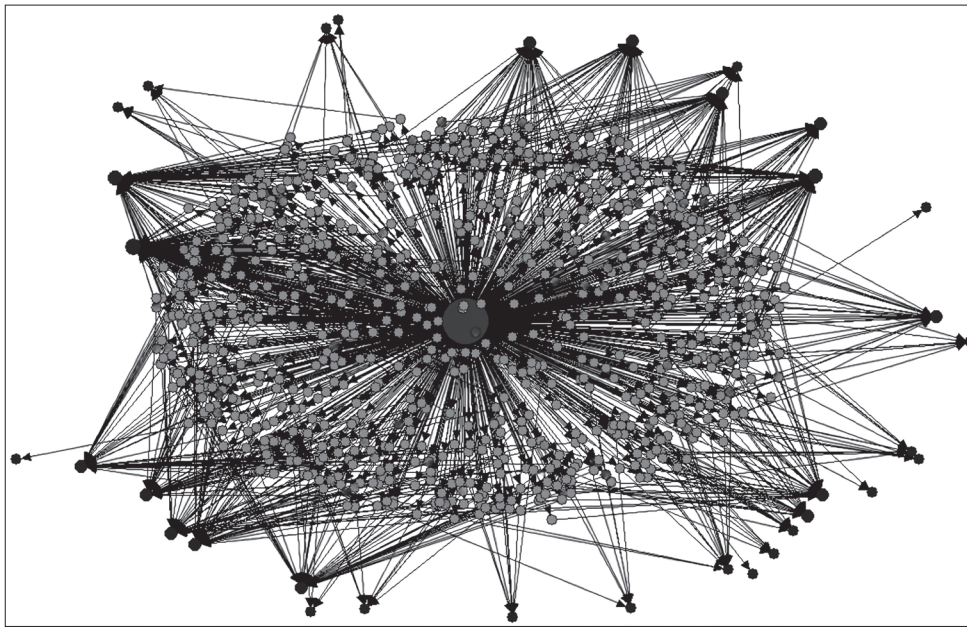
CS3 – inclusive social movement

The third case study about an inclusive and open society movement is built on social development and social empowerment projects organized and financed by the movement represented here as a corporative actor.[22] The structure of the social development and empowerment project network implies a higher level of distribution in less developed Central-Eastern European countries (see Graph 4).

It might also be mentioned, that a weak positive tendency (correlation coefficient R = 0,168) can be revealed between network embeddedness and level of fragility of the countries involved, and a similar tendency can also be recognized if we compare embeddedness and the rate of stabilisation / destabilisation in the same time period (see Figure 7).

Although, of course, it is not a causal relation, there seems to be a pattern that the higher level of social improvement projects in less democratic countries (see Table 2) could meet a less supportive, more rejective social climate. That is, these patterns imply – although it requires a deeper and more proper investigation to further elaborate the findings with more advanced methodological tools – that certain social processes under specific circumstances might also play an important role regarding social stability.

[22] The data coverage of this case study is limited to the EU and NATO member states.



Graph 4 *Network of social development movement (one channel type)*
(Edited by the author based on complex database)

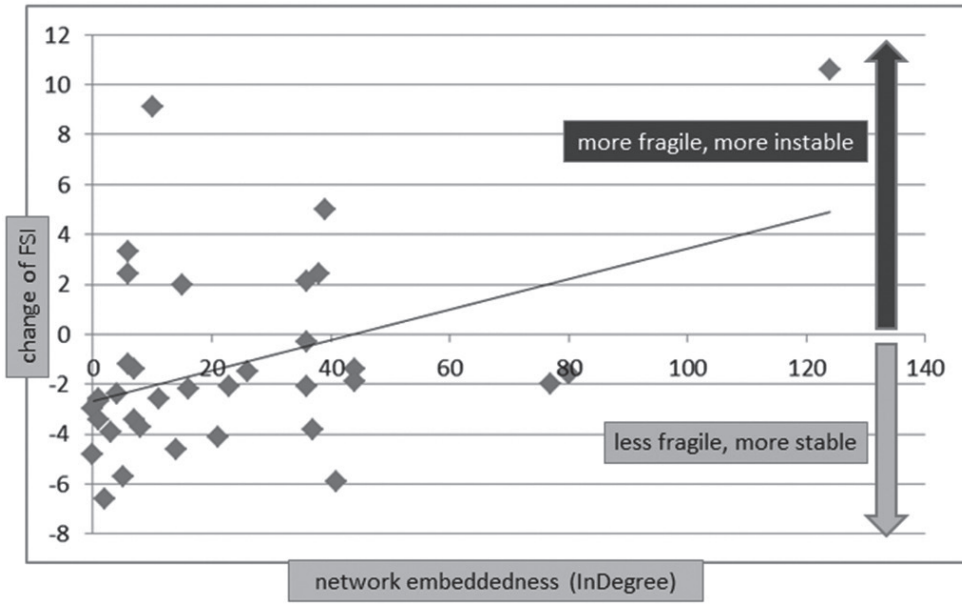


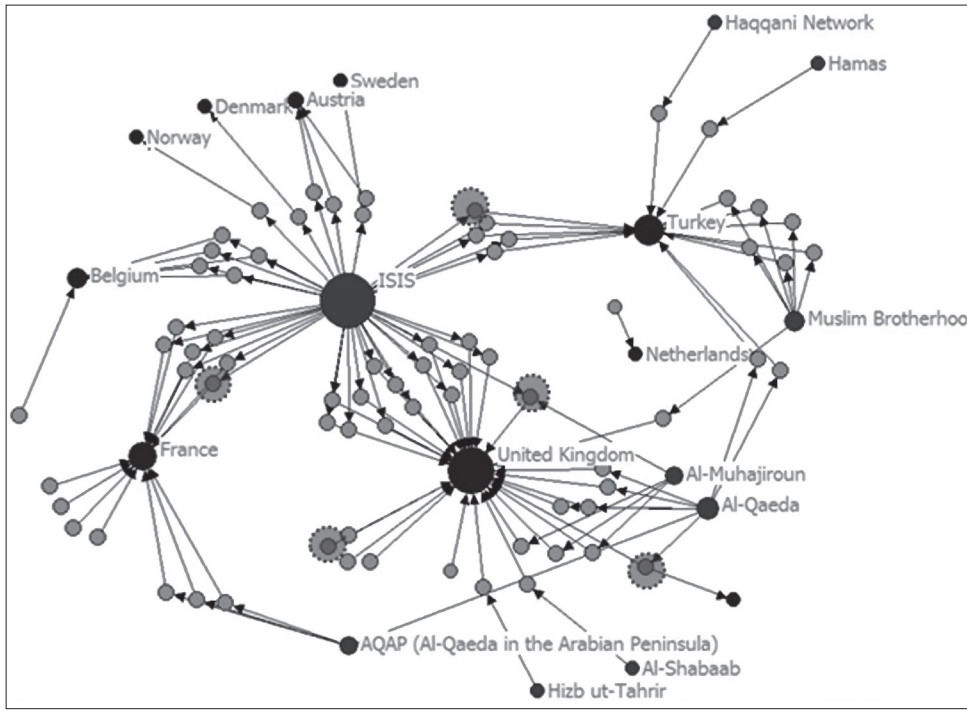
Figure 7 *Illustration of network embeddedness and level of (de)stabilization*
(Calculated and edited by the author)

Table 2 *Descriptive statistics of the development projects (Calculations by the author)*

Democracy Index country groups	Number	Mean
	of social empowerment projects	
Full democracy	195	15,0
Flawed democracy	618	30,9
Hybrid regime	21	7,0
Total	**834**	**23,2**

CS4 – jihadist extremism

The last case study seeks to investigate the role of embeddedness regarding the European jihadist extremism. Based on a research project some basic information has been assembled about jihadist extremists operating in Europe. The data included several different types of actors – spokesmen, supporters, propagandists, facilitators, recruiters, fundraisers, financial managers, representatives of global jihadist movement, some founders, leaders and members of jihadist cells –, and the analysis reveals a rather complex, structured, and partially fragmented network (see Graph 5).



Graph 5 *Network of jihadist extremist movement (one channel type)*
(Edited by the author based on complex database)

In the network, we can identify the most active groups and organizations in the area, as for example Al-Qaeda, Muslim Brotherhood and ISIS – the latter dominates the network with its notable cluster. On the other hand, among the most affected countries we find the United Kingdom, France, Turkey and Belgium. As for the structure, the overlap between certain groups is noticeable; it is worth to mention that with its Arabian branch Al-Qaeda is also present in the network. Furthermore, we can find intermediaries that are affiliated with more groups, or one who operated in more than one country.[23] Finally, it can be added that several propagators carried out their activities on the internet via social media, which again highlights the importance of the cyber domain.

These channels of jihadist groups prove to be useful regarding the export of violence to Europe: if we investigate the relation between the network embeddedness of the countries and presence of terrorism, a positive tendency can be explored. That is, in countries with a higher share of propagandists, fundraisers, etc., the number of terrorist attacks is higher, and more killed and wounded victims can be measured.

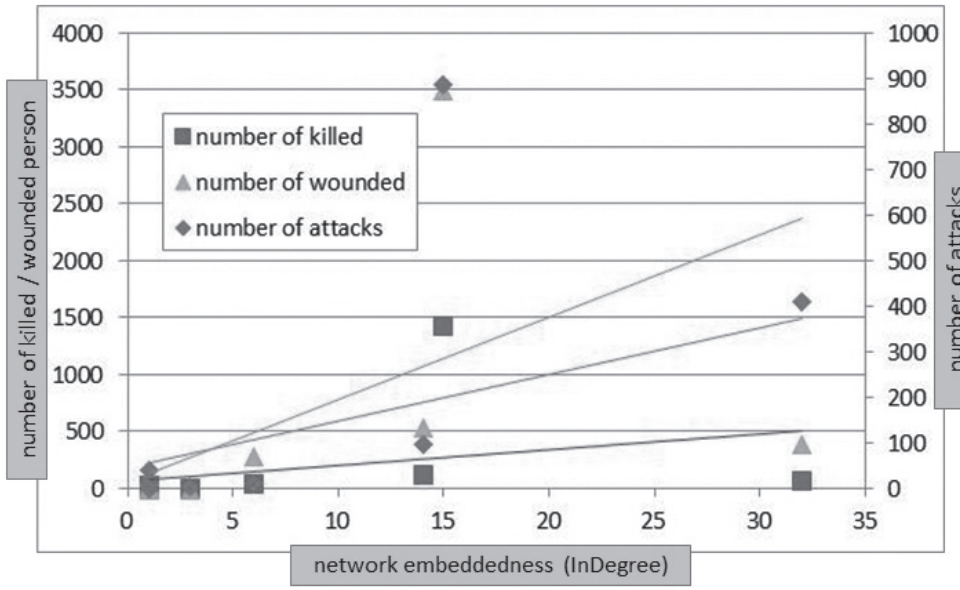


Figure 8 *Illustration of network embeddedness and violent, terrorist activities (Calculated and edited by the author)*

The case studies illustrate how complex the structures of influence channels can develop to be or can evolve in different segments of the society, and showed some examples about the role of network embeddedness regarding certain security issues.

[23] The nodes characterised with the particular positions in the network are highlighted with dashed circles.

CONCLUDING REMARKS

Based on the interpretations and conceptual models of hybrid warfare described in the first section, one of the main characteristics proves to be complexity, which implies an emphasis on coordinated employment of dominantly non-military methods, techniques, and means. In the approach of the study, we also made efforts to demonstrate an interpretation of hybrid operations that are somewhere around the border of warfare and politics, power and authority, in a transitional position between war and peace. The introduced case studies also illustrate that channels and networks of influence can evolve into complex structures and in some cases seem to be effective when employed to facilitate the realization of the objectives by the initiators. Example also shows that certain social processes could contribute to the decrease of integration level of the society and the destabilization of the state. Notwithstanding, these results basically imply the need for a complex approach when both investigating and countering hybrid operations, with a proportionate and adequate composition of non-military *and* military methods. Accordingly, it might be useful to constantly monitor the multiple domains, where several processes can have an effect on the activities of potential hybrid actors. In this regard, it might be emphasized, that the cyber sector proves to be a rather important – although it is not the only one – and relevant area. However, perhaps the significance of the proper participation of the military sector in these processes can be illustrated best if we take into consideration that in certain circumstances, highly embedded influence channels might contribute to further escalating the threats, which could result in asymmetric or even more conventional conflicts, so it is important to have the appropriate capacities and forces to manage them.

BIBLIOGRAPHY

- Bekkers, F. et al. “Hybrid Conflicts: The New Normal?” The Hague Centre for Strategic Studies, 2018.
- Buzan, B. et al. “A biztonsági elemzés új keretei”. In Póti, L. (ed.) Nemzetközi biztonsági tanulmányok. Zrínyi Kiadó, Budapest, 2006, 53–112.
- Clausewitz, C. v. “A háborúról”. Zrínyi Kiadó, Budapest, 2016.
- Farkas, Z. “A hatalom és az uralom fogalma”. Politikatudományi Szemle, 2011, XX/2, 31–49.
- Giannopoulos, G. et al. “The Landscape of Hybrid Threats: A conceptual model”. EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021.
- Kiss Á. P. “A hibrid hadviselés természetrajza”. Honvédségi Szemle, 2019, 147 (4), 17–37.
- Kiss, Á. P. – Somodi, Z. “A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban”. Honvédségi Szemle, 2019, 147 (6), 22–28.
- Lowe, D. – Pitinanondha, T. “Conceptualisation of Hybrid Warfare”. Defence Science and Technology Group, Australia, 2015.
- Richterová, J. “NATO and Hybrid Threats”. Prague Students Summit, Background report. Asociace pro mezinárodní otázky (AMO), Prague, 2015.
- Schmid, J. “Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence”. Journal on Baltic Security, 2019, 5(1), 5–15.
- Weber, M. “Gazdaság és társadalom. A megértő szociológia alapvonalai I”. Közgazdasági és Jogi Könyvkiadó, Budapest, 1987.