Routledge
Taylor & Francis Group

European Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/feus20

Improved conceptualising of hybrid interference below the threshold of armed conflict

Julie Celine Bergaust & Stig Rune Sellevåg

To cite this article: Julie Celine Bergaust & Stig Rune Sellevåg (26 Oct 2023): Improved conceptualising of hybrid interference below the threshold of armed conflict, European Security, DOI: 10.1080/09662839.2023.2267478

To link to this article: https://doi.org/10.1080/09662839.2023.2267478

Published online: 26 Oct 2023.

EUROPEAN SECURITY
https://doi.org/10.1080/09662839.2023.2267478

Routledge
Taylor & Francis Group

Improved conceptualising of hybrid interference below the threshold of armed conflict

Julie Celine Bergaust [a,b] and Stig Rune Sellevåg [a]

[a]Total Defence Division, Norwegian Defence Research Establishment, Kjeller, Norway; [b]Department of Political Science, University of Oslo, Oslo, Norway

ABSTRACT

European policymakers have identified the need to understand influence operations on social media, cyber-attacks or hidden economic investments – activities that can be characterised as hybrid threats or hybrid warfare. Yet, the difference between hybrid threats and hybrid warfare is unclear. In 2019, Mikael Wigell therefore coined the term "hybrid interference" to clarify the distinction between "hybrid warfare" and "hybrid threats". However, less attention has been given to the activities hybrid interference may consist of. To address this gap we have used a morphological analysis, which is a structured tool for analysis that addresses all aspects of a concept. Through this method, we propose categories that make more sense of the complex phenomenon of hybrid interference. These five categories are international politics, coercive diplomacy, priming, covert coercion, and sabotage and assassinations. This article also identifies problems with referring to activities in the category of international politics as hybrid interference activities. The result is novel because we place all combinations of tools and methods within the concept of hybrid interferences in one of the five above-mentioned categories, and as such have provided a detailed operationalising of the concept in a transparent manner.

ARTICLE HISTORY
Received 8 June 2023
Accepted 3 October 2023

KEYWORDS
Hybrid interference; hybrid threats; hybrid warfare; grey zone conflict; security; Europe

Introduction

Hybrid interference refers to "non-military practices for the mostly covert manipulation of other states' strategic interests" (Wigell 2021, p. 51), often with different activities simultaneously, as "hybrid" refers to a combination (Cullen and Reichborn-Kjennerud 2017). This can for instance be influence operations on social media (Applebaum *et al.* 2017, Bergh 2020, Douglas 2021), cyber-attacks on critical infrastructure and gas lines (Juurvee and Arold 2021, Connolly 2022) or hack-and-leak operations in relation to national elections (Shires 2020). Even though hybrid interference is not a new phenomenon, it has received growing international attention

CONTACT Julie Celine Bergaust julie.bergaust@ffi.no

(Hoffman 2014, Palmer 2015, Wither 2016, Cantwell 2017, Wigell 2019, Hadzhiev 2020, Carment 2021, Wigell 2021), also of the critical sort (Stoker and Whiteside 2020). There is an urgency to better understand hybrid interference under the threshold of armed conflict as governments in Europe have started implementing countermeasures against a concept that remains ambiguous (Janičatová and Mlejnková 2021). The unintended consequences of implementing policies against an unclear concept can be problematic. Due to the ambiguity, and what Wigell (2021, p. 13) named a "terminological Babel" in the field, it is necessary to understand which activities the concept of hybrid interference consists of. In other words, there is a need to operationalise the concept. We, therefore, seek to answer the question: *How can hybrid interference be systematically conceptualised?*

To build on the existing literature, and systematically move the discussion further, this article contributes a refined and improved conceptualisation of hybrid interference. For this, we use morphological analysis. This method helps reduce blind spots because it forces the researches to address every combination a complex problem can consist of (Zwicky 1969, Ritchey 2013b). The morphological analysis is useful because it allows us to create a typology of hybrid interference activities and removes those combinations that are inconsistent, before organising the remaining activities in categories. This method is one of many approaches to developing typologies, but we chose the morphological analysis because of its strength in transparency. Using the morphological analysis to conceptualise and operationalise hybrid interference is, to our knowledge, completely novel.

The focus of this article is the integral components of the hybrid interference term, i.e. the interference activities, rather than how these activities in combination may cause escalating effects. This is to give the content of the concept further meaning, as Janičatová *et al*. (2021, p. 334) argue, "conceptualizing hybrid warfare raises the question whether hybrid warfare is not really just a label primarily used for political purposes and it is really more suitable to research particular components such as information or cyber warfare". Therefore, we seek to identify interference activities, that can provide a building block study for further research.

We have selected Europe as a starting point for conceptualising hybrid interference. Nonetheless, we do not reject the possibility of the results being relevant beyond the scope of Europe. If so, the parameters and parameter values going into the consistency analysis must be re-evaluated.

The article has the following structure: We first present the morphological method, followed by the analysis and thereafter present different categories the hybrid interference concept includes. These five categories are international politics, coercive diplomacy, priming, covert coercion, and sabotage and assassinations. Together, these five categories are all-encompassing activities that hybrid interference under the threshold of armed conflict can consist of, but an important distinction is identified when it comes to the category of international politics. After having identified the categories, we present an updated conceptualisation of hybrid interference before we conclude. These updated categories matter for our understanding of the contemporary security environment because the categorisation helps identify the different levels of challenges, as well as identify what should be separated from the concept of hybrid interference. This, in turn, can help policymakers in their efforts to detect, deter and

counter these types of security threats without compromising the democratic values to be protected.

Materials and methods

Understanding hybrid interference

The "hybrid" concept is known by many names: hybrid threats, hybrid warfare, and grey zone conflict. The concept has different names and different understandings. Frank G. Hoffman, who popularised the term, refers to "competitors who will employ all forms of war, perhaps simultaneously" (Hoffman 2009, p. 1). Later, Hoffman (2010, p. 443) described hybrid threats as "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the battlespace to obtain their political objectives" and as such he has a full-spectrum approach the definition. Wither (2016, p. 74) presents hybrid warfare as "the concurrent use of both conventional and irregular forces in the same military campaign". Wigell (2021, p. 51) refers to hybrid interference as "non-military practices for the mostly covert manipulation of other states' strategic interests". These three approaches treat somewhat different yet related challenges, but the terms are used as synonyms by policymakers. In the United Kingdom, for instance, policymakers have used term "hybrid warfare" when referring to disinformation and cyber-attacks in the UK (Janičatová *et al*. 2021, p. 320), activities that according to the above-mentioned definitions are better defined as hybrid interference.

We regard hybrid interference, as introduced by Wigell (2019, 2021), as the most fitting term to address state actors' illegitimate meddling activities when they are conducted under the threshold of armed conflict. Firstly, we see it as problematic to use the label "war" or "warfare" for activities under the threshold of armed conflict. Secondly, the term "interference" is preferred because it more clearly communicates the nature and purpose to create change than "threats". It is useful to read Wigell's (2019) definition in relation to the definition of "interference" itself. Interference has negative connotations, according to Berzina and Soula (2020), who refer to the Cambridge Dictionary (n.d.) definition of interference being "to involve yourself in a situation when your involvement is not wanted or is not helpful". Yet, we do not concur with Wigell (2021) when he does not include military instruments as part of hybrid interference strategies. Certainly, the show of arms or muscle flexing, as seen in recent years (Halas 2022, Kristian Åtland *et al*. 2022) can be part of the conceptualisation. Therefore, our approach to this concept relies on parts of Wigell's (2021, p. 51) definition of hybrid interference, namely, that it is "practices for the mostly covert manipulation of other states' strategic interests". Henceforth, we will exclusively refer to the concept as hybrid interference in our conceptualisation.

Morphological analysis

The General Morphological Analysis (GMA) was initially developed by Fritz Zwicky and is a method of structuring and analysing multidimensional problems (Zwicky 1969, Ritchey 2013a, 2013b). The method is especially suitable for analysing complex questions

because the concept that is analysed must be divided into all its sub-parts (Rittel and Webber 1973, Ritchey 2013a). In the field of security and defence, this method has been used for military scenario modelling (Johansen 2018) and analysis of social media influence operations (Buvarp 2023). The morphological analysis is useful for hybrid interference because of the many components the concept consists of. While we use Zwicky's method throughout the article, the approach is similar to fuzzy set theory (Ragin 2005) and typology development in political science (Ewers-Peters 2022). Our analysis follows a similar logic to typology development as proposed by George and Bennett (2005). Both George and Bennett (2005) and Zwicky (1969) seek to (i) define the overarching concept, (ii) specify the concept's internal construction, (iii) remove combinations that are highly unlikely or impossible, (iv) propose a model for understanding the concept and (v) simplify the model (Zwicky 1969, George and Bennett 2005). While several typology development methods are useful, morphological analysis is a particularly transparent and rigid method.

The morphological analysis is described in detail elsewhere (Ritchey 2013a, 2013b), therefore, only a short description is given here. Morphological analysis has the following steps: (1) Formulation of the problem to be solved; (2) identification and analysis of all parameters that are relevant to the problem; (3) construction of the morphological space; (4) conduct a consistency analysis to remove logically or empirically inconsistent combinations.[1] The result is the solution space; (5) evaluation of steps 1–4 and creation of appropriate and meaningful categories within the solution space.

Formulation of the research problem and choice of parameters

The analytical problem treated in this study is:

> How can hybrid interference be systematically conceptualised?

Understanding the activities of hybrid interference is identified as a key problem to understand within the European security context. Murphy (2022, p. 2) argues that "security professionals remain trapped in outdated frameworks that rely on a nation-state's traditional constructs". We seek to avoid this by aligning ourselves with scholars seeking to widen and deepen the conceptual security lens. The intention of this article is not to debate security theory or different definitions of security, but we want to highlight that by "deeper" security, we mean a referent object beyond the state, and with "wider", we mean sectors beyond the military (Buzan and Hansen 2009, p. 188).

Six parameters describe the research problem. The parameters are based on the following questions, inspired by the morphological analysis for scenario planning in the defence sector written by Johansen (2018):

(1) Threat actor: What type of actors pose a threat to European security?
(2) Objective: What overall objectives are motivating these threat actors?
(3) Target: What societal areas and/or values can be targeted, to reach these objectives?
(4) Method: What methods can the threat actors use to reach their objectives?
(5) Instrument: Which instruments are necessary for utilising a specific method?
(6) Concealment: Will the threat actor conceal its actions?

Parameter values should not overlap, nor should the number of parameter values be too large because this will make the analysis unnecessarily complex. Together the parameters provide a basis for describing an action.

Choice of parameter values

The choice of parameter values is vital for the conceptual understanding. It is important that the parameter values are unspecified to sectors or incidents because too narrow parameter values will create a solution space with blind spots. When we keep the parameter values more general, we can catch the breadth of hybrid interference. This opens the analysis to include incidents that have not yet happened but may in the future. Keeping the analysis open to previously unforeseen incidents is vital for the relevance of the analysis. However, we have no intention to create an exhaustive list of all specific actions, nor would it be possible.

The first parameter value is the *threat actor*. In the EU conceptual model for hybrid interference, both state and non-state threat actors are included (Giannopoulos *et al*. 2021). As mentioned, the purpose of this study is to contribute to an increased understanding of state actors' use of hybrid interference. Non-state actors have therefore been excluded from the analysis. It also is beyond the scope of this article to distinguish between state actor and coalition of states. This is because both a coalition of states and a single state will pose the same challenge. While we acknowledge that actions by separate state actors can have mutually reinforcing effects, for the purpose of this study, we will consider a single state actor and as such only have one value within the *actor* parameter. Furthermore, we chose not to look at specific individual states but rather a generic state actor that may intend to endanger security in Europe. We will still give examples from specific state actors to illustrate contemporary relevance. Through this, the study will help increase the overall understanding of how state actors can threaten security in Europe through hybrid interference, without attempting to consider the unknown limits of a specific state's capability.

The parameter value *objective* means what the threat actor wants to achieve with the intended action. The upper value for the objective will be to deprive governments of all sovereignty. Such an objective can be characterised as *changing political governance*. While we acknowledge the emerging research on democratic backsliding in Europe (Sitter and Bakke 2019, Anna Vachudova 2020), the majority of European countries today are democracies according to democracy indexes provided by for instance Freedom House (2022) and the Economist, with the Nordic and Western European states are most democratic (The Economist Intelligence Unit 2022a, 2022b). In such stable states, changing political governance will require military control over the territory, argues Johansen (2018). For this study, changing political governance is therefore outside the scope. Hybrid interference can, however, be used to influence political decisions by "influencing public and governmental policy" or "destabilizing public institutions" (Bernal *et al*. 2020, p. 3). This may be in the form of forcing political concessions in individual cases or forcing more protracted changes in policy that are beneficial to the threat actor. In this study, we group these objectives in the parameter value-*creating change in policy*. Another goal may be to *weaken agency*. To weaken a state's agency could be related to access to information, technology, or resources, gaining a better negotiating position, or laying the groundwork for more serious, intentional actions. A third parameter value, *undermine trust in societal institutions*,

aims to cover a distinctive feature of a state actor's use of hybrid interference, as identified by Giannopoulos *et al*. (2021). This can for instance be to make (parts of) the population believe democratic elections were rigged. Undermining trust in societal institutions can undermine the legitimacy of the authorities (Lipset 1968, p. 74, Haugsgjerd and Segaard 2020) or make the population more vulnerable to conspiracy theories and the spread of incorrect or misleading information (Dyrendal and Emberland 2019, Bergh 2020). By utilising these three parameter values of objectives, it is possible to create a distinction between different tactics that aim to harm (a) policies, (b) the ability to form policies, and (c) the trust the population has in policies.

To identify a *target* in this study, we have used Cullen and Reichborn-Kjennerud (2017) as a starting point. Cullen and Reichborn-Kjennerud (2017) rely on the PMESII domains, i.e. political (P), military (M), economic (E), social (S), informational (I) and infrastructure (I). We have attempted to be more specific in what these PMESII domains can entail, and the following four categories of *target* groups are identified: *government agencies/civil service* (covering political in PMESII domains), *the Armed Forces/military* (covering military in PMESII domains), *the population* (covering social in PMESII domains) and *business/infrastructure/natural resources* (covering infrastructure in PMESII domains).[2] For the purposes of this study, *government agencies* comprise both the political level and civil servants in ministries and other institutions of the central government. These targets encapsulate the public, private, civilian, and military aspects of a target group.

The parameter *method* can be described as the plan or procedure for action the threat actor will use to achieve its objective, for example by exploiting vulnerabilities in the target group. We seek to identify escalating levels of severity within the parameter method. The suggested parameter values are *influence*, *coercion*, and *damage*. *Influence* can be understood as the "ability to get others to act, think, or feel as one intends" (Banfield 2003, p. 3). A more aggressive method than influence is to exert pressure to achieve a concrete outcome. We refer to this as *coercion*. Coercion is "a bargaining strategy that states implement to compel their adversaries to alter their behavior" (Helal 2019, p. 4). This can involve threats to destabilise the adversary, or to get the adversary to do something it would otherwise not have done (Hodgson 2018, Giannopoulos *et al*. 2021). In other words, we concur with Helal (2019) that coercion can include, but is not limited to, the use of military force, or the threat of it.[3] The most aggressive *method* is *warfare* in which the conflict enters a phase of open use of military instruments. As this study looks at hybrid interference below the threshold for armed conflict, *warfare* is not included. Nevertheless, to cause harm to people and infrastructure, for example through terrorist attacks by proxy actors (non-state actors), can be a component of hybrid interference (Giannopoulos *et al*. 2021, p. 42). We refer to this method as *damage*, to address violent actions, which do not reach the level of armed conflict. This type of method will have the potential to cause physical harm[4] and destroy infrastructure or property.

To implement a method to achieve an objective, it is necessary to use an *instrument*. In the literature, several different instruments have been proposed as part of hybrid interference, both military and non-military instruments (Cullen and Reichborn-Kjennerud 2017, Karlsen 2019, Giannopoulos *et al*. 2021). For this study, we use the so-called MPECI framework utilised by Cullen and Reichborn-Kjennerud (2017) as a starting point because of its structured nature. MPECI stands for military (M), political (P), economic (E), civilian (C) and information and cyber-related (I). We separate civilian and military instruments, where

weapons used by civilians (as proxy actors of states), or military forces operating covertly, have been differentiated from *military* as an instrument. In this article, we refer to these instruments under the category *physical.* Such physical devices may be firearms, stabbing weapons, vehicles against a crowd, or improvised explosives. *Physical* devices may also be non-kinetic devices such as chemical, biological or radiological agents. For *political*, we rely on Hay (2002), who argues that politics is the arena for (overt) decision-making of the government. This can be can be diplomacy, negotiations or expressing support for extremist groups or protest movements. *Economic* instruments[5] can be foreign direct investments in the form of new establishments, mergers and acquisitions, portfolio investments, as well as loans and other financial support like aid, manipulation of import or export flows (e.g. trade barriers imposed as economic sanctions), manipulation or promotion of currency, and several other instruments (Waage *et al*. 2021, pp. 37–39). Illegal economic instruments such as corruption are included here, as scholars have identified strategic corruption as a potential national security threat (Bellows 2020, Giannopoulos *et al*. 2021, Waage *et al*. 2021a, 2021b). An example of strategic corruption is how Russia illegitimately finances far right parties such as Front National in France and AfD in Germany, argues Huss and Pozsgai-Alvarez (2022). We also include *judicial/law* instruments. *Judicial/law* instruments can for instance be the use of law to exploit weaknesses or ambiguities in rules and legislation or to overburden the judiciary system or use law for a strategic advantage (Kittrie 2016, Munoz Mosquera and Bachmann 2016, Dunlap 2017).

The parameter values *informational* and *cyber* instruments include a wide range of possibilities to obtain, manipulate or destroy information (Hodgson 2018). While we acknowledge that it is useful to see these tools in combination, for the purpose of this method, we have chosen to separate the two. The National Institute of Standards and Technology at the US Department of Commerce (NIST) defines "information environment" as "[t]he aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (NIST n.d.-b). Examples of such instruments could be the use of social media to spread misinformation or reinforce existing contradictions and conflicts in a population (Bergh 2019). A report by EUvsDisinfo gives several examples of how disinformation narratives can look like and debunks these narratives. One of these examples is when Russia in 2023 claimed that "Ukrainian refugees smuggle weapons and bring crime to Europe" (EUvsDisinfo 2023a, 2023b).

NIST defines cyberspace as "[a] global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (NIST n.d.-a). This can for instance include denial-of-service (DOS) attacks that block radio signals, also known as jamming (Pelechrinis *et al*. 2011). An example of this is Estonia's experience of a cyber-attack in 2007. Large amounts of spam overloading internet, making banks, journalists and government bodies unable to do their jobs are some examples of what happened in Estonia (BBC News 2017). Cyber instruments can be seen as part of the military, so although we acknowledge this overlap, for the purpose of this study we have decided to specifically identify *cyber* as a tool separate from the armed forces in the military. By *military*, we refer to armed forces within the traditional land, maritime and air domains (NATO 2022).

The last parameter, concealment, describes whether the threat actor chooses to perform *open* or *covert* actions. In Wigell's (2019, p. 263) definition, hybrid interference

is characterised as "more or less concealed". Based on this understanding, both open and covert forms of actions must be included in the morphological analysis. Cormac and Aldrich (2018, p. 478) write that "[t]he orthodox consensus assumes that states engage in covert action when they can plausibly deny sponsorship". Cormac *et al*. (2018, p. 478) continue to problematise the concept of "plausible deniability", referring rather to "non-acknowledged intervention as performance" (Cormac *et al*. 2018, p. 493). We rely on this understanding and refer to overt actions as those that are acknowledged by the actor. According to Stout (2017, p. 94), a covert action is "something done to produce an effect in the world while obscuring who is responsible for it", and it is not limited to lethal actions. For the purpose of this study, covert here then refers to both actions that are hidden (clandestine activities) and actions that have a hidden actor (or at least unacknowledged activities) (Cormac *et al*. 2018, Lamb and Tucker 2019).

Some parameters and parameter values have not been included in this analysis. While investigating the role of non-state actors is interesting, it has been regarded beyond the scope of this article. One parameter that could have been part of this study is the element of *legality* of the action conduction. A legal analysis could provide value for decision-makers for setting thresholds when developing counter-measures. This has however not been included because the analysis does not seek to go into the extensive detail needed to identify the legality of all actions within the solution space. Rather, the focus of the study is on the descriptive level.

Put together, the parameter values for threat actor, objective, method, instruments and concealment provide the morphological space summarised in Table 1.

Limitations

Some of the limitations of this research must be addressed. Our analysis is limited to actions under the threshold of armed conflict and conducted by state actors. Most of the limitations pertain to the use of morphological analysis as our method for conceptualising hybrid interference. As Johansen (2018) explains, common limitation with the morphological analysis are the use of judgmental evaluations throughout the process. As such, it must be highlighted that the method remains subjective. Certainly, there are weaknesses from the point of using only Europe, choosing parameter values and the exclusion of possible combinations. Buvarp (2023), in his updated version of the morphological analysis of influence operations on social media, also highlights that the selection

Table 1. Morphological space for hybrid interference parameter values.

Threat actor	Objective	Target	Method	Instrument	Concealment
State actor	Creating change in policy	Government agencies/ civil service	Damage	Military	Open
	Weakening agency	The Armed forces/military	Coercion	Physical	Covert
	Undermine trust in societal institutions	The population	Influence	Political	
		Business/infrastructure/ natural resources		Economic	
				Judicial/Law	
				Informational	
				Cyber	

of parameters has large consequences for the analysis. While this is true, the morphological analysis is a particularly transparent and reproducible method that allows readers to see exactly how the results were derived and therefore allows critics of our analysis to precisely identify possible weaknesses within the analysis and suggest changes to the morphological matrix (Ritchey 2013a, Johansen 2018).

Consistency analysis

The next step in the morphological methods is to conduct a consistency analysis and remove inconsistent combinations.[6] Inconsistent combinations mean pair-wise combinations that cannot co-occur. This is for instance the combination "open" with "damage", as our analysis is below the threshold of armed conflict. We include two types of inconsistencies: (i) logical and (ii) empirical (Ritchey 2013a). Logical inconsistency, or logical contradictions, occurs when the paired combination is contradictory, while empirical inconsistency occurs when the paired combination is considered not relevant or highly unlikely given the conditions of the analysed problem.

The first step in the synthesis phase is an analysis of internal consistency in the morphological space provided in Table 1. The consistency analysis is based on the question: "Can value X and value Y occur simultaneously?". The answer to this question can be based on both empirical data and logic but is not considering the likelihood of the action taking place. We avoid considering the likelihood to avoid a common issue in defence planning, which is "to confuse the unfamiliar with the improbable" (Schelling 1962, p. vii, Beadle 2016). In other words, the consistency analysis contributes to identifying the unfamiliar. It is not suitable to discuss every combination of parameter values in this study. The discussion is therefore limited to the combinations where the consistency analysis is not immediately evident. In this study, we award most attention to the combinations that have been removed (Table 2).

Removing combinations escalating to armed conflict

Several of the combinations in the matrix are removed based on the possibility of the combinations constituting actions that can cross the threshold of armed conflict. Among the combinations that have been removed are *military* instruments and *damage* as a method, *military* instruments against the *population*, and *military* instruments towards *business*, *infrastructure or natural resources*.

Damage, through either *cyber* or *physical* instruments, for instance, sabotage, are likely to be *covert* to avoid unintended escalation into armed conflict. We also remove the combination of *open* and *damage* from the consistency matrix. *Physical* instruments will most likely be used covertly, as the Skripal poisoning in Salisbury, United Kingdom (UK), is an example of (Wood and Henke 2018, Corera 2020). The combination of *open physical instruments* will become dangerously close to warfare argues Diesen (2018), and hence beyond the scope of this analysis.

Removing logical inconsistencies

Other combinations have been removed from the consistency matrix. For example, the definition of *damage* used in this study involves violent, non-military, incidents with the potential to cause direct physical harm. It will not be possible to *damage* with *political*,

Table 2. The consistency matrix, including the rejected combinations illustrated by a black "X" or black square.

	State actor	Create change in policy	Weakening agency	Undermine trust in societal institutions	Government agencies/civil service	The Armed forces/ military	The population	Business/ infrastructure/natural resources	Damage	Coercion	Influence	Military	Physical	Political	Economic	Judicial/ law	Informational	Cyber	Open	Covert
State actor																				
Forcing change in policy																				
Weakening agency																				
Undermine trust in societal institutions																				
Government agencies/civil service																				
The Armed forces/military		x																		
The population			x																	
Business/infrastructure/ natural resources		x																		
Damage																				
Coercion							x													
Influence																				
Military				x			x	x	x											
Physical											x									
Political				x					x											
Economic				x					x											
Judicial/law							x		x											
Informational									x											
Cyber																				
Open				x					x				x							
Covert														x						

judicial/law and *informational* instruments. These combinations are therefore removed. We also draw upon definitions by Hay (2002) to identify what *political* is, namely (overt) decision-making of the government. Based on that definition, it is logically inconsistent that *political* instruments of another state can be used *covertly*. This combination is therefore removed.

Removing empirical inconsistencies

Military and *political* instruments are removed from the consistency matrix, in combination with *undermine trust in societal institutions* because of the lack of direct link. We have not seen empirical examples of a direct link between the foreign state actors' use of these instruments and lower levels of trust in another state. It is also regarded as unlikely to *weaken agency of European states* by targeting *the population* directly. The people are not able to influence decision-makers' ability to make decisions directly. We admit that states operating with a higher frequency of direct democracy may be more vulnerable to this parameter value combination (Feld and Kirchgässner 2000). We nevertheless remove the combination of *population* and *weaken agency*.

Results

The results, or solution space as it is called in the morphological method, is the final step of the method. In this stage, the subcategories of combination with matching criteria are presented (Ritchey 2013a). In other words, the solution space illustrates the subsets of the concept of hybrid interference, based on the information put into the morphological model. As such, the concept has been operationalised. This operationalisation provides a more precise understanding of the components of hybrid interference. The following five categories are identified: international politics, coercive diplomacy, priming, covert coercion, and sabotage and assassinations. A typology of these categories is presented in Table 3 and a detailed list of subset activities for each category is made available in Appendix.

International politics

We introduced the concept of hybrid interference as something that seemingly covers all parts of society in which everything can be targeted. Yet, as Mälksoo (2018, p. 379) asks: "if everyone becomes connected and potentially targeted in the global 'hybrid war' zone, what is left of politics, and the delicate balancing act between security and democratic liberties?". We, therefore, group activities that by themselves cannot be covered by a term such as hybrid interference, in order to avoid the so-called "militant democracy whereby the very attempt to defend democracy might inadvertently damage it" (Müller 2016, p. 253 in Mälksoo 2018, p. 379). Berzina *et al*. (2020, p. 8) also highlight the need to distinguish international politics from foreign interference, arguing that "public diplomacy has an emphasis on open communication, it should not be confused with foreign interference".

The morphological analysis is a helpful instrument to identify this group of activities, which should be excluded from the hybrid interference term. One category of activities we seek to identify is the open use of influence, with economic, military, informational

Table 3. Overview of categories developed through the morphological analysis as well as the parameter values included in those categories.

		International politics	Coercive diplomacy	Priming	Covert coercion	Sabotage and assassinations
Actor	State actor					
Objective	Creating change in policy					
	Weakening agency					
	Undermine trust in societal institutions	X	X			
Target	Government agencies/ civil service					
	The Armed forces/ military					
	The population		X			
	Business/ infrastructure/ natural resources					
Method	Damage	X	X	X	X	
	Coercion	X		X		X
	Influence		X		X	X
Instrument	Military					X
	Physical	X	X	X		
	Political			X	X	X
	Economic					X
	Judicial/law					X
	Informational					X
	Cyber					
Concealment	Open			X	X	X
	Covert	X	X			

Note: "X" indicate parameter values that are excluded from the different categories.

political or judicial/law instruments. This is simply international politics. Possible examples of this type of action may include economic investments (Waage *et al*. 2021a, Waage and Lindgren n.d.), economic sanctions (Martin 1992, Walentek *et al*. 2021), military exercises expressing military ability through parades or general deterrence (Ametbek 2017, Bukkvoll *et al*. 2017, Sørensen 2017, BBC News 2019).

Activities within the international politics category can form part of longer-term plans of foreign actors, used to prepare for other more forceful or covert activities, similar to coercive diplomacy and priming. Foreign policy is often openly stated and can, of course, include obtaining power on the international stage. Gaining ownership over parts of the infrastructure can be legal, and even encouraged in an open economy and democratic society, and the risk involved must be acknowledged. Yet, these activities by themselves largely constitute legitimate actions any state engages in or encourages.

This is in line with what Wigell (2021, p. 63) has proposed, namely that "democracy and human rights promotion is overt and transparent, and therefore a form of legitimate public diplomacy […] In contrast with hybrid interference". Indeed, it is important to highlight that even though some activities are not wanted, they are a natural part of international affairs.

Identifying that these activities are not hybrid interference by themselves is important to separate the legitimate actions of international politics from the non-legitimate actions. This is imperative, as Mälksoo (2018, p. 276) writes, "because the inherent danger of

becoming a monster in the course of fighting monsters". In other words, it is important to make the distinction for the principle of not jeopardising the values we seek to protect, in our protective efforts.

Coercive diplomacy (blackmail strategy)

We use the category coercive diplomacy to cover similar instruments to that of international politics, but with coercion as a method rather than influence. This is to identify an increase in the intensity of activities. In this study, coercion as a method is identified as the exertion of pressure, for instance through threats, to change behaviour (Giannopoulos *et al*. 2021, pp. 40–41). While George (1994) presents both a defensive and offensive definition of coercive diplomacy in his work, we regard coercive diplomacy in this context through the offensive definition. The offensive definition of coercive diplomacy, or blackmail strategy as George (1994, p. 8) has termed it, is "offensive uses of coercive threats".

Coercion as a concept in international law is prohibited, for instance through the United Nations Declaration on Friendly Relations (UNGA 1970, p. 122) stating "Recalling the duty of States to refrain in their international relations from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of any State". Yet, as Farer (1985, p. 406) points out: " … if read literally, it would outlaw diplomacy", and indeed diplomacy is not outlawed. Farer (1985, p. 406) continues: "Threats, more or less subtle, have always been an important feature of the intercourse of states, even among allies". Limitation of export between the US and USSR during the Cold War, "whose legitimacy is rarely, if ever, questioned", is an example of this (Farer 1985, p. 406). Helal (2019, p. 5) echoes this, stating, "the practice of coercion is not limited to the use of force. States pressure their friends and coerce their foes using military, economic, political, and more recently, cyber instruments of statecraft". George (1994) highlights that the goal is to remain under the threshold of armed conflict to avoid the high military costs that an escalation would entail. This category of actions can include coercing government agents through threats with ultimatums, short deadlines, descriptions of possible escalation, to try to force politicians or civil servants and institutions involved in carrying out policies, to change policies.

There are several contemporary examples of this, and China's coercive diplomacy is on the rise in Scandinavia (Forsby and Sverdrup-Thygeson 2022, Waage *et al*. 2022). For instance, Sweden in 2020 was subjected to warnings about "the negative impact on China-Sweden cooperation and the Swedish businesses operating in China" after Swedish authorities chose to ban Huawei from the digital infrastructure (Forsby *et al*. 2022, p. 1). The Diplomatic isolation from China for those states with friendly relations with the Tibetan leader Dalai Lama has also been experienced by for instance Denmark (2009), Estonia (2011) and Lithuania (2013) (Forsby *et al*. 2022). Other scholars have also found links between limitations on trade and receiving Dalai Lama on an official visit (Fuchs and Klann 2013). These are examples of coercive diplomacy that can form part of hybrid interference.

Priming

After having identified what we regard as part of global affairs, on different levels of intensity, we now seek to identify the more troublesome categories of activities. The

combination of parameters of *covert*, *influence*, *political*, *economic*, *judicial/law* and *informational*, is what we can categorise as priming. The covert nature moves the activities away from acceptable and legitimate actions in international affairs, into an arena that challenges the established understanding of sovereignty and territorial integrity. The actions are like those of international politics, but the actor will typically use a third party, in order to appear disinterested, which can also give the impression of a broader base of support for its views than there is in reality.

Giannopoulos *et al*. (2021) and Gjørv *et al*. (2022) have also identified "priming" as a key part of hybrid interference. Priming, according to these authors, refers to the "long game effect" that can change perceptions in the population (Gjørv *et al*. 2022, p. 91). We argue that the activities identified in this category are a type of priming because these activities can manipulate states' strategic interests as they increase the dependency on an external (state) actor. This contributes to aligning the policies to the strategic interests of the foreign state actor, yet while remaining covert. Examples of what this can entail are influence operations in social media (Wither 2016, Applebaum *et al*. 2017, Bergh 2020), corruption of persons of interest (Goldberg 2018, Karlsen 2019, Ron and Singer 2020) and economic investments through other actors such as shell companies (Waage *et al*. 2021a).

An example of this type of hidden activity that may have long-term effects is the case of foreign ownership of islands in Finland (Ellehuus 2020). In September 2018, the Finnish security and intelligence services raided several islands, one of which was owned through shell companies by a Russian oligarch, named Pavel Melnikov. There were built Several piers, a landing spot for helicopters and satellite dishes on the island were built, which the newspaper *The Independent* described as having "enough housing to accommodate a small army" (Higgins 2018). The island could have been useful and important later, due to the strategic geographical location of the island (Higgins 2018, Ellehuus 2020). This illustrates how certain actions undertaken today can be for the strategic effect gained in the future.

Covert coercion

Like the distinction between international politics and coercive diplomacy, we here distinguish between priming and covert coercion. Basing his work on that of Nutter (2009), Wittmer (2013, p. 15) refers to covert coercion as including "a wide array of tasks such as asset development, political action, propaganda and disinformation, economic warfare, and paramilitary action just to name the main categories". While we have removed political action as part of covert activities, our approaches to covert coercion align. Covert coercive actions meddle with the established norms of territorial integrity and sovereignty beyond the priming category. We have chosen to distinguish covert coercion from priming, because of the intensified aggression these actions represent through the method of coercing over influencing.

An example of covert coercion is China's economic coercion against Lithuania through an export embargo, as a response to Lithuania opening a Taiwan "representative office" in Vilnius in November 2021. China was not open about its process (Blockmans 2021, Reynolds and Goodman 2022). Another example is presented by Hodos (2022), who explored how Russia supported Western political extremists and paramilitary groups, i.e. groups

that are willing to use violence, in countries such as Montenegro, Hungary, Czechia, Slovakia, Serbia and Bosnia Herzegovina. While the direct link between Russian intelligence and extremist groups lacks clear evidence, the possibility of it is an action that can be categorised as covert coercion. GPS jamming during the NATO military exercise Trident Juncture in 2018 (Westbrook 2019) and ransomware (Egloff 2020) can also be categorised as covert coercion.

Sabotage and assassinations

Some of the interference activities are characteristically different from the rest due to their potential to cause physical harm. These activities are categorised as "sabotage and assignations", and have greater hostile potential for people, property, and infrastructure. Within this category, we place the covert use of the cyber and physical instruments. Overt activities of such kind would cause much greater attention and possible unwanted escalation.

Examples of this may include sabotage of critical infrastructure and physical harm to persons of interests, through other actors. The damage on the Nord Stream gas lines in September 2022 was by both Swedish and Danish authorities categorised as deliberate sabotage (Connolly 2022). The Skripal poisoning in Salisbury, UK, is an example that illustrates that the capability to physically harm individuals exists (Wood *et al*. 2018, Corera 2020). The cyber-attacks in Estonia in 2007 in relation to the Bronze Soldier Crisis, is another relevant example of covert damage that makes sense to categorise within the sabotage category (Government 2020, Juurvee and Mattiisen 2020).

Discussion

Thus far, we have dissected the term hybrid interference by splitting the term into its different parts. Thereafter, we developed categories to illustrate commonalities in how the identified activities within each category may operate. While hybrid interference is a concept that addresses activities in combination, the concept addresses more than that. As Wigell (2019, p. 255) explains, hybrid interference "makes use of the liberal values that characterize western democracy, exploiting them as opportunities to drive wedges through democratic societies and undermine governability". Our operationalisation has illustrated the different possibilities that lie within the concept. We have illustrated some differences in severity between the categories and why international politics is distinguished from the rest.

Scholars critical of the "hybrid warfare" and "grey zone conflict" terms argue that these concepts should not be used because they "cause more harm than good and contribute to an increasingly dangerous distortion of the concepts of war, peace, and geopolitical competition" (Stoker *et al*. 2020, p. 2). We argue that it indeed is important to not to distort the concepts of war, peace and geopolitical competition, but simultaneously policy makers must manage to address multisector threats that can be harmful to democracy and national security. With the categories developed in this paper, we have addressed this potential for distortion by filtering out the category of "international politics".

We argue that it is the covertness and/or coercion and damage as a method that moves actions into the interference category. Hénin (2021), at the EU DisinfoLab, states

that "foreign interference is defined as activities going beyond routine diplomatic influence practiced by governments, that may take place in isolation or alongside espionage activities" (Bentzen and Service 2020, p. 3). Berzina and Soula. (2020) conceptualise interference as being with intent and lack of transparency. These arguments illustrate that despite our work to reconceptualise and operationalise the concept, our analysis aligns with that of other experts on the topic. Hybrid interference then becomes a combination of activities within the categories of coercive diplomacy (blackmail strategy), priming, covert coercion, and sabotage and assassinations. Activities within the category of international politics can be part of the activities taking place, but solely relying on actions within this category ought not to be categorised as hybrid interference.

Conclusion

Through the morphological analysis, we have operationalised the concept of hybrid interference and identified several avenues for interference activities and categorised these activities according to their characteristics. Our contribution is the development of a refined conceptual understanding of hybrid interference, with categories to identify the different characteristics. We argue that interference activities can be categorised as either coercive diplomacy, priming, covert coercion or sabotage and assassinations. The combination of interference activities within or across these categories is hybrid interference. The category of international politics has been filtered out of the hybrid interference concept, as its nature provides it with an acceptable place in international affairs. The analysis illustrates the many other forms of harm that can be caused by hybrid interference, despite avoiding direct open military operations. Future research could work to identify the legal and legitimate frames of the categories we have developed and investigate the extent to which our categories also are relevant to other parts of the world. This would be of value to move research on hybrid interference forward and for policymakers in their attempt to detect, deter and counter security threats in the twenty-first century.

Notes

1. In the original method, normative inconsistencies are also removed. We, however, have chosen to only use empirical evidence and logical arguments in this work, to avoid setting up normative blinders in our work.
2. More concrete targets, such as specific vital societal functions, can be included in similar but more detailed morphological analyses of hybrid interference.
3. The use of military force and the threat of using military force is prohibited by international law but the legal considerations are beyond the scope of this study.
4. We use damage to not be confused with the word "attack", which in international law specifically refers to "a particular category of military operations". Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions defines "attacks" as "acts of violence against the adversary, whether in offence or in defence" (Schmitt 2012, p. 285).
5. For a more extensive analysis of economic measures to harm national security, see Waage *et al*. (2021a, 2021b).
6. One way of conducting this analysis could be to do a cost-benefit analysis of undertaking actions. However, as our study is not looking into the budget or capabilities of a specific state as a threat actor, the economic reasoning approach has not been utilized for this study.

Acknowledgements

Earlier versions of this paper were presented at a seminar at the University of Oslo 2–6 May 2022 and the hybrid threat workshop at Nord University, 1–2 June 2022. We are grateful to Ketil Bonesmo, Professor Scott Gates, Associate Professor Stian Kjeksrud, Lea Bjørgul, Kristin Waage, Cassandra Granlund and the participants in the workshop and seminar for their useful feedback. All remaining inconsistencies remain our responsibility.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Norwegian Ministry of Defence.

ORCID

Julie Celine Bergaust http://orcid.org/0000-0003-4830-5631
Stig Rune Sellevåg http://orcid.org/0000-0002-2309-8464

References

Ametbek, D., 2017. *What is the necessity of military parades?* Ankara Center for Crisis and Policy Studies (ANKASAM). Available from: https://www.ankasam.org/what-is-the-necessity-of-military-parades/?lang=en [Accessed 6 Mar 2023].

Anna Vachudova, M., 2020. Ethnopopulism and democratic backsliding in Central Europe. *East European politics*, 36 (3), 318–340. doi:10.1080/21599165.2020.1787163.

Applebaum, A., *et al*., 2017. *"Make Germany great again" – Kremlin, alt-right and international influences in the 2017 German elections*. London: Institute for Strategic Dialogue (ISD). Available from: https://www.isdglobal.org/isd-publications/make-germany-great-again-kremlin-alt-right-and-international-influences-in-the-2017-german-elections/.

Banfield, E., 2003. *Political influence*. 1st ed. New York: Routledge.

BBC News, 2017. How a cyber attack transformed Estonia. *BBC News*, 27 Apr. Available from: https://www.bbc.com/news/39655415 [Accessed 28 Aug 2023].

BBC News, 2019. In pictures: China shows off military might at 70th anniversary parade. *BBC*, 1 Oct. Available from: https://www.bbc.com/news/world-asia-china-49891769 [Accessed 30 Sep 2021].

Beadle, A.W., 2016. *Å forske på Forsvaret i fremtiden – muligheter, begrensninger og kognitive fallgruver*. Kjeller Norwegian Defence Research Establishment, Report number 16/01810. Available from: https://www.ffi.no/publikasjoner/arkiv/a-forske-pa-forsvaret-i-fremtiden-muligheter-begrensninger-og-kognitive-fallgruver.

Bellows, A., 2020. *Defending against the geopolitical weaponization of corruption*. Carnegie Endowment for International Peace. Available from: http://www.jstor.org/stable/resrep24913.5 [Accessed 24 Aug 2023].

Bentzen, N. and Service, E.E.P.R., 2020. *Foreign interference in democracies: understanding the threat, and evolving responses*. European Parliament Briefing.

Bergh, A., 2019. *Social network centric warfare – understanding influence operations in social media*. Kjeller: Norwegian Defence Research Establishment, Report number 19/01194. Available from: https://www.ffi.no/en/publications-archive/social-network-centric-warfare-understanding-influence-operations-in-social-media.

Bergh, A., 2020. Understanding influence operations in social media – a cyber kill chain approach. *Journal of information warfare*, 19 (4), 110–131. Available from: https://www-jstor-org.ezproxy.uio.no/stable/27033648.

Bernal, A., *et al*., 2020. *Cognitive warfare: an attack on truth and thought*. NATO, John Hopkins University. Available from: https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf.

Berzina, K. and Soula, E., 2020. *Conceptualizing foreign interference in Europe*: the German Marshall Fund of the United States (GMF). Available from: https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf.

Blockmans, S., 2021. *Lithuania, China and EU lawfare to counter economic coercion – breaking bad?* Brussels: Centre for European Policy Studies, No 2021/20/December 2021. Available from: https://www.ceps.eu/ceps-publications/lithuania-china-and-eu-lawfare-to-counter-economic-coercion/.

Bukkvoll, T., *et al*., 2017. *10 år med Russisk forsvarsmodernisering*. Kjeller Norwegian Defence Research Establishment, Report number 17/16860. Available from: https://www.ffi.no/publikasjoner/arkiv/10-ar-med-russisk-forsvarsmodernisering.

Buvarp, P., 2023. The space of influence: developing a new method to conceptualise foreign influence in social media. *Journal of information warfare*, 22 (2), 31–51.

Buzan, B. and Hansen, L., 2009. *The evolution of international security studies*. Cambridge: Cambridge University Press.

Cambridge Dictionary, n.d. *interfere*.

Cantwell, D., 2017. Hybrid warfare: aggression and coercion in the gray zone | ASIL. *American society of international law*, 21 (14). Available from: https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone.

Carment, D., 2021. *War's future: the risks and rewards of grey-zone conflict and hybrid warfare*. Canadia Global Affairs Institute. Available from: https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare [Accessed 16 Sep 2021].

Connolly, K., 2022. Size of Nord Stream blasts equal to large amount of explosive, UN told. *The Guardian*, 30 Sep 2022. Available from: https://www.theguardian.com/business/2022/sep/30/nord-stream-blasts-size-equal-to-large-amount-of-explosive-un-told [Accessed 7 Nov 2022].

Corera, G., 2020. Salisbury poisoning: what did the attack mean for the UK and Russia? *BBC News*, 4 Mar. Available from: https://www.bbc.com/news/uk-51722301.

Cormac, R. and Aldrich, R.J., 2018. Grey is the new black: covert action and implausible deniability. *International affairs*, 94 (3), 477–494. doi:10.1093/ia/iiy067.

Cullen, P.J. and Reichborn-Kjennerud, E., 2017. *MCDC countering hybrid warfare project: understanding hybrid warfare. A multinational capability development campaign project*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Diesen, S., 2018. *Lavintensivt hybridangrep på Norge i en fremtidig konflikt*, FFI-rapport 18/00080.

Douglas, K.M., 2021. COVID-19 conspiracy theories. *Group processes & intergroup relations*, 24 (2), 270–275. doi:10.1177/1368430220982068.

Dunlap, C., 2017. *Lawfare 101 a primer*. Military review: Duke Law. Available from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=6434&context=faculty_scholarship.

Dyrendal, A. and Emberland, T., 2019. *Hva er konspirasjonsteorier*. Oslo: Universitetsforlaget.

The Economist Intelligence Unit, 2022a. *Democracy index 2022: frontline democracy and the battle for Ukraine*. London: The Economist.

The Economist Intelligence Unit, 2022b. *The world's most, and least, democratic countries in 2022*. The Economist. Available from: https://www.economist.com/graphic-detail/2023/02/01/the-worlds-most-and-least-democratic-countries-in-2022 [Accessed 14 Mar 2023].

Egloff, F.J., 2020. Public attribution of cyber intrusions. *Journal of cybersecurity*, 6 (1), tyaa012. doi:10.1093/cybsec/tyaa012.

Ellehuus, R., 2020. 'Strange Birds in the Archipelago: Finland's Legislation on Foreign Real Estate Investment', *CSIC.org*. Available from: https://www.csis.org/blogs/kremlin-playbook-spotlight/strange-birds-archipelago-finlands-legislation-foreign-real-estate.

EUvsDisinfo, 2023a. *Deny, deflect, distract, confuse. Repeat*. euvsdisinfo.eu. Available from: https://euvsdisinfo.eu/deny-deflect-distract-confuse-repeat/ [Accessed 28 Aug 2023].
EUvsDisinfo, 2023b. *Disinfo: Ukraninan refugees smuggle weapons and bring crime to Europe*. euvsdisinfo.eu. Available from: https://euvsdisinfo.eu/report/ukrainian-refugees-smuggle-weapons-and-bring-crime-to-europe [Accessed 28 Aug 2023].
Ewers-Peters, N.M., 2022. Positioning member states in EU-NATO security cooperation: towards a typology. *European security*, 1–20. doi:10.1080/09662839.2022.2076558.
Farer, T.J., 1985. Political and economic coercion in contemporary international law. *The American journal of international law*, 79, 405–413. Available from: https://www.jstor.org/stable/pdf/2201710.pdf.
Feld, L.P. and Kirchgässner, G., 2000. *Direct democracy, political culture, and the outcome of economic policy: a report on the Swiss experience*. Amsterdam.
Forsby, A.B. and Sverdrup-Thygeson, B., 2022. *China's coercive diplomacy: why it's on the rise and what it means for Scandinavia*. Norwegian Institute of International Affairs, 6. Available from: https://www.nupi.no/en/publications/cristin-pub/china-s-coercive-diplomacy-why-it-s-on-the-rise-and-what-it-means-for-scandinavia.
Freedom House, 2022. *Change in freedom score*. freedomhouse.org. Freedom House. Available from: https://freedomhouse.org/explore-the-map?type=fiw&year=2023&mapview=trend [Accessed 14 Mar 23].
Fuchs, A. and Klann, N.-H., 2013. Paying a visit: the Dalai Lama effect on international trade. *Journal of international economics*, 91 (1), 164–177.
George, A.L., 1994. Coercive diplomacy: definition and characteristics. *In*: A.L. George, *et al*., eds. *The limits of coercive diplomacy*, 7–11. 2nd ed. Boulder, CO: Westview Press.
George, A.L. and Bennett, A., 2005. *Case studies and theory development in the social sciences*. Cambridge: Belfer Center for Science and International Affairs, John F. Kennendy School of Government, Harvard University.
Giannopoulos, G., Smith, H., and Theocharidou, M., 2021. *The landscape of hybrid threats: a conceptual model*. EUR 30585 EN.
Gjørv, G.H., *et al*., 2022. De siviles rolle i sammensatt krigføring. *In*: G.F. Rongved and P.M. Norheim-Martinsen, eds. *Totalforsvaret i praksis*. Oslo: Gyldendal Forlag, 93–106.
Goldberg, F., 2018. Corruption and lobbying: conceptual differentiation and gray areas. *Crime, law and social change*, 70 (2), 197–215. Doi:10.1007/s10611-017-9727-x.
Government, Affairs, M.o.F., 2020. *Cyber operation against the Parliament (Storting)*.
Hadzhiev, B., 2020. Enablers of hybrid warfare: the Bulgarian case. *Journal of international studies*, 13 (1), 28–43.
Halas, M., 2022. NATO's sub-conventional deterrence: the case of Russian violations of the Estonian airspace. *Contemporary security policy*, 43 (2), 350–381. Doi:10.1080/13523260.2022.2028464.
Haugsgjerd, A. and Segaard, S.B. 2020. *Politisk tillit, lokaldemokrati og legitimitet. Kunnskapsstatus og utviklingstrekk*. Rapport 2020:6.
Hay, C., 2002. *Political analysis – a critical introduction. Political analysis*. New York: Palgrave.
Helal, M., 2019. *On coercion in international law*. New York University Journal of International Law and politics (JILP), Ohio State Public Law Working Paper.
Hénin, N., 2021. *Foreign election interferences: an overview of trends and challenges*. EU Disinfo Lab. Available from: https://www.disinfo.eu/publications/foreign-election-interferences-an-overview-of-trends-and-challenges/ [Accessed 20 May 22].
Higgins, A., 2018. Finnish soldiers find 'secret Russian military bases' after raiding mysterious island. *The Independent*, 1 Nov 2018. Available from: https://www.independent.co.uk/news/world/europe/finland-russia-military-bases-sakkiluoto-putin-dmitry-medvedev-police-a8612161.html [Accessed 3 Oct 2022].
Hodgson, Q.E., 2018. *Understanding and countering cyber coercion, NATO CCD Coe publications*. Tallinn: RAND Corporation.
Hodos, P.N., 2022. Playing to extremes: Russia's choices to support western political extremists and paramilitary groups. *International journal of intelligence and counterintelligence*, 1–23. doi:10.1080/08850607.2022.2109449.

Hoffman, F.G., 2009. *Hybrid threats: reconceptualizing the evolving character of modern conflict*. Institute for National Strategic Studies: National Defense University. Available from: https://www.files.ethz.ch/isn/98862/SF240.pdf.

Hoffman, F.G., 2010. 'Hybrid threats': neither omnipotent nor unbeatable. *Orbis*, 54 (3), 441–455.

Hoffman, F.G., 2014. On not-so-new warfare: political warfare vs hybrid threats. *War on the rocks*. Available from: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ [Accessed 16 Oct 2023]

Huss, O. and Pozsgai-Alvarez, J., 2022. *Strategic corruption as a threat to security and the new agenda for anti-corruption*. corruptionjusticeandlegitimacy.org. Available from: https://www.corruptionjusticeandlegitimacy.org/post/strategic-corruption-as-a-threat-to-security-and-the-new-agenda-for-anti-corruption [Accessed 28 Aug 2023].

Janičatová, S. and Mlejnková, P., 2021. *The ambiguity of hybrid warfare: a qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities*. London: Contemporary Security Policy.

Johansen, I., 2018. Scenario modelling with morphological analysis. *Technological forecasting & social change*, 126, 116–125.

Juurvee, I. and Arold, U., 2021. Psychological defence and cyber security: two integral parts of estonias comprehensive approach for countering hybrid threats. *ICONO 14*, 14 (19), 70–94. doi:10.7195/ri14.v19i1.1628.

Juurvee, I. and Mattiisen, M., 2020. *The bronze soldier crisis of 2007. Revisiting an early case of hybrid conflict*. Tallinn: Internatioanl Centre for Defence and Security (RKK, ICDS). Available from: https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf.

Karlsen, G.H., 2019. Divide and rule: ten lessons about Russian political influence activities in Europe. *Palgrave communications*, 5 (1), 19. doi:10.1057/s41599-019-0227-8.

Kittrie, O.F., 2016. *Lawfare: law as a weapon of war*. New York, NY: Oxford University Press.

Kristian Åtland, T.N. and Pedersen, T., 2022. Military muscle-flexing as interstate communication: Russian NOTAM warnings off the coast of Norway, 2015–2021. *Scandinavian journal of military studies*, 5, 63–78.

Lamb, C. and Tucker, D., 2019. *United States special operations forces*. New York Chichester, West Sussex: Columbia University Press.

Lipset, S., 1968. *Det politiske menneske*. Oslo: Gyldendal.

Martin, D.L.L., 1992. *Coercive cooperation: explaining multilateral economic sanctions*. Princeton, NJ: Princeton University Press.

Mälksoo, M., 2018. Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European security*, 27 (3), 374–392. doi:10.1080/09662839.2018.1497984.

Munoz Mosquera, A.B. and Bachmann, S.D., 2016. Lawfare in hybrid wars: the 21st century warfare. *Journal of international humanitarian legal studies*, 7 (1), 63–87.

Murphy, B., 2022. Decaying national security and the rise of imagined tribalism. *The RUSI journal*, 1–13. doi:10.1080/03071847.2022.2072763.

NATO, 2022. *NATO's approach to space*. nato.int. Available from: https://www.nato.int/cps/en/natohq/topics_175419.htm [Accessed 16 Nov 2022].

NIST, n.d.-a. *Cyberspace*. NIST: U.S. Department of Commerce. Available from: https://csrc.nist.gov/glossary/term/cyberspace [Accessed 3 Jan 1 2022].

NIST, n.d.-b. *Information environment*. NIST: U.S Department of Commerce. Available from: https://csrc.nist.gov/glossary/term/information_environment [Accessed 3 Jan 2022].

Nutter, J.J., 2009. *The CIA's black ops: covert action, foreign policy, and democracy*. Amherst, NY: Prometheus Books.

Palmer, D.A.R. 2015. *Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons*. Research paper No. 120. Available from: https://www.files.ethz.ch/isn/194718/rp_120.pdf.

Pelechrinis, K., Iliofotou, M., and Krishnamurthy, S.V., 2011. Denial of service attacks in wireless networks: the case of jammers. *Ieee communications surveys & tutorials*, 13 (2), 245–257. doi:10.1109/SURV.2011.041110.00022.

Ragin, C.C., 2005. *From fuzzy sets to crisp truth tables*. Department of Sociology, University of Arizona. Available from: http://compasss.org/wpseries/Ragin2004.pdf.

Reynolds, M. and Goodman, M.P., 2022. *China's economic coercion: lessons from Lithuania*. csis.org. Available from: https://www.csis.org/analysis/chinas-economic-coercion-lessons-lithuania [Accessed 10 Nov 2022].

Ritchey, T., 2013a. *General morphological analysis. A general method for non-quantified modelling*. Swedish Morphological Society. Available from: https://www.swemorph.com/pdf/gma.pdf [Accessed 2 Apr 2021].

Ritchey, T., 2013b. Wicked problems. Modelling social messes with morphological analysis. *Acta morphologica generalis*, 2, 1–7.

Rittel, H. and Webber, M., 1973. Dilemmas in a general theory of planning. *Policy sciences*, 4, 155–169.

Ron, A. and Singer, A.A., 2020. Democracy, corruption, and the ethics of business lobbying. *Interest groups & advocacy*, 9 (1), 38–56. doi:10.1057/s41309-019-00073-w.

Schelling, T., 1962. Forword. *In*: R. Wohlstetter, ed. *Pearl Harbor: warning and decision*. Stanford, CA: Stanford University Press, vii–xi.

Schmitt, Michael N. 2012. 'Attack' as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis and K. Ziolkowski, 283–94. NATO CCD COE Publications. https://ccdcoe.org/uploads/2019/03/CyCon_book_2012.pdf.

Shires, J., 2020. Damaging the opponent 'the new way' – understanding the tactics behind hack-and-leak operations. *Atlantisch perspectief*, 44 (4), 20–25. Available from: https://www.jstor.org/stable/48600566.

Sitter, N. and Bakke, E., 2019. *Democratic backsliding in the European Union*. Available from: https://www.duo.uio.no/bitstream/handle/10852/77401/2/Democratic%2BBacksliding%2Bin%2Bthe%2BEuropean%2BUnion%2B10%2BMay%2B2019.pdf.

Sørensen, C., 2017. Constraints on the soft power efforts of authoritarian states: the case of the 2015 military parade in Beijing. *Journal of current Chinese affairs*, 46 (2), 111–134. Available from: https://journals.sagepub.com/doi/pdf/10.1177186810261704600205.

Stoker, D. and Whiteside, C., 2020. Blurred lines: gray-zone conflict and hybrid war – two failures of American strategic thinking. *Naval war college review*, 73 (4), 1–37. Available from: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8092&context=nwc-review.

Stout, M., 2017. Covert action in the Age of social media. *Georgetown journal of international affairs*, 18 (2), 94–103. doi:10.1353/gia.2017.0024.

UNGA, 1970. *Declaration on principles of international law friendly relations and co-operation among states in accordance with the Charter of the United Nations*. Resolution 2625. Available from: https://digitallibrary.un.org/record/202170?ln=fr [Accessed 6 Mar 2023].

Waage, K., *et al*., 2021. *Økonomiske virkemidler for å oppnå strategiske mål – en oversikt*. Kjeller: Norwegian Defence Research Establishment, Eksternnotat 21/00140. Available from: https://publications.ffi.no/nb/item/asset/dspace:7080/21-00140.pdf.

Waage, K., *et al*., 2022. *Kinesisk økonomisk statshåndverk og implikasjoner for norsk sikkerhet*. Kjeller: Norwegian Defence Research Establishment, Report number 22/00422. Available from: https://www.ffi.no/publikasjoner/arkiv/kinesisk-okonomisk-statshandverk-og-implikasjoner-for-norsk-sikkerhet.

Waage, K., Kvalvik, S.N., and Lindgren, P.Y., 2021. *Utenlandske investeringer og andre økonomiske virkemidler – når truer de nasjonal sikkerhet?* Kjeller: Norwegian Defence Research Establishment, Report number 20/03149. Available from: https://www.ffi.no/publikasjoner/arkiv/utenlandske-investeringer-og-andre-okonomiske-virkemidler-nar-truer-de-nasjonal-sikkerhet.

Waage, K. and Lindgren, P.Y., n.d. Økonomisk statshåndverk og nasjonale sikkerhetsinteresser: hvordan kan Kina true Norge? *Article under production*.

Walentek, D., *et al*., 2021. Success of economic sanctions threats: coercion, information and commitment. *International interactions*, 47 (3), 417–448. doi:10.1080/03050629.2021.1860034.

Westbrook, T., 2019. The global positioning system and military jamming geographies of electronic warfare. *Journal of strategic security*, 12 (2), 1–16. Available from: https://www.jstor.org/stable/26696257.
Wigell, M., 2019. Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International affairs*, 95 (2), 255–275. doi:10.1093/ia/iiz018.
Wigell, M., 2021. Democratic deterrence: how to dissuade hybrid interference. *The Washington quarterly*, 44 (1), 49–67. doi:10.1080/0163660X.2021.1893027.
Wither, J.K., 2016. Making sense of hybrid warfare. *Connections*, 15 (2), 73–87. Available from: http://www.jstor.org/stable/26326441.
Wittmer, L.A., 2013. *Covert coercion: a formal analysis of unconventional warfare as an interstate coercive policy option*. Thesis. Monterey, CA: Naval Postgraduate School. Available from: http://hdl.handle.net/10945/34764.
Wood, S., and Henke, O., 2018. The salisbury poisoning case and German–Russian relations: ambiguity and ambivalence. *The political quarterly*, 89, 702–708.
Zwicky, F., 1969. *Discovery, invention, research through the morphological approach*. Toronto, Ontario, Canada: Macmillan.

Appendix

International politics

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Create change in policy	Government agencies/civil service	Influence	Military	Open
State actor	Create change in policy	Government agencies/civil service	Influence	Political	Open
State actor	Create change in policy	Government agencies/civil service	Influence	Economic	Open
State actor	Create change in policy	Government agencies/civil service	Influence	Judicial/law	Open
State actor	Create change in policy	Government agencies/civil service	Influence	Informational	Open
State actor	Create change in policy	Government agencies/civil service	Influence	Cyber	Open
State actor	Create change in policy	The population	Influence	Political	Open
State actor	Create change in policy	The population	Influence	Economic	Open
State actor	Create change in policy	The population	Influence	Informational	Open
State actor	Create change in policy	The population	Influence	Cyber	Open
State actor	Weakening agency	Government agencies/civil service	Influence	Military	Open
State actor	Weakening agency	Government agencies/civil service	Influence	Political	Open
State actor	Weakening agency	Government agencies/civil service	Influence	Economic	Open
State actor	Weakening agency	Government agencies/civil service	Influence	Judicial/law	Open
State actor	Weakening agency	Government agencies/civil service	Influence	Informational	Open
State actor	Weakening agency	Government agencies/civil service	Influence	Cyber	Open
State actor	Weakening agency	The Armed forces/military	Influence	Military	Open
State actor	Weakening agency	The Armed forces/military	Influence	Political	Open
State actor	Weakening agency	The Armed forces/military	Influence	Economic	Open
State actor	Weakening agency	The Armed forces/military	Influence	Judicial/law	Open
State actor	Weakening agency	The Armed forces/military	Influence	Informational	Open
State actor	Weakening agency	The Armed forces/military	Influence	Cyber	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Influence	Political	Open
State actor	Weakening agency		Influence	Economic	Open

(*Continued*)

Continued.

Threat actor	Objective	Target	Method	Tool	Concealment
		Business/infrastructure/natural resources			
State actor	Weakening agency	Business/infrastructure/natural resources	Influence	Judicial/law	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Influence	Informational	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Influence	Cyber	Open

Coercive diplomacy

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Create change in policy	Government agencies/civil service	Coercion	Military	Open
State actor	Create change in policy	Government agencies/civil service	Coercion	Political	Open
State actor	Create change in policy	Government agencies/civil service	Coercion	Economic	Open
State actor	Create change in policy	Government agencies/civil service	Coercion	Judicial/law	Open
State actor	Create change in policy	Government agencies/civil service	Coercion	Informational	Open
State actor	Create change in policy	Government agencies/civil service	Coercion	Cyber	Open
State actor	Weakening agency	Government agencies/civil service	Coercion	Military	Open
State actor	Weakening agency	Government agencies/civil service	Coercion	Political	Open
State actor	Weakening agency	Government agencies/civil service	Coercion	Economic	Open
State actor	Weakening agency	Government agencies/civil service	Coercion	Judicial/law	Open
State actor	Weakening agency	Government agencies/civil service	Coercion	Informational	Open
State actor	Weakening agency	Government agencies/civil service	Coercion	Cyber	Open
State actor	Weakening agency	The Armed forces/military	Coercion	Military	Open
State actor	Weakening agency	The Armed forces/military	Coercion	Political	Open
State actor	Weakening agency	The Armed forces/military	Coercion	Economic	Open
State actor	Weakening agency	The Armed forces/military	Coercion	Judicial/law	Open
State actor	Weakening agency	The Armed forces/military	Coercion	Informational	Open
State actor	Weakening agency	The Armed forces/military	Coercion	Cyber	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Coercion	Political	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Coercion	Economic	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Coercion	Judicial/law	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Coercion	Informational	Open
State actor	Weakening agency	Business/infrastructure/natural resources	Coercion	Cyber	Open

Priming

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Create change in policy	Government agencies/ civil service	Influence	Military	Covert
State actor	Create change in policy	Government agencies/ civil service	Influence	Economic	Covert
State actor	Create change in policy	Government agencies/ civil service	Influence	Judicial/law	Covert
State actor	Create change in policy	Government agencies/ civil service	Influence	Informational	Covert
State actor	Create change in policy	Government agencies/ civil service	Influence	Cyber	Covert
State actor	Create change in policy	The population	Influence	Economic	Covert
State actor	Create change in policy	The population	Influence	Informational	Covert
State actor	Create change in policy	The population	Influence	Cyber	Covert
State actor	Weakening agency	Government agencies/ civil service	Influence	Military	Covert
State actor	Weakening agency	Government agencies/ civil service	Influence	Economic	Covert
State actor	Weakening agency	Government agencies/ civil service	Influence	Judicial/law	Covert
State actor	Weakening agency	Government agencies/ civil service	Influence	Informational	Covert
State actor	Weakening agency	Government agencies/ civil service	Influence	Cyber	Covert
State actor	Weakening agency	The Armed forces/military	Influence	Military	Covert
State actor	Weakening agency	The Armed forces/military	Influence	Economic	Covert
State actor	Weakening agency	The Armed forces/military	Influence	Judicial/law	Covert
State actor	Weakening agency	The Armed forces/military	Influence	Informational	Covert
State actor	Weakening agency	The Armed forces/military	Influence	Cyber	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Influence	Economic	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Influence	Judicial/law	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Influence	Informational	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Influence	Cyber	Covert
State actor	Undermine trust in societal institutions	Government agencies/ civil service	Influence	Economic	Covert
State actor	Undermine trust in societal institutions	Government agencies/ civil service	Influence	Judicial/law	Covert
State actor	Undermine trust in societal institutions	Government agencies/ civil service	Influence	Informational	Covert
State actor	Undermine trust in societal institutions	Government agencies/ civil service	Influence	Cyber	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Influence	Economic	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Influence	Judicial/law	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Influence	Informational	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Influence	Cyber	Covert
State actor	Undermine trust in societal institutions	The population	Influence	Economic	Covert
State actor	Undermine trust in societal institutions	The population	Influence	Informational	Covert
State actor	Undermine trust in societal institutions	The population	Influence	Cyber	Covert
State actor			Influence	Economic	Covert

(*Continued*)

Continued.

Threat actor	Objective	Target	Method	Tool	Concealment
	Undermine trust in societal institutions	Business/infrastructure/ natural resources			
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Influence	Judicial/law	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Influence	Informational	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Influence	Cyber	Covert

Covert coercion

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Create change in policy	Government agencies/civil service	Coercion	Military	Covert
State actor	Create change in policy	Government agencies/civil service	Coercion	Physical	Covert
State actor	Create change in policy	Government agencies/civil service	Coercion	Economic	Covert
State actor	Create change in policy	Government agencies/civil service	Coercion	Judicial/law	Covert
State actor	Create change in policy	Government agencies/civil service	Coercion	Informational	Covert
State actor	Create change in policy	Government agencies/civil service	Coercion	Cyber	Covert
State actor	Weakening agency	Government agencies/civil service	Coercion	Military	Covert
State actor	Weakening agency	Government agencies/civil service	Coercion	Physical	Covert
State actor	Weakening agency	Government agencies/civil service	Coercion	Economic	Covert
State actor	Weakening agency	Government agencies/civil service	Coercion	Judicial/law	Covert
State actor	Weakening agency	Government agencies/civil service	Coercion	Informational	Covert
State actor	Weakening agency	Government agencies/civil service	Coercion	Cyber	Covert
State actor	Weakening agency	The Armed forces/military	Coercion	Military	Covert
State actor	Weakening agency	The Armed forces/military	Coercion	Physical	Covert
State actor	Weakening agency	The Armed forces/military	Coercion	Economic	Covert
State actor	Weakening agency	The Armed forces/military	Coercion	Judicial/law	Covert
State actor	Weakening agency	The Armed forces/military	Coercion	Informational	Covert
State actor	Weakening agency	The Armed forces/military	Coercion	Cyber	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Coercion	Physical	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Coercion	Economic	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Coercion	Judicial/law	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Coercion	Informational	Covert
State actor	Weakening agency	Business/infrastructure/ natural resources	Coercion	Cyber	Covert
State actor	Undermine trust in societal institutions	Government agencies/civil service	Coercion	Physical	Covert
State actor	Undermine trust in societal institutions	Government agencies/civil service	Coercion	Economic	Covert

(*Continued*)

Continued.

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Undermine trust in societal institutions	Government agencies/civil service	Coercion	Judicial/law	Covert
State actor	Undermine trust in societal institutions	Government agencies/civil service	Coercion	Informational	Covert
State actor	Undermine trust in societal institutions	Government agencies/civil service	Coercion	Cyber	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Coercion	Physical	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Coercion	Economic	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Coercion	Judicial/law	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Coercion	Informational	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Coercion	Cyber	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Coercion	Physical	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Coercion	Economic	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Coercion	Judicial/law	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Coercion	Informational	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/ natural resources	Coercion	Cyber	Covert

Sabotage and assassinations

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Create change in policy	Government agencies/civil service	Damage	Physical	Covert
State actor	Create change in policy	Government agencies/civil service	Damage	Cyber	Covert
State actor	Create change in policy	The population	Damage	Physical	Covert
State actor	Create change in policy	The population	Damage	Cyber	Covert
State actor	Weakening agency	Government agencies/civil service	Damage	Physical	Covert
State actor	Weakening agency	Government agencies/civil service	Damage	Cyber	Covert
State actor	Weakening agency	The Armed forces/military	Damage	Physical	Covert
State actor	Weakening agency	The Armed forces/military	Damage	Cyber	Covert
State actor	Weakening agency	Business/infrastructure/natural resources	Damage	Physical	Covert
State actor	Weakening agency	Business/infrastructure/natural resources	Damage	Cyber	Covert
State actor	Undermine trust in societal institutions	Government agencies/civil service	Damage	Physical	Covert
State actor	Undermine trust in societal institutions	Government agencies/civil service	Damage	Cyber	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Damage	Physical	Covert
State actor	Undermine trust in societal institutions	The Armed forces/military	Damage	Cyber	Covert
State actor	Undermine trust in societal institutions	The population	Damage	Physical	Covert

(*Continued*)

Continued.

Threat actor	Objective	Target	Method	Tool	Concealment
State actor	Undermine trust in societal institutions	The population	Damage	Cyber	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/natural resources	Damage	Physical	Covert
State actor	Undermine trust in societal institutions	Business/infrastructure/natural resources	Damage	Cyber	Covert