ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2024 (35)

SOME ELEMENTS OF DEFINING INFORMATION WARFARE

Vykintas STUMBRYS
Kauno University of Applied Sciences
Pramonės av. 20, LT-50468 Kaunas, Lithuania
E-mail vstumbrys@gmail.com
ORCID ID: 0009-0008-9184-9216

DOI: 10.13165/PSPO-24-35-21

Abstract. *Information itself in a much broader sense is the weapon. Some bad news come every day forming public opinion and raising fear. Democracies around the world face rising levels of disinformation. Can we be defeated before the conventional war even started? Collective memory recalls some devastating informational attacks before the Russian invasion of Ukraine. Nowadays politics recognize threats to our public matters and democratic political system. In such an environment states face a decline of trust in democratic institutions. Trust in government and parliament is at a record low. Aggressors understand the importance of an approach that seeks to influence the population of target countries through information operations, proxy groups, and other influence ways. The potential for a democratic process to overcome pervasive foreign manipulation must be supported by international law. The paper overviews key challenges in international law describing informational war. The paper observes some changes in doctrine and strategies to deal with this challenge. The present work aims to help understand information war within the context of hybrid warfare.*

Keywords: *hybrid war, hybrid actions, hybrid threats, Information Warfare, hybrid warfare, democracy, international law, disinformation, propaganda.*

Introduction

Information Warfare has no beginning or end. Long before conventional war aggressors prepare the victim state, its own people, and the international community to approve their actions. Sometimes response is late but Europe is waking up from the deceiving friendship with the aggressor. The President of European Commission U. von der Layen has stated in her speech on 2024 April, "that in the last years, many European illusions have been shattered. The illusion that peace is permanent. The illusion that economic prosperity might matter more to Putin than destroying a free and democratic Ukraine. The illusion that Europe on its own was doing enough on security – be it economic or military, conventional or cyber. As we look around us, it is clear there is no room for any more illusions" (EU Commission 2024).

These illusions were not created in one day, it was a long way of consistent hybrid information campaigns and diplomatic work. Well known political scientist Herbert A. Simon described (Rzevski 2023) "In recorded history, there have perhaps been three pulses of change powerful enough to alter Man in basic ways. The introduction of agriculture... The Industrial Revolution... (and) the revolution in information processing technology of computer."

Russia's military and non-military campaigns in Ukraine opened another, new page of hybrid actions for the international community. We are faced with a situation where legal regulation is not sufficient to respond to these actions.

Lately, the head of the Belarusian KGB, Ivan Tertel, reported that in Lithuania and Poland, radicals are producing combat drones that should strike the most important objects in Belarus. He claimed that the KGB allegedly prevented the impact of military drones from the territory of Lithuania on objects in Minsk and its surroundings (15min 2024). That was later denied by Lithuanian authorities. This April, I. Kant's congress in Kaliningrad was held to fight in European information theatre in the ecological sphere. Well, nothing new here, it was proven

that Russia supports far-right extremists and green ideas to create confrontation in society and to preserve Russia's interests in selling oil and gas. As a result, natural gas was mentioned as green energy in the European "Green Deal" (Europarliament 2022).

Western countries are affected by information more than authoritarian countries. First of all we have free media and press. Any information can be published and accessed freely. Some scientists think that postmodern culture is unfavorable for ethical consideration because it rejects compromised meta-narratives. Due to the plurality of society, ethics emerge as the problem of the justification of norms, because the traditional foundations of positive and natural law are already rejected. The ethics of duty are no longer applicable due to the fact that civilization is going through a crisis and there is no stable structure of social responsibilities. It is possible in postmodern civilization to rely only on ethics that introduced the criterion of benefit-utilitarian. It has two big disadvantages: it is closed to the material field and it is egoistic. Limitations of utilitarian ethicists are attempted to go beyond J. Habermas's discursive ethics project. Unlike the ethics of maxims, it has no ideological content, i.e. states the mere process of how ethical conflicts might be resolved (Micevičiūtė, J., 2002, p. 31). So society may be not that resistant to false information, because it is used to have different opinions and views. Finally some part of society believes in disinformation. Our strategic goal is to counter the Kremlin's disinformation rather than deal with the narratives spread by the russian disinformation campaigns.

The defense of values of Western civilization challenges the dominance of military power, scientific thought and capabilities. New powers are emerging that, unable to challenge directly, seek to compete for dominance in their region or the world through other means, including informational warfare.

Nowadays information society is continuing its (r)evolutionary process. As long as the globalization and human creativeness brings up technological developments, the information society will be definitely gaining new defining features. It can be described as the post-industrial society which is based consistant production and distribution of information and in which information technology is transforming every aspect of political, economic, social and cultural life in a manner of recreating individuals' daily routines (Akgün, 2012).

All these factors influence the need for the analysis of the Information Warfare phenomenon in the context of legal regulation. The article aims to reveal the concept of Information Warfare and emerging problems. In this paper, the author will discuss different concepts of information war.

The definition of information and disinformation

The term "information" was coined in the 13th century meaning "a written testimony." The use of this term was restricted to the legal field.

There exist different definitions of information used in different sciences. Information is not always linguistic, it can be visual, emotional or other, according to our reception. In essence, information is the building block of knowledge, and without it, we would struggle to make sense of the world around us (Ashikuzzaman. 2014). Information is meaning assigned to data within some context for the use of that data (Watters, 1992).

Prytherch (2016) states that "Information is an assemblage of data in a comprehensible form capable of communication. This may range from content in any format – written or printed on paper, stored in electronic databases, collected on the Internet, etc. - to the personal knowledge of the staff of an organization."

Roszak, (1994), Stonkienė (2006) recognise the qualitative concept of information. That is based on the realization that the social value of information is the content of information, to which the sender attaches a certain need and the receiver gives meaning. The qualitative concept of information means that the term of information may not be what is transmitted (bits, bytes), but what is transmitted and may be perceived by the human being (data, information), i.e. it can turn into this. Where meaning co-occurs with social information.

The importance of information is reflected in strategic NATO documents, particularly in NATO Standard AJP-3.10 Allied Joint *Doctrine For Information Operations*. It states that „information awareness and perceptions gained from analysis of collected information and personal observations have long been an integral part of human existence; those with a superior ability to gather, understand, control and use information have gained a substantial advantage. The ability to manage and employ information underpins activities in diplomatic, military, economic and other areas of activity, maintaining Allied freedom of action. From the strategic to the tactical level and across the range of military operations, information plays a vital role in the manner in which decisions are made. In military operations, the ability to defeat adversaries or potential adversaries may rest on the perception of all actors involved, particularly the local population. There is therefore considerable benefit to be gained by affecting the flow of information through a decision-maker and his understanding of that information"(NATO, 2015).

Hybrid CoE Information Expert Pool Members as well as discussions at the meeting held with multidisciplinary experts in Helsinki in November 2019 four trends were identified: 1. Fragmentation of the concept of truth, 2. Comprehensive changes of media as an industry 3. Hegemony of private media platforms 4. New technologies that give rise to new tools for interference and influence (Hybrid Coe , 2019).

We can summarise, Hybrid Coe states that from the hybrid threat perspective, disinformation is part of priming the target, and building up the capabilities of the actor behind the disinformation. The coordination behind the repetition of a message is often difficult to detect and needs long-term monitoring in different languages. Disinformation is a confusing mix of strategic messages stemming from state and non-state actors (frequently disguised and hard to attribute) that consider the democratic state system to pose a threat to them. It is combined with advertising from commercial entities and mis- and dis-information that is disseminated by aware or unaware regular users This all points to that the distinction between fact and opinion is becoming blurred and we are facing a return of ideological media (Hybrid Coe, 2019).

Language is one of the main sources of information. "Socrates said, '*The misuse of language induces evil in the soul.*' He wasn't talking about grammar. To misuse language is to use it the way politicians and advertisers do, for profit, without taking responsibility for what the words mean. Language used as a means to get power or make money goes wrong: it lies" (Le Guin, 2018).

Historical context of using the term of Information Warfare

McCornack (1992, 1997) formulated the Information Manipulation theory. It is a theory of deceptive discourse production. It concludes that deception often is easier than truthtelling, which is why people do it. So, people are used to lying in some circumstances. In Information Warfare, actors are using information deliberately and seeking some political goals.

Information Warfare tactics, such as propaganda, deception, and psychological operations, have been used throughout history. Ancient civilizations employed various means, such as

spreading rumors, forging documents, and manipulating public opinion, to gain strategic advantages in conflicts (Libicki, 1995).

According to Hutchinson (2006), Deception was not thought to be an important factor in public-government contact in the West. This was thought to be more a characteristic of totalitarian regimes. In the Marxist-Leninist Soviet Union, there was little distinction between the military and diplomatic facets of government. The deception was a function of state craft and not confined to the military (where it was an accepted practice in wartime, even with Western publics). The doctrine of deception became known as maskirovka. Broadly, the Soviet concept of maskirovka includes deception, disinformation, secrecy, feints, diversions, imitation, concealment, simulation and security although it is not restricted just to these.

Ajir, Vailliant (2018) analyzing concept of modern Russia's hybrid warfare, found out that early Soviet regime used information weapons to help achieve greater long-term goals. The first known use of the words "active measures" was in a Bolshevik document in 1919. By definition, active measures involve influencing events and behaviour in, and the actions of, foreign countries. Active measures were employed to influence nations around the globe; however, the United States was always considered the main enemy, and the Soviets did not differentiate between peacetime and war. Today, the same logic is employed. According to the Russian government, "The leadership and the command staff of all levels directly participate in the organization of the activity in the information space during peacetime and in wartime." The Soviets created the most threatening influence of its kind in the modern world (Ajir, Vailliant 2018).

When a change in Western mindset did occur, the role of the manipulation of information for advantage came to the forefront. It was the access to and the use of information that were the fundamental determinants of superiority. The practice of deception is a natural extension of the acceptance of information as the dominant element in competitive advantage. If information is of value in decision-making, then its control and manipulation must also be important.

In the United States in the middle of the 20th. century covert operations were understood to be all activities which are conducted or sponsored by government against hostile foreign states or groups or in support of friendly foreign states or groups but which are so planned and executed that any US Government responsibility for them is not evident to unauthorised persons and that if uncovered the US Government can plausibly disclaim any responsibility for them. Specifically, such operations would include any covert activities related to: propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-communist elements in threatened countries of the free world. Such operations did not include armed conflict by recognized military forces, espionage, counter-espionage, and cover and deception for military operations (National Security Council Directive on Office of Special Projects, 1948). One of the aims of using covert action is to avoid being implicated in clear breaches of international law.

The definition included propaganda into Covert operations, but do not call them information war according to the current understanding.

The origins of the term 'Information Warfare' can be traced back to the late 1980s when the expression was specific to the military domain. It became a 'living' concept in the Gulf War of 1991. Information Warfare's origins are electronic warfare, military deception, psychological operations and information/operational security. However, the most significant element in its evolution was the development of electronic computing and communications technology. By the 1990s, the role of this technology in warfare had been proven in the 1991

Gulf War (Campen, 1992). Information or more specifically, information technology had given the edge in battlefield intelligence, targeting, and command and control. However, the emphasis was still on the technology rather than the 'information' per se. Nevertheless, another component was developing in this war – media management. Since the war in Vietnam, the military had been developing their tactics. The war in Vietnam was a watershed for the relationship between the media and the military (and thus, government). Reporting from the Vietnam War was, largely, an open situation for journalists (Louw, 2005)

In 1996 Molander, Riddile and Wilson described The Basic Features of Strategic Information Warfare: 1. *Low entry cost*. Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites. 2. *Blurred traditional boundaries*. Traditional distinctions public versus private interests, warlike versus criminal behavior and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure. 3. *Expanded role for perception management.* New information-based techniques may substantially increase the power of deception and of image - manipulation activities, dramatically complicating government efforts to build political support for security-related initiatives. 4. *A new strategic intelligence challenge.* Poorly understood strategic Information Warfare's vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. We may therefore have to develop a new field of analysis focused on strategic Information Warfare. 5. *Formidable tactical warning and attack assessment problems.* There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage or accidents. 6. *Difficulty of building and sustaining coalitions.* Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks, giving opponents a disproportionate strategic advantage. 7. *Vulnerability of the US homeland*. Information-based techniques render geographical distance irrelevant; targets in the United States are just as vulnerable as in-theater targets.

Hutchinson (2006) describes that the concept of Information Warfare began as a technology oriented tactic to gain information dominance by superior command and control. This soon developed into a realization of the power of information as both a 'weapon' as well as a 'target'. The importance of information rather than its associated vehicle – information technology − created a situation where influence became a critical factor in conflict. As the nature of conflict changed to being an almost ongoing situation, control over mass communication became a high priority task for governments as well as the military. As such, the manipulation of information became an essential function. Thus, the world of deception became an integral part of official communications between governments and their constituency.

There are two main definitions of Information Warfare, one includes Cyberwarfare in definition.

According to NATO, cyberspace and the related area of new technologies provide an important field for Information Warfare. Cyberwar activities may consist of cyber attacks, destroying information systems of the opponent, but these may also involve so-called social cyber-attacks, by creating in people's minds a specific image of the world, consistent with the goals of the Information Warfare conducted by a given country (NATO 2005).

Dan Kuehl of the National Defence University defined Information Warfare as the "conflict or struggle between two or more groups in the information environment".

All forms of struggle over control and dominance of information are considered essentially one struggle, and the techniques of Information Warfare are seen as aspects of a single discipline. Author would agree with the opinion of Libicki (1995) that, "those who master the techniques of Information Warfare will therefore find themselves at an advantage over those who have not; indeed, Information Warfare will, in and of itself, relegate other, more traditional and conventional forms of warfare to the sidelines".

Another important tool of Information Warfare has always been, - keeping people in controlled information environment. The language education and the language component have become crucial factors in countering hybrid threats in Ukraine. As Ukraine faces ongoing challenges, including external aggression and attempts at cultural assimilation, understanding the role of language in countering these threats becomes imperative (Averianova and Voropayeva 2019).

Russian Empire, the Soviet Union, and Russia, for a long time executed strong assimilation policy. Notably, after open aggression, the effect was the opposite. 41% of Russian-speaking Ukrainians have already transitioned fully or partially to Ukrainian since the invasion. The study also found a decrease in the proportion of Ukrainian residents speaking only Russian at home, from 37% to 13% between 2012 and 2022 (Verbytska, Babii, Botvyn, Konivitska, Khlypavka 2023)

Recognizing the importance of language education as a tool for resilience, Ukraine has been actively investing in initiatives that foster linguistic unity, enhance critical thinking, and promote media literacy among its population.

Speaking about the history of the use of the term, it is still in the process. New challenges, like managing biotechnology data and biometrics of humans, using AI for influencing political views are still waiting for the attention of a scientists.

Information Warfare in context of hybrid warfare

The European security environment is becoming increasingly hybrid in nature. The information war is not over – and won't end anytime soon. Despite some optimistic takes by Western commentators, no one in Ukraine would consider that the information war has already been won and that they could cease their efforts. Everyone understands that Russia's information aggression will continue adapting to new circumstances, and that it is of the utmost importance to continue fighting against it (Kalenský J., Osadchuk, R., 2024, p. 5).

Hybrid warfare term of modern conflicts has similar terminologies in the Russian doctrine (Non-Linear or New Generation Warfare) and Chinese doctrine (Unrestricted Warfare). From the Russian perspective, through what is known as the "Gerasimov Doctrine", the modern methods of waging warfare are by the broad use of political, economic, informational, humanitarian, and other non-military means, supplemented by civil disorder among the local population and concealed armed forces (Al Aridi, 2022).

In 2014 and the war in eastern Ukraine for the first time different kind of conflict was taking place. Instead of a clear enemy, his structures, in Crimea we saw "green men" without distinguishing marks. Russian President Vladimir Putin initially insisted that "these are not our soldiers", although he later rewarded them and publicly acknowledged their involvement. At the time, Ukraine was under diplomatic and economic pressure and a veritable information war, cyber-attacks and subsequent actions by special operations forces. (Bajarūnas, Keršanskas, 2016). So we saw combined usage of different hybrid warfare actions including Information Warfare.

Hybrid threats are defined as fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives. NATO defines hybrid warfare as a mixture of military means and non-military means. Hybrid CoE defines hybrid threats as actions carried out by state or non-state actors whose purpose is to harm or weaken the target by influencing its decision-making at the local, regional, state or at the institutional level. Thus all the definitions stress the use of various methods in pursuit of specific political and military objectives (Vasiliauskienė, V., Stumbrys, V., 2023).

China has issued "The Political Work Guidelines of the People's Liberation Army (PLA)" in 2003, a new warfare concept for the PLA which is the Three Warfare (in Chinese it is known as "San Zong Zhanfa") to be applied during both peacetime and wartime. This document highlights three main concepts:

- "Public Opinion or Media warfare such as using distorted information, spread fake news,
- Psychological warfare refers to the application of military and nonmilitary measures to disrupt adversaries.
- Legal warfare (lawfare), which helps the state to undermine other states' foreign policy goals through the international environments, especially that justifying China's actions in international law and establishing positions in domestic law is an important factor for the PLA (Al Aridi, 2022 p. 84), (Burke E., Gunness K., Cooper C. and Cozad M., 2020).

Using term „Information Warfare" is usually included in the understanding of hybrid warfare by various authors and international organizations.

The main feature of hybrid war is the constant combination of military and non-military methods of influence, which poses unusual political tasks for both the army and the security services (Dykyi, Kharchenko, 2016, p. 8). F. G. Hoffman (2009) has defined hybrid threats as "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives." One of the well-known international organisations analysing the hybrid threat, Hybrid Centre of Excellence, defines "hybrid threat" as an action carried out by state or non-state actors whose purpose is to harm or weaken the target by influencing its decision-making at the local, regional, state or at the institutional level. (Hybrid CoE, 2023a)

In this field, some different definitions are being used. Well known for hybrid warfare studies centre of excellence Hybrid Coe uses three basic terms in this field: disinformation, understood as false information spread deliberately with the intention to deceive; propaganda, understood as information, sometimes biased or misleading, used to promote a political cause or interest; and information aggression, an umbrella term that covers most of the terms, plus various active measures facilitating the impact of information operations (e.g., creating proxies, fake civil society or using agents within the adversary's camp) (Kulakov, Yermolenko, Rybak, 2018).

Mikael Wigell (2021) thinks it specifically involves the use of disinformation and economic inducements to recruit and assist these actors inside the target country, detach their loyalties from the target government, and use them as interlocutors to transform the established social order and its structures of authority and norms. The aim is to weaken democratic governance and norms as a means of enhancing their own authoritarian standing. Not only are weakened democracies less able to directly confront these authoritarian aggressors, but they will also look less appealing as models of success and partners for others. By portraying Western democracies as corrupt and ungovernable, authoritarian regimes such as China, Iran, Russia, and Turkey are less at risk of being overthrown by their own populations.

When discussing hybrid threats and warfare designed to stay under the triggering threshold of armed conflict. Accumulation theory comes to help. Fogt (2021) states that "The

accumulation of events theory is of particular importance. The information war is committed over a long period of time, and being dosed weakly or monthly. The asymmetric hybrid character of the low-level use of force, the flexibility regarding intensity and rapid adaptability coupled with disinformation and fake news targeted at the entire society as such may collectively constitute an "armed attack" and, thus, justify a necessary and proportionate act in self-defense." We can assume that the theory of accumulation is suitable for the legal definition of hybrid threats. It helps to properly assess that a legal threshold has been crossed, from which retaliatory action can be taken. Regulating the use of force is a primary function of international law because if states could freely resort to force the ideal of the rule of law in international society would be impossible (Vasiliauskienė, Stumbrys 2023).

The question whether one may take into account several incidents which in accumulation then would together constitute an armed attack is raised by the accumulation of events theory. Fard, et. al. (2023) state that the ICJ has confirmed the existence of a severity threshold to distinguish between "the most severe forms" and "less severe forms" of the use of force.

"Hybrid interference" is a concept coined to capture non-military practices aimed at mostly covert manipulation of other states' strategic interests (Wigell, 2019). As such it is similar to what was called "active measures" etc. during the Cold War, and recently in Russian strategic discussions as "Gibridnaya voyna" (translated from Russian "hybrid warfare"). The idea behind the "Gibridnaya voyna" is to avoid the traditional battlefield in order to destroy the political cohesion of the enemy from within, using a carefully crafted hybrid of non-military means and techniques that intensify political, ideological, economic and other social polarisation in western society, leading to its internal collapse (Fridman, 2018, p. 96). Keeping diplomatic relations intact and thus not crossing any formal threshold of war, the aggressor mobilises opposition and radicals in the target state through a variety of means, from disinformation campaigns to the corruption of political figures and the financing of subversive movements, carefully synchronised to intensify the conflict (Wigell, 2021).

Furthermore in Russia, even huge media companies are controlled by the Ministry of Defense. Emphasis is laid on the army's involvement in government propaganda via a separate, military module of the propaganda apparatus, of which the Krasnaya Zvezda media holding and its associated traditional and electronic media are part (Darczewska, J., OSW Studies (2016) Zvezda was sanctioned by the Ukrainian government on 21 May 2021, with an official report referring to the channel as producing "news content in accordance with Kremlin policy to justify Russia's actions". In October 2022, the Canadian government sanctioned Zvezda amid the Russian invasion of Ukraine. In June 2023, the European Union added Zvezda to its list of sanctions.

Part of hybrid warfare involves exploiting the openness of Western democracies to seize strategic economic sectors, such as critical infrastructure, finance, and media, through which these authoritarian actors can attempt to destabilise Western democracies and purposefully damage them (Heather, et. al., 2016). Democracies urgently need to find ways to defend themselves against such hybrid interference without jeopardising the values they are supposed to defend. Expanding state control of civil society is not a viable liberal democratic strategy.

When outside actors with the mentality to undermine and hurt the target start to use information domain's "paradise", an unhealthy polarization occurs that can lead in the worst case to the destabilization of a state. This unhealthy polarization creates an "us versus them" mentality (Bremmer, 2018). Western democracies should also not resort to countermeasures such as corruption, disinformation, election interference, and other hybrid measures of interference, as this would only further erode liberal democratic values around the world. More

dangerous to the West are the more subtle, non-military activities that authoritarian regimes use to infiltrate democratic societies.

Contemporary definition of Information Warfare in international organisations

European Union uses the term Foreign information manipulation and interference (FIMI) as defined in Action plan against Disinformation (2018), that describes a mostly non-illegal pattern of behavior that threatens or has the potential to negatively affect values, procedures, and political processes. Such activity is manipulative in character and conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory. The EU has long recognised the importance of tackling FIMI and stepped up efforts to combat the issue long before the latest Russian aggression against Ukraine in February 2022. When in 2015, the concern first appeared on the EU's political agenda, the European Council highlighted the need to challenge Russia's disinformation campaigns. Later, in 2018, following the Salisbury chemical attack in the UK and the related European Council conclusions, the EU focused its efforts on bolstering resilience against hybrid threats. Over the years, the EU has developed a more precise understanding and diagnosis of the issue, from fake news and disinformation to foreign information manipulation and interference, and it has improved the means of preventing, deterring, and responding to FIMI. Among the milestones in this journey are the Action Plan against Disinformation (2018) and the European Democracy Action Plan (2020). The war in Ukraine brought this work to the forefront of political attention. The European Strategic Compass (2022) and the Council Conclusions on FIMI (2022) provided further impetus.

Action Plan against Disinformation (2018) defines that Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Disinformation campaigns, in particular by third countries, are often part of hybrid warfare, involving cyber-attacks and hacking of networks.

The legal framework at the European level that is composed of many legal instruments and supported by declarations and resolutions, plays an important role in establishing a tighter legal net to counter the new threats that arise due to the rapid technological development.

However, the use of the term "information war" in UN documents is not widespread. The UN (2021), particularly through the work of the International Telecommunication Union (ITU) and the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, has discussed the implications of Information Warfare. The UNGGE has produced reports that touch on norms, rules, and principles for responsible state behavior in cyberspace.

The latest report reaffirms that the serious Information and communications technologies (ICT) threats persist. It underlines serious concerns about 1. harmful ICT activity against critical infrastructure; 2. an increase in states' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another state; 3 malicious ICT activity aimed to exploit vulnerabilities.

NATO defines Information Warfare as an operation conducted in order to gain an information advantage over the opponent. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information Warfare is not a new phenomenon, yet it contains innovative elements as the effect

of technological development, which results in information being disseminated faster and on a larger scale.

To define Information Warfare operations, NATO uses the term Info Ops. According to NATO, information operations include two main branches, one is to affect the will of the target, and the other, is to affect information systems. The definition of Info Ops and information activities are as follows:

a. Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives.

b. Information activities are actions designed to affect information and or information systems. They can be performed by any actor and include protective measures.

In this document it is clear that Info Ops are part of military activity, therefor can be described as military actions itself. Info Ops is an integral part of military activity at every level of command. It is therefore critical that Info Ops factors are considered in the Operational Planning Process (OPP) from the beginning. Planning of effects and activities in the information environment must directly support the commander's intent, guidance and desired end-state.

Further explaining information warfare as important part of hybrid warfare it should be noted that NATO's interpretation of hybrid warfare depicts it as a mixture of military means and non-military means, including propaganda and cyber activities. For NATO officials, hybrid warfare is "the highly integrated use of a wide range of overt and covert military, paramilitary and civilian means" (NATO, 2014). This depiction describes a combination of political and non-traditional means of coercion and influence. These activities include the coercive use of military force and more subtle forms of harmful influence in the political and informational spheres.

Hybrid warfare is not equivalent to armed action in most cases, but its consequences can be similar to armed action. It is therefore important to consider the cluster of acts together to determine whether the threshold of armed conflict has been reached.

In 2014 under the auspices of NATO's CCDCOE The Tallinn Manual on the International Law Applicable to Cyber Warfare, was developed. It outlines how international law, particularly the laws of armed conflict, applies to cyber operations, including those that could be considered Information Warfare. The Tallinn Manual has become an influential resource for legal advisers and policy experts dealing with cyber issues. Emerging State practice and the taking of public positions on international cyber law many States since the Manual's publication necessitates an update of the 2017 edition. Accordingly, in 2021, the CCDCOE has launched the Tallinn Manual 3.0 Project, a five-year venture that will involve the revision of existing chapters and the exploration of new topics of importance to States.

However, there is still no official definition of Information Warfare in the western world. It includes physical, cognitive and informational aspects. It is used to manage information to pursue a competitive advantage in both offensive and defensive operations (Wilson, 2022). Information Warfare has been used to describe narrower activities like network operations, electronic warfare, psychological operations, military deception, and operations security – all of which are components of Information Warfare.

Conclusions

Information and communication technologies hold immense potential to enhance our lives. We must conclude that all the biggest countries are involved at Information Warfare.

Therefore, those who master the techniques of Information Warfare will become superior to those who do not; it is likely that Information Warfare will by itself push aside other, more traditional and conventional forms of warfare. States have described Information Warfare in their strategic and operative documents of their military headquarters and recognised by politicians, scientists, and inteligence agencies.

Difference between undemocratic countries and democratic is in the goals they are trying to achieve. As emphasiszed by Wilson (2022), Western practices of free speech and free press allow potential adversary nations a virtually free hand in running disinformation campaigns in Western nations. It would be a necessity to begin engaging governmental agencies, and possibly liaise with private entities, to conduct effective Information war campaigns that promote our culture and values while simultaneously attempting to neutralise adversary efforts in the same space. Such campaigns should promote Western values of democracy, freedom of speech and trade, international law, and respect for nations that support the same values.

When transplanting Western theories onto Russian soil, government deliberately confuse the concepts of attack and defense, adjusting them to Russia's own geostrategy of revenge. Authoritarian and semi-authoritarian states and non-state actors project strategic narratives that include distorted information through media outlets in foreign languages define strategic narrative as a means by which political actors attempt to construct a shared meaning of the past, present, and future of international politics to shape the behavior of domestic and international actors.

Modern Information Warfare term is being mostly understood as part of hybrid warfare, with the same problems of defining the threshold of understanding of armed attack under international law. Here accumulative theories come into help. The doctrine of accumulation events refers to a series of minor hybrid incidents that have accumulated until they reach the threshold of an armed attack, and is also known as the "spiking" theory, which some governments use to justify their right to self-defense.

Information Warfare's definition includes various hybrid actions. We can conclude that the definition can be understood as including all kinds of hybrid actions connected with the spread of information having the goal of affecting the target population or decision-making. Typically, Information Warfare is a long-term project, but has more active phases. The alternative definition is more cyberspace-oriented and used for more technical hybrid operations.

As the nature of Information Warfare evolves with technological advancements, international organizations continuously update their definitions and doctrines to address new challenges. Important to admit that new challenges, like managing biotechnology data and biometrics of humans, using AI for influencing political views in social nets are still waiting for the attention of scientists. Policymakers need to initiate collaboration with experts to better anticipate security risks arising from the combination of artificial intelligence and biotechnology.

References

1. Ajir, M., Vailliant. B., (2018) Russian Information Warfare: Implications for Deterrence Theory [online] Available at: https://www.jstor.org/stable/26481910?seq=1 (Accessed: 15 April 2024).
2. Akgün, N., (2012) "Adaptive Intelligence Communities in the Information Society". Romanian Intelligence Studies Review [online] Available at: https://www.ceeol.com /search/article-detail?id=111178 (Accessed: 11 April 2024).

3. Al Aridi, A., (2022) The Problem of Hybrid War in International Law [online] Available at: https://doi.org/10.15388/vu.thesis.401 (Accessed: 10 April 2024).
4. Ashikuzzaman, Md. (2014) Types of information. [online] Available at: https://www.liseduneTwork.com/definition-and-types-of-information/ (Accessed: 15 April 2024).
5. Bajarūnas, E., Keršanskas, V. (2016) 'Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome', *Lithuanian Annual Strategic Review* 16(1):123-170 [online] Available at: https://www.researchgate.net/publication/330316025_Hybrid_Threats_Analysis_of_Content_Challenges_Posed_and_Measures_to_Overcome (Accessed: 15 May 2024).
6. Burke E., Gunness K., Cooper C. and Cozad M., People's Liberation Army Operational Concepts, RAND Corporatio, Research Report 2020, p. 14-16. [online] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394- 1/RAND_RRA394-1.pdf (Accessed: 11 April 2024).
7. Darczewska, J., (2016) Russia's armed forces on the information war front Strategic documents, OSW Studies [online] Available at: https://www.ceeol.com/search/book-detail?id=552459 (Accessed: 14 April 2024).
8. Dykyi E., Kharchenko S., (2016) *Hibridinis Rusijos karas: Ukrainos patirtis Baltijos šalims,* Generolo Jono Žemaičio Lietuvos karo akademija, ISBN 978-609-8074-47.
9. Ekman, I., Nilsson, P., (2023) Ukraine's Information Front Strategic Communication during Russia's Full-Scale Invasion of Ukraine, [online] Available at: foi.se/rest-api/report/FOI-R--5451--SE (Accessed: 15 April 2024).
10. EU Commission, (2024) [online] Available at: https://ec.europa.eu/commission/presscorner/detail/es/speech_24_1186 (Accessed: 15 April 2024).
11. Europarliament, (2022) [online] Available at: https://www.europarl.europa.eu/news/en/press-room/20231204IPR15648/green-deal-agreement-on-reform-of-eu-gas-and-hydrogen-market-governance (Accessed: 16 April 2024).
12. Fard, M. A., Hatami, M., Azadbakht, F. 'The doctrine of the accumulation of events in resorting to legitimate defense', *International Law Review* [online] Available at https://www.cilamag.ir/article_704061.html?lang=en (Accessed 13 May 2024).
13. Fogt, M., (2021) 'Legal Challenges or "Gaps" by countering hybrid warfare – building resilience in jus ante bellum', *Southwestern Journal of International Law*, Vol. XXVII:1 [online] Available at: https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf (Accessed 14 May 2024).
14. Fridman, O. (2018) *Russian "Hybrid Warfare": Resurgence and Politicization* [online] Available at: http://www.studiapolitologiczne.pl/pdf-136135-64183?filename=OFER%20FRIEDMAN_%20Russian.pdf (Accessed: 3 May 2024).
15. Hartig, F., (2015) Communicating China to the World: Confucius Institutes and China's Strategic Narratives [online] Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-9256.12093 (Accessed: 15 April 2024).
16. Heather A. Conley, Mina J., Stefanov R., Vladimirov, M., (2016) *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Lanham: Rowman and Littlefield, 2016.
17. Hybrid CoE (2023) *Hybrid Threats* [online] Available at: https://www.hybridcoe.fi/hybrid-threats/ (Accessed: 04 May 2024).

18. Hoffman, F. G. (2009) 'Hybrid vs. Compound War: The Janus Choice: Defining Today's Multifaceted Conflict', *Armed Forces Journal* [online] Available at: http://armedforcesjournal.com/hybrid-vs-compound-war/ (Accessed: 13 May 2024).
19. Hutchinson, W., (2006) Information Warfare and Deception, Informing Science, Volume 9, 2006 Editor: Eli Cohen Edith Cowan University, Perth. Australia [online] Available at: https://www.inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf (Accesssed: 25 March 2024).
20. Intelligence Studies Review 07:5-26. [online] Available at: https://www.ceeol.com/search/article-detail?id=111178 (Accessed: 5 April 2024).
21. Kalenský J., Osadchuk, R., (2024) Hybrid CoE Research Report 11, How Ukraine fights Russian disinformation: Beehive vs mammoth, [online] Available at: 20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf (hybridcoe.fi) (Accesssed: 1 May 2024).
22. Kulakov, A., Yermolenko, V., Rybak V., (2018) Taming The Hydra: How To Resist Kremlin's Information Aggression, Recommendations For Information Policy. [online] Available at: Policy Paper_ENG.pdf - „Google" diskas (Accessed: 15 April 2024).
23. Le Guin, U., K., (2018) A Few Words to a Young Writer, [online] Available at: https://www.ursulakleguin.com/a-few-words-to-a-young-writer (Accessed: 15 April 2024).
24. Libicki, Martin C. (1995) What is information warfare? Center for Advanced Concepts and Technology Institute for National Strategic Studies, [online] Available at: What Is Information Warfare? (dtic.mil) (Accessed: 15 April 2024).
25. McCornack, S.A. (1997). The generation of deceptive messages: Laying the groundwork for a viable theory of interpersonal deception. In J.O. Greene (Ed.) Message Production: Advances in Communication Theory. Mahwah, NJ: Lawrence Erlbaum Associates (pp. 91-126)
26. Micevičiūtė, J. (2002) "Etikos pagrindimo problema postmoderniojoje kultūroje", Problemos, 61, pp. 18–32. doi:10.15388/Problemos.2002.61.6734. [online] Available at: https://www.journals.vu.lt/problemos/article/view/6734/4583 (Accessed: 10 April 2024).
27. Miskimmon., A., O'Loughlin., B. (2017) Vol 5, No 3 (2017): Narratives of Global Order Russia's Narratives of Global Order: Great Power Legacies in a Polycentric World [online] Available at: https://www.cogitatiopress.com/politicsandgovernance/article/view/1017 /631 (Accessed: 11 April 2024).
28. Molander, R. C., Riddile, A. S., Wilson, P. A., (1996) "Strategic Information Warfare: A New Face of War," Parameters 26, no. 3, doi:10.55540/0031-1723.1794.
29. *National Security Council Directive on Office of Special Projects.* (1948) [online] Available at: https://history.state.gov/historicaldocuments/frus1945-50Intel/d292?fbclid=IwAR3wSAcQ8n7IgCExlaTd-0QoHvqhW5vntjQ2CDlX9BB0p4EXxoBOlmGxous (Accesssed: 21 May 2024).
30. NATO (2005) Information warfare [online] Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (Accessed: 5 April 2024).
31. NATO (2010) *Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, 25 August 2010 [online] Available at:

https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (Accessed 12 May 2024).

32. NATO (2014) *Wales NATO Summit Communique*, 4 September 2014 [online] Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en (Accesssed: 13 May 2024)
33. NATO (2015) Standard AJP-3.10 Allied Joint Doctrine For Information Operations Edition A Version 1 December 2015, [online] Available at: NATO-IO.pdf (publicintelligence.net) (Accessed: 15 April 2024).
34. Prytherch, R. (2016). *Harrod's Librarians' Glossary and Reference Book* (0 ed.). Routledge. [online] Available at: https://doi.org/10.4324/9781315586243 (Accessed: 1 April 2024).
35. Roszak, T. (1994). The Cult of Information. A neo-Luddite treatise on high-tech, artifi-cial intelligence, and the true art of thinking. Seconded. Berkley and Los Angeles: University of California Press. ISBN 0520085841
36. Rzevski, G., (2023) The Future is Digital: How Complexity and Artificial Intelligence will Shape Our Lives and Work 1st ed. 2023, Springer, ISBN-10 3031378091.
37. Stonkienė, M. (2006) "Theoretical definition of information law in the context of knowledge society: two identities of information law". Informacijos mokslai 39:93-102. [online] Available at: https://www.ceeol.com/search/article-detail?id=49713 (Accessed: 15 April 2024).
38. Strategic Thinking on the Three Warfare, The Jamestown Foundation, August 2016, Vol. 16, issue 13. [online] Available at: https://jamestown.org/program/the-plas-lateststrategic-thinking-on-the-three-warfares (Accessed: 15 April 2024).
39. Tackling foreign information manipulation and interference together (2023) [online] Available at: https://www.eeas.europa.eu/delegations/united-kingdom/tackling-foreign-information-manipulation-and-interference-together_en?s=3225 (Accessed: 15 April 2024).
40. Tallin Manual, The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub [online] Available at: https://ccdcoe.org/research/tallinn-manual/ (Accessed: 15 April 2024).
41. Trends in the Contemporary Information Environment, Hybrid CoE Trend Report 4 (2020) [online] Available at: Hybrid-CoE-Trend-Report-4.pdf (hybridcoe.fi) (Accessed: 5 April 2024).
42. *United Nations Charter* [online] Available at: https://www.un.org/en/about-us/un-charter (Accessed: 05 April 2024).
43. UN (2021) Developments in the field of information and telecommunications in the context of international security, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security [online] Available at: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf (Accessed: 05 April 2024).
44. Vasiliauskienė, V., Stumbrys, V., (2023) Problematic aspects of the legal definition of hybrid warfare Visuomenės saugumas ir viešoji tvarka, [online] Available at: https://vb.mruni.eu/object/elaba:170364501/170364501.pdf (Accessed: 14 April 2024).
45. Verbytska, L., Babii, I., Botvyn, T., Konivitska, T., Khlypavka, H., (2023) The language education and the language component as an element of countering hybrid threats in Ukraine, Multidisciplinary Science Journal 5:2023ss0504 [online] Available at:

https://www.researchgate.net/publication/375357795_The_language_education_and_the_language_component_as_an_element_of_countering_hybrid_threats_in_Ukraine (Accessed: 15 April 2024).

46. Wagnsson, C., Barzanje, C., (2021) A framework for analysing antagonistic narrative strategies: A Russian tale of Swedish decline, Media, War & Conflict 2021, Vol. 14(2) 239–257 [online] Available at https://journals.sagepub.com/doi/pdf/10.1177/1750635219884343 (Accessed: 17 April 2024).
47. Watters, C. (1992). *Dictionary of Information Science and Technology*. Academic Press. [online] Available at https://books.google.lt/books?id=NzeDW6GdHuEC&lpg=PP1&ots=tft0DYOHuj&dq=Watters%2C%20C.%20(1992).%20Dictionary%20of%20Information%20Science%20and%20Technology.%20Academic%20Press.&lr&pg=PP1#v=onepage&q=Watters,%20C.%20(1992).%20Dictionary%20of%20Information%20Science%20and%20Technology.%20Academic%20Press.&f=false (Accessed: 17 April 2024).
48. Wigell, M. (2019) 'Hybrid Interference as a Wedge Strategy', *International Affairs* 95, no. 2: 255–275, [online] Available at: https://www.researchgate.net/publication/330957623_Hybrid_Interference_as_a_Wedge_Strategy_A_Theory_of_External_Interference_in_Liberal_Democracy (Accessed: 28 March 2024).
49. Wigell, M. (2021) 'Democratic Deterrence: How to Dissuade Hybrid Interference', *The Washington Quarterly* [online] Available at: https://www.tandfonline.com/doi/full/10.1080/0163660X.2021.1893027 (Accessed: 15 May 2024).
50. Wilson, G., (2022) Information Warfare: what is it, and why should we care? [online] Available at: https://cove.army.gov.au/article/information-warfare-what-it-and-why-should-we-care-0 (Accessed: 16 April 2024).
51. 15min, (2024) Minskas paskleidė melą, kad iš Lietuvos bandyta atakuoti dronais [online] Available at: https://www.15min.lt/naujiena/aktualu/lietuva/minskas-paskleide-mela-kad-is-lietuvos-bandyta-atakuoti-dronais-56-2230982?utm_medium=copied (Accessed: 26 April 2024).