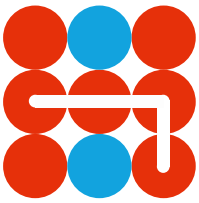
APRIL 2019

Hybrid CoE Strategic Analysis 15

How states use non-state actors: A modus operandi for covert state subversion and malign networks

MAGNUS NORMARK



Hybrid CoE

Hybrid CoE Strategic Analysis 15

How states use non-state actors: A modus operandi for covert state subversion and malign networks

> *States with a strong and long-term interest in influencing, manipulating and creating events in other countries to promote their interests will probably utilize different non-state actors in a systematic manner. – writes Magnus Normark*

The term hybrid threat refers to coordinated and synchronized actions conducted by an actor whose goal is to undermine or harm the target by influencing its decision-making at the local, regional, state or institutional level. As such, hybrid threats could be conducted by both state and non-state actors. Finding clear and explicit examples of hybrid threat manifestations deriving solely from a non-state actor is somewhat more difficult as most criminal and terrorist groups tend to rely primarily on violence or the threat of violence.

A quick review of the existing literature on hybrid threats reveals that the specific use of non-state actors in hybrid campaigns has not been the focus of researchers and academics. Traditionally, these type of challenges, often referred to as "proxy warfare", have arisen in connection with the Iranian use of Hizballah in its long-term, low-intensity conflict with Israel. More recent events have brought the proxy warfare dilemma to the fore due to state support for militant rebel factions in contemporary conflicts, such as the wars in Iraq, Syria and Yemen, to either promote policy interests and/or counter those of other states.

States operating through different non-state entities

States acting through third parties, or those disguised as such, for the purposes of influencing and taking hostile measures against other states is certainly not a new phenomenon. **Using other entities in order to influence, manipulate and obstruct can have a number of advantages, providing insights into the conceptual understanding of non-state manifestations of hybrid threat campaigns.** The active non-state entity may be a direct construct of the foreign state, a long-term ally formed through established relationships and mutual dependency, a short-term ally for achieving common objectives in a local or specific issue, or simply a "useful idiot" that may not be aware that it serves a purpose in a hybrid threat campaign. States with a strong and long-term interest in influencing, manipulating and creating events in other countries to promote their interests will probably utilize all of the above in a systematic fashion.

Acting covertly through a third entity

Directing activity through non-state entities presents an opportunity to conduct activities of a harmful nature against other countries covertly. This is a particularly attractive approach as it makes it more difficult for the targeted states to detect the harmful activity and respond before it occurs, but also because it impedes the targeted state's ability to attribute the harmful operation to the foreign state behind the event or series of events. **Acting covertly through a third entity might even contribute to the foreign state being able to reach its desired objectives without the targeted state being aware that it has been subjected to harmful activities.** The Russian Federation's use of the Pro-Russian nationalist group Night Wolves MC in the early phase of the annexation of Crimea in February 2014 serves as an example. The Night Wolves Sevastopol chapter was utilized to collect intelligence, distribute propaganda and organize protests prior to the annexation, thus serving as an important covert part of the Russian offensive capability. During the annexation, the Night Wolves came to play a small but active part in armed operations and intimidation measures, duly providing another useful advantage of employing entities with an established capacity for using violent means.

The deployment of Private Military Corporations (PMCs)

Acting in a covert mode provides for the ability to deny and refute any potential accusations of involvement in the events. This would be convenient for foreign states with an interest in engaging in activities in politically sensitive areas. **The deployment of Private Military Corporations (PMCs) for risky operations in conflict zones or in support of regimes where deniability of involvement is of vital interest serves as a case in point.** Many states have employed PMCs in conflict zones over the years and a recent case of relevance from a European perspective would be the Russian PMC 'the Wagner Group', which has reportedly been observed in the conflict in Eastern Ukraine as well as in Syria, South Sudan, Central African Republic, and most recently in Venezuela.

Skillsets suitable for specific activities

Another feature pertinent to hybrid threat activities is the opportunity to deploy entities in the target country with certain skillsets suitable for specific activities. The ability to enter the market within critical infrastructure sectors, for example through investments of relevance to the targeted state using entities under the control of foreign states, would be highly useful for exerting influence and conducting obstructive measures of some consequence. **Leverage building is often performed within legal boundaries, making it difficult for law enforcement and security services to identify such occurrences and, if they do, to allocate resources for proper investigations**. The case of the Airiston Helmi real-estate company in Finland is an instructive case, which could have potentially been a very convenient overt entity for making strategically important investments and preparing properties for future use to the detriment of the targeted state. In addition to some fairly standard components of international financial crime schemes, the case entailed Russian citizens purchasing properties with highly unusual security features, advanced technical equipment and exceptional capacity for housing a large number of individuals and large transport platforms in a strategically important geographical area in the Finnish

archipelago. The properties are located in an area through which a majority of sea cargo to Finland is transported, where the Finnish coastal fleet with all its naval combat vessels is based, and in proximity to key seabed communication cables. **This case clearly illustrates one of the many features of hybrid threats manifested through non-state actors when considering how foreign states can act through third parties to influence, interfere in or obstruct affairs in another state, with the aim of producing negative consequences or fostering the ability to do so when desired**.

Criminal organizations

Even a criminal organization with operations and networks in the target state could prove to be a very useful entity for foreign state activities in a hybrid threat context. Exploiting criminal organizations could entail utilizing established smuggling networks, the ability to provide forged documents, financial crime schemes, or simply the ability to threaten, intimidate, pressure or harm strategically important individuals or groups in a specific situation for political purposes. The Iranian relationship with the powerful and multifaceted terrorist organization Hizballah is a case in point, as the organization's operatives have been present and active in Europe for many years as a part of its criminal enterprises and terrorist activities, with tentacles extending to almost every corner of the world. As such, it has become a useful entity through which Iran can track potential targets of strategic interest, and for intimidation and assassination operations.

Social-media and cyber tools

Social-media and cyber tools, which have increased the possibility to influence and manipulate target audiences, have clearly been used in hybrid campaigns by state actors. To some extent, this is also the case vis-à-vis organizations such as the Islamic State, which are guided by radical, anti-democratic agendas and are intent upon punishing infidels and the heretic lifestyle in the West, and promoting their agenda in Western states. The ability to perform such actions to inflict harm on Western societies has been limited thus far, however, apart from those terrorist attacks perpetrated by sympathizers with the organization's propaganda and narrative. But another manifestation of such practices by radical followers of conservative Salafi/jihadi ideology would, however, serve as a clear and growing challenge of a hybrid threat nature.

The case of Salafi/jihadi influence activities in Sweden

A recent comprehensive Swedish study described the development of Salafi-jihadi influence activities in Sweden. The findings provide insights into a wide range of influencing activities conducted in a systematic manner through vulnerable sectors of society and directed at a broad target audience. The avenues for these influencing activities have expanded from preaching to congregations in close-knit gatherings, social media video lectures and street *dawa* to establishing institutions within welfare-funded sectors such as the education and healthcare sectors.

These activities not only open a gateway to radicalization, giving rise to violent acts in the targeted society, but also constitute a source of increasing segregation and polarization, resulting in an increasing number of people that reject democratic institutions and processes. The actor in this case is not a hierarchical organization but rather a loose set of

networks inspired by a handful of leaders who know each other through family bonds or close friendships and a common objective. These networks often have transnational linkages and connections to social networks, religious groupings and states with semi-independent financial institutions.

This manifestation of a hybrid threat has strong links to state actors as many of the key Salafi leaders have been groomed in Saudi Arabian institutions. Institutions established in Sweden such as Salafi-inspired mosques and schools are financially supported by actors in Gulf States that support the spread and practice of the ideology. The study focuses on networks and developments in Swedish society, but this is not a national challenge per se. **The leading figures in these networks and the growing number of institutions promoting their ideology have grown out of an international movement and have direct links to organizations in other European countries.**

Hybrid threats from non-state actors

Many non-state groups have emerged as a reaction against democratic societies and values. Thus far, few of these extremists, terrorists and criminals have conducted operations that indicate a capacity and strategic ability to launch coordinated and systematic campaigns by various means, targeting vulnerable sectors of society. This, however, should not lead to the conclusion that we can disregard these categories of actors when we work to strengthen our ability to detect and respond to hybrid threats. To all intents and purposes, when harmful activities occur in a coordinated and systematic manner, it is highly likely that there will be manifestations through non-state actors. **Our initial ability to understand whether or not these activities are related to covert state direction and support will be very limited. From several viewpoints, not least a political one, knowing who is instigating the harmful events will be of utmost importance when determining the response and how to deter such threats in the future.** For this reason, it is imperative for academics and researchers to look beyond current events linked to states of most concern within the hybrid threat domain. It is important to achieve increased understanding of the diversity of hybrid threats in order to be able to meet the ever-changing manifestations of future security challenges and to limit their impact.

The use of non-state actors embedded in the target country or target audience to conduct such actions will most likely be an integral and growing part of hybrid threat manifestation in the future.

Author

Magnus Normark is a senior analyst at the Swedish Defence Research Agency (FOI). His areas of work include terrorism threat assessment (CBRN, technology and financing), intelligence studies and studies of hybrid threats from non-state actors. Mr Normark supports the Center for Asymmetric Threat Studies (CATS) at the Swedish Defence University in terrorism research studies and leads the Sub-COI on non-state actors at the European Centre of Excellence for Countering Hybrid Threats. He has published several studies on terrorism modus operandi, arms control and international counter-proliferation challenges. He is the co-editor of *Understanding Terrorism Innovation and Learning. Al-Qaeda and beyond*, published by Routledge in 2015, and co-author of *Between Salafism and Salafi-Jihadism: Influence and Challenges for Swedish Society*, published by the Swedish Defence University in 2019.

Literature:

Bellingcat (2019). Wagner Mercenaries With GRU-issued Passports: Validating SBU's Allegation. Available at: https://www.bellingcat.com/news/uk-and-europe/2019/01/30/wagner-mercenaries-with-gru-issued-passports-validating-sbus-allegation/.

Bingham, J. and Muzyka, K. (2018). Private companies engage in Russia's non-linear warfare. Jane's Military & Security Assessments Intelligence Centre, IHS Markit.

Cilluffo, F. J. and Clark, J. R. (2014). Thinking About Strategic Hybrid Threats – In Theory and in Practice. *Prism*, Vol. 4, No. 1, Washington.

Kragh, M. and Åsberg, S. (2017). Russia's strategy for influence through public diplomacy and active measures: the Swedish case. *Journal of Strategic Studies*, Vol. 40, No. 6, Routledge.

Lauder, M. A. (2018). Wolves of the Russian Spring: An Examination of the Night Wolves as a Proxy for the Russian Government. *Canadian Military Journal*, Vol. 18, No. 3.

Levitt, M. (2019). Hezbollah's Procurement Channels: Leveraging Criminal Networks and Partnering with Iran. *CTC Sentinel*, Vol. 12, Issue 3.

Marshall, A. (2016). From civil war to proxy war: past history and current dilemmas. *Small Wars and Insurgencies*, Vol. 27, No. 2, Routledge.

Ranstorp, M. et al. (forthcoming). *Between Salafism and Salafi-Jihadism: Influence and Challenges for Swedish Society*, Swedish Defence University.

Rondeaux, C. and Sternman, D. (2019). Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World. *New America*. Available at: https://www.newamerica.org/international-security/reports/twenty-first-century-proxy-warfare-confronting-strategic-innovation-multipolar-world/.

Treverton, G. F. et al. (2018). Addressing Hybrid Threats. Swedish Defence University, Stockholm.

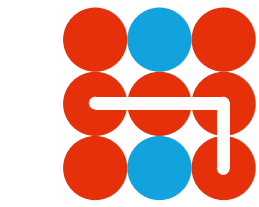
The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-46-5
ISSN 2670-2282

Second version of the publication. Previously published as "Strategic Analysis 1/2019: How states use non-state actors. A modus operandi for covert state subversion and malign networks."

April 2019

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



Hybrid CoE