Original Study **Open Access**

Ilkka Tikanmäki[1,*], Harri Ruoslahti[2]

Exploring crisis management response to hybrid threats and warfare

DOI 10.2478/jms-2024-0009
Received: October 09, 2023; Accepted: June 03, 2024

Abstract: Crisis management (CM) operations and organisations may face internal, external and hybrid threats (HTs) against their information and/or personnel. This research looks at how selected European Union (EU), North Atlantic Treaty Organization (NATO) and national perspectives address internal, external and global HTs and influence, even warfare, and maps some relevant strategies to prepare against them in a CM context. Strategies to fight against HTs include relevant political debate and decision-making, integration of EU- and national-level security into critical infrastructure and regular preparedness exercises. Responses to HTs call for relevant technical, situational awareness and problem-solving skills. This research shows how collaboration and situation understanding can assist in detecting and responding to possible cyber and HTs against CM operations. This study examines how collaboration and understanding the situation assist in detecting and responding to HTs to CM operations. There is evidence that information exchange and collaboration are important elements in the fight against hybrid influence and war. Combating misinformation through public education campaigns can support both the civilian and military elements of CM operations. Specific training can be designed to counter aggressive propaganda and disinformation efforts against personnel in CM operations. This maintains one's initiative and trust in the aims of the mission.

Keywords: crisis management, hybrid threats, hybrid warfare, situation awareness, resilience

***Corresponding author: Ilkka Tikanmäki,** Safety, Security & Risk Management, Laurea University of Applied Sciences, Vanha maantie 8, 02650 Espoo, Finland; Department of Warfare, National Defence University, Kadettikouluntie, 00860 Helsinki, Finland, E-mail: ilkka.tikanmaki@gmail.com
Harri Ruoslahti, ResLab, Laurea University of Applied Sciences, Vanha maantie 8, 02650 Espoo, Finland

1 Introduction

War impacts military personnel and civilians in many terrible ways, so where there is war, there is a need for crisis management (CM). Conflicts and crises can devastate states, break societies and governmental structures, cause civilian victims and damage economic and human development (Hyttinen and Kallonen 2018). Many forms of humanitarian crises require a response. Especially in the context of modern warfare, there is a need to coordinate between military and civilian CM organisations.

Violent conflicts seem to escalate in stages that range from stable, through unstable and open conflict to crisis, and even war; and de-escalating back through similar stages (Swanström and Weissmann 2005). Uppsala Conflict Data Program (UCDP) logged a total of 189 conflicts worldwide in 2022, of these 49 incidents or conflicts were listed as one-sided, 84 as non-state and 56 as state-based violence. The number of violent conflicts has increased over the past decade, with the number of violent conflicts recorded 82 in 2010 (Davies et al. 2023 and Uppsala Universitet 2024). Conflicts between dates have increased significantly, even though the definition of violent conflict has not changed. All of these have presented some measure of need for CM, be it military, civilian or both. Disaster preparedness measures aim at enhancing life safety when a disaster occurs, including actions that enhance the ability to undertake emergency actions containing disaster damage, disruption and protection of property, and the ability to engage in post-disaster restoration and early recovery activities (Sutton and Tierney 2006).

There is growing potential for security threats and landscapes due to the impacts of conflict, crisis, radicalisation, global geopolitical changes and interconnectedness. Improvement of conflict preparedness, response capabilities and effective use of resources can create long-term impacts. Hyttinen et al. (2017) note that security challenges need to be addressed in a multi-disciplinary and comprehensive manner to provide a solid foundation for information and evidence-based research (Hyttinen et al.

2017), involving policy-makers, authorities, practitioners and academia (Ruoslahti and Hyttinen 2019). According to Jaques (2007), CM as an active process has four main phases with three sub-phases in each: crisis preparedness (planning process, systems manuals, training simulations), crisis prevention (early warning scanning, issue and risk management, emergency response), Crisis incident management (crisis recognition, system activation/response, CM) and post-CM (recovery/business resumption, post-crisis impacts, evaluation/modification).

Holohan (2019) notes that in each peacekeeping mission peacekeeping personnel from diverse organisations and nations must coordinate together. Communication and cooperation, vital to achieving peacekeeping mission goals, are made difficult due to the diversity of participating organisations (militaries, police forces, civil organisations) and the genders and cultures (national, ethnicity, religion) of the participating people (Holohan 2019). However, national caveats which are (mostly classified) political instructions by officials of the civilian government, may greatly restrict what actions the deployed armed forces on operations can take during the conflict and on behalf of the nation in question (Auerswald and Saideman 2009). National caveats can be civilian or military, and they do not permit humanitarian organisations or military commanders to deploy their assets according to their operation plans (Kingsley 2014).

Many modern crises occur in a state of non-warlike conditions. For example, in September 2021 Poland accused Belorussia of allowing large numbers of refugees to cross into Poland as a means of hybrid warfare (HW; Tidey 2021). This caused Poland to declare a state of emergency in the area, which cut access from not only reporters but also humanitarian aid to the area. Using migration as a hybrid weapon, such as between Belarus and Poland, remains a major challenge for the European Union (EU) and North Atlantic Treaty Organization (NATO), because immigrants of conflict-related migration may be vulnerable and numerous (Hall et al. 2021). The security of Finland's eastern border is affected by the tensions in the security environment in Europe and its neighboring regions. The issue of migrants being instrumentalised has been a problem in Finland since autumn 2023. This is one of Russia's tactics for influencing Finland's national security and internal order (Ministry of the Interior 2024).

From a CM perspective, it is possible to consider what this means for logistics, long-term operations, recovery, integration and migration management, as 'weaponisation' and 'instrumentalisation' are powerful terms, but appropriate descriptions when immigrants are used to forcing negative changes in a target country (Steger 2017; Galeotti 2021). Migrant refugees may flee security threats and be forced out of their home country as a means of hybrid influence or even hybrid war. Immigration policies and the use of migration as a hybrid influence to create an impact on other people are very different things. The intention to forcibly relocate immigrants to another country to create internal pressure is not linked to immigration policy but is intended to undermine the security of the destination country.

The purpose of this research is to explore possible CM responses to hybrid threats (HTs) and HW, and present and define these concepts. The term HW appeared in Nemeth's (2002) thesis 'Future War and Chechnya: A Case for Hybrid Warfare' at the US Naval Postgraduate School. The EU defines HW as a combination of military and non-military measures, deployed against the political, economic and social situation of the country under attack; targeting the EU, its partners, institutions and citizens of its Member States (European Parliament 2016). Both states and multiple non-state actors are capable of conducting HTs and warfare. Hoffman (2007) states that 'Hybrid Wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder' (Hoffman 2007, p. 14).

The United Nations uses the term asymmetric threats in the context of peace operations (Andersson and Tardy 2015). In each CM mission, personnel from diverse organisations and nations must coordinate together. Communication and cooperation, vital to achieving CM mission goals, can be made difficult due to the diversity of participating organisations (militaries, police forces, civil organisations), and the genders and cultures (national, ethnicity, religion) of the participating people. HT and HW look for weaknesses and attack these elements.

The research questions of this study are:

RQ1: How can cooperation for situational awareness help respond to HTs against CM operations?

RQ2: How can collaboration for situational awareness help respond to HTs against CM operations?

2 Methodology

The data for this research are from scientific articles, research reports and selected educational programmes discussing the field of HTs and HW. The data collection method for this study is reading materials (Denzin and Lincoln 2011). Examples of educational programmes are the University of Jyväskylä course on changing security environments and HTs, Capacity Building International and International Emergency Management Society

webinar series of International Models in Emergency Management and NATO CM and Disaster Response Course.

Yin 2009 states that qualitative data is commonly used as sources of evidence in case studies, and thus the study was conducted as a qualitative study. Denzin and Lincoln (2011) argue that observing interactions, conducting interviews or reviewing materials can be used to collect data. Data sources that are valuable include brochures, annual reports, memos, journal articles, regulations and official and unofficial documents (Patton 2002) and it is recommended to use multiple sources of evidence (Yin 2009). Comprehensive and extensive phenomena require thorough research, making case studies a useful tool (Dubé and Pare 2003), as the process of conducting qualitative research is based on knowledge requiring general theories or methods (Alasuutari 1996, 2003).

The eight pre-selected areas are based on a listing of critical functions of society (The Security Committee 2017). These areas served as the basis for the data extraction to provide an approach to frame our understanding of how the sources deal with and would defend against HTs. These elements are discussed in relation to methods of hybrid influence against CM and hybrid influence countermeasures. The eight relevant areas of interest within CM: (1) Leadership, (2) International and EU actions, (3) Defence capabilities, (4) Internal security, (5) Economy, (6) Security infrastructure and supply, (7) Capabilities of and services for the population and (8) Mental resilience (The Security Committee 2017, 2018).

A data extraction table (DET) was formed according to these eight critical functions of society, with a ninth classification as 'Other'. Hybrid influence in CM situations with matching and relevant hybrid influence countermeasures were then identified and extracted from the literature and selected trainings. The section of this paper Results is structured accordingly.

3 HTs and hybrid warfare

3.1 HTs

There are several views on what constitutes an HT, e.g. the US Army describes the HT as 'The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting effects' (Department of the Army 2021, p. 50). Also, HTs may refer to regular forces that disregard standard rules of warfare and use irregular forces in different battlefield domains (Kirk 2023).

According to The European Centre of Excellence for Countering HTs (Hybrid CoE) term HT is '… an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means' (Hybrid CoE 2021, p. 1).

The EU and NATO have separate definitions for HTs. The EU considers HTs to be hostile campaigns below the generally accepted level of warfare, given that HTs combine conventional and unconventional, military and non-military, open and covert operations (Aaronson et al. 2011 and Andersson and Tardy 2015). Reports show that Russia has intensified its hybrid actions against Western countries. Its measures include attempts to interfere in electoral and democratic processes; political and economic pressure and intimidation; extensive disinformation campaigns; harmful cyber functions; and letting cybercriminals, including those that target to disrupt critical infrastructure, operate on its territory (NATO 2021a).

HTs can be tackled through broad cooperation, common situational awareness and crisis resilience throughout society (European Commission 2018). Proper communication in hybrid cases requires open communication, good relationships, plans and flexibility between actors (Paturas et al. 2016). The tools for combating HTs are international cooperation and strong social crisis resilience and identifying common vulnerabilities and preparing for disruptions is key, especially in the area of critical infrastructures (European Commission 2018). HTs can be implemented by various actors who are founded, supported, sponsored or in some way inspired by the state. Implementers of HTs include military forces, criminal networks, political organisations, religious groups, Non-government Organisations (NGOs) and Government Organised NGOs (GONGOs; NATO StratCom COE 2015). 'An actor engaging in HW may use a wide range of military, political, economic, civilian and informational (MPECI) instruments of power aimed at the political, military, economic, social, informational and infrastructure (PMESII) vulnerabilities of a target' (MCDC 2019, p. 13). Hybrid tools increase pressure on the destination country, and fighting the HT requires policy coordination and, indeed, close cooperation. For instance, the EU and NATO strategic processes, the EU Strategic Compass and the new NATO strategy should help in the fight against HTs (European Commission 2020).

3.2 HW

While the cyber threat landscape is evolving fast, there are strong indications of state actors commissioning

cyber-attacks or digital underground services and tools from cyber criminals combining elements of cyber and terrorism and using cyber capabilities, e.g. cyber piracy in military hybrid operations; deepening the cyber dimensions of HW (Ducaru 2016). The increase in hybrid risks tests the fragmented security systems of the EU, as HTs involve conventional and non-conventional means, which can be very difficult to detect and measure. Governments, companies, the public and other institutions can become victims of hybrid incidents and attacks (Demertzis and Wolff 2019).

EU Member States were targeted by cyber-attacks and disinformation campaigns in 2019: the Spanish and Lithuanian Ministries of Defence and the Finnish Ministry of Justice were the targets of cyber-attacks, and a cyber-attack that led to the theft of personal data of 5 million citizens was carried out against the Bulgarian tax authorities. There was also a widespread fear that European elections would be the subject of disinformation campaigns aimed at casting voters in the EU Member States. So the EU took steps to impose 'cyber sanctions' for harmful attacks against the Union and its Member States (Fiott and Theodosopoulos 2020).

'The blurring of modes of war, the blurring of who fights, and what technologies are brought to bear, produces a wide range of variety and complexity that we call HW' (Hoffman 2007, p. 14). Ducaru (2016) defines HW as a shift away from a 'traditional force-on-force models' to approaches that combine non-military and military methods of deliberate and synchronised campaigns aiming to 'destabilize and gain political leverage over an opponent' (Ducaru 2016, p. 10). Military objectives can be achieved through deliberate actions in the cyber environment and using a variety of military and non-military means of pressure to influence another state (Limnéll 2020). Raitasalo (2017) suggests that HW as a concept becomes better understood when broken into more precise concepts such as: 'coercion, extortion, bribery, lying, proxy wars, psychological manipulation, propaganda, and others that have been the essence of statecraft over several millennia' (Raitasalo 2017, p. 38).

The terms HW and terrorism are ambiguous and both can be defined in various ways and have even contradictory interpretations (Gasztold and Gasztold 2020). The evolution of viewpoints regarding non-kinetic warfare (Lehto and Limnéll 2017) influences today's definitions of HW, which in turn can be looked at as a continuum of viewpoints on competition and conflict between international actors (MCDC 2019).

US Army expands the term 'irregular warfare' to 'HW'. In irregular warfare, both military and non-military capabilities are utilised in several domains, including overt, secret and covert. The use of other methods, including military domination of the enemy, can lead to it by both state and non-state actors, either in conjunction with or separately from conventional warfare. Irregular warfare's main objective changes depending on the political situation (Department of the Army 2022). The rise of so-called irregular challengers is a high probability. Terrorism, insurgency, unrestricted warfare and guerilla warfare are becoming more sophisticated and scaled, which presents challenges to US security interests worldwide. The purpose of these irregular challengers is to exploit tactical advantages at a time and place they choose (Mattis and Hoffman 2005; Hoffman 2009). The approaches can be incorporated into and precede HW in the form of individual HTs. Lehto and Limnéll (2017) contend that 'HW has brought a state that may precede traditional warfare, to occur after the active phase of war, or without traditional warfare' (Lehto and Limnéll 2017, p. 191). The tactics of HW use a mixture of conventional and irregular approaches to conflict rather than a single method to different hybrid forms of warfare. To succeed in a hybrid war, troops must become more adaptable and flexible to defeat their opponents (GAO 2010). Hybrid activities combine and blend recourses to dominate the battlefield both physically and mentally (Lasconjarias and Larsen 2015).

The Multinational Capability Development Campaign (MCDC) framework is based on three interdependent elements: (1) critical functions and vulnerabilities, (2) means of synchronisation (horizontal escalation) and (3) effects and non-linearity. The synchronised use of multiple power tools is tailored against specific vulnerabilities in a wide array of societal functions to achieve synergistic effects. (Cullen and Reichborn-Kjennerud 2017 and MCDC 2019). MCDC claims that 'Although the term HW is used to explain the overall concept, a hybrid attack may not necessarily include the use of armed force' (MCDC 2019, p. 17).

Hybrid approaches use information management, media and all possible other means to weaken the position of the counterparty; this may also include the traditional use of military force, where both state and non-state actors (with or without state support) can conduct HW (Lasconjarias and Larsen 2015). The three components, detect, deter and respond, of the MCDC framework can be used as guiding phases when using appropriate thresholds to strategically combat hybrid aggressors and attacks. The Detect component first addresses the issue of the existence of HTs or attacks that require building situational awareness and understanding. HTs can be very difficult to detect, and traditional enemy-centred threat analysis may be insufficient to comprehend these

complicated situations. The Deter component seeks ways to limit the impact of HTs and the actions of hybrid aggressors. The Respond component discusses how to respond to hybrid attacks. Vulnerability identification and other appropriate actions and measures and thresholds should be addressed in all three phases. Strategic countermeasures can be attacking suppression with counteractions to prevent and disrupt attacks (Cîrdei 2016; MCDC 2019).

HW may precede traditional warfare (Lehto and Limnéll 2017) and it may include a combination of elements such as coercion, extortion, bribery, lying, proxy wars, psychological manipulation and propaganda (Raitasalo 2017). A HW campaign is designed to gain political influence over an adversary through deliberate and synchronised tactics (Treverton et al. 2018). A hybrid attack may not necessarily include the use of armed force (MCDC 2019).

3.3 Situation awareness of HTs and warfare

A situation picture is formed when information relevant to one's sector becomes extracted from the data. A common understanding of the situation can be established when conclusions are drawn together in real-time. Common understanding can be understood as 1) recently detected or obtained 2) the latest confirmed inquired true observation 3) the best continuity estimate at the time of decision making or 4) the best forecast at the time influencing the decision. (Hyytiäinen, 2021).

Tikanmäki and Ruoslahti (2019) combine definitions of situation awareness to include 'knowing and understanding of what is happening, and an understanding of possible future changes or problems, predictions of future situations and making decisions on these bases' (Tikanmäki and Ruoslahti 2019, p. 424). Ongoing data development processes are required to collect, analyse, store and share information in order to build a commonly shared comprehension between political, civilian and military organisations and among systems and actors in the operating environment (Thiele 2015).

A situation picture can be called a summary of the information related to a specific situation; situation understanding is how decision-makers and their assistants understand the situation, what has happened and the circumstances that affect them, the goals of all different parties and possible options of how the events may develop, all elements that are needed to make decisions on a particular issue or subject such as hybrid attacks (Tikanmäki and Ruoslahti 2019).

The question of legal jurisdiction and ethics concerning effective HT management should be addressed, because of the unclear distinction between politics and war (Mälksoo 2018). The ambiguous qualities of modern HTs present great difficulties for counter-terrorist awareness (Mumford 2016). 'The crucial problem, however, is the correct assessment of a multitude of information and drawing timely conclusions. Knowledge development needs to provide indications and warning of an emerging hybrid security problem' (Thiele 2015, p. 11).

HW can be seen as a mixture of soft- and hard-power measures, and to counteract such a challenge requires integrated security-management systems for states to be prepared against both conventional and attacks that are carried out in cyberspace (Gasztold and Gasztold 2020). As HTs may emerge from both state and non-state sources, intelligence functions and effective deterrence become difficult (Mumford 2016).

The development of security related to the operating environment of international crises requires a common picture of the situation from the authorities and the sharing and utilisation of up-to-date information. The difficulty of operational activities is the lack of a common concept in terms of the situation and understanding of the situation. The common language and concepts are especially emphasised in situations where there is collaboration/cooperation between several authorities and a common understanding of the situation is sought.

Cooperation among the authorities should be reinforced. For instance, national and European security databases are important for enhancing public security in response to hybrid influence and threats. 'Rapid and up-to-date exchange of information between security authorities is needed to maintain situational awareness'. Tikanmäki and Ruoslahti (2021, p. 429). The importance of situational awareness created and shared by security stakeholders relies on updated information and assessments. The wider the common ground there is between a common understanding of the situation and the stakeholders who share it, the better the result will be. Security actors implementing situational awareness in CM operations carry out foresight work from very different starting points and with different objectives. However, the differentiation of systems causes competition between systems, which takes attention away from the core and content, solutions for overall security. Capacity should be strengthened by a culture of cooperation based on essential skills needed to counter hybrid influence.

3.4 CM

In recent decades, the EU and its Member States have faced challenges in building appropriate capacities to respond to new situations and HTs (Aaronson et al. 2011; Andersson and Tardy 2015). CM mechanisms need to react quickly to different situations because lives can be on the line and minutes may count. Responding to cyber-attacks and other forms of HW call for responses that require flexibility in individuals and organisations, as well as cross-training to become more aware of the elements of hybrid influence, and to be better prepared to deter and respond to it and its effects (European Parliament 2021).

Hyttinen et al. (2017) on Common Security and Defence Policy (CSDP) find that 'the rationale for focusing the study on civil-military aspects of CSDP lies in partly the changing security landscape in which CSDP missions and operations are (to be) deployed, requiring an increasing the need for more integrated civil-military CM operations. Terrorism, HTs, cyber security, energy security and organized crime are just some of the complex modern threats that require for multidimensional approach' (Hyttinen et al. 2017, p. 54). Conventional and unconventional forms of conflict have increased with HW (Lasconjarias and Larsen 2015) and CM is needed to help people and the state in crisis areas to manage the impact of natural disasters, political disorder, war, etc. (Hyttinen and Kallonen 2018).

In most cases, there is a need for humanitarian aid. CM operations are mostly either civilian in nature or combine military and civilian elements. Building dialogue with the surrounding civil society can benefit from a strong civil-military response to novel, unexpected security challenges during conflicts and crises (Hyttinen and Kallonen 2018). Increasing understanding among the diverse personnel of both international and local organisations (e.g. police forces) increases in understanding, communication and cooperation to enhance the efficiency of the CM operation (Holohan 2019).

Solidarity between member states has been enhanced by joint threat assessment, collective decision-making, processes and collaboration within the CSDP Framework (Tardy 2015). In the new security environment, interoperability challenges are likely to increase. Hyttinen et al. (2017) offer 'closer civil-military co-operation (CIMIC), greater participation of 3rd states and future integrated/hybrid/joint missions.' and closer integration of military and civilian elements 'through, for example, provisions of security, logistics, strategic planning. Integration can thus support both civilian and military actors in achieving their objectives as well as strengthen pooling and sharing' (Hyttinen et al. 2017, p. 60).

Hybrid influencing may contain kinetic and non-kinetic elements that have objective physical, information or psychological impact (Ducheine 2016). Due to the growing role of digital solutions, HTs gradually include cyber threats and disinformation. The targets of these can be military, civilian administration, critical infrastructure, business, local government and citizens (as groups and individuals; Cederberg and Eronen 2015). Because there are so many potential aspects of hybrid effects, they can be difficult to detect and even more difficult to counter without well-coordinated responses. Sharing of information and cooperation have been shown to be important in the fight against hybrid influence and warfare (Cîrdei and Ispas 2017).

NATO and CM have a history where security and humanitarian interests intersect in complex and fast-evolving contexts, which has increased the role of NATO in emergency management (NATO 2020). One complex aspect of disaster relief is the interaction between civilian actors and military authorities (Tardy 2015), who participate simultaneously in disaster relief operations, and cooperation between them can be difficult; planning must consider the needs of both civilian and military parties involved, particularly as military authorities become more and more participating in non-military missions (Weijers 2015).

To facilitate cooperation and to improve relationships between civilian and military actors, the CIMIC will assist in 'coordination and cooperation in support of the operation' between military and civilian actors, 'including national populations and local authorities, as well as international, national and non-governmental organizations and agencies' (NATO 2003, pp. 9–10). Most CM operations unite the two aspects of civilian and military, and this has become one of its key features in CM (Tardy 2015).

The NATO crisis response system (NCRS) is composed of five parts: preventive options, crisis response measures, counter-surprise, counter-aggression and alert states. 'CM is one of NATO's core tasks for which it employs an appropriate mix of political and military tools to manage a crisis in an increasingly complex security environment: (a) increasing connectivity of key services, (b) critical civilian structures and (c) national resilience' (NATO 2020, p. 1). 'In its military dimension, CM implies the deployment of troops in contexts that differ from traditional war-fighting or openly coercive operations in several respects' (Tardy 2015, p. 10). The use of military resources in disaster situations includes immediate search and rescue (SAR), preserving relief operations by delivering aid to prevent the situation from deteriorating, and rehabilitation and reconstruction (SIPRI 2008), and e.g. 'The Euro-Atlantic Disaster Response Coordination Centre (EADRCC) is

NATO's principal civil emergency response mechanism in the Euro-Atlantic area' (Atlantic Council 2020; NATO 2021b, p. 1).

The European Security Strategy shows a change in the security environment and highlights cyber security, critical infrastructure security, combating illegal content and preventing terrorism. Although there is no common defence or CM in the EU, the Commission is considering making proposals for an overall CM system (European Commission 2020).

Communication and networking are major challenges in CM, and efficient communication among civil and military operations is important (Daniels 2012). The cooperation, innovation and development of many stakeholders can create strong CM expertise that creates new solutions for international operations. In the international field of CM expertise, practical solutions may be lacking (OCHA Services 2016). NATO and the EU are designed for military and economic alliances, not for CM, and so they now strive to find ways in which to provide comprehensive CM. One of the biggest challenges for the EU in CM is the varying levels of engagement between EU members and partners. NATO's consensus-based decision-making, in turn, will lead to a stronger commitment from member countries (Gross 2010; NATO 2011).

Our societies are becoming more connected in regard to CM, the United Nations, EU, NATO and many others in the global community, for example, work towards joint goals; coordination of disaster relief on just the European level can better ensure that assistance is tailored to the needs of victims (Kaspersen and Sending 2005; Gross 2010; Tardy 2015). NATO provides opportunities for its members to negotiate and cooperate on defence and security issues in problem-solving, confidence-building and conflict prevention (NATO 2010). These opportunities increase CM capacities, and thus, coordination across organisations (EU, UN, NATO, etc.) is important in CM. In the EU, Member States are primarily responsible for responding to HTs, and they 'must cover the full spectrum of action from early detection, analysis, awareness, building resilience and prevention through to crisis response and consequence management' (European Commission 2020, p. 14).

4 Counter measures to hybrid influence

Potential targets must recognise hybrid actions that target them to successfully counter hybrid strategies; targets need to be able to react quickly and efficiently by having the flexibility to counter these hybrid actions, being prepared to counter them, and having processes for rapid assessment and decision-making, along with the ability to respond effectively (Jungwirth et al. 2023).

Prevention represents the best possible means of countering HW; 'The concept of security sector reform (SSR), embedded in United Nations Security Council (UNSC) Resolution 2151 offers an indispensable tool to tackle the challenges of HW. SSR aims to strengthen a state's ability to provide public safety and secure the rule of law, while embracing transparency and accountability' (Pindják 2014, p. 3). According to Raitasalo (2017) 'globalization has progressed based on technological development—particularly in the field of information technologies—and political decisions' (Raitasalo 2017, p. 25). Thiele (2015) notes that opponents will exploit hybrid opportunities because they are effective, as HW targets people and affects decision-makers and key policies with subversive clandestine actions (Thiele 2015).

NATO should ensure that its Allies prepare to counter hybrid attacks, deter hybrid attacks on the Alliance and, when necessary, defend the Allies concerned, where hybrid scenarios escalate towards military conflict (Ducaru 2016). Strong social resilience to crisis and international cooperation are key conditions for combating HTs (Radulescu 2015). One way to prepare against hybrid and other possible threats is to take resilience into account in the design of CM systems and operations with what innovative solutions and technologies are available (Thoma et al. 2016). The EU has a three-part approach to increase resilience: regulations and standards, preparedness and testing, and governance (Demertzis and Wolff 2019). Cyber-terrorism and cyberespionage by hostile entities are serious threats, which call for proactive policies to detect and protect operations in the cyber-sphere, both organisations and states that are increasingly reliant on cyberspace need to seek new approaches to build needed levels of IT resilience (Gasztold and Gasztold 2020).

Resilience is 'The ability of individuals and communities to maintain their performance in changing circumstances, the readiness to face disruptions and crises and the ability to recover from them. The term resilience is partially used to mean the same as crisis resilience' (Finnish Government 2021, p. 80). The ability to create generic capabilities in complex and technical systems, with the help of solutions from the engineering sciences, enables them to withstand, survive and adapt to disruptions. Thoma et al. (2016) offer resilience engineering (RE), which in the military context is also known as broad utility, as a concept to provide society 'with means, methods and technologies

to overcome unexampled events with as less harm as possible and to come out even stronger and better prepared afterwards' (Thoma et al. 2016, p. 3). Responding requires coherent governmental and intergovernmental security policies, together with appropriate legal instruments and organisational structures that coordinate counter-terrorism activities and strengthen law enforcement capabilities (Gasztold and Gasztold 2020).

Building countermeasures to HW can benefit from the breakdown approach by Raitasalo (2017), where appropriate proactive countermeasures can be planned and built against each identified sub-threat (e.g. coercion, extortion, bribery, lying, proxy wars, psychological manipulation, propaganda; Raitasalo 2017). According to Hämäläinen and Vataja (2020), resilience refers to the ability to adapt, regenerate and recover: originally, the concept has been used in psychology and science to relate to an individual's ability to cope and recover from traumatic events or the ability of organisms to cope with extreme variations in environmental conditions (Hämäläinen and Vataja 2020).

The seven Baseline Requirements of resilience defined by NATO are (1) Continuity of Government and critical government services; (2) Resilient Energy Supplies; (3) Ability to deal effectively with the uncontrolled movement of people; (4) Resilient Food and Water Resources; (5) Ability to deal with Mass Casualties; (6) Resilient Communication Systems; and (7) Resilient Civilian Transportation Systems (Shea 2016). Mumford (2016) suggests developing a common definition of 'HW' with categories within its key constituent activities (including terrorism) to enable a stronger NATO counter-terrorism response in hybrid war situations (Mumford 2016).

Providing catalogues of good practices, new solutions and approaches helps enhance the CM capabilities of the EU (Hyttinen and Kallonen 2018) while responding to hybrid attacks requires combining a wide array of national instruments, and even information sharing and assistance from other friendly nations and a wider international community (Ducaru 2016). Networking knowledge helps organisations prepare, strengthen situational awareness and support collaborative planning to determine how to best operate together against hybrid challenges; more comprehensive and adaptive perspectives based on shared trust help the systematic capture of knowledge to support leaders and organisations (Thiele 2015). Constructing flexible enough legal rules may allow governments to protect their societies against HTs (Gasztold and Gasztold 2020). Hyttinen and Kallonen (2018) note how large security threats by radicalised individuals and transnational criminality complicate the security landscape for EU CSDP missions and operations (Hyttinen and Kallonen 2018). Complex, dynamic, interrelated threats in conflict/region call for combined and tailor-made responses, with an intensified focus and attention on interoperability, including efficient CIMIC, with appropriate harmonisation and standards (Hyttinen et al. 2017).

Combating HTs can be achieved through societal cooperation, common situational awareness and crisis resilience across society, and close international interaction, with regular preparedness exercises and political debate, as well as the integration of EU security into critical infrastructure (Radulescu 2015). Gasztold and Gasztold (2020) note the need for international-level anti-terrorism policies, an example of which they offer the emphasis on key areas (awareness, capabilities and engagement) by the NATO Policy Guidelines on Counter-Terrorism (Gasztold and Gasztold 2020). Military systems need to adapt military training, defence planning, force equipment and training programmess to future threats and challenges. Conditions for success in military operations, including HW, are created by flexible and adaptive command and control structures (Radulescu 2015). In changing operating environments, decision-makers and organisations can effectively improve their ability to handle disturbing and unexpected events with CM exercises (Got 2020).

Understanding the historical context in contemporary acts of terrorism as hybrid war scenarios (e.g. Russia and Syria) may help to identify key challenges for NATO to counter terrorism in hybrid conflicts, develop a forward-looking assessment of future counter-terrorism trends and efficiently apply counter-terrorism strategies (Mumford 2016). Openness in society is good in the fight against HTs. That is why openness and honesty are also good in the language of security policy. False misinformation and intentional disinformation must be combated and the authorities must be active in providing citizens with correct information (Mälksoo 2018, p. 25). However, the emerging institutions and counter practices against HW, highlight a paradox, where defence against HTs may become detrimental to the core principles of democracy (Ducaru 2016). Timely detection of the hybrid actions is crucial, although there are difficulties in balancing the deterrent tool to avoid provocations that can trigger unnecessary conflict (Mälksoo 2018).

5 Conclusions

The literature examined clearly raises the importance of Situation awareness in detecting HTs and countering hybrid attacks. These aspects are seen in the different approaches, e.g. EU and NATO. Situation awareness

builds on the Situation picture, which is creating relevant information from data collected from multiple sources. Making sense of this information will enable seeing the 'big picture' of how the CM actors, organisations and mission may be influenced by hybrid attacks and warfare. By adding further layers of understanding, of decision-makers and people involved, about the events and circumstances, goals, parties, and possible development options needed to make appropriate decisions and to deter and respond to deliberate actions of hybrid warfare by the aggressor. Training the staff in CM actor organisations to build situation picture, awareness and understanding is recommended.

People, systems and operations need to increase their resilience. HW takes many forms and uses a multitude of simultaneous attacks that focus on what vulnerabilities are subject to threats and aggression. Measures to build resilience are increasing individuals' awareness of threats and abilities to properly protect from and react to once encountering them. Navigating the maze of data to build information for a relevant situation picture and situation awareness that are needed to build an understanding situation calls for relevant technical, situational awareness, problem-solving and sector-specific skills for individuals and organisations alike. Training relevant skills increases the abilities to detect and address HTs, and to counter (deter and respond) to hybrid aggression and attacks.

The three-part approach to increase resilience (regulations and standards, preparedness and testing, governance) provides a common framework for the identification of common vulnerabilities in CM and critical infrastructures, as disaster preparedness is a strong focus for the EU. Resilience promotes organisational and systemic abilities to withstand and cope with crises and flexibly work in disturbances, rapidly recover from them and develop by learning from the crisis. Emerging threats, such as attacks on civilians by weapons or in case of natural disasters, pose a risk to civilians and civilian infrastructure. The above means that ensuring the resilience of the civilian administration, infrastructure systems and the civilian population is an integral part of collective defence. Research is recommended to better understand how to promote overall resilience through a combination of individual, organisational and societal resilience.

Due to the complexity and surprise of HTs to security, it must be accepted that it is not always possible to predict them accurately. However, it is precisely for this reason that the importance of resilience and multifaceted cooperation between security actors in the production of security is also emphasised in CM. In complex environments, it becomes especially important for international organisations to be effective, efficient and adaptable. Instead of individual actors or instruments, a holistic perspective and cooperation can ensure that actions are based on a common situation picture and analysis and are coordinated into situation understanding.

Civil preparedness is an important element for several reasons, the population can be seen as a resource, planning for the worst is essential, and baseline resilience requirements are needed. Many stakeholders are involved in building resilience and thus, civilian preparedness protects against a wide range of threats and vulnerabilities. The principle of mutual assistance is useful in helping the network, strengthening points of tension and creating opportunities for cross-curricular learning, mutual learning, skills development and further training. That is to say, the principle of mutual assistance supports flexibility.

Countering disinformation with public information campaigns can support civilian and military CM operations. The purpose of these campaigns is to combat aggressive propaganda and disinformation efforts and to maintain initiative and public confidence. Information sharing and collaboration are shown to be important elements in fighting against hybrid influencing and warfare. This is one area where further study and actions are recommended to better understand the mechanisms behind polarisation that is fed for disinformation and hybrid influence. Events to inform and counter disinformation campaigns in social media are one recommended way forward.

References

Aaronson, M., Diessen, S., Kermabon, Y. D., Long, M. B., & Miklaucic, M. (2011). NATO countering the hybrid threat. *Between States, 2*(4), 111-124.

Alasuutari, P. (1996). Theorizing in qualitative research: A cultural studies perspective. *Qualitative Inquiry, 2*(4), 371-384.

Alasuutari, P. (2003). The globalization of qualitative research. In: Seale, C. Silverman, D. Gubrium, J. F. & Gobo, G. (eds.), *Qualitative Research Practice*. SAGE Publications Ltd, London. pp. 595-608. Available at https://www.torrossa.com/gs/resourceProxy?an=5018485&publisher=FZ7200#page=526.

Andersson, J. J., & Tardy, T. (2015). *Hybrid: What's in a Name?* European Union Institute for Security Studies. Available at http://www.jstor.org/stable/resrep06844.

Atlantic Council. (2020). Six Reasons NATO's Euro-Atlantic Disaster Response Coordination Centre is Important for Our Future Security. Atlantic Council. Available at https://www.atlantic-council.org/.

Auerswald, D., & Saideman, S. (2009). *NATO at War: Understanding the Challenges of Caveats in Afghanistan*. McGill University, Montreal.

Cederberg, A., & Eronen, P. (2015). *How can Societies be Defended against Hybrid Threats?* (Strategic Security Analysis 9; p. 11). Geneva Centre for Security Policy – GCSP, Geneva.

Cîrdei, I. A. (2016). Countering the hybrid threats. *Land Forces Academy Review, 21*(2), 113-119.

Cîrdei, I. A., & Ispas, L. (2017). A possible answer of the European Union to hybrid threats. *Scientific Bulletin-Nicolae Balcescu Land Forces Academy, 22*(2), 71-78. doi: 10.1515/bsaft-2017-0009.

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *Understanding Hybrid Warfare* (p. 36). The Multinational Capability Development Campaign Project, Oslo, Norway.

Daniels, C. E. (2012). Building a Capabilities Network to Improve Disaster Preparation Efforts in the European Command (EUCOM) area of responsibility. (p. 93) [MBA Professional Report]. Naval Postgraduate School, Monterey, CA. Available at https://www.semanticscholar.org/paper/Building-a-capabilities-network-to-improve-disaster-Daniels/39043b8c99265f15eefd553b00f504485b06f586.

Davies, S., Pettersson, T., & Öberg, M. (2023). Organized violence 1989-2022 and the return of conflicts between states. *Journal of Peace Research*, *60*(4), 691-708.

Demertzis, M., & Wolff, G. (2019). Hybrid and Cybersecurity Threats and the European Union's Financial System. Bruegel Publications, Brussels, Belgium, p. 14.

Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE Handbook of Qualitative Research*, 4th edn. Sage Publications, Thousand Oaks, California.

Department of the Army. (2021). *Field Manual 1-02.1: Operational Terms*. Department of the Army. Available at https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34799-FM_1-02.1-000-WEB-1.pdf.

Department of the Army. (2022). *Field Manual 3-0: Operations*. Department of the Army. Available at https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.

Dubé, L., & Pare, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly, 27*(4), 597-635. doi: 10.2307/30036550.

Ducaru, S. D. (2016). The cyber dimension of modern hybrid warfare and its relevance for NATO. *Europolity - Continuity and Change in European Governance, 10*(1), 7-23.

Ducheine, P. A. L. (2016). Non-kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting. In Ducheine, P. A. L. Schmitt, M. N. & Osinga, F. P. B. (eds.), *Targeting: The Challenges of Modern Warfare*. T.M.C. Asser Press, The Hague, pp. 201-230. doi: 10.1007/978-94-6265-072-5_10.

European Commission. (2018). *Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* (Joint Communication to The European Parliament, The European Council and The Council Join (2018) 16 final; p. 11). European Commission.

European Commission. (2020). *The EU Security Union Strategy* (Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee Of The Regions Com(2020) 605 final; p. 28). European Commission.

European Parliament, D. G. for P. R. Services. (2021). *Strategic Communications as a Key Factor in Countering Hybrid Threats*. Publications Office. https://data.europa.eu/doi/10.2861/14410.

European Parliament. (2016). European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda Against it by Third Parties (2016/2030(INI)) (Resolution 2016/2030 (INI); p. 10). European Parliament. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016IP0441.

Finnish Government. (2021). *Government's Defence Report*. (Government's Defence Report 2021:80; p. 65).

Fiott, D., & Theodosopoulos, V. (2020). *Yearbook of European Security 2020*. European Union Institute for Security Studies (EUISS), Paris. Available at http://www.iss.europa.eu.

Galeotti, M. (2021, December 7). *How Migrants Got Weaponized*. Available at https://www.foreignaffairs.com/articles/2021-12-02/how-migrants-got-weaponized.

GAO. (2010). GAO-10-1036R Hybrid Warfare, United States Government Accountability Office Washington, DC, p. 28.

Gasztold, A., & Gasztold, P. (2020). The Polish counterterrorism system and hybrid warfare threats. *Terrorism and Political Violence, 34*(6), 1259-1276. doi: 10.1080/09546553.2020.1777110.

Got, A. (2020, February 7). NATO Review - NATO crisis management exercises: Preparing for the unknown. *NATO Review, 7*, 1-6.

Gross, E. (2010). EU Conflict Prevention and Crisis Management: Roles, Institutions, and Policies. Routledge, London.

Hall, B., Fleming, S., & Shotter, J. (2021, December 5). How migration became a weapon in a 'hybrid war.' *Financial Times*. Available at https://www.ft.com/content/83ece7e4-cc71-45b5-8db7-766066215612.

Hämäläinen, T., & Vataja, K. (2020, September 3). The coronavirus revealed the vulnerability of society. *Sitra*. Available at https://www.sitra.fi/en/articles/the-coronavirus-revealed-the-vulnerability-of-society/.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, Arlington, VA.

Hoffman, F. G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict. *Strategic Forum, 240*, 8.

Holohan, A. (2019). Transformative training in soft skills for peacekeepers: Gaming for peace. *International Peacekeeping, 26*(5), 556-578.

Hybrid CoE. (2021). Hybrid Threats. *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. Available at https://www.hybridcoe.fi/hybrid-threats/.

Hyttinen, K., & Kallonen, M. (2018). *How to improve EU's conflict prevention activities to achieve longterm impact?* (p. 7) [Prevention]. Available at https://www.researchgate.net/profile/Kirsi-Aaltola/publication/320101431_How_to_improve_EU's_conflict_prevention_activities_to_achieve_longterm_impact/links/5c07c51e299bf169ae33729a/How-to-improve-EUs-conflict-prevention-activities-to-achieve-longterm-impact.pdf.

Hyttinen, K., Hario, P., & Österlund, P. (2017). *Improving the Effectiveness of Capabilities (IEC) in EU conflict prevention*. Available at https://www.theseus.fi/handle/10024/134725.

Hyytiäinen, M. (2021, May 20). Data integrity and situation picture of management [Invited presentation]. In: *Scientific Advisory Board for National Defense (MATINE) Research Seminar 2021*, Webinar, Helsinki, Finland.

Jaques, T. (2007). Issue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review, 33*(2), 147-157. doi: 10.1016/j.pubrev.2007.02.001.

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso, V., Lebrun, A., & Giannopoulos, G. (2023). *Hybrid threats:*

A comprehensive resilience ecosystem (Science for Policy Report JRC129019; p. 124). European Union. Available at https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf.

Kaspersen, A., & Sending, O. (2005). *The United Nations and Civilian Crisis Management*. Norwegian Institute of International Affairs, Oslo, Norway.

Kingsley, R. (2014). Fighting against allies: An examination of "national caveats" within the NATO-led International Security Assistance Force (ISAF) campaign in Afghanistan & their impact on ISAF operational effectiveness, 2002-2012 Doctoral dissertation, Massey University. Available at http://hdl.handle.net/10179/6984.

Kirk, J. A. (2023). Irregular and hybrid warfare. *NCO Journal*, July 2023, p. 1-4.

Lasconjarias, G., & Larsen, J. A. (2015). *NATO's response to hybrid threats* (Forum Paper 24; p. 372). NATO Defence College, Rome, Italy. Available at http://www.nato.int/cps/en/natohq/topics_156338.htm.

Lehto, M., & Limnéll, J. (2017). Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede ja ase*, *75*. Available at https://journal.fi/ta/article/view/67730.

Limnéll, J. (2020). Kybervarautuminen edellyttää poliittista ohjausta ja johtajuutta. In: Heino, O. Huotari, V. & Laitinen, K. (eds.), *Varautuminen eilen-varautuminen huomenna: Puheenvuoroja Suomesta*. PunaMusta Media Oyj. Available at https://www.theseus.fi/bitstream/handle/10024/348345/POLAMK_Raportti_136.pdf?sequence=4&isAllowed=y.

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: The emerging practices of the EU and NATO. *European Security*, *Query date: 2021-05-07 13:40:55*. https://www.tandfonline.com/doi/abs/10.1080/09662839.2018.1497984.

Mattis, J. N., & Hoffman, F. (2005). Future warfare: The rise of hybrid wars. *U.S. Naval Institute, 131*(11), 18-19.

MCDC. (2019). *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare* (p. 94) [Handbook]. The Multinational Capability Development Campaign. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

Ministry of the Interior. (2024). *Combating the instrumentalization of immigration and strengthening border security* (Decision VN/5349/2024-SM-1; p. 2). Ministry of Interior, Helsinki, Finland.

Mumford, A. (2016). *The Role of Counter Terrorism in Hybrid Warfare* (p. 50) [A report prepared for NATOs Centre of Excellence for Defence Against Terrorism (COE DAT)].

NATO StratCom COE. (2015). *Hybrid Threats: A Strategic Communications Perspective*. NATO Strategic Communications Centre of Excellence.

NATO. (2003). *NATO Civil-Military co-operation (CIMIC) Doctrine* (Doctrine AJP-9; p. 57). NATO.

NATO. (2010). *Strategic Concept 2010* (p. 40) [Concept]. NATO. Available at http://www.nato.int/cps/en/natohq/topics_82705.htm.

NATO. (2011). *NATO's Assessment of a Crisis and Development of Response Strategies*. NATO. Available at http://www.nato.int/cps/en/natohq/official_texts_75565.htm.

NATO. (2020, October 8). *Crisis Management*. NATO. Available at http://www.nato.int/cps/en/natohq/topics_49192.htm.

NATO. (2021a, June 14). Brussels Summit Communiqué Issued by the Heads of State and Government participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021 [Press Release (2021) 086]. NATO. Available at https://www.nato.int/cps/en/natohq/news_185000.htm.

NATO. (2021b, September 20). *Euro-Atlantic Disaster Response Coordination Centre*. NATO. Available at https://www.nato.int/cps/en/natohq/topics_52057.htm.

Nemeth, W. (2002). *Future war and Chechnya: A case for hybrid warfare*. Naval Postgraduate School, Monterey, CA. Available at http://hdl.handle.net/10945/5865.

OCHA Services. (2016, August 29). *Evaluating Military Engagement in Disaster Response—World* [Press Release]. ReliefWeb. Available at https://reliefweb.int/report/world/evaluating-military-engagement-disaster-response.

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods*, 3rd edn. Sage Publications, Thousand Oaks, California.

Paturas, J., Smith, S., Albanese, J., & Waite, G. (2016). Inter-organisational response to disasters. *Journal of Business Continuity & Emergency Planning, 9*, 346-358.

Pindják, P. (2014). Deterring hybrid warfare: A chance for NATO and the EU to work together. *NATO Review*, *Query date: 2021-05-07 13:40:55*. Available at https://www.academia.edu/download/62870633/Deterring_hybrid_warfare__a_chance_for_NATO_and_the_EU_to_work_together_.pdf.

Radulescu, M. (2015). Counter-hybrid warfare. Developments and ways of counteracting hybrid threats/ war. In: *International Scientific Conference "Strategies XXI," 2*, pp. 132-144. Available at https://www.proquest.com/docview/1692922163/abstract/5AF916CA31CF422APQ/5.

Raitasalo, J. (2017). Getting a Grip on the So-Called "Hybrid Warfare." *ASPJ Africa & Francophonie, Query date: 2021-05-07 13:40:55*. Available at https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-08_Issue-3/raitasalo_e.pdf.

Ruoslahti, H., & Hyttinen, K. (2019). Comprehensive approaches to cooperation for organisational resilience to promote safety and security in arctic. In: *Exploring the Future of Management*. EURAM 2019 Conference, Lisboa, Portugal. Available at https://www.theseus.fi/handle/10024/332987.

Shea, J. (2016). Resilience: A core element of collective defence. *NATO Review, 30*(3), 8.

SIPRI. (2008). *The effectiveness of foreign military assets in natural disaster response:* (726642011–001) [dataset]. Stockholm International Peace Research Institute. https://doi.org/10.1037/e726642011-001.

Steger, N. D. (2017). The Weaponization of Migration: Examining Migration as a 21st Century Tool of Political Warfare. Naval Postgraduate School, Monterey, CA.

Sutton, J., & Tierney, K. (2006). Disaster preparedness: Concepts, guidance, and research. *Colorado: University of Colorado, 3*(1), 44.

Swanström, N. L. P., & Weissmann, M. S. (2005). *Conflict, Conflict Prevention and Conflict Management and Beyond: A Conceptual Exploration*. Central Asia-Caucasus Institute and Silk Road Studies Program, Uppsala, Sweden.

Tardy, T. (2015). *CSDP in Action: What Contribution to International Security?* Publications Office. https://data.europa.eu/doi/10.2815/634719.

The Security Committee. (2017). *Security Strategy for Society* (Government Resolution 2.11.2017; p. 101). The Security Committee. Available at https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

The Security Committee. (2018). *Vocabulary of Cyber Security* (p. 43). Sanastokeskus TSK ry.

Thiele, R. (2015). Crisis in Ukraine–the emergence of hybrid warfare. *ISPSW Strategy Series: Focus on Defense and International Security*, *Query date: 2021-05-07 13:40:55*. Available at https://www.files.ethz.ch/isn/190792/347_Thiele_RINSA.pdf.

Thoma, K., Scharte, B., Hiller, D., & Leismann, T. (2016). Resilience engineering as part of security research: Definitions, concepts and science approaches. *European Journal for Security Research, 1*(1), 3-19.

Tidey, A. (2021, September 30). *Poland carried out migrant push-back at Belarus border, Amnesty says*. Euronews. Available at https://www.euronews.com/2021/09/30/poland-carried-out-migrant-push-back-at-belarus-border-amnesty-says.

Tikanmäki, I., & Ruoslahti, H. (2019). How are situation picture, situation awareness, and situation understanding discussed in recent scholarly literature? In: *Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. SCITEPRESS Science and Technology Publications, 419-426. doi: 10.5220/0008494104190426.

Tikanmäki, I., & Ruoslahti, H. (2021). Interdependence of internal and external security. In: *Conferences Proceedings of 20th European Conference on Cyber Warfare and Security*, Academic Conferences International Limited, Reading, UK, 425-432.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). *Addressing Hybrid Threats*. Swedish Defence University, Sweden.

Uppsala Universitet. (2024, April 4). *UCDP - Uppsala Conflict Data Program*. Uppsala Conflict Data Program Department of Peace and Conflict Research. Available at https://ucdp.uu.se/.

Weijers, B. (2015). *NATO disaster relief operations: An analysis of an underexposed field of activity of the Alliance.* Dissertation, Catholic University of Portugal. Available at https://repositorio.ucp.pt/handle/10400.14/18819.

Yin, R. K. (2009). *Case Study Research: Design and Methods*, (1; 4th edn. Vol. 14). Sage Publications, Thousand Oaks, CA. Available at https://journals.nipissingu.ca/index.php/cjar/article/view/73.