Shay Attias[1]

Home Front Resilience, Civilian Consciousness and Information Protection in the Hybrid Digital Age

Rather than focusing on the known "hard" power, this chapter offers to examine the nonviolent face of digital hybrid warfare and focuses on the home front's growing re-emergence in the digital age. Under the new media's technological capabilities, the civilian front is under constant 24/7 digital attack against their most important "currency" of our digital-information age: their "consciousness" and the "information" they must consume. Today, the "ordinary" citizens are organised worldwide through "peer-to-peer networks" that consume, produce and spread information in a way that humankind did not know before. Therefore, the fear of harm and greater fragility than in previous eras rises in the hybrid era in which the outside is mixed with the inside, blurring boundaries between the "real" and the "virtual" and "domestic" and "external", which all coalesced into one dimension. The civilian front of every country is under attack, even if not during a declared "war". In contrast to older times, today's citizens know a greater power to exert pressure on the decision-makers and the military. Thus, while utilising Russia's test case, this textbook chapter sheds light on the importance of strengthening the digital consciousness of citizens in the hybrid era in which "war" is becoming increasingly constant, vague and very difficult to define. My conclusions will benefit both the bodies entrusted with strengthening "national resilience" and contribute to the military practitioners involved in the field of diplomacy and consciousness. In addition, it will allow policymakers to understand the greatness of the challenge. "The fear of harm and greater fragility than in previous eras rises in the hybrid era in which the outside is mixed with the inside, blurring boundaries between the "real" and the "virtual" and "domestic" and "external", which all coalesced into one."[2] Since the beginning of the 2000s, more and more voices have been heard among

[1] Bar-Ilan University.

[2] Wassermann 2018: 16.

DOI: https://doi.org/10.36250/01236_11

military practitioners and war studies scholars who refer to the current ongoing wars and conflicts as belonging to a "new" era entitled "hybrid warfare", but is it a new concept? "Hybrid warfare", in the contemporary era, became increasingly popular in policy debates following two critical developments. First, in 2005, two U.S. military officials wrote about the "rise of hybrid wars" and emphasised the combination of conventional and unconventional strategies, methods and tactics in contemporary warfare and the psychological or information-related aspects of modern conflicts.[3] Second, Russia invaded Crimea in 2014 and achieved its objectives by conflating "deniable" special forces, local armed actors, economic clout, disinformation and exploiting socio-political polarisation in Ukraine. Hybrid warfare remains a contested concept, and no universally agreed definition exists. It has been criticised for lacking conceptual clarity, being merely a catch-all phrase or a buzzword, and not bringing anything distinctly new to policy debates. Nevertheless, the concept furnishes critical insights into contemporary and future security and defence challenges.[4] However, before this chapter deals thoroughly with this critical question, we suggest a more needed evolutionary perspective. Instead of looking only at this question, we will delve deeper into the changes that have taken place in the international digital arena and the way interactions are made or become "hybrid", which requires a profound rethinking. First, the core of this chapter will not focus on changing military tactics of "command and control". However, it will emphasise the importance of the increasingly double-edged sword: the rising global and local need for information consumption and production by the "home front", and becoming a more convenient target for manipulations, disinformation, and fake news which according to Iranian agents in Israel, can lead to "Dystopia". In other words, as the dependence on information gluttony increases, so will the weakness and fragility of the "civil world" to defend itself against the defacement of its consciousness by the enemy's army. Second, this guiding textbook piece is to demonstrate and explore more about the complicated "military–society relations during the war in the digital hybrid age". This matter has become a major strategic issue discussed thoroughly in every command headquarters in modern armies. However, there have never been so many psychological and information technology available tools to re-engineer the enemy's and public's minds and hearts as today. Yes, the use of propaganda is ancient, but social media and other digital faking tools

[3] Hoffman 2007: 8.

[4] Weissman 2019; Hourcade et al. 2006.

enable unprecedented capabilities. Therefore, the civilian element, the “soft underbelly” of every country and its army is now at the forefront of the war for consciousness, which has many faces.

Soft war and home front

All ancient-historical, modern and now so-called “hybrid” war contains two essential components: one, a “hard” brutal element which is the bayonet, the sword, the rifle or the tank that fires, and another one, a “soft” one uncovered in the “nonviolent” face of war, which has been previously known as psychology warfare or more recently, consciousness re-engineering. The “soft” world of consciousness and the “nonviolent side” of wars clearly indicate a fast notice of the essential “currency” of our digital age: “information” has dramatically changed. Not for nothing, policymakers and commanders named the rush for information “the blood life”, which every government and army desired to control. The mass media revolution at the beginning of the last century and, since its end, the global media revolution and the rise of global news networks known as the “CNN effect”[5] have both increased the demand for information and decreased the ability to control it. Nevertheless, since the Millennium, social media giants have broken into our lives and created abundant faces for information technology, making it a different level to explore. Since the social-digital age, the international arena has enabled far-reaching digital capabilities to be created. Above all, the simple and fast way of global interactions has made our world much more global and flatter. With these digital changes, human wars, which also include significant struggles in “soft power” areas, are affected[6] by the ability to communicate with any person at any point in the world, wholly erasing the element of space and time. Now, the “ordinary citizens” know much more about what is happening and consume information about their country and others beyond physical borders, bypassing almost every obstacle. New technological capabilities allow a two-way communication and multi-dimensional feedback to governmental or military entities. Citizens worldwide demand to know more consistently, and they use social and traditional media to generate intense international pressure that can bring the country to change its policy. This “power shift” to the citizens over

[5] Jakobsen 2000.

[6] Bjola–Holmes 2015; Adesina 2017; Attias 2012; Hallams 2010.

states is connected to an ideological revolution of "global citizenship" or "cosmopolitanism" and the "power transition" concepts.[7] Both theories lie in the thought that citizens can have a universal influence without national affiliation and promote common goals. Adding to their new social media capabilities, they were later called "digital civic networks" or "peer-to-peer networks". In other words, two trends here affect a third one: conceptual and technological, which have come together and created a kind of "mutation" of digital citizens formed as global networks that create a challenging "front" to any army that tries to defeat its opponent. These human networks can influence armies and countries before, during and after the war. They consume astronomical amounts of information and react so quickly that sometimes they are ahead of politicians or even army commanders during conflicts. Oxymoronically, the more information consumed by the citizens of our digital age world, the more vulnerable they become to misinformation. However, not only do the citizens become more sensitive but also armies and state bodies invest more and more money and effort in public diplomacy to improve "how the world sees them" and "what others think of them"; "which story they tell the world"; and how much "legitimisation" do they have for their military activities. Therefore, the social media age contains much more mental and psychological elements than before, which only amplifies the complexity of the relationship between society and the armed forces. The so-called "home front" or "civilian front" are definitions that include the totality of all actions involving civilians during wartime. World War II was a much more "total war" than its predecessors in that the defence of the home front became as important as the offensive military power or the ability to create coalitions and alliances during a world war.[8] Slowly, more and more governments began to understand the great importance of the civilian front and, since then, began to establish more units and bodies responsible for the "national resilience" of the country's citizens in times of war. With the thinking adopted to achieve "maximum civilian protection", experts and scholars began to understand that the civilian front differs from the military and includes much more psychological, communicative and cognitive elements than those in the military field. Looking through the citizen's prism, during an emergency of a war, citizens have a double challenge: on the one hand, the army of their country asks for their "national resilience" in order to support the continuation of the fighting until the goals are achieved, and on the other hand, the citizens

[7] Chan 2007; Nye 2010.

[8] Storey–Kay 2017.

are subjected to psychological and informational attacks that range from ancient psychological warfare to sophisticated digital methods that are available today: public diplomacy, fake news, fake social media accounts, interfering in elections, harming the nation's legitimacy and reputation, activation and creation of protests within the citizens of the rival country and more.[9] Special attention must be given to the fake news industry, which has vastly grown and has become more sophisticated and challenging to detect. The military is forced to act increasingly in the arena of consciousness so that the enemy does not damage national resilience and spread harmful rumours. While in the previous ages of modern war (particularly in WW2), civilians were required to nationalise their products and help provide eggs, clothes and cars to the army, in the hybrid digital era, they are asked to carry out unclear orders such as "protect the mind", and "do not believe fake news", help to strengthen the national and army's legitimacy and more recent requests that are hard to understand and measure. The already known principle that war causes severe disruption in the functioning of the "home" has been redesigned into a disruption in the consciousness that is waged 365 days a year and sometimes even several times in a minute.[10] Therefore, in the digital age in which most of the world is connected to almost any source of information, the civilian front becomes constantly threatened at any given moment. On the other hand, at any given moment, any citizen can consume false information. Another change that probably pinpointed the digital hybrid era is the final blurring boundaries between the "real" and the "virtual" and "domestic" and "external", which all coalesced into one dimension.[11] Hence, and since the last decade, it is not surprising that the concept of national security has changed and evolved into more non-typical military and nonviolent topics in recent years.

National security in the age of heredity

Before the digital age, national security was defined using mainly military concepts.[12] The relationship between the traditional national security concept and the army's operational concept was based on three legs: deterrence, warning and decision. Over the years, the concept was adapted to the security challenges that

[9] Monsees 2020; Haigh et al. 2019.

[10] Bachmann et al. 2020.

[11] Jordan 2009.

[12] Lebel 2010.

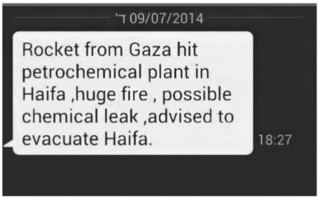
developed following the attacks on the home front using long-range weapons and suicide terrorism, and the fourth leg – defence (or defensiveness) – was explicitly defined. Over the years, defence has gradually taken an increasingly central place in security concepts because the home front has become the enemy's main front of action trying to harm the civilian population in various ways.[13] This "old–new" situation has emerged in which the readiness of the home front plays a decisive role in the decision-making process: the more heightened readiness of the home front, the greater the flexibility of the decision-making process in the activation of the military response. That is why this issue was defined as one of the defensive efforts of many armies. For example, the Israel Defense Forces announced that the intelligence assessments state that "widespread shooting against the civilian population will be a central tool in shaping the future characteristics of the next war". At the same time, the importance of preparing the home front against a missile and rocket attack to save lives remains the same. The "quality of the functioning of the civilian" becomes more critical in building natural resilience. One concept that describes this cruciality, "Casualty Panic", has recently impacted military policy, mainly "in liberal democratic states". With the growing public opinion and social media, the hesitation to enter into military engagements for fear of incurring casualties is a consequence of "moral panic" among the political and military leadership. This concept draws a solid and active connection between civil and military relationships through "Casualty Panic", which can influence military strategy and tactics.[14] But as for all the world countries, "hard power" threat is not the only one for Israelis or for other nations. One of the many examples was in 2014 when, as part of Hamas's efforts to sow panic and fear, threatening text messages[15] were sent with false information about a rocket hitting the petrochemical plant in Haifa and the death of dozens of Israelis. In what appears to be part of Hamas's psychological warfare efforts, the message reads in English: "Now: 25 Israelis have been killed by a missile strike in Haifa"; "a rocket from Gaza hit the petrochemical plant in Haifa"; "large fire, a possibility of a chemical leak, it is recommended to evacuate Haifa".[16]

[13] For example, in the "low intensity conflict" and army operations over the years, the residents of the State of Israel were subjected to a heavy and prolonged attack of rockets and missiles. According to the IDF's attribution threat, in a future conflict thousands of missiles are expected to be fired at the civilian home of the State of Israel by hostile countries and elements for several days to weeks.

[14] Lebel 2010: 183.

[15] Orpaz – Siman-Tov 2021.

[16] Bender 2014.



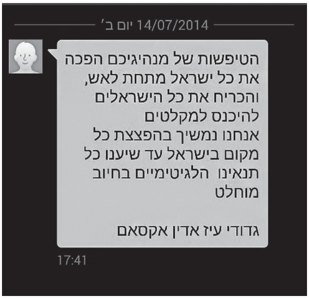
09/07/2014 ד'

Rocket from Gaza hit petrochemical plant in Haifa ,huge fire , possible chemical leak ,advised to evacuate Haifa.

18:27

Figure 1: Fake Hamas message (originally in English) claims Haifa chemical plant hit by Gaza rocket

Source: Bender 2014



14/07/2014 יום ב'

הטיפשות של מנהיגיכם הפכה
את כל ישראל מתחת לאש,
והכריח את כל הישראלים
להיכנס למקלטים
אנחנו נמשיך בהפצצת כל
מקום בישראל עד שיענו כל
תנאינו הלגיטימיים בחיוב
מוחלט

גדודי עיז אדין אקסאם

17:41

Figure 2: Fake Hamas message (originally in Hebrew):

“ישראל מתחת לאש, והכריח את כל הישראלים להיכנס למקלטים. אנחנו נמשיך בהפצצת כל מקום בישראל עד שיענו כל
תנאינו הלגיטימיים בחיוב מוחלט. גדודי עיז אדין אקסאם” (השגיאות במקור)”

In English:

“The foolishness of your leaders has put all of Israel under fire, forcing all Israelis into shelters. We will continue bombing every place in Israel until all of our legitimate demands are fully met. Izz ad-Din al-Qassam Brigades” (original errors retained).

Source: Ynet 2014

That was not the first time that Hamas has sent messages to Israelis to sow fear and panic in the public. Messages of this type were sent during the “Pillar of Cloud” operation initiated by the IDF against Hamas in November 2012. The terrorist organisation then sent similar messages to Israeli citizens, with the aim of threatening the civilian population and disrupting their daily lives. Even if the Hebrew language skills of Hamas agents remain poor, it seems that the technological capabilities of the organisation have improved. The text messages sent in the “Pillar of Cloud” operation were from random cell phone numbers, their content was fragmented, they were written in unintelligible Hebrew and were sent to the Western and Southern Negev regions. The level of sophistication of Hamas has increased and to increase their credibility and create fear among tourists, the messages were sent in English, all over Israel, using the number of the "Haaretz" newspaper. We can draw two significant conclusions from these hybrid changes: Firstly, states face challenges in controlling information and shaping narratives, thereby impacting the legitimacy of their actions. Secondly, the effectiveness of lethal force strategies in achieving strategic goals is weakened. It is important to acknowledge that the use of lethal force often carries political consequences for state armies, leading many to avoid such measures. Consequently, in addition to the aspiration to develop non-military tools of influence encompassing ideology, culture and economics, the concept of "soft power" has gained prominence in the West. It serves as the foundation for the security and foreign policies of numerous powers and countries. The concept of "soft power" refers to the ability to persuade others to act as you wish without using physical force and was based on the use of non-lethal resources and abilities, such as: economic, legal, diplomatic, cultural and ideological.[17] The components of "national power" encompass diplomacy, information, military and economic factors. While the military is typically considered a measure of last resort, particularly in Western democracies, the United States military has consistently played a crucial role in various aspects of soft power. This includes advancing democracy and strengthening partner nations through military-to-military relationships. These cooperative efforts are manifested through bilateral and trilateral exercises, which aim to support established Operation Plans, NATO, the United Nations and Theater Security Cooperation. Through active engagement in these activities, the U.S. military significantly contributes to the promotion of global stability and security. Through these efforts, among others, the U.S. military helps to carry out the diplomatic mission of the United States (military diplomacy paved the way for NATO, the European Union, and the World Trade Organization, for instance).[18] In the context of military-diplomatic matters, when military units engage in bilateral or multilateral exercises with other countries, there are multiple objectives at play. These exercises aim to enhance interoperability between the participating militaries, foster cultural exchange and understanding, and provide an opportunity to develop and test capabilities in the context of potential contingencies. The significance of military diplomacy

[17] Nye 1990.

[18] Ebitz 2019.

in foreign engagements lies in its ability to establish dialogue that can facilitate ongoing communication and, importantly, prevent misunderstandings between different cultures during times of crisis. By engaging in these activities, nations can strengthen their relationships and promote clearer communication channels, thus enhancing overall international cooperation. Moreover, in places where the U.S. military has maintained a long-term presence (e.g. Japan, South Korea, Germany), we see that military interoperability enhances regions economically – directly through commercial contracting and the resulting employment, service member contributions through commerce, and in some cases, contributions of military gear and equipment through foreign military sales or otherwise.[19] In the era of hybrid digital warfare, the dissemination of false information poses a significant threat, potentially leading to paralysis in safeguarding the civilian home front. Consequently, it becomes crucial for armies to foster strong multinational cooperation with other nations to effectively counter this threat. One essential component is the establishment of a capable Home Front Command, responsible for managing, disseminating and protecting critical information during times of combat and emergencies. The primary objective is to enhance national resilience by providing reliable information, a sought-after goal for any hybrid attack. Additionally, the Home Front Command aims to save lives by preparing the civilian population for the possibility of conflict, providing support during rescue operations and advocating for the protection of the home front. Furthermore, post-conflict, the Command assists in the swift rehabilitation of the civilian home front, contributing to its recovery and stability. During ordinary times, the Home Front Command plays a crucial role in providing guidance to the population on emergency protocols. It coordinates with local authorities, government ministries and infrastructure entities to ensure their effective response in civil defence emergencies. In times of crisis, the Home Front Command activates the rescue and recovery system, issues warnings to residents in the face of imminent threats, provides instructions on how to respond and assists local authorities and government ministries in carrying out their emergency civil defence duties. Ultimately, the responsibility for individual and family preparedness in emergencies lies with the citizens themselves. It is vital for them to access and consume reliable and accurate information. The "hybrid" nature of ambiguity and deniability, which can potentially be exploited by certain actors like Russia, poses a risk of reaching the threshold of Article 5 without actually triggering it. This situation has the potential to disrupt institutional and

[19] Gilman et al. 2014.

political mechanisms of collective defence. The ‘hybrid’ qualities of ambiguity and deniability – which, it is feared, would be manipulated by Russia to come close to the “Article 5” threshold but never reaching it – can paralyse the institutional and political mechanisms of collective defence.[20] Therefore, due to the lack of a universally agreed-upon definition of hybrid aggression, any discussion on this matter within the North Atlantic Council would be highly politicised, time-consuming and subjective. Even if there were a more precise and formalised specification of an automatic trigger for a collective response, such as the suggestion by former NATO SACEUR Phillip Breedlove of attributing “infiltration of foreign forces on sovereign territory” to account for instances like the presence of unidentified troops (referred to as “little green men”), it would not necessarily resolve the problem. In fact, the clearer the threshold, the easier it becomes for Russia or any other potential aggressor to tailor their actions to stay just below it. Recognising these gaps in Article 5, which could be exploited by hybrid aggressors and lack obvious solutions, NATO leaders in Warsaw assigned the primary responsibility for protection against hybrid threats to individual member states. However, the final Communique also emphasised that the Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence; and “the Council could decide to invoke Article 5”.[21]

National resilience

Improving resilience against the exploitation of Western societies by politically competing or potentially hostile actors is a crucial aspect that needs to be addressed. While it is evident that Russia is involved in such activities, including propaganda, funding populist parties across the political spectrum, and undermining established governing institutions and actors, the challenge lies in determining how to effectively respond. Below are some potential approaches to enhancing resilience:

1. Strengthening democratic institutions: Focus on reinforcing the transparency, accountability and integrity of democratic institutions. This includes promoting strong electoral systems, combating corruption and ensuring independent media.

[20] NATO 2023.

[21] NATO 2023.

2. Enhancing digital literacy: Invest in educating the public about critical thinking, media literacy and online security. By fostering a population equipped with the skills to discern reliable information from disinformation, societies can become more resilient to manipulative tactics.
3. Promoting social cohesion: Foster inclusive societies that value diversity and promote social cohesion. By building strong community bonds and promoting dialogue across different social and political groups, societies can mitigate divisions that can be exploited by external actors.
4. Strengthening cybersecurity: Recognise the importance of robust cybersecurity measures to protect critical infrastructure, government systems and private data. Enhancing cybersecurity capabilities and fostering cooperation among governments, the private sector and civil society is vital in countering hybrid threats.
5. International cooperation: Foster collaboration among like-minded nations to share best practices, intelligence and lessons learned in countering hybrid threats. By working together, countries can build a united front against actors seeking to exploit vulnerabilities.

Addressing the question of what should be resilient, defended, protected and strengthened in Western societies is a highly political matter that requires careful consideration. It is crucial not to leave these decisions solely in the hands of security or military experts, or to be driven by the logic of warfare.

While some argue for approaches such as strengthening national resilience around homogenous ethnic communities or resorting to economic nationalism and protectionism to address challenges posed by Russia, these strategies do not provide comprehensive security for Western societies. In fact, they often exacerbate political contestation and inadvertently play into the strengths of aspiring Great Powers like Russia. A more effective strategy lies in bolstering the resilience of liberal modes of government and societal organisation, rooted in democratic principles, fundamental rights, the rule of law and economic openness. It is important to draw from the lessons learned through successful domestication of foreign policy within the EU and its member states when seeking to protect perceived interests and confront hybrid threats. Discussions surrounding the European Global Strategy and EU foreign policy emphasise the significance of upholding a rules-based international order that supports values-based multilateral actors, moving beyond a narrow pursuit of self-interests or reverting to power politics. It is essential to navigate the changing geopolitical landscape while maintaining the resilience of this approach, particularly in the face of hybrid threats and challenges. Moreover, media plays a vital role in building resilience. Cultivating a diverse and independent media landscape that promotes accuracy, reliability, critical thinking and media literacy is crucial. Media outlets should uphold democratic values, provide platforms for informed public discourse and actively counter disinformation campaigns. Investing in media resilience contributes significantly to the overall resilience of societies in countering hybrid threats.[22] Resilience is mainly about how states and societies resist collapse due to disastrous events. They must cope and deal with such events, adapt to them and recover from their effects in a short period. Post-facto resilience is only possible if the state and the society can anticipate the potential consequences of a series of events, be it man-made, a natural disaster, or an external challenge, like a crisis or war. Consequently, resilience is contextual; it has many forms depending upon the informational context.[23] Resilience has much to do with state capacity, governance and cohesion, and thus the support of society for its state institutions and leaders. Hence, it would be easy to conclude that so many factors contribute to resilience that it would be best to identify the concept with good governance. However, this would be a gross simplification as resilience must be developed in anticipation of scenarios that are likely to occur. This harks back to resilience in those areas from whence the challenge comes. This is not very easy to the perceptional foundations of analysis, including those problems that are of low likelihood. However, the exceptionally high risk (e.g. a nuclear attack or a significant reactor accident) cannot be ignored. No state has unlimited resources. Hence, the priority areas must be backed by resource allocation. It also may be easier said than done as there is rivalry for resources on the national agenda. Furthermore, due to various factors, some states – irrespective of their national efforts – cannot become resilient against specific concentrated, high-intensity challenges. In many cases, the public relies on a combination of formal and informal information sources, with social media often playing a role in sharing links from government websites that are deemed helpful to communities. This process not only acts as a filter for information but also amplifies the dissemination of "official" information. This chapter explores how social media, leveraging its strengths in timely information exchange and connectivity, can serve as a source of psychological first aid during the early stages of a disaster and contribute

[22] Dunay–Roloff 2017.

[23] Humprecht et al. 2020; DeWit et al. 2020.

to community resilience. A robust and healthy media landscape demonstrates resilience and adaptability to the dynamic and ever-changing social, political and economic conditions within its context. In functioning democracies, both state and non-state actors rely on strong, independent and sustainable media organisations to access reliable news and information services. These organisations also play a critical role in facilitating open debate and dialogue among various stakeholders. By upholding the principles of independence and sustainability, the media can effectively respond to the needs of the society it serves. This entails remaining responsive to the evolving media landscape and adapting to new technologies and communication channels. A resilient media landscape is one that can effectively navigate the complexities of its environment, ensuring the availability of credible information and fostering an environment conducive to open discussions and informed decision-making.[24] Recent studies keep showing more and more that social media has become a primary instrument of hybrid warfare to shape public opinion and to see its impact on different bodies of state.[25] The 21st century dawned alongside an emerging form of warfare that, in its nature and character, is remarkably diverse and whose scope extends beyond conventional elements of war. In polarised political environments, citizens are confronted with different deviating representations of reality, making it increasingly difficult to distinguish between false and correct information. Thus, *societal polarisation* is likely to decrease resilience to online disinformation. Moreover, research has shown that *populism* and partisan disinformation share a binary Manichaean worldview, comprising anti-elitism, mistrust of expert knowledge and a belief in conspiracy theories. Due to these combined influences, citizens can obtain inaccurate perceptions of reality. Thus, online users are exposed to more disinformation in environments with high levels of populist communication.[26] Previous research has consistently highlighted the crucial role of trust in news media as a determining factor for resilience against online disinformation. When there is a higher level of distrust in news media, individuals tend to be less exposed to diverse sources of political information and are less likely to critically evaluate the information they encounter. Furthermore, people's level of knowledge about public affairs plays a significant role in their ability to navigate online disinformation. Studies have shown that countries with strong public

[24] Hook–Verdeja 2022.

[25] Svetoka 2016; Ducaru 2016.

[26] Humprecht et al. 2020.

service media tend to have citizens with higher knowledge levels compared to countries where public service media is marginalised or weakened. Consequently, it can be inferred that environments with weakened public broadcasting services (PBS) are less resilient in the face of online disinformation. Trust in news media and individuals' knowledge about public affairs are closely intertwined with resilience to online disinformation. When trust is diminished, individuals are less inclined to seek out diverse information sources and critically analyse the information they come across. Moreover, the erosion of public service media environments can undermine citizens' knowledge levels and further exacerbate vulnerability to online disinformation.[27]

Increasing global synergies and awareness

As the focus is on improving awareness, it is proposed to establish dedicated mechanisms to exchange information with Member States and to coordinate the EU's capacity to deliver strategic communications. An EU Hybrid Fusion Cell within the EU Intelligence and Situation Centre[28] of the European External Action Service (EEAS) will offer a single focus for the analysis of external aspects of hybrid threats. The Fusion Cell will receive, analyse and share classified and open-source information from different stakeholders within the EEAS, the Commission and Member States specifically relating to indicators and warnings concerning hybrid threats. In liaison with relevant bodies at the EU and at national level, the Fusion Cell would analyse external aspects of hybrid threats, affecting the EU and its neighbourhood, to rapidly analyse relevant incidents and inform the EU's strategic decision-making processes, including by providing inputs to the security risk assessments carried out at EU level. The Cell would enhance awareness and provide inputs to security risk assessment processes which support policymaking at national and EU levels.[29] As announced in the European Agenda on Security, the Commission facilitates common assessments of security risks in a variety of policy areas like transport security (in particular aviation), anti-money laundering and terrorism financing,

[27] Humprecht et al. 2020.

[28] Voronova–Bakowski 2022.

[29] Davies 2021.

border control, etc. One notable example of a significant initiative in countering various threats, including disinformation, is the establishment of "The Joint Framework Program".[30] Introduced on 6 April 2016, this program outlines proposals aimed at building resilience in key areas such as cybersecurity, critical infrastructure protection, combating illicit use of the financial system and addressing violent extremism and radicalisation. A crucial initial step in implementing these proposals involves the EU and its Member States adopting agreed strategies and fully implementing existing legislation. This ensures a coordinated and unified approach towards enhancing resilience against these threats. Moreover, concrete proposals have been put forward to further strengthen these efforts, indicating a commitment to continuous improvement and adaptation. While the Joint Framework Program is primarily focused on addressing the complex challenges posed by hybrid threats, it is pertinent to recognise that EU action extends beyond the mere countering of hybrid threats. The program's ambit encompasses a wider range of objectives, showcasing the EU's comprehensive approach to safeguarding its member states and societies from an extensive array of risks and challenges. By encompassing domains such as cybersecurity, critical infrastructure protection, financial system integrity and counter extremism, the Joint Framework Program exemplifies a multifaceted approach to resilience-building. This proactive stance underscores the EU's unwavering commitment to effectively confront not only disinformation but also other pressing threats that possess the capacity to undermine security, stability and societal well-being. These joint assessments at EU level provide a comprehensive analysis of the threats, consequences and vulnerabilities to support policymaking with a view to mitigate the risks. The Commission facilitates these processes with the participation of Member States' experts and other EU services. The assessments of hybrid threats, produced by the EU Hybrid Fusion Cell, will provide relevant input to feed risk assessments at the EU and national levels.[31] Critical vulnerabilities may differ from Member State to Member State, as do levels of protection ensured nationally. Nonetheless, there exist numerous sectors characterised by a significant reliance on critical services, rendering countries and societies particularly vulnerable to hybrid threats. These sectors encompass energy security and supply, space

[30] European Commission 2016.

[31] Kert-Saint Aubyn 2016.

infrastructure, maritime security, public health, transportation (including aviation, maritime and rail), cybersecurity, communications and financial systems. Hybrid threats have the capacity to exploit vulnerabilities within societies, thereby posing challenges to fundamental values and liberties or targeting marginalised groups. Adopting a comprehensive and interconnected approach to counter hybrid threats can bolster the security and resilience of each of these sectors. By adopting a "joined-up" strategy, these sectors can enhance their ability to withstand and mitigate the impacts of hybrid threats, promoting overall security and societal well-being.

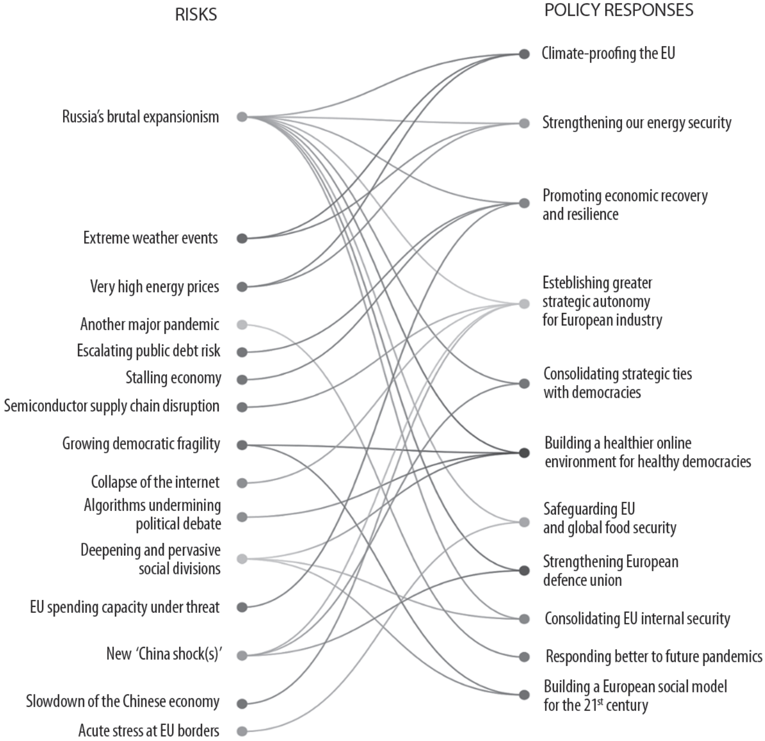

RISKS
POLICY RESPONSES
Russia's brutal expansionism
Extreme weather events
Very high energy prices
Another major pandemic
Escalating public debt risk
Stalling economy
Semiconductor supply chain disruption
Growing democratic fragility
Collapse of the internet
Algorithms undermining political debate
Deepening and pervasive social divisions
EU spending capacity under threat
New 'China shock(s)'
Slowdown of the Chinese economy
Acute stress at EU borders
Climate-proofing the EU
Strengthening our energy security
Promoting economic recovery and resilience
Esteblishing greater strategic autonomy for European industry
Consolidating strategic ties with democracies
Building a healthier online environment for healthy democracies
Safeguarding EU and global food security
Strengthening European defence union
Consolidating EU internal security
Responding better to future pandemics
Building a European social model for the 21st century

Figure 3: EU security landscape

Source: Voronova–Bakowski 2022

"In a rapidly changing and increasingly interconnected world, the EU security landscape has become very complex and unpredictable."[32]

What is the "mutual defence clause"[33] and is it relevant in this context? According to Article 42(7) of the Treaty of the European Union (TEU): "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations charter."[34] If multiple serious "hybrid threats" constitute armed aggression against an EU Member State, this mutual assistance clause could be invoked to provide an appropriate and timely response. It does not require Member States to take military action, but Member States are required to provide aid and assistance, providing that it shall not prejudice the specific character of the security and defence policy of certain Member States. However, the challenge is that many of the nonviolent hybrid threats are hard to define so can one demand to activate this article if its citizens were misinformed? Or had a special media attack by sophisticated bots?[35] One of the offered responses was "The IPCR arrangements"[36] that were adopted by the Council of the European Union on 25 June 2013 to reinforce the EU's ability to take rapid actions when facing major crises requiring a common response. The IPCR arrangements are flexible and scalable, enabling a tailored response and providing the necessary support from EU institutions and services in the context of a crisis and its evolution. They make full use of synergies between stakeholders and existing resources, structures and capabilities. They do not replace existing instruments and arrangements at sectorial level. The Commission and the EEAS contribute notably by producing regular Integrated Situational Awareness and Analysis (ISAA) reports to inform decision-making. IPCR has been activated by the Presidency of the Council for the first time in October 2015 to respond to the migration and refugee crisis. IPCR arrangements support the implementation of Article 222 of the Treaty on the Functioning the European Union.[37] Based on the IPCR, the EU will make best use of its cooperation with partner countries,

[32] Voronova–Bakowski 2022.

[33] Solidarity clause.

[34] See www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede200612mutualdefsolidarityclauses_/sede200612mutualdefsolidarityclauses_en.pdf

[35] Orabi et al. 2020.

[36] Council of the European Union 2016.

[37] Osula 2014.

including with its immediate neighbours, in countering hybrid threats. Through its external assistance, the EU will continue to strengthen its partners' national capacities in the fight against organised crime, terrorism and illegal trafficking, including in the field of border management. Further, the EU will pay specific attention to protection of critical infrastructure and develop actions to enhance cyber resilience which would ultimately contribute to countering hybrid threats in third countries. The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and "crisis prevention and response" to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation's decision-making process.[38] The actions proposed require cooperation and coordination of all relevant actors at EU and national level. Some of the proposed actions come under the responsibility of Member States, others require implementation by Member States. The EU can provide support and advice as required, including through best practices. The actions proposed in the Joint Frameworks and their implementations will be discussed in the Council of the European Union. The proposals will also be discussed by the European Parliament.[39] Private initiatives, such as specialised websites like Stopfake.org, have proven to be more effective in recognising disinformation compared to many public agencies. These initiatives relieve governments of the burden of building their own capacities. However, the number of private initiatives in this field remains limited. It is in the interest of NATO countries to systematically develop their private capacity by providing grants through the alliance and other international entities focused on security issues. Financial support should not be limited to public diplomacy but should also cover analysis. By building a network of experts, both NATO and individual allies can enhance their resilience to hybrid challenges. Hybrid warfare encompasses a range of activities and employs different instruments to destabilise societies by influencing their decision-making processes. To strengthen society against these threats, the author proposes the following actions:

1. Interference in electoral processes: Adversaries may employ various techniques, including media campaigns, social network manipulation and securing financial resources for favoured political groups, to influence election outcomes in their favour.

[38] NATO 2016.

[39] European Commission 2016.

2. Disinformation and false news: Adversaries can create and propagate a parallel reality by spreading false information, leading to social fragmentation. This disorientation makes it challenging for governments to garner public support for NATO policies or operations.
3. Cyberattacks: Adversaries can exert pressure on NATO governments by threatening with devastating cyberattacks targeted at civilian infrastructure such as hospitals, electricity grids, or water supplies. These attacks aim to discourage mutual assistance among NATO members during times of crisis.
4. Financial influence: Adversaries can exert long-term political pressure by making investments, establishing unfavourable energy supply agreements, or offering loans that render a country vulnerable to manipulation.

Addressing these challenges requires a comprehensive approach that involves countering disinformation, enhancing cybersecurity, and safeguarding financial and energy sectors. By taking proactive measures and strengthening societal resilience, NATO countries can effectively respond to hybrid threats and maintain their security and sovereignty.

Can public diplomacy help against hybrid warfare?

One available tool for any country is public diplomacy. Through transparency and open engagement, public diplomacy can counter the perception of government propaganda and bridge the trust gap. By demonstrating accountability, actively listening to public concerns and addressing them genuinely, public diplomacy can foster a sense of trust and credibility among the public. This, in turn, strengthens the effectiveness of public diplomacy in countering hybrid threats, as trust is crucial for the public to perceive and evaluate the information provided by governments. However, in the age of social media, the biggest problem of traditional public diplomacy was that, for years, it was perceived as government propaganda. Government information was treated with scepticism, as it was considered both inauthentic and unreliable. Governments would often say what they wanted people to believe, and never admitted any policy failure, thus affecting their credibility and making it hard for the public to believe them. Today, the world's citizens capture the power to administer information. People across the globe are increasingly connected. The internet is the common denominator that connects people of different cultures, languages and nations. The combination of endless social media platforms has created the phenomenon of so-called "peer-to-peer (P2P) diplomacy", also called Peer-2-Peer diplomacy.[40] Every citizen with direct internet access can receive news instantaneously and become an entire "walking news system", analysing information, commenting upon it and distributing it to their peers. As a result, governments want to harness new social media platforms to promote their policies and diplomatic efforts. Nevertheless, governments lack both resources (financial, human and structural) and credibility. However, it seems that there is still a role for governments to play in P2P diplomacy. Governments that can harness the communication potential of their citizens will be the ones to conduct effective public diplomacy offensives. Therefore, this new model of P2P public diplomacy consists of the public – meaning the citizens – not only carrying the message but, more importantly, shaping it.[41] Generally, governments are at a disadvantage when adapting to new media and technology. New media and technology move very quickly and change how people communicate, operate and live their lives. Governments, meanwhile, move slowly. While the big fish had a distinctive advantage in the old diplomacy model, the fast, adaptable fish had a clear advantage in the new public diplomacy model. The age in which we live promotes self-expression and enables unlimited technological capabilities. Therefore, the rise of "civilian power"[42] is not limited to the public diplomacy field; it is a multi-disciplinary phenomenon and hence, there are limitations and future challenges to effective diplomacy especially in this hybrid age in which it is most needed:

- The "civilianisation" of the government's public diplomacy platform has demands: legal, financial and bureaucratic changes must occur to collaborate with civilians and diasporas.
- The government must realise that it cannot control the message these people will carry; in other words, it must cede control and accept critical voices as part of the project.
- The government must reorganise this new relationship between the state and its citizens (not as a condition). The civilian society can empower the state, which maintains the relevance of the national state through mutual collaboration.

[40] Attias 2012.
[41] Jun Ayhan 2020.
[42] Clinton 2010.

– Public diplomacy efforts by the government can only be practical if they are based on civilian determination.[43]

Conclusion

The current management and regulation of social networks often facilitate the rapid spread of disinformation. While regulation falls outside NATO's jurisdiction, the alliance can advocate for sensible legislation that enhances the resilience of social networks against abuse. This can include measures to improve the identification of false profiles and strengthen penalties for hate speech. However, the most effective weapon against disinformation lies in professional journalism. NATO and its member states should invest more in investigative journalism to provide credible alternatives to false news. Surveys indicate that approximately 70% of media references to "hybrid threats" are inaccurate.[44] NATO can contribute by supporting the development of journalists' expertise in adequately covering and monitoring this issue. Educated and informed media serve as vital partners in raising social awareness and educating citizens about coping with various forms of hybrid pressures. NATO can provide training and lead campaigns to enhance awareness of hybrid challenges, thereby bolstering local media capabilities in this domain. Election interference has long been utilised as a foreign policy tool by state actors, but it has gained greater prominence due to Russia's attempts to influence the 2016 U.S. presidential election. Existing scholarship on election interference primarily focuses on its role in promoting specific candidates or parties. However, the concept of hybrid warfare offers a powerful alternative framework for understanding election interference. Hybrid warfare theory recognises that modern conflicts are characterised by the coordinated use of diverse tactics. By adopting this perspective, NATO can gain deeper insights into the complexities of election interference and develop more effective strategies to address this hybrid threat.[45] Examining the 2016 American presidential election, the 2018 Taiwanese local elections and the 2016 Brexit referendum reveals that election interference caused an intensification of internal

[43] Clinton 2010.

[44] Treverton et al. 2020.

[45] Davies 2021.

divisions in all three countries where it occurred. In each case, external actors attempted to manipulate the electoral outcomes, exploit societal divides and fuel polarisation within the respective societies. These interference attempts deepened existing tensions, eroded trust in democratic processes and undermined social cohesion. By leveraging disinformation campaigns, targeted messaging and hacking activities, external actors exacerbated internal divisions and weakened the fabric of these nations' democratic systems. Safeguarding elections from interference, promoting transparency, countering disinformation and enhancing cybersecurity are crucial measures in mitigating the negative impact of interference and fostering a more cohesive democratic environment.[46] Election interference is conceptualised as "a tool of hybrid warfare which can be used to undermine the strength and legitimacy of a target state".[47] It is ideally suited to this role thanks to its potential deniability, inexpensive nature, and effectiveness at exploiting internal divisions within target states. Moreover, modern technologies such as social media, the internet and even artificial intelligence facilitate election interference by making it easier than ever before to create and disseminate disinformation. Deterrence of election interference is very difficult because it does not conform to traditional concepts of warfare. Not all election interference can be classified as hybrid warfare. However, intervention in a state's democratic processes can be a key component of such aggression because of its ability to undermine the foundations of a target's government, society and popular legitimacy. Given that hybrid warfare breaks down the distinction between civilian and military domains, many experts have expressed concern that hybrid attacks might profoundly affect domestic politics in eastern Europe and examined the lessons that can be learned from their experiences, since at least 2007, Russia has pursued an "all out, mainly convert, political war on the west".[48] This operation has relied on information warfare and hacking, which afford Russia a degree of plausible deniability. Russia's intervention in the 2016 U.S. presidential election can be seen as a firm clash in this continuing hybrid assault on western countries.[49]

[46] Davies 2021.

[47] Wither 2016.

[48] Orenstein 2022.

[49] Babiracki 2018.

Questions

1. What are the emerging forms of nonviolent digital hybrid warfare tactics in today's landscape?
2. What are the prominent threats posed by misinformation and fake news in the hybrid era, and what are the potential negative consequences they can bring?
3. How has the Russian–Ukraine case study contributed to our understanding of the evolving forms and definitions of hybrid warfare?
4. What is the concept of national resilience, why is it crucial in addressing hybrid threats, and can it be precisely defined?
5. In the digital hybrid age, what role does the home front play in countering hybrid warfare and protecting national security?
6. How do media actors contribute to hybrid warfare tactics, and what role do they play in influencing public opinion and perceptions?
7. What joint efforts and working groups have been established by EU countries to address hybrid threats and enhance collective security?
8. How has public diplomacy been utilised as a tool to counter hybrid threats, and what impact has it had on promoting international collaboration and cooperation?
9. What measures have been taken by governments and international entities to build private capacity in countering disinformation and hybrid warfare?
10. How has the evolution of social media and peer-to-peer communication shaped the dynamics of public diplomacy in countering hybrid threats?

References

Adesina, Olubukola S. (2017): Foreign Policy in an Era of Digital Diplomacy. *Cogent Social Sciences,* 3(1). Online: https://doi.org/10.1080/23311886.2017.1297175

Attias, Shay (2012): Israel's New Peer-to-Peer Diplomacy. *The Hague Journal of Diplomacy,* 7(4), 473–482. Online: https://doi.org/10.1163/1871191X-12341235

Babiracki, Patryk (2018): Book Review on Evgeny Dobrenko – Natalia Jonsson-Skradol (eds.): *Socialist Realism in Central and Eastern European Literatures. Institutions, Dynamics, Discourses.* New York: Anthem Press, 2018. *Slavic Review,* 78(3), 835–836. Online: https://doi.org/10.1017/slr.2019.183

Bachmann, Sascha-Dominik Dov – Lee, Doowan – Dowse, Andrew (2020): Covid Information Warfare and the Future of Great Power Competition. *The Fletcher Forum of World Affairs,* 44(2), 11–18.

Bender, Dave (2014): Fake Hamas Message Claims Haifa Chemical Plant Hit by Gaza Rocket. *The Algemeiner,* 9 July 2014. Online: www.algemeiner.com/2014/07/09/fake-hamas-message-claims-haifa-chem-plant-hit-by-gaza-rocket/

Bjola, Corneliu – Holmes, Marcus (2015): *Digital Diplomacy. Theory and Practice.* London: Routledge. Online: https://doi.org/10.4324/9781315730844

Chan, Steve (2007): *China, the U.S. and the Power-transition Theory. A Critique.* London – New York: Routledge. Online: https://doi.org/10.4324/9780203940662

Clinton, Hillary R. (2010): Leading through Civilian Power: Redefining American Diplomacy and Development. *Foreign Affairs,* 89(6), 13–24.

Council of the European Union (2016): *The EU Integrated Political Crisis Response – IPCR – Arrangements in Brief 2016.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2860/412159

Davies, Jonathan (2021): Foreign Election Interference and Hybrid Warfare. *Senior Independent Study Theses,* (9443). Online: https://openworks.wooster.edu/independentstudy/9443

DeWit, Andrew – Djalante, Riyanti – Shaw, Rajib (2020): Building Holistic Resilience: Tokyo's 2050 Strategy. *The Asia Pacific Journal,* 18(7), 1–15.

Ducaru, Sorin D. (2016): The Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO. *Europolity – Continuity and Change in European Governance – New Series,* 10(1), 1–17.

Dunay, Pál – Roloff, Ralf (2017): *Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank.* Online: www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0

Ebitz, Amy (2019): *The Use of Military Diplomacy in Great Power Competition: Lessons Learned from the Marshall Plan.* Online: www.brookings.edu/blog/order-from-chaos/2019/02/12/the-use-of-military-diplomacy-in-great-power-competition

European Commission (2016): *FAQ: Joint Framework on Countering Hybrid Threats.* Online: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250

Gilman, Derek – Nichols, Robert – Totman, Jade C. – Minarich, Christine (2014): *Foreign Military Sales. Direct Commercial Sales.* Washington, D.C.: Defense Security Cooperation Agency – Covington & Burling LLP.

Haigh, Maria – Haigh, Thomas – Matychak, Tetiana (2019): Information Literacy vs. Fake News: The Case of Ukraine. *Open Information Science,* 3(1), 155–165. Online: https://doi.org/10.1515/opis-2019-0011

Hallams, Ellen (2010): Digital Diplomacy: The Internet, the Battle for Ideas & US Foreign Policy. *CEU Political Science Journal,* 5(4), 538–574.

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

Hook, Kristina – Verdeja, Ernesto (2022): *Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities.* Online: www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities/

Hourcade, Jean-Charles – Jaccard, Mark – Bataille, Chris – Ghersi, Frédéric (2006): Hybrid Modeling: New Answers to Old Challenges. Introduction to the Special Issue of *The Energy Journal. The Energy Journal,* 27(Special Issue), 1–12.

Humprecht, Edda – Esser, Frank – Van Aelst, Peter (2020): Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics,* 25(3), 493–516.

Jakobsen, Peter V. (2000): Focus on the CNN Effect Misses the Point: The Real Media Impact on Conflict Management Is Invisible and Indirect. *Journal of Peace Research,* 37(2), 131–143. Online: https://doi.org/10.1177/0022343300037002001

Jordan, Brigitte (2009): Blurring Boundaries: The "Real" and the "Virtual" in Hybrid Spaces. *Human Organization,* 68(2), 181–193. Online: https://doi.org/10.17730/humo.68.2.7x4406g270801284

Jun Ayhan, Kadir (2020): A Typology of People-to-People Diplomacy. Online: https://uscpublicdiplomacy.org/blog/typology-people-people-diplomacy

Kert-Saint Aubyn, Mari (2016): *EU Policy on Fighting Hybrid Threats.* Online: https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/

Lebel, Udi (2010): "Casualty Panic": Military Recruitment Models, Civil-Military Gap and Their Implications for the Legitimacy of Military Loss. *Democracy and Security,* 6(2), 183–206. Online: https://doi.org/10.1080/17419166.2010.492175

Monsees, Linda (2020): Cryptoparties: Empowerment in Internet Security? *Internet Policy Review,* 9(4), 1–19. Online: https://doi.org/10.14763/2020.4.1508

NATO (2016): *Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.* Online: www.nato.int/cps/en/natohq/official_texts_138829.htm

NATO (2023): *Collective Defence and Article 5.* Online: www.nato.int/cps/en/natohq/topics_110496.htm

Nye, Joseph S. Jr. (1990): Soft Power. *Foreign Affairs,* 80(Autumn), 153–171. Online: https://doi.org/10.2307/1148580

Nye, Joseph S. Jr. (2010): The Future of American Power: Dominance and Decline in Perspective. *Foreign Affairs,* 89(6), 2–12.

Orabi, Mariam – Mouheb, Djedjiga – Al Aghbari, Zaher – Kamel, Ibrahim (2020): Detection of Bots in Social Media: A Systematic Review. *Information Processing & Management,* 57(4). Online: https://doi.org/10.1016/j.ipm.2020.102250

Orenstein, Mitchell (2022): *Russia vs. the West and the New Politics of Hybrid War.* Online: https://events.ceu.edu/2022-03-10/russia-vs-west-and-new-politics-hybrid-war

Orpaz, Inbal – Siman-Tov, David (2021): The Unfinished Campaign: Social Media in Operation Guardian of the Walls. *The Institute of National Security Studies,* 12 September 2021. Online: www.inss.org.il/publication/guardian-of-the-walls-social-media/

Osula, Anna-Maria (2014): *EU Solidarity Clause and 'Cyber Disaster'.* Online: https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/

Storey, Neil R. – Kay, Fiona (2017): *The Home Front in World War Two.* Stroud: Amberley Publishing.

Svetoka, Sanda (2016): *Social Media as a Tool of Hybrid Warfare.* NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/177

Treverton, Gregory F. – Thvedt, Andrew – Chen, Alicia R. – Lee, Kathy – McCue, Madeline (2020): *Addressing Hybrid Threats.* Swedish Defence University – Center for Asymmetric Threat Studies – The European Centre of Excellence for Countering Hybrid Threats. Online: www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

Voronova, Sofija – Bakowski, Piotr (2022): *Future Shocks 2022: Consolidating EU Internal Security.* Online: https://epthinktank.eu/ 2022/05/22/future-shocks-2022-consolidating-eu-internal-security/

Wassermann, Felix (2018): The Blurring of Interstate Wars, Civil Wars, and Peace – "Hybrid War" as an Expression of Conceptual and Political Disorientation in the Twenty-first Century. *Sicherheit und Frieden (S+F) / Security and Peace,* 36(1), 14–20.

Weissman, Steve (2019): The Meaning of Reliability. *Natural Gas & Eletcricity,* 35(12), 1–7. Online: https://doi.org/10.1002/gas.22126

Wither, James K. (2016): Making Sense of Hybrid Warfare. *Connections,* 15(2), 73–87. Online: https://doi.org/10.11610/Connections.15.2.06

Ynet (2014): SMS מחמאס: “נפציץ כל מקום בישראל“ [Hamas SMS: "We will bomb every place in Israel."] *Ynet,* 14 July 2014. Online: https://www.ynet.co.il/articles/0,7340,L-4543488,00.html

Further reading

Cullen, Patrick J. – Reichborn-Kjennerud, Erik (2017): *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.* Norfolk: Allied Command Transformation.

Huhtinen, Aki-Mauri – Rantapelkonen, Jari (2016): Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere. *Journal of Information Warfare,* 15(4), 50–67.

Mills, Claire (2015): *France and Article 42(7) of the Treaty on the European Union.* Online: https://commonslibrary.parliament.uk/research-briefings/cbp-7390/