

This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Tikanmäki, I. & Ruoslahti, H. (2022) How are Hybrid Terms Discussed in the Recent Scholarly Literature? In Thaddeus Eze, Nabeel Khan and Cyril Onwubiko (Eds.) Proceedings of the 21st European Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited, 296-304.

doi: 10.34190/eccws.21.1.457

Available at: <https://doi.org/10.34190/eccws.21.1.457>

[CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)

How are Hybrid Terms Discussed in the Recent Scholarly Literature?

Ilkka Tikanmäki^{1, 21} and Harri Ruoslahti¹²

¹Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland

²Department of Warfare, National Defence University, Helsinki, Finland

Ilkka.Tikanmaki@laurea.fi

Harri.Ruoslahti@laurea.fi

Abstract: Hybrid threats range from cyber-attacks on critical systems to disruption of critical services (such as energy and financial services), influencing public confidence, and polarization within society. Awareness, resilience, and response to threats are central to countering hybrid threats. Hybrid warfare is not a new phenomenon, it has existed throughout the history of warfare, however, hybrid threat and hybrid warfare were re-defined as the western concept, as discussed in this paper, in 2014. Securing vital functions of society, i.e., managing overall security includes preparing for threats, and managing and recovering from disruptions and emergencies. Energy policy, which relies on cross-border energy transmission infrastructures (e.g., Russian gas line imports to Europe), can be a tool to influence foreign policy (Geo-economics). Trolls and cyber weapons can be used to impact information and elections, and their activity are based on supranational Information Technology (IT) infrastructure. The vital functions of society are prime targets for political, economic, and military pressure from external actors. Hybrid warfare deliberately blurs the boundaries between peacetime and wartime, which makes it difficult for targeted organizations and countries to plan appropriate and timely countermeasures. The threat of hybrid disruptions can be addressed with resilience. Multifaceted hybrid threats require planning and testing one's defensive possibilities, so that the various actors of society will be able to respond to possible hybrid attacks and commit all areas of society for an effective defence. Identifying and understanding hybrid warfare is challenging. Situation awareness is a prerequisite, so societies and their organization can meet these challenges

Keywords: hybrid threats, hybrid influence, hybrid interference, hybrid warfare, hybrid operations

1. Introduction


Hybrid threat and hybrid warfare were re-defined as western concepts in 2014 when Russia occupied the Crimea peninsula and started military actions in Eastern Ukraine by using so-called "green men", deputy warriors (rebels), cyber-attacks and information warfare. Russia achieved its political goals without using its military power (Raitasalo 2019). Raitasalo (2019) notes that hybrid warfare contains elements of cyber warfare and information warfare. He envisions it as a necessary conceptual tool for Western nations, who have been lulled in believing that international relations had entered a new era of co-operation after the end of the Cold War, to plan and prepare to defend against hybrid threats. Finland, for example, published the first Strategy for securing the vital functions of society to guide Finnish authorities, businesses, and organizations design, prepare, and practice long-term responses to a wide range of possible security threats (Finnish Government 2003). Securing vital functions of society (i.e., managing overall security) includes preparing for threats, and managing and recovering from possible disruptions and emergencies (Terminology Centre 2017). Critical functions in society include leadership, international and European Union (EU) action, defence capabilities, internal security, economy, security of infrastructure and supply, capabilities of and services for the population, and mental resilience (Terminology Centre 2017).

This study is organized as follows. Section 1 presents the content of the study and outlines the case study method used. Section 2 summarizes hybrid threats, influence, interference, warfare, and operations. The findings are discussed and concluded in Section 3. The study is a literature study, and the research question of this study is "How are hybrid terms discussed in recent scholarly literature?"

1.1 Methods

The study was conducted as a qualitative study and the research method is descriptive. The results of qualitative research are based on the researcher's reasoning (Huttunen & Metteri 2008). The research problem is discussed in the constructive research approach. According to Yin (2009), there are six sources for case studies: documentation, archival records, interviews, direct observation, and participation in observing and physical

¹  <https://orcid.org/0000-0001-8950-5221>

²  <https://orcid.org/0000-0001-9726-7956>

objects. It is recommended that several sources of evidence be used in the case study. The research data was collected from scientific reports, collected articles and literary reviews.

2. Hybrid terms in recent scholarly literature

This chapter explains hybrid terms, which in the context of this study are hybrid threats, hybrid influencing, hybrid interference, hybrid warfare and hybrid operations.

2.1 Hybrid threats

A hybrid threat is the simultaneous and adaptive use of an embedded combination of (1) political, military, economic, social, and media, and (2) traditional, irregular, terrorism, and disruptive/criminal conflict methods (GAO 2010). Hoffman (2007, p. 8) argues that hybrid threats are “Threats that incorporate a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both states and a variety of non-state actors”.

Hybrid threats range from cyber-attacks on critical systems to disruptions of critical services (e.g. energy and financial services), which can influence public confidence, and even create polarization within society. Threats to critical vulnerabilities seek to hamper effective decision-making (European Union 2018). One defining characteristic is the continuous utilization of identifiable asymmetries, both during a non-violent phase and in actual war. Asymmetric warfare refers to the usage of Special Forces, precision bombs and missiles, electronic warfare, guerrilla warfare, terrorist attacks, and the utilization of biological and chemical weapons (Mack 1975; Arreguín-Toft 2001). Asymmetries are utilized as a combination of surprise, abuse, and deception (Cederberg & Eronen 2015).

According to key efforts to combat against hybrid threats on the EU level are awareness, resilience, and response. Combined, these efforts can improve abilities to detect and understand adverse actions at early stages and help improve the sustainability of critical infrastructure, societies, and institutions. These above actions are essential in improving the abilities of the EU to withstand and recover from attacks. Action by EU Member States and closer cooperation between them, and with partner countries and NATO are needed to combat hybrid threats (European Union 2018).

2.2 Hybrid influencing

The Finnish Institute of International Affairs (FIIA) divides hybrid influence into geo-economics, information, and electoral impact; Energy policy, which relies on cross-border energy transmission infrastructure, can be used as an instrument to influence foreign policy (geo-economics); for example Russian gas imports to Ukraine and Europe. Trolls and cyber weapons can be used for information and electoral impacts that are based on a supranational IT infrastructure. (FIIA 2018.) The Security Strategy for Society defines hybrid engagement as an activity that pursues its own goals through a variety of complementary means and by exploiting the weaknesses of the target. Means of hybrid influence can be economic, political, or military, and can be used simultaneously or sequentially with technology and social media (Security Committee 2017).

Puistola (2018) presents the operation line of the hybrid influencing (Figure 1) on Diplomatic, Informational, Military and Economic (DIME) levels in three phases of pressure.

As shown in Figure 1, the operation line in the “New normal” -stage may start with pressure (1), which is followed by reconnaissance and recruitment (2), denigration (3), troop deployment, exercises, acquisition of strategic areas (4), pressure (5), and finally disruptions in the energy market and cyber-attacks (6). In the “Growing tensions” phase, activities become followed by import and export bans (7), territorial violations, cyber-attacks, acts of terrorism (8), false reporting, suppression of international aid, agitation (9), and invitations to negotiate (10). The “Exceptional conditions” stage could continue with the use of special forces (11), use of conventional armed forces (12), crushing of defender morale (13), and compelling peace (14). Sub-goals 1-4 aim at the final goal, where the target country makes military, political and economic national and international decisions in the interests of the influencer. (Puistola 2018.)

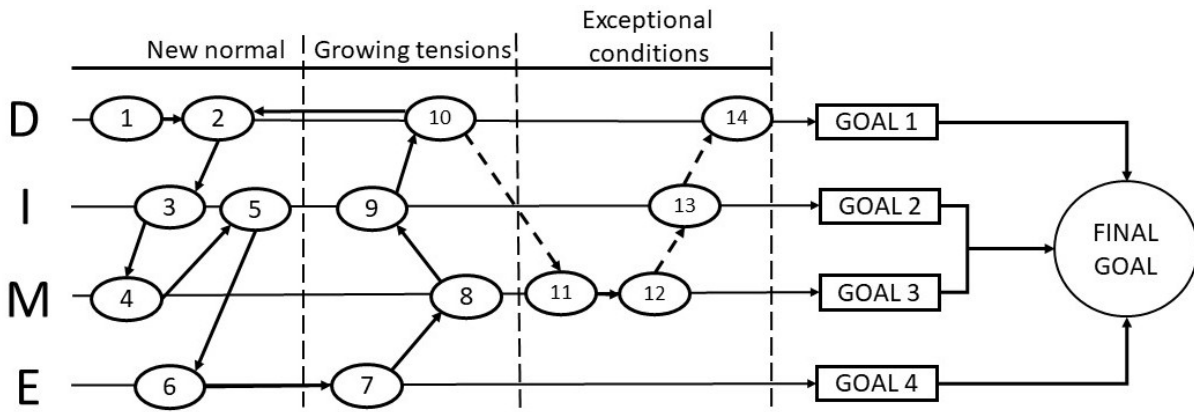


Figure 1: Operation line of the hybrid influencing (Adapted from Puistola, 2018).

Mäkelä (2018, p. 13) describes hybrid action as "a systematic activity in which a state or non-state actor can simultaneously utilize various military means or, for example, economic or technological pressure, as well as information operations and social media." In conclusion, Mäkelä concludes that often the aim is to keep the hybrid effect at a level where escalation into open conflict does not occur; to apply effects in ways that are disputable. Puistola (2018) sees information influence as a strategic deception in which the subject's perception of reality is obscured to achieve the attacker's strategic goals.

Social media can be a powerful contributor in shaping civic opinion. As reported by Puistola (2018) the means used for strategic deception are 1) deception and prohibition; 2) hiding of final goals; 3) maintaining the legality facade; 4) military defiance and threats, and 5) global input of one's narrative through various mediums. Tiilikainen (2020) states that hybrid influence is characterized by the use of shadow regions: a threat can come from just somewhere you cannot expect. Therefore, the Finnish model, combining different administrative sectors, is a policy that could be used in the wider world.

Hybrid influence, as reported by the Institute for International Affairs (2018), means synchronized use of multiple ways of harassment, aimed at generating deep dividing lines, within the societies of targeted countries, by leveraging non-military techniques. An actor seeking to influence will want to disrupt the political process in the target country so that the target country paralyzes its decision-making ability itself. Influencing can be sabotaged, seeking to disintegrate communities, and emphasizing its aggressive nature. (FIIA 2018.) Hybrid interference may include the elements presented in Table 1.

Table 1: Elements of hybrid interference (FIIA 2018)

Concept	Description
Hybrid influence	Synchronized harassment aimed at generating deep dividing lines within the societies of the target countries by leveraging non-military techniques, the aspirant wants to disrupt the political process in the target country so that the target country itself paralyzes its decision-making ability.
Elements of hybrid interference	cyber operations spreading false news dissemination of propaganda financing political extremism influencing key institutions of democracy (e.g., elections and governance) control of critical infrastructure providing financial incentives
Key efforts to counter hybrid disruptions	The threat of hybrid disruption can be addressed with resilience.

Multifaceted hybrid threats require planning of defenses to respond to hybrid threats by committing all areas of society to be alert and defend against all threats. Comprehensive (hybrid) defense requires patiently building national capabilities. In the short term, deficiencies in hybrid defense can be reduced by leveraging allied capabilities and performance. (Cederberg & Eronen 2015; Lalu & Puistola 2015) Cederberg and Eronen see hybrid warfare as a concept that the West is trying to classify based on Ukrainian events. Hybrid warfare can be

long lasting because quick victory over an opponent is not necessary, also the active and passive stages of the conflict can vary. (Cederberg & Eronen 2015.)

The vital functions of society are the prime targets of political, economic, and military pressure from an external actor. The threat of hybrid disruption can be addressed with resilience. Resilience refers to the ability of society to resist, withstand and recover quickly from malfunctions (FIIA 2018). According to de Bruijne et al. (2010, p. 9), “resilience refers to the ability of a social system (such as an organization, city, or society) to proactively adapt to and recover from disorders that it considers to be beyond normal and expected disorders.”

2.3 Hybrid warfare

Gärdestrom (2018, p. 2) states that “hybrid warfare is the combination of instruments and means of influence to subvert states, institutions, and societies”. An article by Hyytiäinen (2018) describes a model for hybrid action and hybrid warfare that can be used in other potential security situations and can be used as a tool for preparedness. Table 2 shows the components of hybrid warfare as presented by Hyytiäinen and the Munich Security Conference (2015), which for the most part are very similar. The main difference is that Hyytiäinen also includes infrastructure and energy as concepts of hybrid warfare.

Table 2: Hybrid warfare concepts comparison. (Munich Security Conference 2015; Hyytiäinen 2018)

Munich Security Conference (2015)	Hyytiäinen (2018)
Special forces	Special Forces
Irregular forces	Non-State Forces (Rebels)
Support of local unrest	Social harmony
Information warfare / propaganda	Information influence and propaganda
Diplomacy	Diplomacy
Cyberattacks	Cyberattack
Economic warfare	Economic Sanctions
Regular military forces	Military Action
	Infrastructure and energy

The model of Hyytiäinen is based on the hybrid warfare model presented by NATO, with infrastructure and energy added. The hybrid warfare model of Hyytiäinen does not include extensive military influence: it describes the non-military components of hybrid warfare and the supporting military activities. (Hyytiäinen 2018.) The Munich Security Conference (2015) hybrid warfare model corresponds to the NATO model. Infrastructure and energy are integral functions of society, and as such justified as additional components. Hybrid warfare blends conventional and irregular warfare throughout the conflict. Figure 2 shows an example of approaches that could be included in hybrid warfare, which combines elements of irregular pressure and conventional warfare to create pressure without conventional warfare.

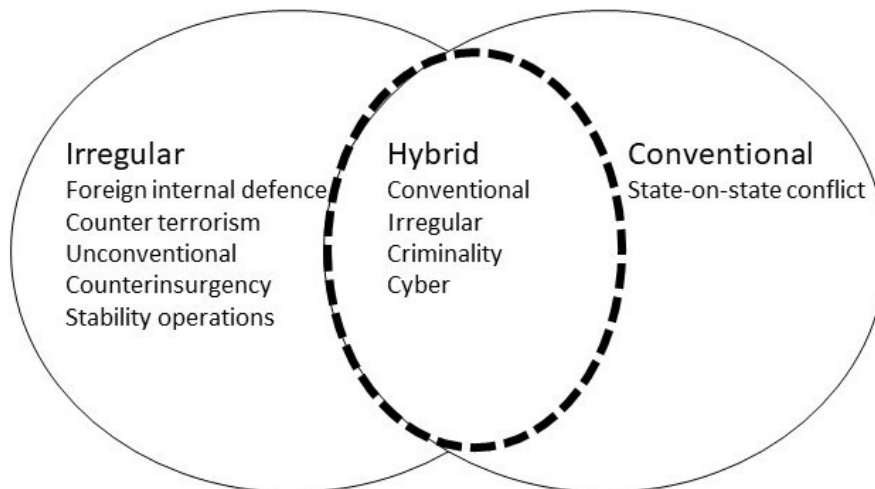


Figure 2: The hybrid warfare concept (Source: GAO 2010)

As seen in Figure 2, conventional warfare is a form of warfare between states that uses direct military confrontation to defeat an opponent's armed forces, destroy an opponent's warfare capacity, or conquer or maintain an area to force a change in an opponent's government or policy. "Conventional warfare can also be called "traditional" warfare". Irregular warfare, in turn, is a violent struggle between state and non-state actors to gain legitimacy and influence over the populations concerned. As stated by the US Air Force "Hybrid warfare is more powerful and complex than irregular warfare due to increased pace, complexity, diversity, and broader orchestration across national borders". Hybrid warfare can be described as conflicts that carry either state and/or interstate threats that use multiple forms of warfare, including conventional abilities, irregular tactics, and criminal disruption. (GAO 2010, pp. 16-18.)

Hybrid warfare is primarily strategic, but it also has an impact on the operational and tactical levels. Hybrid warfare can begin long before armed actions begin and can even offer the opportunity to win a war despite its defeat. Hybrid warfare has existed throughout the history of war and thus, is not a new phenomenon. The invasion of disguised Russian soldiers ("green men") in the Crimea, with Russia denying its involvement in the invasion, introduced hybrid as a concept to the broad public. (Hybrid CoE 2019)

The ultimate purpose of hybrid warfare is to achieve a set of goals without fighting or with little use of force. Thus, in hybrid warfare, it is impossible to say when battles or violence takes place, as can be identified in the classic form of war. Hybrid warfare blurs the line between traditional Western thinking of peace and civilian activities, and military operations. The blurring of boundaries is achieved by combining both violent military actions and non-violent means, without crossing the threshold of war (Cederberg & Eronen 2015). Open democratic societies are particularly prone to hybrid warfare. Hybrid warfare uses strategic domains and sources of power: politics, diplomacy, intelligence, information, defense forces (including military actions), economics, financial elements, technology, culture, legal, psychology, morality, and other means of influence. Hybrid warfare also involves the use of force (Hybrid CoE 2019).

After 2014, the term hybrid threat was intended to refer to hidden vulnerabilities in Western countries that could be exploited by potential adversaries. While projecting your own vulnerabilities into an opponent's means of selection, the Western world today speaks of hybrid warfare. Raitasalo's (2019) conclusion is that hybrid warfare is a Western concept that seeks to conceptualize and understand the surprise of traditional Russian superpower policies in the West.

2.4 Hybrid operations

In the first phase of typical hybrid operations, the weaknesses of the target country (political, economic, social, infrastructure) are explored. The second phase is to attack the target country's administration and seize critical military and civilian targets. In the third phase, the stabilization phase, an apparent government is formed in the conquered region (Järvenpää 2017). According to Chekinov and Bogdanov (2013) new generation (e.g. hybrid or information) operations begin with a months-long non-military campaign against the target country. There are several ways to pressure the target, such as information, moral, psychological, ideological, diplomatic, economic, etc. Propaganda aims to influence the population, armed forces, and administration of the target country. There are provocations, insecurities, and terrorist acts in the target country. Prior to an armed conflict, critical objects are identified and paralyzed by armed force. Following the operation, military force invades the target country, isolating key targets and stopping potential resistance (Chekinov & Bogdanov 2013).

The structure of the hybrid operation consists of three main phases of pressure, where the aggressor uses multiple means of hybrid action against various functions of the targeted state and its society to achieve desired strategic goals. Sub-goals for hybrid operations are 1) Creating a threatening diplomatic climate; 2) Increasing distrust of government leadership; 3) Increasing the ambiguity of the situation picture, and 4) Increasing distrust of services and the functioning of critical infrastructure. The final goal is that the policies of Finland and the Baltic Sea states favour the policies of the influencing state. Following Table 3 describes the phases and events of the hybrid operation.

Table 3: The events and their descriptions of the hybrid operation. (Puistola, 2018)

Phase	Description / Elements
I	Fake news at a meeting of heads of state Agitating controversies between Churches Child Abduction Event Banking disruption, card payment interruptions Cyber-disruption in news communications, alternative media
II	Military exercises in the Baltic Sea - quick implementation Land acquisition attempts near power grid hubs - data for 3 years Information leakage in government - revealed 5 years later Airspace violations - multiple within 3 weeks Restricting the movement of merchant ships in the Baltic Sea
III	Terrorist's strike False news from ministers, spoofing campaigns Unidentified persons near power network nodes Disruption of gas supply Fostering citizen insecurity between botnets and critical communities

Hybrid operations aim to outperform the opponent's strengths and attack specific weaknesses with varying tactics and tools and intensity (FIIA 2018). A hybrid operation involves the means of achieving the desired political outcomes of two or more states. The range of means may include political and economic instruments, cyber warfare, the use or threatening of military force, cyber operations, and the use of Special Forces. The focus of hybrid operations will be identified weaknesses or weaknesses in the target country. (Cederberg & Eronen 2015.)

Tikanmäki and Ruoslahti (2021) note that internal and external security are becoming increasingly difficult to separate, as the operational environment is constantly changing in today's globalized world; there are situations, where external security can be influenced by internal security and vice versa.

The Ministry of the Interior of Finland (2016) recommends that actors and authorities exchange staff to better develop operating models towards improved situational awareness, and lessening cross-sector barriers that prevent information exchange between administrative sectors. Tikanmäki and Ruoslahti (2021) present a model, where situation understanding (aided by e.g., common information sharing systems) is recognised as a building block for deeper collaboration between authorities to focus on societal preparedness and combine both internal and external perspectives of security (Figure 3).

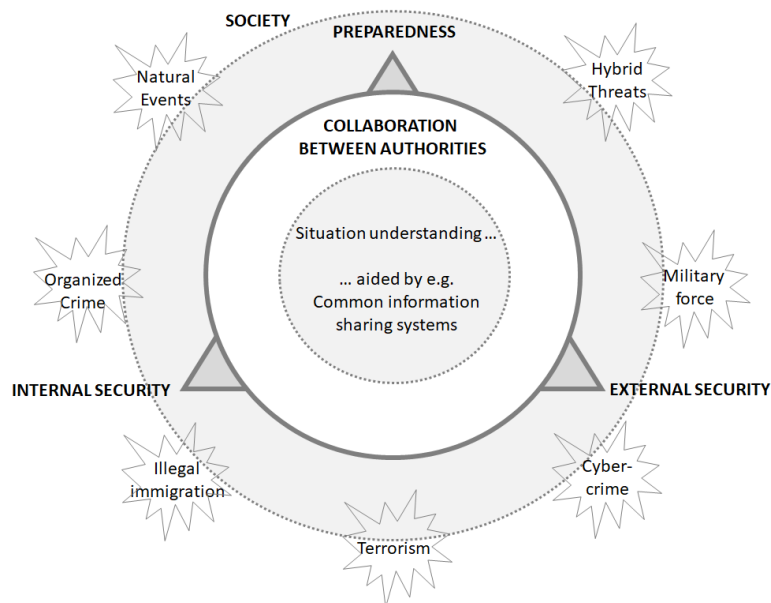


Figure 3: Authority collaboration and societal preparedness in internal and external security (Source: Tikanmäki & Ruoslahti 2021).

As seen in Figure 3, enhanced cooperation between authorities, through e.g. national and EU-wide security databases, is important in strengthening overall security against hybrid influence and threats. “Rapid and up-to-date exchange of information between security authorities is needed to maintain situational awareness.” (Tikanmäki & Ruoslahti 2021, p. 340). The Ministry of the Interior (2016) aims at strengthening the exchange of information between authorities and with relevant actors that may need information across organizational boundaries (Ministry of Interior 2016).

3. Discussion and conclusions

The key efforts to counter hybrid threats – awareness, resilience, and response – are addressed on state and multi-state levels. In the EU, this calls for close cooperation first between the Member States, but also on wider international platforms of collaboration.

Each Member State has the responsibility to build systems that detect and alert of possible hybrid threats. This and building resilience and effective responses to these threats call for statewide coordination and cooperation. Especially those companies and actors that provide critical infrastructure and services (e.g. communications, energy and food supply) must find ways to share information on threats and build resilience together as a system-of-systems, rather than each actor by themselves.

Some main ways of hybrid influence can be geo-economics, information, or electoral impact, with the means of economic, political, or military pressure. These can be used all at once simultaneously or sequentially in phases. Today’s high reliance on technology and open usage of social media, have increased possibilities to take advantage of possible weaknesses in resilience to create societal unrest. For example, cyber-attacks can be used to create continuity problems for critical infrastructure and services, or social media used to create division between different groups of society, or to steer unrest and demonstrations.

Hybrid influencing can occur on many levels. Puistola (2018) for example, lists four levels, which are diplomatic, informational, military, and economic (DIME), and it can be argued that technology could be added to this list to make it DIMET.

Hybrid influencing requires hybrid engagement or hybrid action, which can be defined as activities that pursue certain set goals and use a variety of means that complement each other to exploit the weaknesses of the target. The target begins to see signs of and experience systematic activity by a state or non-state actor where various military, economic or technological pressure, as well as information operations and social media campaigns are applied simultaneously. As discussed, the main ways to counter hybrid threats are resilience and response, and these require awareness, it is vital that the actors within and the state have an open culture and practice of information exchange to spot hybrid influencing as soon as possible. This can be easier said than done, as when targeted by strategic information influence and deception, the subject's perception of reality becomes obscured, and society becomes divided. This is done to achieve the strategic goals of the attacker.

Seeing signs of hybrid interference at an early stage can help the state and society counter with the needed resilience and effective defensive response. The state and its main actors can be targeted by synchronized use of multiple ways of harassment that aim to generate deep dividing lines within the society, possibly also leveraging techniques that threaten to disrupt political processes that paralyze its decision-making ability. These are listed in Table 2, as is a list of the main means of strategic deception by Puistola (2018). Thus, some of the warning signs of hybrid interference and cyber operations are false news, propaganda, political extremism, influence on elections or governance control over critical infrastructure, and financial incentives. The Institute for International Affairs (2018) is clear on its recommendation: the threat of hybrid disruption can be addressed with resilience.

Hybrid warfare can be a combination of instruments and means of influence to subvert states, institutions, and societies. Hybrid warfare is used in conflicts on state or interstate levels. It poses threats of multiple forms of warfare that exploit hybrid threats and apply means of hybrid influencing. Some components of hybrid warfare can be military action, special forces, rebel non-state forces, breaking of social harmony, information influence and propaganda, diplomacy, cyber-attacks against e.g. infrastructure and energy, and economic sanctions.

Defense against hybrid threats requires planning defenses and the commitment of a wide spectrum of actors in the society. The first line of defense is being alert and ready to defend against possible threats. Building national capabilities is a co-creative effort across all wakes of society.

Hybrid operations may proceed in phases. In the first phase, possible weaknesses of the target country (political, economic, social, infrastructure) are explored. The second phase will produce attacks against administration and infrastructure and will aim to seize critical military and civilian targets. The third and final phase is stabilization, where an apparent government is formed in the conquered region. The process will begin with a months-long non-military campaign, where several ways of applying pressure can be identified: information, moral, psychological, ideological, diplomatic, and economic. Table 4 lists possible forms of hybrid operations.

Table 4: Forms of hybrid operations

Hybrid operations		
Concept	Description / Elements	Source
Hybrid operations	<p>1st phase: weaknesses of the target country (political, economic, social, infrastructure) are explored.</p> <p>2nd phase: attack target country's administration and seize critical military and civilian targets.</p> <p>3rd phase: stabilization: an apparent government is formed in the conquered region.</p> <p>Begin with a months-long non-military campaign against the target country. There are several ways to pressure the target, such as information, moral, psychological, ideological, diplomatic, economic, etc.</p>	<p>Järvenpää (2017)</p> <p>Chekinov and Bogdanov (2013)</p>
Hybrid operation events	<p>1st goal: Creating a threatening diplomatic climate</p> <p>2nd goal: Increasing distrust of government leadership</p> <p>3rd goal: Increasing the ambiguity of the situation picture</p> <p>4th goal: Increasing distrust of services and the functioning of critical infrastructure.</p>	Puistola (2018)
Hybrid operations aim	At outperforming opponent's strengths and attacking specific weaknesses with varying tactics and tools and intensity	The Finnish Institute of International Affairs (2018)

Hybrid operations aim to outperform the strengths of the target state and attack its specific weaknesses. Varying tactics, tools, and intensity are used to achieve this aim and modern European societies should be aware of possible hybrid threats, build resilience against hybrid influencing, and have capabilities, societal unity, and international collaboration to defend against possible hybrid warfare.

This research contributes to the academic body of knowledge on hybrid threats and warfare by examining hybrid concepts and providing a basis of building some practical measures to build awareness, resilience, and defenses against hybrid influencing and activities. Future research could address societal resilience from the perspective of intentional hybrid disturbances, and co-creation of state and multi-state resilience. One interesting area of study is the study of situation awareness and situation understanding, and especially with the increasing importance of IT solutions, in the field of cyber security, where e.g. Early Warning Systems, and other methods of identifying cyber threats can increase cyber security and build resilience against hybrid threats and activity.

References

Arreguín-Toft, I. (2001) "How the weak win wars: A theory of asymmetric conflict." *International Security* 26, no. 1 (2001): 93-128. doi:10.1162/016228801753212868.

de Bruijne, M., Boin, A., and van Eeten, M. (2020) "Resilience: Exploring the concept and its meanings." In *Designing Resilience: Preparing for Extreme Events*, eds. Louise K Comfort, Arjen Boin, and Chris C Demchak, 13-32. Pittsburgh: University of Pittsburgh Press.

Cederberg, A. and Eronen, P. (2015) "How can Societies be Defended against Hybrid Threats?" *Strategic Security Analysis*, no. 9 (September 2015). (Geneva: Centre for Security Policy, GCSP).

Chekinov, S.G. and Bogdanov, S.A. (2013) "The Nature and Content of a New-Generation War." *Military Thought* 4 (2013): 12-23.

- European Union. (2018) "A Europe that Protects: Countering Hybrid Threats." Available at: https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en. (Accessed 13 November 2019)
- GAO. (2010) *Hybrid Warfare*, GAO-10-1036R, United States Government Accountability Office. Washington, DC September 10, 2010, 16-18.
- Gärdström, J. (2018) "Hybridisodankäynti - uutta vai vanhaa?" (Master's Thesis, National Defence University, 2018), 2.
- FIIA. The Finnish Institute of International Affairs. (2018) "Hybridivaikuttaminen ja demokratian resilienssi - ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa". *FIIA Report 55/2018*. ISBN 978-951-769-567-1.
- Finnish Government. (2003) "Strategy for Securing the vital functions of society". (In Finnish: Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia), Valtioneuvoston periaatepäätös 27.11.2003. Available at: https://www.defmin.fi/files/248/2515_1687_Yhteiskunnan_elintärkeiden_toimintojen_turvaamisen_strategia_1.pdf. (Accessed 9 January 2020)
- Hoffman, F.G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.
- Huttunen, M. and Metteri, J. (eds.). (2008) *Ajatuksia operaatiotaidon ja taktiikan laadullisesta tutkimuksesta. Maanpuolustuskorkeakoulu*. Taktiikanlaitos. Julkaisusarja 2 no 1/2008. Helsinki: Edita Prima Oy.
- Hybrid CoE. (2019) "Hybrid Warfare – a very short introduction." The European Centre of Excellence for Countering Hybrid Threats. COI Strategy & Defence Conception Paper, May 2019. ISBN 978-952-7282-20-5.
- Hyytiäinen, M. (2018) "Hybridivaikuttaminen", in *Turvallinen Suomi 2018 - Tietoja Suomen kokonaisturvallisuudesta*. Helsinki: Lönnberg Print & Promo.
- Järvenpää, M. (2017) Viranomaisten toimivaltuudet kohteiden suojaamisessa hybridiuhkia vastaan. *Tiede ja Ase 74* (February 2017). Available at: <https://journal.fi/ta/article/view/60630>. Accessed 9 January 2020)
- Lalu, P. and Puustola, J-A. (2015) "On the concept of hybrid warfare." *Finnish Defence Research Agency Research Bulletin 01-2015*. Helsinki: Finnish Defence Research Agency.
- Mack, A. (1975) "Why big nations lose small wars: The politics of asymmetric conflict." *World Politics* 27, no. 2 (1975): 175-200. doi:10.2307/2009880.
- Ministry of Interior. (2016) Interdependence of Internal and External Security. Will the operational culture change with the operational environment? Available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79230/37_2017_Interdependence%20of_nettiin.pdf. (Accessed 4 March 2020)
- Munich Security Conference. (2015) "Munich Security Report 2015: Collapsing order, reluctant guardians?" Published on the occasion of the MSC 2015. Available at: <https://securityconference.org/en/publications/munich-security-report-2015>. (Accessed 19 July 2020)
- Mäkelä, J. (2018) "Merelliset hybridiuhat." CMD Juha Mäkelä's presentation at Sotatieteenpäivät 23.5.2018.
- Puustola, J-A. (2018) "Kokonaisturvallisuus ja hybridivaikuttaminen." CAPT (N) Juha-Antero Puustola's presentation at Sotatieteenpäivät 23.5.2018.
- Raitasalo, J. (2019) "Hybridisota ja hybridiuhat – paljon vanhaa, onko mitään uutta?" in *Tiede ja Ase 76* (January 2019). Available at: <https://journal.fi/ta/article/view/7754>. (Accessed 31 January 2020)
- Security Committee. (2017) "The Security Strategy for Society. Yhteiskunnan turvallisuusstrategia". Valtioneuvoston periaatepäätös 2.11.2017. Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf. (Accessed 1 February 2020)
- Terminology Centre. (2017) *Vocabulary of Comprehensive Security*. ISBN 978-952-9794-36-2 (PDF). Available at: http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf. (Accessed 1 February 2020)
- Tiilikainen, T. (2020) "Hybridivaikuttaminen on kylmävään laajaa". In ERVE Uutiset 21.1.2020. Available at: https://erveutiset.erillisverkot.fi/teija-tiilikainen-hybridivaikuttaminen-on-kylmaavan-laajaa/?utm_source=cremailer&utm_medium=email&utm_campaign=Erve+Uutiset+Maaliskuu+14+2019&utm_content=%5Bemail%5D. (Accessed 7 February 2020)
- Tikanmäki, I. and Ruoslahti, H. (2021) Interdependence of Internal and External Security. Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS 2021), University of Chester 24th - 25th June 2021, pp. 425-432.
- Yin, R.K. (2009) *Case Study Research. Design and Methods*. London: SAGE Publications.