Hybrid CoE Research Report 6

Hybrid threats from non-state actors: A taxonomy

Hybrid CoE

Janne Jokinen, Magnus Normark – June 2022

Hybrid CoE Research Reports are thorough, in-depth studies providing a deep understanding of hybrid threats and phenomena relating to them. Research Reports build on an original idea and follow academic research report standards, presenting new research findings. They provide either policy-relevant recommendations or practical conclusions.

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

ISBN (web) 978–952–7472–22–4
ISBN (print) 978–952–7472–23–1
ISSN 2737–0860

June 2022

Cover photo: Babaroga / Shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Introduction[1]

The employment of non-state actors (NSA) by state actors (SA) to gain levers of influence for foreign and security policy objectives is as old as the existence of states. There are many examples of both weak and powerful states which have resorted to this tool. Innovations in fields such as information technology and financial services have enhanced the power of non-state actors in relation to states, making them even more potent proxies, partners and rivals to states.

During the 2000s, when the focus of much of the international community was on countering violent extremism and terrorism, the adversaries were non-state actors as well as state sponsors of terrorism. In the 2010s, the picture became more complex as inter-state conflict reasserted itself. The evolution of concepts such as asymmetric warfare, grey zone tactics, hybrid interference and hybrid threat activities has brought to the fore the diversity of adversaries and targets. Regimes that are unhappy about their position in the present international system and concerned about foreign threats – real or imagined – to their internal stability have been particularly attracted to hybrid threat activities, including the use of non-state proxies, in their security strategies.[2]

The extensive employment of hybrid threat methods by the Russian Federation in its invasion and illegal occupation and annexation of parts of Ukraine in 2014 created a sense of urgency in the international community for understanding the threat and finding more effective counters to it. The role that NSAs may play received increasing attention. This is reflected in many security policy documents which have been drawn up in Europe, North America and some parts of the Asia-Pacific after 2014.[3] To mention just one example, the Joint Communication to the European Parliament and the Council by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, which came out in 2016, proposed a joint framework for countering hybrid threats and listed a number of areas of concern, in all of which NSAs may play a central if not a primary role.

At the end of 2020, the European Centre of Excellence for Countering Hybrid Threats conducted a survey among its Participating States, the European Union and NATO to explore their views on the role of NSAs in the context of hybrid threats. The replies confirmed the broad awareness of how important this role is, but also reflected how difficult it is to detect, understand and counter the threat that NSAs may pose in all of their diversity. The roles they play are context-specific and tend to evolve with time. Trends in the application of technology to economic and social activity point towards an increase in the vulnerabilities that NSAs are

1 The authors would like to express their appreciation for the invaluable contributions made by Michael Fredholm to the report as a whole, and especially to the sections presenting case studies and the taxonomy of non-state actors, and to Vladimir Rauta for his comments on the taxonomy as well as on the applicable research and the analytical basis of the report.

2 See e.g. G. Giannopoulos, H. Smith & M. Theocharidou, 'The Landscape of Hybrid Threats: A Conceptual Model - Public Version', The European Commission and the European Centre of Excellence for Countering Hybrid Threats, 26 November 2020, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/, 19–22. [Unless otherwise indicated, all links were last accessed on 17 February 2022.]

3 Vladimir Rauta and Sean Monaghan, 'Global Britain in the gray zone: Between stagecraft and statecraft', *Contemporary Security Policy*, Volume 42, Issue 4, (2021): 475.

well-suited to exploit. Democratic societies with open market economies face particular challenges in maintaining a proper balance between making countermeasures effective and safeguarding the norms and values underpinning their model of political organization.

This Hybrid CoE Research Report seeks to provide a basic conceptual perspective on hybrid threats involving NSAs, with the purpose of facilitating a better understanding of the ways in which such threats may manifest themselves. The point of departure is the *Conceptual Model for Hybrid Threats* developed by the European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre of the European Commission in 2020.[4] The report includes information and perspectives collected through workshops and activities organized by the European Centre of Excellence for Countering Hybrid Threats, as well as references to relevant research literature and other contributions by experts.

The introductory part of this report discusses the meanings given to the term 'non-state actor' in international discourse. As most NSA-related hybrid threat activities emanate from foreign state interests and directives, the report takes a closer look at the relationship between the non-state actor engaged in hybrid threat activities and the state actor that functions as its task master. The report then explores the types of powers that NSAs may deploy in order to affect the targets, as illustrated by a number of case studies.

The elements derived from both a consideration of the relations between states and NSAs serving as hybrid threat actors on their behalf, as well as the powers that these NSAs may bring to bear, are used to propose an analytical framework, a taxonomy, as an aid for future work. The segment on the taxonomy concludes with a section discussing the potential role of NSAs as hybrid threat actors in their own right, namely without state support or influence. Finally, the report presents some general observations and makes suggestions for further study.

The taxonomy, as indeed this report as a whole, is proposed as a starting point for a discussion that will highlight some of the key issues that should be explored to gain a more thorough understanding of the role of NSAs in the hybrid threat landscape. The ultimate objective is to equip policymakers and practitioners to make sense of this landscape, detect the most serious threats, and devise effective countermeasures to them.

4 Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats'.

Definitions: Non-state actors and hybrid threats

Non-state actors come in many forms. They range from individuals to private corporations, religious institutions, humanitarian organizations, armed groups and *de facto* regimes in actual control of territory and population. The one common characteristic would be, as the name suggests, that they exist independent of internationally recognized states.[5] However, the understanding of what this means varies greatly. Authoritarian political systems discourage the existence of independent sources of authority, which would in effect remove the distinction between state and non-state actors. While democracies seek to foster a civic space free of government interference, they rely on NSAs to perform many public functions, and the state may have partial or complete ownership of enterprises that otherwise operate as private businesses.

Public international law does not provide a clear definition of what constitutes an NSA as it has traditionally been more concerned with relations between states.[6] Private international law has largely focused on commercial relationships among private enterprise. International humanitarian law does include references to non-state actors, notably the International Red Cross and Red Crescent Societies and the International Committee of the Red Cross. The prominent role of NSAs in armed conflict has spurred efforts to make them more compliant to international humanitarian law. International human rights law recognizes the individual as a subject with both certain rights and certain obligations. However, the emphasis with regard to the individual is as rights holder, while the obligations are mainly allotted to the state.

Both international humanitarian law and international human rights law struggle with the inclusion of non-state actors as they lack a clear legal definition. Moreover, giving them independent agency under international law would change their status vis-à-vis states. This might lead to a dilution of state sovereignty, which is the cornerstone of the present international system and jealously guarded by state actors. In the context of hybrid threats, the erosion of the principle of state responsibility would make it even harder to attribute malign actions to states and call them to account for activities undertaken by NSAs under their jurisdiction or control.

Even if no clear legal definition exists, the independent role that NSAs play in the hybrid threat context is broadly recognized. During the Cold War, all sides made active use of NSAs. The study of hybrid threats in the present sense first emerged in the analysis of armed conflicts of the 1990s, in which NSAs engaged with state actors (e.g. the Chechen wars or the conflicts deriving from the dissolution of Yugoslavia) employing asymmetric methods.[7] The rise of al-Qaida and the so-called Islamic State of Iraq and al-Sham (ISIS) to international prominence during the first two decades of the 21st century provided a reminder that independent NSAs can acquire the power to challenge states. The re-capture of the Afghan state by the Taliban in mid-2021 is worthy of careful analysis as

5 Agata Kleczkowska, 'States vs. non-state actors – a public international law perspective', Hybrid CoE Strategic Analysis 20, 2020, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-20-states-vs-non-state-actors-a-public-international-law-perspective/, 3.

6 Ibid.

7 See e.g. the works by Dr Frank Hoffman. For one example, see Frank Hoffman, 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges', *PRISM*, Volume 7, Issue 4, (2018).

an example of a non-state actor successfully waging a hybrid threat campaign against an internationally recognized – and supported – government.

The debate on the basic concepts that should be used continues, as do efforts to gather data on real-life examples of NSAs performing as hybrid threat actors. Concepts continue to evolve and migrate. The divergence in intellectual points of departure is a persistent challenge; including whether the NSAs are studied under conditions of armed conflict – that is, in the context of hybrid warfare – or under conditions of (real or nominal) peace.[8] The strategic thinking of the major actors engaged in hybrid threat activities does not make such distinctions; indeed, they often try to exploit ambiguity and jurisdictional and bureaucratic boundaries to make detection and deterrence difficult. This makes it all the more important to adopt a holistic approach, and to use all the analytical tools that are relevant and available to allow for the understanding and deterrence of hybrid threat activities involving NSAs. Indeed, as writers such as Vladimir Rauta and Sean Monaghan point out, pragmatism should be the guiding principle.[9]

According to the conceptual model developed by the European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre of the European Commission, the term 'hybrid threat' can be meaningfully applied when an actor with malign intent deliberately combines and synchronizes action, specifically targeting the systemic vulnerabilities in democratic societies. The action may be characterized by the following:

- **Using multiple synchronized tools to create linear and non-linear effects;**
- **Creating ambiguity (covert action, plausible deniability) and hiding the real intent;**
- **Exhibiting deliberate threshold manipulation when it comes to detection and response;**
- **Exploiting the seams within a democratic society, as well as the divisions between different jurisdictions;**
- **Often including a distraction element, such as action in one place while the actual target is somewhere else.**[10]

The landscape of hybrid threats can be described as a continuum that encompasses conditions of peaceful influencing, interference and warfare aimed at priming, destabilization or coercion by the hybrid threat actor of the targeted society. The phases may follow a timeline; they may also take place simultaneously in different fields of action, or backtrack to a less openly coercive phase. The guiding principle

8 See Vanessa Meier, 'Making the Clandestine Public: Challenges in Collecting Data on External Support and Ways Forward', *International Studies Review*, (2021): 23–25. Some of the conceptual challenges are even greater when it comes to situations beyond armed conflict. See also Mikael Wigell, 'Democratic Deterrence – How to Dissuade Hybrid Interference', (FIIA Working Paper 110, September 2019), 4; Rauta and Monaghan, 'Global Britain in the gray zone', 475. See also Sean Monaghan's observations on the proper approach to 'boiling peace' in Sean Monaghan, 'Bad Idea: Winning the Gray Zone', Defense 360, Center for Strategic and International Studies, 2021, https://defense360.csis.org/bad-idea-winning-the-gray-zone/.

9 Wigell, 'Democratic Deterrence', 4–6; Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 19–22; Rauta and Monaghan, 'Global Britain in the gray zone', 476.

10 Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 11.

here is having the maximum desired impact on the target while minimizing the risks and costs to the actor. Legal or other definitions related to armed conflict, emergency or 'normalcy' do not govern the tool box; they may appear simply as distinctions employed by the targeted society, which can be exploited.[11]

The Conceptual Model describes non-state actors in the hybrid threat context as entities that play a part in international relations, and that exercise sufficient power to interfere, influence and cause change without any affiliation to the established institutions of a state.[12] The characteristics of hybrid threats point to the fact that NSAs are a particularly effective tool in all phases of a hybrid threat campaign. They can be simultaneously employed in a broad range of sectors in the targeted society. They provide both access and expertise related to the targeted society, which a foreign state actor would find difficult to achieve. They play influential roles such as controllers of critical infrastructure and services in the targeted society and can thus be a force multiplier. Using a proxy NSA grants its patron cover. With the rights and freedoms NSAs enjoy in democratic societies, they can operate below the threshold of countermeasures more easily than foreign state actors. NSAs are well suited for priming activities in which the adversary seeks to mould the targeted society over time to become more receptive to its influence.[13]

11 Frank Hoffman, 'Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict', *Strategic Forum*, No. 240 (April 2009): 8; Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 36–37.

12 Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 22.

13 Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 23–24.

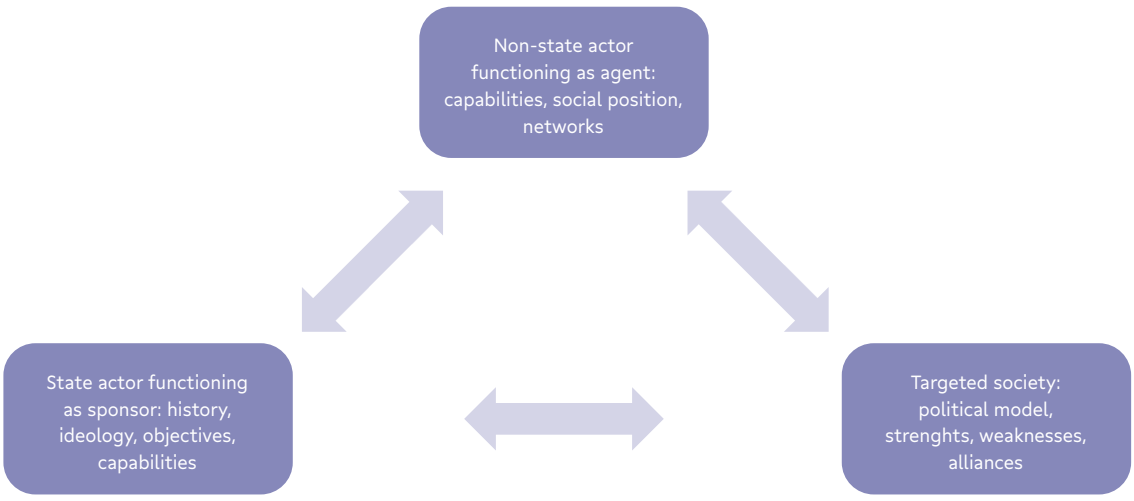
Building a taxonomy

Relations between state and non-state actors in the context of hybrid threat activities

The ability to identify a hybrid threat and to make decisions on preventive or responsive measures is intrinsically interlinked with the ability to identify the entity behind the activity. Current understanding of non-state hybrid threats as a complex, diverse and highly adaptable security challenge emanates from the multitude of different entities that may be involved in hybrid threat operations. As hybrid threat activities need to meet certain thresholds regarding the actors' capabilities and intentions in accordance with the definition of hybrid threats, most non-state entities in this domain will likely have some kind of relationship with a foreign state.

If identifying a particular type of NSA as especially prone to being turned into a tool for hybrid threat activities is impossible, where then to look to detect a looming threat? The analysis should start with the targeted society. What is its model for political organization? Where do NSAs hold particularly powerful positions by themselves or through networks? Can the targeted society rely on partnerships with other actors to detect and counter this kind of threat? The second step would be to study the potential opponents. Do they exhibit a preference for NSAs exercising particular types of power in their efforts to influence their own societies and other states? Do similar NSAs hold influential positions within the targeted society? Does the state actor have access to such NSAs in the targeted society, and the means to influence them?

Figure 1. Analyzing hybrid threats: state sponsor, non-state proxy actor, the target and channels of influence



The assessment of the relative strengths and weaknesses of societies targeted with hybrid threat activities is a relatively well established part of the efforts to build resilience against as well as to detect and counter such threats. The strategic culture and traditions of the major state actors engaged in hybrid threat activities have also received attention. While further work is definitely needed on both subjects, it is arguably the third element, the characteristics of NSAs and their interplay with state sponsors, which contains the broadest analytical lacunae.[14]

Since the early 2000s, and especially since the invasion of Ukraine and the annexation of Crimea by Russia in 2014, the academic community has become more interested in understanding and conceptualizing the different manifestations of hybrid warfare. Even within this domain, there is a diversity of emphases and points of view, such as between scholars approaching the subject from the perspective of proxy warfare and those focusing on external support in civil wars.[15]

Apparent disciplinary divisions do not necessarily run so deep, however, as to require completely separate analytical tool boxes, as Karlén and Rauta, for example, point out in their discussion of the apparent differences between scholars of proxy warfare and those studying external support in civil wars. They propose **conflict delegation** as an umbrella term to bring these approaches together: "...a strategy in which a foreign government commits material resources or military expertise to a non-state armed group to target a perceived adversary".[16] The idea of a continuum of hybrid threats serves the same purpose in the Conceptual Model, as discussed above: all contingencies fall within the same framework. This of course is the experience of practitioners in the field: all hybrid threat activities need to be pre-empted, detected, deterred and countered regardless of whether one finds oneself in conditions of real or nominal peace, or armed conflict.

The key elements in conflict delegation are the interaction between the state sponsor (or sponsors) and the actor, namely the transfer of capabilities from the principal to the agent; and the resulting control by the former over the latter, that is, exerting influence over the actor's aims, strategies and tactics. The mechanisms of delegation vary.[17] Arguably, the capabilities and influence may also flow in the other direction, from the NSA towards its state patron.[18] It is also possible for state and non-state actors to simply be allies, or to work in parallel towards similar goals without any hierarchical relationship. The special category of 'useful idiots' cannot be

14 Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 22.

15 See Niklas Karlén & Vladimir Rauta, 'Forum: Conflict delegation in civil wars. Introduction', *International Studies Review*, Volume 23, Issue 4 (2021): 2050–2052.

16 Ibid., 2051. See also Andrew Mumford's discussion in the same volume: Andrew Mumford, 'Forum: Conflict delegation in civil wars. In Search of Proxy War Studies', *International Studies Review*, Volume 23, Issue 4 (2021): 2054–2056.

17 Karlén & Rauta, 'Forum: Conflict delegation in civil wars. Introduction'; Niklas Karlén & Vladimir Rauta, 'Forum: Conflict delegation in civil wars. Complex Conflict Delegation in Civil Wars', *International Studies Review*, Volume 23, Issue 4 (2021): 2058–2060.

18 Alexandra Chinchilla, Rickard Kit and Giuseppe Spatafora, 'Ways Forward: A Research Agenda on Conflict Delegation', *International Studies Review*, Volume 23, Issue 4 (2021): 26.

Table 1. NSAs' perceived relational embeddedness and relational morphology with state actors according to Rauta (2019)

MORPHOLOGY	EMBEDDEDNESS		
		Direct	**Indirect**
	Supplementary	Auxiliary	Surrogate
	Delegatory	Affiliate	Proxy

overlooked either. Moreover, the relationship may change over time. In the extreme case, the non-state actor may succeed in becoming a state actor itself.[19]

Vladimir Rauta's 2019 development of a typology of NSA relationships with states in the hybrid warfare context builds upon the NSAs' perceived **relational embeddedness** and **relational morphology** with state actors.[20] Relational embeddedness describes the structural relationship between the state and the non-state armed group. The degree of embeddedness can be **direct**, as in fighting alongside or in close cooperation with each other, or **indirect** as in the armed group fighting on behalf of or for the state. Relational morphology delineates between the non-state armed group's different roles in relation to the state actor. The character of the morphology distinguishes between **supplementary** value, where the armed group adds a complementary function to the state in a hybrid warfare situation, and a **delegatory** function where the armed group fully replaces the state. The matrix of typology then provides four different types of relationships: **auxiliary** (direct and supplementary), **affiliated** (direct and delegatory), **surrogate** (indirect and supplementary) and **proxy** (indirect and delegatory).

This typology is a helpful framework for understanding functional relationships between states and non-state actors. To use the conflict in Ukraine from 2014 until Russia's full-scale invasion in February 2022 as an example, the Night Wolves MC could be characterized as an **auxiliary** group fighting for or together with Russian forces, whereas the Wagner Group would be an **affiliated** entity fighting in a delegatory capacity in relation to regular state forces in target areas where the Russian regular forces were not deployed.

This concept could also apply to entities engaged in hybrid threat activities outside armed conflict, for instance hackers employed by states as **affiliated** to interfere in or manipulate critical democratic functions and processes in target states. The typology can also serve to differentiate between the various roles that a specific NSA plays in different contexts, such as the reliance by the Syrian regime's regular forces on Hezbollah's support as a **surrogate** entity in the war in Syria, and the Iranian regime's long-term use of the same organization as a **proxy** in the struggle against Israel.

Relationships outside situations of armed conflict do offer additional complexity as they can be more superficial and opportunistic in character, and the exact nature of the relational

19 As noted e.g. by Idean Salehyan. See Idean Salehyan, 'A Decade of Delegation', *International Studies Review*, Volume 23, Issue 4 (2021). Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 23; Hoffman, 'Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict', 8.

20 Vladimir Rauta, 'Towards a typology of non-state actors in "hybrid warfare": proxy, auxiliary, surrogate and affiliated forces', *Cambridge Review of International Affairs*, Volume 33, Issue 3 (2019): 2.

embeddedness and morphology may be difficult to pin down. One example are foreign registered business entities which are bound by the regulations of their home state to act in the home state's interest abroad if and when the state so chooses. Another example is temporary foreign support for, or the exploitation of, trending activism related to a politically sensitive issue in a targeted society, which may be of limited duration (e.g. influencing an election campaign) but still have long-term effects that the foreign state considers desirable.

Consequently, the multitude of relationships between NSAs and state actors in the landscape of hybrid threats will range between long-term commitments and short-term interactions in combination with the assessed level of shared interests and objectives. An extreme example of a long-term relationship would be entities not officially part of the foreign government but in reality created by the state through capacity-building and directional control, such as private military companies or advanced and persistent hacker entities. At the other end of the spectrum would be a foreign state's temporary hire of abilities and actions related to an NSA in a very specific context, such as a contract killing of a target abroad as part of a strategic operation.

These examples highlight the wide variety of different levels of shared objectives where the first examples may characterize entities created solely for the objectives of a state, and the latter provide examples where the NSA conducts activities for the foreign state without shared objectives or interests, but rather driven by financial motivation, other opportunistic benefits or by regulation-based coercion (e.g. the obligation to participate in intelligence-gathering).

Characteristics of non-state actors engaged in hybrid threat activities

Successfully addressing hybrid threats requires a common understanding by analysts, policymakers and practitioners of what constitutes a hybrid threat actor. This is particularly important when dealing with NSAs since they are so diverse and, unlike many state actors engaged in hybrid threat activities, tend to be characterized by multiple and sometimes conflicting objectives. Not all NSAs are hybrid threat actors; indeed the vast majority are not. However, practically all types of NSAs can be turned into a tool for malign foreign influence under the right circumstances.[21]

21 Under certain conditions, some NSAs may exceed the threshold of becoming a hybrid threat actor in their own right, as will be discussed later in this report. Examples include organized crime groups in Colombia (Pablo Escobar and Los Extraditables, 1984), Sweden (PKK, 1984), Italy (Sicilian Mafia, 1993), Mexico (Los Zetas, 2009), and certain insurgent groups (notably the Afghan Taliban movement, from 2001 onwards). See Michael Fredholm, T*ransnational Organized Crime and Jihadist Terrorism: Russian-Speaking Networks in Western Europe* (London: Routledge, 2016), 30–33; Michael Fredholm, 'The Hybrid Threat Capability of the Afghan Taliban Movement, 2001–2014', in *Vernetzte Unsicherheit: Hybride Bedrohungen im 21. Jahrhundert*, ed. Anton Dengg and Michael Schurian (Vienna: Landesverteidigungsakademie, 2015), 313–346. As for the PKK, the organization attempted to use hybrid threats, including terrorist power to maintain control over the Kurdish population of Sweden. As part of the campaign, the PKK murdered two defectors (Enver Ata in Uppsala in 1984, and Çetin Güngör in Stockholm in 1985). However, the method backfired. As a result of widespread media reporting, some of which derived from the PKK itself, the organization found itself for some time in the unenviable position of being treated as the prime suspect of the 1986 murder of Swedish Prime Minister Olof Palme.

Approaching the activities of NSAs according to categories of **operational capacities (power)** will help in assessing their hybrid threat potential. This is the approach chosen in the 2015 volume edited by Anton Dengg and Michael Schurian on hybrid threats (that is, threats of a hybrid nature employed by hostile actors in times of peace as well as under conditions of armed conflict). Their work provides a long list of hybrid threat actors, divided into the following general categories based on the type of power employed:[22]

Hard power
- **State power**
- **Cyber power**
- **Privatized power**
- **People's power**
- **Terrorist power**

Soft power
- **Real economic power**
- **Financial power**
- **Diplomatic power**
- **Civil power**
- **Scientific and technological power**
- **Media power**

Of these categories, each of which may include numerous subcategories, all but one are applicable to NSAs. The exception is, unsurprisingly, the category of **state power** (defined as consisting of military, law enforcement, intelligence, and judicial actors), which is the exclusive realm of states. Even the category of **diplomatic power** contains a significant number of subcategories which may involve NSAs. For this reason, the types and numbers of NSAs de facto or potentially engaged in hybrid threat activities greatly outnumber those of state actors engaged in such activities.

Establishing a taxonomy

Based on the aforementioned general types of applied power, and the types of relationships NSAs may have with state actors, it is possible to construct a preliminary taxonomy of NSAs engaged in hybrid threat activities. Comparative studies of the NSAs will enable the identification of further salient characteristics, including those related to the NSA's agenda and operations. An NSA's relationship to a given state actor tends to belong to one of the following **classes**:

- **Ally**
- **Non-aligned**
- **Rival**

As described above, the morphology and the embeddedness of the relationship further yield the **categories** of:

- **Auxiliary**
- **Surrogate**
- **Affiliate**
- **Proxy**

To describe the relationship further, its **duration** in time should be determined:

- **Long-term relationship**
- **Short-term relationship**
- **Temporary exploitation**

22 Dengg & Schurian, *Vernetzte Unsicherheit: Hybride Bedrohungen im 21. Jahrhundert*, 55–56.

Moreover, one of the following **qualities** of the relationship will commonly apply:

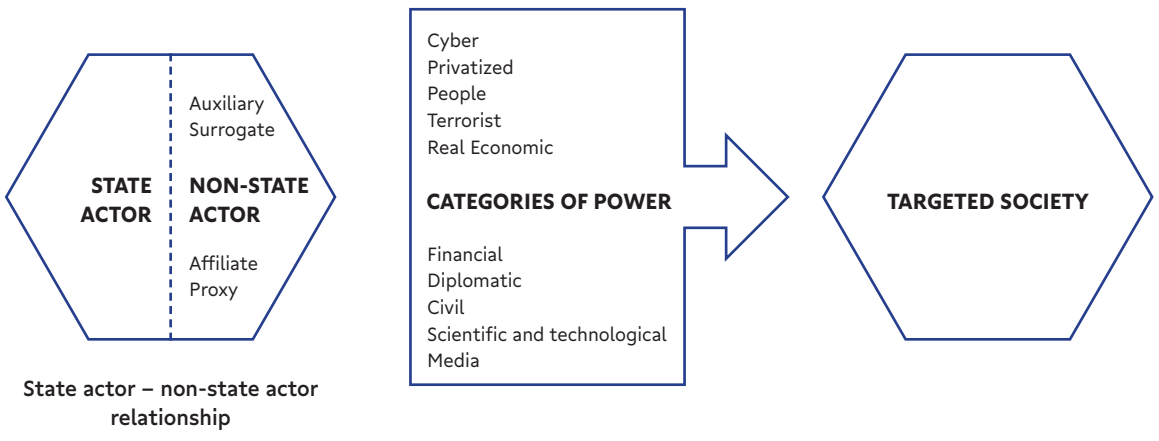
- **Established by SA**
- **Funded by SA**
- **Dependent on SA**
- **Compelled by SA**
- **Hired by SA**

Finally, the NSA will typically have several, or even all, of the following characteristics, which can be listed as a **comment** on the taxonomy:

- **State agenda**
- **Shared goals**
- **Independent agenda**

This proposed set of categories, as well as the morphology and the embeddedness criteria and other salient characteristics, will be tested by applying them to the case studies that follow.

Figure 2. Hybrid threat activities through non-state actor clients



State actor – non-state actor relationship

Case studies

Cyber power

Cyber power is deployed in a variety of forms, including the creation or modification of hardware for malicious purposes, cyberattacks by hackers, identity theft by organized cybercrime groups, phishing, data interception and manipulation, alteration of website content for reasons of propaganda or sabotage, suppression of web services, and so on. Cyber power can also be deployed for the interception and surveillance of web-based communications, and for the manipulation and sabotage of critical infrastructure which relies on web-based services. Moreover, cyber power has the potential to take advantage of the new applications, processes, and business models in the financial services industry, generally referred to as FinTech (financial technology). NSAs play a predominant role in the deployment of contemporary cyber power.

The opaque groups that engage in cyber crime are often collectively referred to as Advanced Persistent Threats (APT). Perhaps the most widely reported case is that of APT41, also known as Double Dragon or Cicada, which is generally assessed to be a Chinese state-sponsored group that engages in cyber espionage on behalf of the government, while simultaneously participating in financially motivated cybercrime for personal gain. The group's activities have been traced back to 2012.[23] In terms of the taxonomy, APT41 could be described as a long-term ally and proxy of China, which is dependent on and/or compelled by the state to share its agenda in addition to implementing its own.

Another well-documented example of a non-state actor combining the functions of a state- sponsored hacking operation and a hacker for hire was the Mabna Institute, which was established in Tehran around 2013. The Institute first functioned as a private enterprise to assist Iranian universities and scientific and research organizations in gaining access to non-Iranian scientific resources. It used both legal and illegal methods. According to an investigation by the United States Federal Bureau of Investigation (FBI), the Mabna Institute also undertook illegal cyber intrusions at the behest of the Islamic Revolutionary Guard Corps (IRGC), targeting over a hundred thousand accounts of academics and private sector employees throughout the world, as well as conducting a computer hacking campaign against various governmental and non-governmental organizations within the United States, as well as the United Nations and the United Nations Children's Fund.[24]

With regard to its relationship with Iran, the Mabna Institute could be described as an ally and a proxy with a long-term relationship to its state sponsor. It was probably compelled into this role but also benefited from it financially. Its agenda was originally independent but later became shared if not controlled by the state.

23 FireEye, 'Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation', Milpitas, California: FireEye, Inc., 2019; US Department of Justice, Office of Public Affairs, 'Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More Than 100 Victims Globally', Press Release No. 20–942, September 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

24 Department of Justice, U.S. Attorney's Office, Southern District of New York, 'Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps', Press Release No. 18–089, 23 March 2018, https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic.

Privatized power

Privatized power is, by definition, primarily associated with NSAs. The NSAs may be, in order of ascending respectability, organized crime groups (OCGs, including the subcategories of pirates and terrorists who are in it for profit), insurgent groups and warlord-led militias, private military companies (PMCs) and paramilitary security firms. They are capable of deploying force for the purpose of carrying out armed attacks, killings, hostage-taking, intimidation, extortion, blackmail, and/or other illegal activities such as black-market trading and corruption. The relationship may be long term but can also be limited to one instance, such as a contract killing. Although OCGs may well be able to provide, among other things, access to smuggling networks for individuals, goods, and money, as well as safe houses, vehicles, weapons, and forged identity documents, they do constitute a blunt instrument. In short, they are violent but unskilled.

One well-documented example of the use of an OCG as an instrument for hybrid threat activities is the so-called D-Company. The originally Indian and later Emirati-based crime group was formed in the mid-1980s. It developed a relationship with Pakistani security services and Islamist extremists, and was involved in terrorist acts, including the Bombay bombings of 1993. Throughout the history of the organization, its motives appear to have mixed ideology with financial and other crime-related gains.[25]

In the case of the D-Company, the relationship between the non-state and the state actor lasted for several decades. The organization started as an independent actor with an agenda of its own but was later co-opted by a state. The goals became partly shared. The relationship was long but remained indirect and supplementary, so the D-Company could be defined as an auxiliary to Pakistan.

One probable example of a short-term engagement was the attempted assassination, in February 2020, of the Chechen blogger Tumso Abdurakhmanov. He was living in exile in Sweden at the time of the attempt, and was engaged in social media activities against the Chechen government. The would-be assassin, Ruslan Mamayev, failed and was caught. In the ensuing trial, the court concluded that there was evidence supporting an allegation that the failed attempt had in fact been motivated by a 'blood feud' between the target and an individual in the Chechen government, and not by any political agenda.[26] However, had the attack succeeded, it would have neutralized a perceived media threat to actors linked to the Chechen government and served as a warning to other political opponents.

If indeed Chechen authorities were the instigators of Mr. Mamayev's activities, he could be defined as an NSA engaged in a hybrid threat activity who served as a temporary surrogate for the state actor. The quality of the relationship is not known; he could have been hired or compelled to attempt the assassination.

Privatized power is not the exclusive domain of organized crime. Private military

25 Ryan Clarke & Stuart Lee, 'The PIRA, D-Company, and the Crime-Terror Nexus', *Terrorism and Political Violence*, Volume 20, Issue 3 (2008): 376–395, 385–391; Fredholm, *Transnational Organized Crime*, 28. On ISI and LeT, see also Michael Fredholm, 'Kashmir, Afghanistan, India, and Beyond: A Taxonomy of Islamic Extremism and Terrorism in Pakistan', *Himalayan and Central Asian Studies*, Volume 15, Issue 3 (2011): 24–80.

26 Judicial proceedings, Hovrätten för Nedre Norrland, dom 2021–04–01, mål B 82–21.

companies (PMCs) can be utilized in similar ways. The employment of a PMC will allow some degree of deniability, although commonly not to the same extent as hiring an NSA within organized crime. Instead, a PMC generally operates within the law, which in itself insulates its activities from the state patron. Moreover, PMCs are more commonly employed when a long-term relationship with the state actor is desirable. The relationship may be one of shared goals, or a more business-like relationship involving long-term funding. The links are reinforced by the fact that the leadership as well as the majority of the employees of PMCs tend to consist of former military or security officers of the state which employs the PMC. Typical examples of PMCs include South Africa's Executive Outcomes (in operation 1989–1998), Britain's Sandline International (in operation 1994–2004), and Russia's Wagner Group (in operation since 2014).[27]

People's power

People's power is deployed by insurgents, extremists, and revolutionaries, but also by malcontents and impoverished or otherwise marginalized groups who have become mobilized and, wittingly or unwittingly, act on behalf of an actor with the capacity to arouse them. Demonstrations, riots and violent unrest may be the result of genuine sentiments, but they can be hijacked by demagogues, extremist groups, as well as ill-intentioned foreign states. They are attractive tools for hybrid threat activities because they don't have to be persuaded to be critical of conditions they face and the authorities perceived to be responsible for the situation. Moreover, in democratically governed countries, any large group of protesters is likely to receive favourable attention from the media, especially if they can appeal to human rights and democratic principles.

The use of an armed exile group against an adversary constitutes one of the oldest types of hybrid threat activity. The purpose may be to use armed force to destabilize or overthrow the political system of the targeted society without becoming openly involved. However, it may also be to enhance the political influence of a state actor inside that society, or the status of domestic actors linked to a foreign state actor, for example by ethnicity or ideology to lay the groundwork for future hybrid influence and interference. The state actor may also aim to gain a stronger voice in a peace process seeking to manage and resolve a conflict. The Cold War provides a number of examples. In Afghanistan, such groups have been formed and supported by several foreign state actors since at least the 1970s.[28]

The Syrian civil war, which started as a conflict between the state and domestic protesters in 2010, quickly devolved into a setting for regional and great-power rivalries, which have been fought by proxy both inside Syria as well as at the international level as various actors have sought leverage over the management and

27 See Margarete Klein, 'Private Military Companies, A Growing Instrument in Russia's Foreign and Security Policy Toolbox', Hybrid CoE Strategic Analysis 17, 2019, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-17-private-military-companies-a-growing-instrument-in-russias-foreign-and-security-policy-toolbox/. See also Kimberly Marten, 'Russia's use of semi-state security forces: the case of the Wagner Group', *Post-Soviet Affairs*, Volume 35, Issue 3 (2019).

28 Michael Fredholm, *Afghanistan Beyond the Fog of War: Persistent Failure of a Rentier State* (Copenhagen: NIAS Press, 2018), 157–158.

resolution of the conflict.[29] Syria's civil war has also been played out among the diaspora beyond the country's borders.

Non-state actors have even threatened violence against third countries if their policies have been deemed insufficiently supportive of one side or the other, such as in Sweden in 2015, where the sentencing of a member of the Free Syrian Army (FSA) to prison for torturing a captive led to threats against the court and the Swedish government.[30] These protests combined media power and diplomatic power, and even carried a faint suggestion of a threat of terrorist power. While it is clear that the FSA itself had a strong interest in maintaining a broad international coalition applying pressure on the Syrian government and its allies, this was also in the interest of the group of states that were seeking to influence the conflict through the organization. One could therefore conclude that the FSA in this case was a long-term ally of these states, serving in an indirect and delegatory capacity – that is, as a proxy – with funding and other types of support from the states whose goals it shared to a degree.

Terrorist power

Terrorist power may be deployed by NSAs or SAs. Either way, it involves the carrying out of violent attacks, killings, and acts of sabotage. Attacks do not need to be simple; many terrorists are fascinated by chemical, biological, radiological and nuclear agents and weapons of mass destruction, but few know how to deploy them. Some states actively support terrorists. However, it is more common for a state to provide passive support to those terrorist organizations with which it shares goals, insofar as the state in question can tolerate and turn a blind eye to their activities; this usually means keeping bloodshed below a certain threshold (for an example of the latter, see the section on civil power below).

State cooperation with terrorist NSAs was quite widespread during the Cold War but, due to the increasing risk of exposure and attribution, became less ubiquitous afterwards. Yet state links with terrorist entities were characterized by relationships of a hybrid nature even then. In addition to engaging in threats and actual acts of violence, the terrorist entities were used for gathering intelligence and even as conduits for clandestine arms exports.[31] Such relationships also persist today, especially in conflict zones or regions where various state actors compete for influence. Using terrorist organizations as proxies is quite risky, however, as they may be more strongly motivated by their own ideological objectives than by their

29 Joseph Holliday, 'Syria's Armed Opposition', Institute for the Study of War, 2012, 14; Joseph Holliday, 'Syria's Maturing Insurgency', Institute for the Study of War, 2012, 9; Elizabeth O'Bagy, 'The Free Syrian Army', Institute for the Study of War, 2013, 11.

30 Judicial proceedings, Södertörns tingsrätt, dom 2015–02–26, mål B 13656–14; Syria Justice and Accountability Centre (SJAC), 'Sweden's First Steps towards Justice Prove Controversial among Syrians', SJAC website, 9 March 2015, https://syriaaccountability.org/updates/2015/03/09/swedens-first-steps-towards-justice-prove-controversial-among-syrians/.

31 Przemysław Gasztold, 'Polish Military Intelligence and Its Secret Relationship with the Abu Nidal Organization', in *Terrorism in the Cold War 1: State Support in Eastern Europe and the Soviet Sphere of Influence*, ed. Adrian Hänni, Thomas Riegler, and Przemysław Gasztold (London: I.B. Tauris, 2020), 85–106.

relationship with the state actor. They may even turn against their patron, of which the twists and turns of the conflicts in Afghanistan provide object lessons.

Another example of the risks involved is the reported interaction between the so-called Chatayev Group of the Caucasus Emirate and Georgian authorities in the early part of the 2010s. The alleged purpose was to form a group to engage in violent attacks in Russia. The plan never came to fruition however.[32] If the plan had succeeded, the Chatayev Group would have become a long-term ally and proxy of the Georgian state that had established it. The Group would have probably been dependent on Georgia for funding and other types of support. The agenda would have been determined by the state actor, although it might have evolved over time to include other interests as well.

Real economic power

Real economic power is mostly deployed by states. However, some multinational firms and conglomerates have at their disposal resources that match or exceed those of SAs, so NSAs are active within this sphere. While they frequently act as proxies for states, they may also have agendas of their own. The projection of real economic power displays itself in a variety of activities. These include, but are not limited to, the acquisition of strategic resources, infrastructure, and control over transportation routes, the imposition of monopolies and prices favorable to the stronger party, and the interruption of the supply of raw materials, fuels, critical components and services as a means to force compliance with other demands. The deployment of real economic power may be straightforward with regard to intention but tends to involve large numbers of commercial and other entities, and complex series of negotiated agreements.

Major infrastructure projects, such as oil and gas pipelines, are particularly prone to becoming a part of hybrid threat activities. When a pipeline, communication link, port or other major piece of infrastructure has been built, it cannot be moved. For the investment to make sense, the volume transported has to be large. This in turn creates dependence. Investing for example in an oil or gas pipeline leading to a single end customer makes the supplier vulnerable to demands from the customer to re-negotiate the price of imports, after the investments have already been made and the project is committed. At the same time, the customer may be highly reliant on a single provider and thus vulnerable to coercion.

In Europe, the construction of the Nord Stream 1 and Nord Stream 2 gas pipelines from Russia to Germany through the Baltic Sea has involved several states, central and local authorities, state and privately owned enterprises, and non-governmental organizations. In addition to the obvious financial and economic interests, the project has raised major environmental and security concerns during a period when relations between Russia and Western countries have deteriorated and tensions in the Baltic Sea

32 Fredholm, *Transnational Organized Crime*, 175–178; Report of the Public Council at the Public Defender's Office of Georgia on the Special Operation of 28 August 2012 near the village of Lapankuri, Lopota Gorge, Georgia, https://www.ombudsman.ge/eng/spetsialuri-angarishebi/report-of-the-public-council-at-the-public-defenders-office-of-georgia-on-the-special-operation-of-28-august-2012-near-the-village-of-lapankuri-lopota-gorge-georgia; Statement of the State Security Service of Georgia, 1 December 2017, https://ssg.gov.ge/en/news/291/saxelmtsifo-usafrtxoebis-samsaxuris-gancxadeba.

region have increased. The project itself is, to a considerable extent, an expression of Russia's security policy.[33] As such, and because of its great impact on the economic development and energy security of Europe, it has been regarded very differently among the countries of the Baltic Sea region and the United States.[34] The intertwining of state and private interests provides fertile ground for hybrid influencing and the use of non-state proxies by state actors.

The promotion of the project in the European countries in question by the Russian state and by Nord Stream AG, the international consortium responsible for the project, has raised many questions. The efforts have included sizable investments in local communities, aggressive media campaigns, as well as efforts to engage in elite capture through the recruitment of high-profile former leaders and key government advisers in the important littoral states. Some of these influencers were hired by local and international public relations companies that were contracted to organize and execute the influence campaigns, further expanding the distance between the state actor involved and the concrete influence activities.[35] From the perspective of the taxonomy, Nord Stream AG could be seen as an auxiliary and/or surrogate for the Russian state. The relationship has been a long one. The consortium has been dependent on Russia and shared its agenda.

Financial power

Similarly to real economic power, financial power is mostly deployed by states. However, again some multinational firms and conglomerates have resources at their disposal on a level similar to or exceeding those of states. Financial power projection displays itself in a variety of activities. Most common seem to be the imposition of trade barriers, financial sanctions (particularly punitive tariffs and embargoes, which are often employed in conjunction with diplomatic sanctions), foreign direct investment (FDI) including the strategic application of sovereign wealth funds to gain specific objectives, and the manipulation of exchange rates for reasons of speculation, or for inducing targeted indebtedness in states regarded as adversarial. However, financial power projection can also be applied as a means of taking advantage of manipulated stock market fluctuations. If so, the manipulation has typically been carried out by other, non-financial means, which makes the activity a hybrid threat. However, FinTech and similar new technologies signify fresh vulnerabilities in this field.[36]

33 'Energeticheskaya strategiya Rossii na period do 2020 goda' ('Energy Strategy of Russia to the Year 2020'), Government of the Russian Federation Decree No. 1234-r, 28 August 2003. Approved on 23 May 2003 and confirmed by the Russian government on 28 August 2003.

34 See e.g. Michael Fredholm, 'Power Projection by Pipeline: Russia, Sweden, and the Hybrid Threat from the Nord Stream Project, 2005–2009', in *Vernetzte Unsicherheit*, ed. Dengg and Schurian, 263–332.

35 Fredholm, 'Power Projection by Pipeline', 288, 320–323; Kristoffer Morén, 'Energy issues are being dealt with by a variety of actors; Governance and cooperation are lacking', *Baltic Worlds*, Volume 4 (2010): 15. See also Nord Stream, Secure Energy for Europe: The Nord Stream Pipeline Project 2005–2012 (Zug: Nord Stream, 2013), 71, 121, 129.

36 See e.g. Aleksi Aho, Catarina Midões & Arnis Šnore, 'Hybrid threats in the financial system', Hybrid CoE Working Paper 8, June 2020, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-8-hybrid-threats-in-the-financial-system/.

Reports about the covert application of financial power as a hybrid threat appear from time to time, but they tend to be impossible to verify through open sources. One well-documented case was the 23 April 2013 hack of the Twitter account of the US news agency Associated Press (AP), for which the Syrian Electronic Army (SEA), a group of hackers who operated in support of the Syrian government, claimed responsibility. Three years later, the FBI charged three members of the SEA with this and other hacks. Having gained control of the AP Twitter account, the hackers asserted that President Barack Obama had been wounded in an explosion at the White House. Reportedly, more than 1.9 million people followed the AP reports on Twitter. As a result, USD 136.5 billion was erased from the US S&P 500 stock index value, and the Dow Jones Industrial Average index dropped 0.98% within seconds. Although the market quickly recovered, the SEA hack showed the vulnerability of the financial sector.[37]

If such a group of hackers indeed aimed to cause a negative impact on the financial markets on behalf of an SA, and if the SA was in a position to take advantage of the market impact, neither of which seems to have been the case in connection with the SEA hack of the AP Twitter account in 2013, this would constitute a covert application of financial power as a hybrid threat, since the operation would affect (at least) the financial, media, and cyber domains. Mere cyberattacks against the capability of individual banks to employ SWIFT services might produce a short-term effect but would not reach the strategic threshold for a hybrid threat.[38] The SEA would have acted as a proxy of the Syrian state with shared goals.

The SWIFT system itself has been discussed as a potential tool for the application of financial power. SWIFT is a cooperative company under Belgian law, owned and controlled by its shareholders, which consist of financial institutions from across the world. The shareholders elect a Board of Independent Directors. Overseen by the G-10 central banks (Belgium, Canada, France, Germany, Italy, Japan, Switzerland, Sweden, the Netherlands, the United Kingdom, and the United States), as well as the European Central Bank, the lead overseer of SWIFT is the National Bank of Belgium. Since virtually all international financial transactions go through the SWIFT system, the suspension of access to SWIFT would have particularly devastating and immediate effects on the targeted state or private entity.

SWIFT's role has come up in connection with the imposition and execution of international sanctions. In 2018, it was drawn into a dispute between the United States and the European Union over the means by which Iran should be persuaded to give up its nuclear programme and modify its activities in the Middle East. SWIFT had already been affected by EU and US actions related to Iran. In 2012, following an EU Council decision, SWIFT discontinued its communications services to Iranian financial institutions

37 Alina Selyukh, 'Hackers Send Fake Market-moving AP Tweet on White House Explosions', Reuters, 23 April 2013, https://www.reuters.com/article/net-us-usa-whitehouse-ap-idUSBRE93M12Y20130423; Department of Justice, Office of Public Affairs, 'Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army', Press Release No. 16–329, 22 March 2016, https://www.justice.gov/opa/pr/ computer-hacking-conspiracy-charges-unsealed-against-members- syrian-electronic-army/.

38 For a more detailed discussion on the use of financial power in the hybrid threat context, see e.g. Aho, Midões & Šnore, 'Hybrid threats in the financial system'.

as a result of European sanctions (specifically, EU Regulation 267/2012).[39] Iran's oil exports plunged. The sanctions imposed through the discontinuation of SWIFT services were widely seen as instrumental in bringing Iran to the negotiating table, which led to the 2015 Iran nuclear deal.

In 2018, the EU did not share the view of the United States that new sanctions should be imposed on Iran. This led to a discussion in the Trump Administration about using SWIFT to make US sanctions more effective. To compel SWIFT to adhere to the US sanctions despite the lack of EU support, the Trump administration noted that it would specifically include those who provided 'specialized financial messaging services to the Central Bank of Iran and Iranian financial institutions' among those against whom US sanctions would be enforced. Financial sanctions would target the banks represented on the SWIFT board or individual SWIFT officials rather than the cooperative as a whole. Thus, SWIFT operations in themselves would not be interrupted by the sanctions, even if some of its shareholders and officials might be severely affected.[40]

On 5 November 2018, SWIFT announced that it would comply with the restored US sanctions on Iran, despite the EU's efforts to defy the US action with new EU rules that forbade companies from complying with the US Iran sanctions.[41] SWIFT subsequently explained its action as follows: "In exceptional circumstances, and where the interest of the stability and integrity of the wider global financial system are at risk, SWIFT may also need to restrict customers' access to the network. In an isolated event in November 2018, SWIFT thus suspended certain Iranian banks' access to the messaging system. This step, while regrettable, was taken in the interest of the stability and integrity of the wider global financial system, and based on an assessment of the economic situation."[42]

The SWIFT case is significant because it became a non-aligned, indeed an unwilling proxy of a state actor that was compelled to take certain actions. These actions clearly increased the effectiveness of the sanctions regime. It is not surprising that demands for the use of SWIFT as a means to apply pressure now occur regularly among a variety of actors, for example in the European Parliament.[43] The SWIFT case also

39 SWIFT Press Release, 'SWIFT instructed to disconnect sanctioned Iranian banks following EU Council decision', 15 March 2012, https://www.swift.com/insights/press-releases/swift-instructed-to-disconnect-sanctioned-iranian-banks-following-eu-council-decision.

40 'Iran Threat Reduction and Syria Human Rights Act of 2012', Public Law 112–158, https://www.congress.gov/112/plaws/publ158/PLAW-112publ158.pdf; U.S. Department of the Treasury, 'Frequently Asked Questions Regarding the Re-Imposition of Sanctions Pursuant to the May 8, 2018 National Security Presidential Memorandum Relating to the Joint Comprehensive Plan of Action (JCPOA)', 8 May 2018, 3. The same threat was repeated in the 6 August 2018 update of the document.

41 U.S. Department of the Treasury, 'U.S. Government Fully Re-Imposes Sanctions on the Iranian Regime as Part of Unprecedented U.S. Economic Pressure Campaign', Press Releases, 5 November 2018, https://home.treasury.gov/news/press-releases/sm541; Michael Peel, 'Swift to Comply with US Sanctions on Iran in Blow to EU', *Financial Times*, 5 November 2018, https://www.ft.com/content/8f16f8aa-e104–11e8–8e70–5e22a430c1ad.

42 SWIFT, 'Compliance', https://www.swift.com/es/node/11306.

43 See e.g. European Parliament, 'Joint Motion for a Resolution on Russia, the Case of Alexei Navalny, the Military Build-up on Ukraine's Border and Russian Attacks in the Czech Republic (2021/2642(RSP))', 28 April 2021, Section 8, https://www.europarl.europa.eu/doceo/document/RC-9–2021–0236_EN.html.

points to the fact that international non-governmental organizations, including those of a very technical nature, can be highly useful tools in carrying out hybrid threat activities.

Diplomatic power

Diplomatic power is typically deployed by states. It customarily involves, for example, persuasion, inducements, threats and sanctions, as well as the crafting and introduction of resolutions, which may be expressions of political will or the basis for concrete action, by international organizations over which the state has some level of influence or in which it is able to find support from like-minded states. The purpose is often to isolate the target state from the international community in order to reduce its freedom of manoeuvre, which translates into the reduction of its capacity to pose a threat. A dominant state might be able to utilize an international organization as a proxy, in which case the international organization functions as an NSA in relation to the SA, and the activity, if carried out in conjunction with the application of other powers, may qualify as a hybrid threat activity. However, international organizations also have agendas of their own and may engage in hybrid threat activities by themselves. The same goes for some other types of NSAs, such as insurgent organizations and governments-in-exile, which frequently employ their diplomatic power, such as it may be, in hybrid threat activities.

Whenever an NSA has the ambition to remake itself into a state, it will sooner or later have to create a capacity for diplomatic power. As long as the NSA in question enjoys state support, it may well be treated as a diplomatic proxy. Most successful insurgent movements throughout history at one time or another went through a parallel development. States may also lift the profile of proxy NSAs to gain leverage in crisis management and conflict resolution. The various negotiations and 'peace processes' related to the Syrian conflict provide a number of examples. In cases such as these, the efforts to make peace processes, and international diplomacy in general, more inclusive and accessible to civil society actors are turned on their head – which of course may well be one of the strategic objectives of authoritarian state actors.

The various roles played by the Afghan Taliban movement, from its inception in the 1990s until today, provide examples of the employment of diplomatic power by a non-state actor. Afghanistan has arguably been one of the most prominent settings for great-power competition enacted by proxy. Various foreign states have acted as patrons of the movement.[44] In the early 1990s, Pakistan took the lead in a campaign aimed at moving Afghanistan's representation at the United Nations to the Taliban in the belief that, if it could assist the movement in becoming recognized as the new government of Afghanistan, this government would be amenable to Pakistani interests in the region and at the international level. By 1996, the United States had initiated diplomatic links with the Taliban government, and the issue of the United Nations seat came up in the discussions.[45] Meanwhile, Pakistan found allies to recognize

44 For full details on the Pakistani involvement in the establishment of the Afghan Taliban, which was noted by diplomats at the time, see Fredholm, *Afghanistan Beyond the Fog of War*, 192–202.

45 U.S. Department of State, 'Afghanistan: Taliban Rep Won't Seek UN Seat For Now', Cable, 13 December 1996, Confidential. Declassified and available from the National Security Archive, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB97/.

the Taliban government as Afghanistan's legitimate representative. In May 1997, Pakistan, Saudi Arabia, and the United Arab Emirates, in this order, recognized the Taliban Emirate of Afghanistan.[46] However, other events ultimately blocked the development, and the Afghan Taliban, once established, proved little more cooperative than Pakistan's previous proxies in Afghanistan.

After the 2001 invasion of Afghanistan by the international coalition, the Taliban developed their own hybrid threat capacity, including in diplomatic power projection. It focused on two distinct targets: the states participating in the International Security Assistance Force (ISAF) and the worldwide Muslim community.[47] A major aim was to negotiate the withdrawal of the international coalition, with threats and violence if necessary, so that the Taliban could return to power. For this task, the Taliban also relied on diplomatic power, with negotiations conducted through friendly Muslim countries such as Pakistan, Saudi Arabia, the United Arab Emirates, and Qatar.[48] The Taliban diplomatic campaign eventually paid off in the form of a more public, international presence, aimed less at the West than at the worldwide Muslim community, to whom the Taliban leadership wished to appear as a responsible and religiously legitimate party.

In 2018, Taliban representatives took part in an international meeting in Moscow together with Russia, China, Pakistan, Iran, India, and the five Central Asian republics. The United States was present as an observer.[49] Direct negotiations were established between the Taliban and the United States in Qatar. These led to a peace agreement signed in February 2020.[50] Since the Afghan Taliban deployed their diplomatic power in conjunction with several types of hard power, notably privatized and terrorist power, the Taliban activities qualified as a hybrid threat campaign.[51] While the support of foreign states was at times instrumental, the Taliban performed predominantly as an independent actor with its own interests and goals, some of which coincided with those of their foreign patrons.

Civil power

Civil power can be described as the soft-power version of people's power. It is customarily deployed by NGOs, charities, law firms and

46 Fredholm, 'The Hybrid Threat Capability of the Afghan Taliban Movement, 2001–2014', 356. In turn, the Taliban government recognized the separatist government in the Russian republic of Chechnya in January 2000. Jane's Sentinel: Afghanistan, 1 June 2000.

47 Fredholm, 'The Hybrid Threat Capability of the Afghan Taliban Movement, 2001–2014', 313–46.

48 Ahmed Rashid, 'The Truth behind America's Taliban Talks', *Financial Times*, 29 June 2011, http://www.emma-bonino.it/press/world/9402.

49 BBC News, 'Afghanistan war: Taliban attend landmark peace talks in Russia', 9 November 2018, https://www.bbc.com/news/world-asia-46155189.

50 'Agreement for Bringing Peace to Afghanistan between the Islamic Emirate of Afghanistan which is not recognized by the United States as a state and is known as the Taliban and the United States of America', 29 February 2020, https://www.state.gov/wp-content/uploads/2020/02/Agreement-For-Bringing-Peace-to-Afghanistan-02.29.20.pdf; BBC News, 'Afghan conflict: US and Taliban sign deal to end 18-year war', 29 February 2020, https://www.bbc.com/news/world-asia-51689443.

51 For details on the series of meetings, see Fredholm, 'The Hybrid Threat Capability of the Afghan Taliban Movement', 335–336, and Michael Fredholm, 'The Fog of War Again Descends on Afghanistan', NIAS Press Blog, 10 May 2020, https://www.niaspress.dk/the-fog-of-war-again-descends-on-afghanistan/.

PR agencies which operate on behalf of interested parties, and by some international organizations. Civil power is commonly deployed in the form of protests, demonstrations, consumer boycotts, fundraisers, and the like.

Although the use of civil society for hybrid threat activities has a long history, the method became increasingly widespread during the Cold War. Perhaps the most widely reported example is that of how Soviet intelligence during the Cold War infiltrated and gained control over parts of the anti-war and anti-nuclear protest movements in North America and Western Europe, thus turning them into hybrid threat actors against the Western alliance and its ongoing reliance on nuclear weapons for deterrence. Although the degree of impact was different in each country, the Soviet influence, for example in Cold War-era Sweden, has been recognized as significant by both security service officials and scholars.[52]

The harnessing of civil power for hybrid threat activities figures prominently in the tool box that the Chinese Communist Party applies to influence foreign countries. The United Front approach provides the framework through which the Party seeks to manipulate diaspora organizations as well as foreign business and academic associations, political parties and individual influencers while maintaining nominal deniability.[53] Russia is making vigorous efforts to infiltrate Western civil society networks, for example through wealthy individuals and foundations that are affiliated with the Russian Orthodox Church with the aim of positioning itself as a source of inspiration and as a leader of nationalistic, traditionalist political forces in Europe and North America.[54] In terms of the taxonomy, such foundations could be seen as long-term allies and proxies of the Russian state, which are dependent on the state and fully share its agenda.

Scientific and technological power

Scientific and technological power, including in the form of technological innovations, can be utilized, in part or in whole, to further a political or economic agenda. This type of power is frequently deployed by SAs, but NSAs in the form of certain multinational firms and conglomerates also have the capacity. The new technologies can be used as enablers. In the West, public

52 Magnus Hjort, *Den farliga fredsrörelsen: Säkerhetstjänsternas övervakning av fredsorganisationer, värnpliktsvägrare och FNL-grupper 1945–1990* (Stockholm: SOU 2002:90), 326–327; Michael Fredholm, *Hemligstämplat: Svensk underrättelsetjänst från Erlander till Bildt* (Stockholm: Medström, 2020), 187–196, with references, 213–14. See also Frances Stonor Saunders, *Who Paid the Piper? The CIA and the Cultural Cold War* (Granta Books, London, 1999).

53 Jukka Aukia, 'China as a hybrid influencer: Non-state actors as state proxies', Hybrid CoE Research Report 1, June 2021, https://www.hybridcoe.fi/publications/hybrid-coe-research-report-1-china-as-a-hybrid-influencer-non-state-actors-as-state-proxies/.

54 See e.g. Robert C. Blitt, 'Religious Soft Power in Russian Foreign Policy: Constitutional Change and the Russian Orthodox Church', Berkley Center for Religion, Peace and World Affairs, Brookings Institution, May 2021, https://berkleycenter.georgetown.edu/publications/religious-soft-power-in-russian-foreign-policy-constitutional-change-and-the-russian-orthodox-church; 'Tip of the Iceberg: Religious Extremist Funders against Human Rights for Sexuality and Reproductive Health in Europe 2009–2018', European Parliamentary Forum for Sexual and Reproductive Rights, June 2021, https://www.epfweb.org/node/837, 21–29.

services, both government run and privately provided, are increasingly placed on privately owned technology platforms. The public information space is built to a great extent on information and communication technology that has been developed during the past 20 years and is controlled by a small number of very large corporations. These developments invite attempts to gain control over and manipulate the activities of the technology companies for the purposes of intelligence-gathering, influencing, interference and disruption. New technologies can also be used as influencers.

The ongoing Covid-19 pandemic is a case in point. Before the pandemic, the production of vaccines and protective equipment was centralized in a few countries. With the virus appearing and spreading seemingly uncontrollably, public authorities, private companies and the general population were willing to pay practically any price to get them. This led to both criminal activity, such as selling falsified or substandard products, but also to so-called vaccination diplomacy by countries where governments control the industry. For example, the deliveries of Russian and Chinese medical products to Serbia have constituted a central element of anti-Western narratives in that country.[55]

The pandemic provides valuable case studies on how, under the conditions of a medical emergency, it is possible to employ deliveries of medicines as levers of influence in small countries, since they tend to be dependent on the manufacturers of pharmaceuticals in other countries. Assuming the intention is there, either the manufacturers themselves, or the countries under whose jurisdiction they operate, may use the supply, or denial, of medical products to induce a state of panic in a population which has an urgent need for them. Such a panic might under certain circumstances provide fertile ground for social destabilization, which could easily be translated into acquiescence in the face of political or economic demands. If so, scientific and technological power would be applied in conjunction with other powers, duly producing a hybrid threat.

China's determined drive towards dominance in technology, and the ways in which it has been seen using technology domestically and in foreign influence operations, have raised particular concerns. In February 2020, US officials announced that China had the capacity to covertly access mobile networks created by Huawei Technologies Co. through backdoors.[56] The company has denied this, but what is undeniable is that any Chinese corporation is legally obligated to serve the state's security needs whenever and in whichever manner state agencies deem necessary.[57] China's efforts to control and manipulate the global information space through both technology and the mobilization

55 See e.g. Michael Leigh: 'Vaccine diplomacy: soft power lessons from China and Russia?', Bruegel Blog, 27 April, 2021, https://www.bruegel.org/2021/04/vaccine-diplomacy-soft-power-lessons-from-china-and-russia/.

56 Bojan Pancevski, 'U.S. Officials Say Huawei Can Covertly Access Telecom Networks', *Wall Street Journal*, 12 February 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256. Notably, no evidence on Huawei backdoors was released, only managed leaks to trusted journalists.

57 Aukia, 'China as a hybrid influencer', 22.

of state and non-state resources are also widely documented.[58] Huawei would thus act as a long-term auxiliary to the Chinese state, with the latter compelling the company to implement the state's agenda in addition to its own commercial goals.

Media power

Media power is deployed by almost all actors engaged in hybrid threat activities, including by both SAs and NSAs. The deployment of media power is probably the most pervasive means of influence. Its impact has been unparalleled since the fifteenth-century introduction of the movable-type printing press, which enabled the mass production of printed leaflets and newsletters. The use of such media for purposes of propaganda and disinformation began almost at once, and even though the media currently employed are different, the nature of media power remains unchanged. Media power is deployed to direct and influence public opinion, whether in the cyber domain, in social media networks, or by means of mass-media coverage. NSAs involved in media power projection commonly include NGOs as well as media firms, public relations agencies and other commercial entities, but also other NSAs such as insurgent and terrorist groups.[59]

Beyond the ideal of enabling the free exchange of ideas in liberal democracies, media power is customarily employed to attain two linked but different objectives: (1) to exert influence on states and societies through information, disinformation, propaganda, and the manipulation of information, based on the principle that what is perceived becomes the truth; and (2) to interrupt an adversary's channels of communicating with the public and the denial of access, for the adversary, to alternative sources of media dissemination. Denial of access may consist of denial of service by physical means or the successful mobilization of available media sources. Either method translates into supremacy within the information domain. If the media power deployment takes place in conjunction with other means, the activities qualify as a hybrid threat campaign.

During the Cold War, the Soviet Union attempted to split the unity of the opposing group of Western states and their allies with what it referred to as 'active measures'. The primary target was the concord between the United States and Western Europe but active measures were also used to disrupt national

58 For further analysis, see e.g. Antonio Missiroli, 'Geopolitics and strategies in cyberspace: Actors, actions, structures and responses', Hybrid CoE Paper 7, June 2021, https://www.hybridcoe.fi/publications/hybrid-coe-paper-7-geopolitics-and-strategies-in-cyberspace-actors-actions-structures-and-responses/; Samantha Hoffman, 'Engineering global consent – the Chinese Communist Party's data-driven power expansion', Policy brief Report No. 21 (Australian Strategic Policy Institute, 2019); Jakob Bund: 'Finding China's Edge – Engineering Influence Operations within the Limits of Social Media Platform Rules', Cyberdefense Report, Cyberdefense Project (Center for Security Studies, ETH Zürich, July 2021).

59 For further analysis on the use of media power and disinformation, see e.g. Isabella Garcia-Camargo & Samantha Bradshaw, 'Disinformation 2.0: Trends for 2021 and beyond', Hybrid CoE Working Paper 11, July 2021, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-11-disinformation-2–0-trends-for-2021-and-beyond/; Jean-Baptiste Jeangène Vilmer: 'Effective state practices against disinformation: Four country case studies', Hybrid CoE Research Report 2, July 2021, https://www.hybridcoe.fi/publications/hybrid-coe-research-report-2-effective-state-practices-against-disinformation-four-country-case-studies/.

unity within these countries. Active measures encompassed various means including clandestine support for local communist parties and activist organizations such as those within the peace movement.[60] The purpose of active measures was regarded as distinct from both espionage and counterintelligence, on the one hand, and from traditional diplomatic and informational activities, on the other. Relying on deception, the goal of active measures was to influence the opinions and/or actions of individuals, governments, and/or the public.[61]

A key tool for manipulating the information space in targeted societies was the planting of false information in publications. In one well-documented case, the KGB used two Indian publications, the daily newspaper *Patriot* and the weekly *Blitz*, to introduce disinformation that was then picked up by the Soviet press agency TASS and distributed throughout the world, thus amplifying the effect while hiding the true source of the material.[62] The most successful disinformation campaign was the introduction of the theory that the HIV/AIDS pandemic was created and set off by the CIA; a conspiracy theory that is still in circulation.[63] Taken as a whole, the KGB operations certainly constituted hybrid threat activities, since they involved the combination of numerous types of power beyond the obvious one of media power. The newspapers in question served as long-term surrogates of the Soviet state, relying on it for resources and sharing its goals.

60 See e.g. CIA study on Trends and Developments in Soviet Active Measures, released at a hearing on Soviet active measures before the Permanent Select Committee on Intelligence, House of Representatives, Washington, D.C., 13–14 July 1982, 56–60, 61–9.

61 United States Department of State, 'Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns' (Washington, DC: Department of State, 1986); United States Department of State, 'Soviet Influence Activities: A Report on Active Measures and Propaganda', 1986–87 (Washington, DC: Department of State, 1987).

62 Aleksandr Kaznacheyev, a Soviet diplomat who defected to the West in 1959, described how articles were received from the KGB in Moscow, sent to Soviet embassies abroad, translated, and planted in local newspapers, among them the Blitz. The published articles were returned to Moscow through TASS channels. The Soviet press then republished the materials as if they were genuine foreign articles. Alexander Kaznacheev, *Inside a Soviet Embassy: Experiences of a Russian Diplomat in Burma* (Philadelphia: J. B. Lippincott, 1962), 172–3, 177. For full details, see Michael Fredholm, 'Soviet Active Measures in West, Southeast, and East Asia with regard to Afghanistan, 1980–1982', *Journal for Intelligence, Propaganda and Security Studies* (JIPSS), Volume 13, Issue 1, (2019): 56–74.

63 See e.g. Thomas Boghardt, 'Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign', *Studies in Intelligence*, Volume 53, Issue 4 (December 2009): 1–24.

Non-state hybrid threats independent of state influence

This report is primarily concerned with a conceptual discussion of hybrid threats directed or instigated by foreign states and carried out through the actions of non-state entities. The primary reason for this, as previously stated, is that few NSAs have given proof of an independent capability and the strategic outlook needed to conduct concrete, systematic operations against multiple vulnerable sectors in a targeted society over time; that is, applying several types of power in a coordinated and sustained way. Most terrorist and criminal groups operating in Western countries tend to rely primarily on violence or the threat of violence and hence do not cross the threshold of representing a hybrid threat. As terrorism is a crime committed with the intent to spread fear among the general public for a political purpose, the application of power tends to be overt in nature.[64]

In other parts of the world, terrorist organizations have, however, shown that NSAs may in fact become hybrid threat actors in their own right. This was exemplified by the early expansion of the Islamic State in Iraq and al-Sham (ISIS) during the period from 2011 to 2014. ISIS's exploitation of political disorder, sectarian divisions and Sunni grievances, its hierarchical structure, its success in recruiting fighters from practically all over the world, and its ability to adapt to exploit opportunities to take control of strategically important areas and functions certainly portrayed an organization capable of conducting a hybrid campaign of significant strategic ramifications. ISIS has employed a variety of different means and tactics, including propaganda and disinformation operations, as well as technical tools, such as drones and chemical weapons. Some of its activities have approached the level of posing a strategic threat to Western countries. To mention just one example, it has been successful in radicalizing a considerable number of individuals, and thus increased the occurrence of potential and actual terror attacks long into the future.

It should be noted that the emergence of ISIS and its capacity to evolve into this multifaceted threat was to some extent made possible through the support it received from state actors with strategic interests in the region. However, this support has arguably never been the decisive factor in its successes and failures, and has never swayed it from its independently chosen path.

The information domain has been a particularly prominent avenue of systematic influencing for religiously and ideologically based radicalized movements active in Western societies. The distribution of Salafi-inspired messages through social media, lectures, preaching, street da'wa, and physical corrections of what is perceived as deviating behaviour, has occasionally amounted to a significant challenge to democratic societies as it restricts the democratic rights and freedoms of considerable segments of the citizenry.[65] The same applies to some other ideologically inspired movements that seek to undermine the position of minority populations and women.[66] Both the religiously and the

64 Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 24–25.

65 Magnus Ranstorp et al., 'Between salafism and salafi-jihadism: Influence and challenges for Swedish society', Center for Asymmetric Threat Studies, Swedish Defence University, 2018, http://fhs.diva-portal.org/smash/get/diva2:1313715/FULLTEXT01.pdf.

66 See e.g. Damjan Denkovski, Nina Bernarding & Kristina Lunz, 'Power over Rights: Understanding and countering the transnational anti-gender movement', Volumes I and II, Centre for Feminist Foreign Policy, March 2021.

ideologically based movements have made extensive use of international networks. There are also examples of organized crime groups (OCG) that have conducted activities on a broad and systematic scale with the intention of increasing their power in society. Some notable cases from Europe and Latin America, which occurred in the 1990s and 2000s, include the OCGs' systematic use of intimidation through targeted violence, assassinations and indiscriminate acts of terrorism, followed by information campaigns through communiqués, news articles and other media activities.[67] OCGs do, however, mainly feature in hybrid-related contexts as entities for hire given their often well-established capabilities for, among other things, smuggling, violence, the provision of safe houses, forging documents and, perhaps more prominently, serving as entities that state actors may employ to conduct covert activities abroad.

As pointed out by Michel Wyss and Assaf Moghadam, non-state actors may also act as sponsors of other non-state actors. Examples include al-Qaida in the Arabian Peninsula, Hezbollah in Lebanon, the National Patriotic Front of Liberia, and the People's Protection Units in Iraq. Wyss and Moghadam propose four indicators of whether a sponsor-proxy relationship exists between non-state actors: coercion, physical proximity, material and/or financial preponderance, and external support that the sponsor can channel to the proxy.[68] The taxonomy presented above should retain its analytical power also when it comes to relationships among non-state actors; however, this should be explored further both in situations of armed conflict and peace.

67 See e.g. the activities of the Los Extraditables and Pablo Escobar in Colombia in 1984, the Sicilian mafia in Italy in 1993, and Los Zetas in Mexico in 2009. Some of the activities of the Kurdistan Workers' Party (PKK) in Sweden in the 1980s fall into this category.

68 Michel Wyss and Assaf Moghadam, 'Conflict Delegation by Non-State Actors', *International Studies Review*, Volume 23, Issue 4 (2021): 15–17.

Conclusions

The purpose of this report is to facilitate a better understanding of the role that NSAs play as hybrid threat actors. The point of departure has been the concept of hybrid threats employed by the European Centre of Excellence for Countering Hybrid Threats, and its perception that the hybrid threat landscape is a continuum where conditions of real or nominal peace flow into and intertwine with those of armed conflict. Non-state hybrid threat actors have been approached as entities that act independently of state structures, and that have the requisite capabilities to cause change in the targeted society.

From the point of view of the practitioner, a sound theoretical framework is necessary to make sure that concrete action is based on the correct data and reliable analysis, and finite resources can be focused on detecting and deterring the most serious threats. Consequently, the organization of knowledge with relatable definitions and categories is important. The taxonomy proposed here is intended to make this more systematic and efficient. The modes of behaviour by NSAs and their state patrons, which are illustrated in the case studies, reveal some indicators that will hopefully be useful for early detection of malign activity.

The role played by NSAs in the context of hybrid threats is likely to continue to gain importance. The variety of NSAs suitable for such a role is also likely to increase in the future. Further research is thus necessary when it comes to the very definition of the term 'non-state actor'. While most NSAs engaged in hybrid threat activities are probably linked with a state actor, there are also those operating independently or at the behest of another NSA. Specific scholarship is necessary to understand the consequences of this distinction.

While efforts to draw up international legal norms with regard to hybrid threats and the role NSAs play in this context seem unlikely to yield speedy results, they do provide opportunities for taking conceptual work forward. Bringing together scholars focusing on conditions of armed conflict, and those primarily concerned with hybrid threat activities taking place under conditions of real or nominal peace, will be valuable for the same reason.

Aside from gaining a better, and more widely shared idea of what we are talking about when we use the term 'non-state actor', the taxonomy should be further developed through a discussion that encompasses the entire spectrum of hybrid threats. It is absolutely vital that the voice of practitioners is heard here, so that the tool box of detecting and countering NSAs engaged in hybrid threat activities becomes and remains as relevant as possible. A key element in this discussion should be the division of labour among, on the one hand, public authorities, and, on the other, private actors including civil society organizations, private enterprise, and the population at large. At the international level, agreement should be sought on how targeted societies can cooperate to shield themselves against NSAs engaged in hybrid threat activities, as well as to take countermeasures when necessary. Again, both scholars and practitioners should have a voice.

Hybrid threats target all parts of society. NSAs are attractive tools because they evade many of the mechanisms with which states seek to protect themselves against malign

foreign influence. NSAs are, more often than not, woven into the social fabric of the targeted society. Engage the adversary too bluntly and you risk fraying that social fabric, and harming the values, the democratic political model, and the respect for human rights which you wish to maintain and foster. How to find the right balance between effective counter-action and safeguarding democracy should be the object of both committed scholarship and active political discussion.

Hybrid threat activities have broad consequences for the targets. There are the obvious ones, like the online services disrupted by a cyberattack, mistrust of the political system fermented by disinformation, or political pressure applied through elite capture. The broader psychological, social and political effects are poorly understood. Once again, NSAs should be a particular object of study as they are so deeply embedded in the targeted society.

Authors

Magnus Normark is a senior analyst at the Swedish Defence Research Agency (FOI). His areas of work include chemical, biological, radiological and nuclear threat assessment, intelligence studies and counter-proliferation. Between 2017 and 2021, he supported Hybrid CoE in Helsinki on challenges related to non-state actors and hybrid influencing. Previously, he has served as a national delegate in international regimes and mechanisms such as the Australia Group, the Proliferation Security Initiative, and the Global Initiative to Combat Nuclear Terrorism, and has working experience from international UN missions.

Janne Jokinen is the Deputy Director of the Community of Interest on Hybrid Influence at Hybrid CoE, on secondment from the Ministry for Foreign Affairs of Finland. Mr Jokinen is a career diplomat. He served as Deputy Director for Policy Planning and Research at the Ministry for Foreign Affairs of Finland from 2017 until 2020. From 2013 to 2017, he served as Head of the Political Section at the Embassy of Finland in Washington D.C. In his previous positions, he has dealt with the Middle East and North Africa; Finland's human rights policy at the United Nations and the European Union; and the Korean Peninsula.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats