Chief Editor:
Orlin Nikolov

Associate editors:

Assoc. Prof. Lyubka Pashova,
(The Geodesy Department of the National Institute of Geophysics, Geodesy and Geography – Bulgarian Academy of Sciences)

Assoc. Prof. Mihaela Kouteva-Guentcheva, PhD, Eng.
(University of Architecture, Civil Engineering and Geodesy)

Irena Nikolova, PhD
(Bulgarian Modeling and Simulation Association – BULSIM)

Doncho Doychev
(Crisis Management and Disaster Response Centre of Excellence)

Nikolay Tomov
(Bulgarian Modeling and Simulation Association – BULSIM)

Technical support:
Desislav Zmeev, Boris Guenov, Vassil Rousinov

Table of Contents

HEAT WAVES OVER THE BALKANS. TOWARDS PREDICTIVE MACHINE LEARNING MODEL. A STATISTICAL ANALYSIS, POSSIBLE CAUSES AND PHYSICAL DRIVERS.

Hristo Popov[1]*, Oleg Stepanyuk*[2]

Abstract: Heat wave is a period of prolonged abnormally high surface temperatures relative to those normally expected. Heat waves may form when high pressure system strengthens and remains over a region from several days up to several weeks. Severe and exceptional heat waves, such as those that occurred over the Balkans (2007), France (2003), or Russia (2010), are associated with increased mortality, health hazards, reduced labor productivity and have significant economic impacts by compromising agricultural harvest. Extremely high air temperature values in the Balkan Region are associated with anticyclones formed at the Azores maximum or high-pressure ridges and advections of hot air from the south and southwest. In our project we perform analysis of the occurrence, durability, intensity and possible drivers and physical causes of the heat waves over the Balkan Peninsula for the period 1950-2020 based on historical data, reanalysis datasets and data products provided by ECMWF resources. We give outline of our results for the period (1980-2000) between heat waves occurrence and North Atlantic Oscillation Index and certain historical meteorological data for Atlantic and

[1] St. Kliment Ohridski Sofia University
[2] iAthena7 Labs, UATL Private Research University

Mediterranean regions aiming to figure out possible causes and physical drivers of this phenomena.

Key words: Heat waves, NAO, Mediterranean Oscillation, Machine Learning, Balkans

Extremely high temperatures are a phenomenon that has a direct impact on human health and especially on the elderly population, as well as those with health problems. At the same time, extremely high temperatures have an economic impact by creating conditions for compromising agricultural harvest. Heat waves are often accompanied by droughts, leading to reduced water availability for irrigation and drinking water supplies. River temperatures are often raised during heat waves, which can cause serious problems for cooling of power stations. Lower river and lake levels during heat waves can lead to algal blooms, causing mass mortality of fish and birds and posing a serious health threat to both animals and humans. Better understanding of the physical and dynamical processes governing European heat waves is essential for improved predictability and adaptation measures.

Increase in occurrences and lengths of heat waves for the recent decades have been found over much of Europe. One study [1] found that average summer heat wave lengths in western Europe had increased by about 1.3 days per century between 1880 and 2005. Another [2] identified an increase in the frequency of heat waves of 0.6 per decade in the Spanish central plateau between 1961 and 2010. In the Southern Alpine region, the lengths of the longest heat waves had increased by 2.7 days per century over the period 1874–2015 [3]. A study of heat waves in Lublin, southeast Poland [4], used data recorded over 1951–2015. The number of heat waves over this period had not changed, but heat waves after about 1990 had higher maximum temperatures and longer durations. Significant positive trends in numbers of heat wave days and heat wave lengths were identified in many southeastern European cities [5], although the period of data used was short (1980–2015). In a study of heat waves in Ukraine using temperatures recorded over 1951–2011, the largest numbers of heat waves were found in the most recent decade (2001–2010), and the fewest in 1961–1970 and 1971–1980 [6]. In contrast, large variations in numbers of hot days and lengths of heat waves between 1901 and 2003 were found for Basel, Switzerland, but no long-term trends [7].

Malcheva et al. [8] have studied Climatology of extremely hot spells in Bulgaria for period 1961-2019. They used threshold 32 °C and other variabilities which characterize duration of hot days and hot spells.

The number of hot days has been increasing over the last few decades. In the last 30 years the upper limit has more than doubled, reaching 36.1 days above the norm, but the speed of the change is relatively reduced. In over 90% of the stations there is a statistically significant trend of increasing the number of hot days by an average of about 3.5-3.6 days per decade.

North Atlantic Oscillation and Mediterranean Oscillation

The North Atlantic Oscillation (NAO) index is a fundamental mode of the climatic variability in the northern hemisphere ([9,10,11]; see [12] for a review). It represents the dipolar pattern of the Sea level pressure (SLP) characteristic of the North Atlantic-European region, with one center in the Azores high and the other one in the Iceland low. Stronger/weaker phases of the NAO are related to variations in the position and intensity of the North Atlantic Jet Stream (NAJS) and the storm track, along with large-scale changes in the zonal and meridional heat and moisture transport, which are reflected in changes in the temperature and precipitation patterns of wide regions, including the Mediterranean Sea.

Positive NAO phases are associated with an increase in the SLP over most parts of continental Europe and the Mediterranean Sea. Both poles, the Azores high and the Iceland low, are intensified, modifying the direction of the westerlies and associated storm tracks, thus leading to a decrease in the precipitation over the Mediterranean and Southern Europe (south 45° N) and an increase over Northern Europe. On the other hand, negative NAO generates negative SLP anomalies in Southern Europe and the Mediterranean basin, increasing the precipitation in these regions [11,13,14–22].

Although the NAO index shows high interannual and multidecadal variability, long periods of positive and negative phases are common. Switches from negative to positive NAO phases are followed by noticeable changes in the average precipitation of the Mediterranean basin, such as the decrease observed between the mid-1960s and the 1990s.

Positive NAO phases favor negative evaporation anomalies that can reach −160 mm/y in the Gulf of Lions and the Levantine basin [21,22], areas of formation of the Western Mediterranean Deep Water (WMDW) and Levantine Intermediate Water (LIW), respectively. Consequently, the reduction of latent heat losses associated with evaporation may result in a decrease in the amount of LIW and WMDW produced (see [23,24] for a detailed discussion of convective processes). Anti-correlation is expected since, under a negative state, anomalously low pressure over the whole basin is observed and more severe weather conditions over the Eastern and Northern Mediterranean are generated by the colder and drier air masses that flow from continental regions. Under this scenario, the enhancement of evaporative losses to the atmosphere is expected. In contrast, positive values are followed by higher-than-average pressure over the Mediterranean and North Africa that induce a change in the wind trajectories toward lower latitudes. Moister and warmer air masses are then advected to the Mediterranean, producing milder winters and, consequently, a decrease in the evaporative losses.

Gaetani et al. [25] study influence of West African Monsoon on the summer Euro-Atlantic circulation.

Wulff et al. [26] work on tropical forcing of the Summer East Atlantic Pattern. They used SNAO (Summer North Atlantic Oscillation). There are indications that during the positive SNAO phase the frequency of extreme warm days over central Europe is enhanced [27]. Cassou et al. [27] find a regime in addition to the SNAO related to exceptionally high temperatures over France. They refer to this regime as the Atlantic Low (AL) pattern since it is characterized by a large cyclonic anomaly with its center over the North Atlantic (NA), west of the British Isles and south of Iceland. The AL resembles the positive phase of the East Atlantic (EA) pattern [28]. The European summer heat wave of 2003 was influenced by the presence of the AL regime in June [27].

Heat waves over the Balkans are influenced by a variety of factors, including atmospheric circulation patterns, local geography, and sea surface temperatures [28]. The Mediterranean oscillation (MO) index is one of the factors that can contribute to the development and intensity of heat waves over the Balkans. The first definition of the MO [29] described it as a dipolar behavior of the atmosphere between the Western and Eastern Mediterranean. Since then, some authors have attributed the differences in key atmospheric and oceanographic parameters between both basins to this mode [29–32]. The index measuring the intensity of the dipole was primarily defined as the normalized 500 hPa height difference anomalies between Algiers (36.4◦ N, 3.1◦ E) and Cairo (30.1◦ N, 31.4◦ E) [30]. An alternative definition [31] estimated the MO index as the difference in the normalized SLP between the northern frontier of the Strait of Gibraltar (36.1◦ N, 5.3◦ W) and the Lod Airport in Israel (32.0◦ N, 34.5◦ E) [34]. A third definition [35] is offered for a better representation of the Central Mediterranean behavior, choosing the normalized SLP difference between Marseille and Jerusalem. Using this index, the authors found good (anti-)correlation with the precipitation and the number of wet days in Italy (around −0.4 on a yearly basis and up to −0.7 for wintertime depending on the location). More recently [23,36], the Mediterranean index has been introduced as the sea level pressure difference between South France (45◦ N, 5◦ E) and the Levantine Sea (35◦ N, 30◦ E). These two points are orientated in a NW-SE direction and are likely to reflect more accurately the realistic dipole pressure pattern. An approach based on the analysis of the EOF of the SLP anomaly fields over an extended Mediterranean region has been proposed [37]. Elsewhere [38], this paradigm is also used to analyze the influence of the MO index on the variability of the flow exchange through the Strait of Gibraltar. More recently [40], it was analyzed in detail these different paradigms of the Mediterranean oscillation teleconnection index: station-based definitions (Algiers–Cairo, MOAC, Gibraltar–Israel, MOGI, Marseille–Jerusalem, MOMJ or France–Levantine, MOFL) and the principal component (PC) approach in which the Mediterranean Oscillation Principal Component (MOPC) index was obtained as the time series of the first mode of normalized SLP anomalies over the extended Mediterranean region included in the limits [30◦ W–40◦ E, 30◦ N–60◦ N], which exhibits a single center located over the Central and Western Mediterranean that remains fairly steady in all seasons. They correlated interannual to interdecadal precipitation (P), evaporation (E), E-P (evaporation minus precipitation = freshwater deficit) and net heat flux with the different MO indices to compare their relative importance in the long-term variability of heat and freshwater budgets over the Mediterranean Sea. The accuracy of the index based on the different definitions to describe the interannual and interdecadal variability of the basin freshwater and heat budget components has also been analyzed [40]. They concluded that the most effective representation of the basin large-scale atmospheric forcing is achieved by the MO index based on PC analysis since it provides optimal representation of the full spatial pattern. Station-based indices show very poor correlation with the climatic variables analyzed (P, E and E-P) and only affect a reduced region of the basin. The noise introduced by the local small-scale and transient meteorological events in the SLP measurements causes the poorer results of the station-based indices [41,42].

During winter, when the dynamic activity of the atmosphere increases and the impact of the large-scale atmospheric variability is higher, the large-scale patterns over the basin are more marked and stable, improving the capacity of the station-based indices to capture the atmospheric variability. Unfortunately, this capacity is strongly reduced for the rest of the year. On the other hand, the PC analysis captures the variability of the whole region, filtering out the small-scale events and hence providing a better representation of the climatological evolution of the atmospheric processes over the basin independent of the season. MOAC shows better correlation for most winter-averaged variables and reveals more clearly the well-known dipole response of the eastern and western basins. However, all MO indices show fairly similar results, especially at decadal timescales [40]. It is worth pointing out that, while NAO, EA and EA–WR can be considered independent modes of the same EOF (Empirical orthogonal function) analysis, this is not the case for the MO. The NAO and MO patterns have important similarities, both with positive (negative) phases characterized by higher (lower) SLP anomalies over the Mediterranean. The two indices are strongly influenced by the Northeast Atlantic low systems that force the Mediterranean cyclogenesis [43], and thus their annual time series are highly correlated (~0.6 [22]). The MO can be understood as an oscillation of sea level pressure anomalies in the Central and Western Mediterranean, an important source of cyclogenesis. Since the appearance of these cyclones is partially connected with the activity of North Atlantic fronts governed by NAO, a high correlation is expectable. During winter, the southern center of the NAO is placed closer to the Mediterranean and, hence, the best correlation for all variables is always achieved by the winter NAO index. However, in summer and spring, the southern center of the NAO moves westward [14] and lower correlation is observed. On the contrary, since its center remains rather stable, the influence of MO in the Mediterranean is noticeable in all seasons. The MO index is also able to capture the effects of other low-frequency atmospheric modes in the Mediterranean SLP field. In particular, the influence of the EA (East Atlantic) (annual correlation of 0.43) but also the winter EA–WR (East Atlantic – West Russia) and Scandinavian (SCAN) modes [36] are noticeable. Therefore, this provides a more complete picture of the large-scale atmospheric impact over the Mediterranean, emerging as a rather accurate index to describe the basin climatological freshwater and (especially) heat budgets. Particularly, it is important to point out some features of the MO index with respect to the other indices [22]: (i) the annual correlations between the MO index and the climatic variables (E, P, E-P and heat flux) are higher than for the other indices; (ii) specifically, the influence of the MO negative phase is stronger than the NAO and is linked to an increase in precipitation and, in particular, intensification of the evaporation in the Levantine basin. In both MO phases, the SLP pattern induces wind trajectories that are closely related to the evaporation and net heat flux variability: warmer and moister air masses are transported to the Central and Western Mediterranean in the MO positive phase, as a consequence of the positive SLP anomaly dipole structure between North Africa and Central Europe, resulting in milder winters and the subsequent decrease in evaporation and heat loss. Conversely, negative MO phases are characterized by a dipole of low SLP anomalies between Turkey and Central Europe, enhancing the flow of cold and dry air masses from continental regions to the Mediterranean. This results in severe winters in the Aegean and Levantine basins that increase evaporation and heat losses, favoring the convective processes that generate the LIW.

Data and Methods

We use ECMWF ERA-5, ERA-Interim Reanalysis and ground station data. ERA5 provides hourly estimates of a large number of atmospheric, land and oceanic climate variables. The data cover the Earth on a 30km grid and resolve the atmosphere using 137 levels from the surface up to a height of 80km. Reanalysis datasets are created by assimilating ("inputting") climate observations using the same climate model throughout the entire reanalysis period in order to reduce the affects of modeling changes on climate statistics. Reanalysis combines model data with observations from across the world into a globally complete and consistent dataset. Within current project we perform analysis of extreme temperature conditions over the Balkan peninsula. Analysis starts with determining all extreme heat weather events happened within past decades starting from 1950 based on a World Meteorological

Organization 5-degree °C criteria. A preliminary correlation analysis between NAO index and ground temperatures is performed. Correlation analysis between parameters on various pressure levels across the Atlantic, Mediterranean and Balkans is performed with further application of these parameters for training of Long short-term memory (LSTM) and Convolutional Neural Networks (CNN).

Data assimilation, averaging, extreme heat events detection and plotting is done with Python and iAthena7 Geowizard framework. Data is projected on orography/heights map for easier interpretation.

Results

Figures 1 and 2 show extreme hot weather occurrences according to 35 °C and 5 °C WMO criteria for selected years between 1980 and 1999, while Figures 3 and 4 focus on summer months 1994, with distinct extreme heat weather conditions for July and September. Most often heat waves occur in Lower Struma Valley, Lower Vardar Valley and Southern Parts of Haskovo province. In Lower Thracian Valley and Danube Valley, heat waves occur distinguishably less often, with 25% and 15% less probability respectively.

The maximum air temperatures are affected by the shape of the terrain. In most cases, the absolute maximum values are related to meteorological conditions covering significant areas. Weather conditions over various parts of the Balkan peninsula are largely dependent on the orography of the region with complex interplay of mesoscale factors with strong involvement of orographically uplift and adiabatic cooling of air by rising motion. Obviously with increase of the altitude, probability of extreme heat weather conditions decreases, while forming of stable synoptic-scale weather systems require the area to be large enough. In Danube Valley extreme heat weather conditions observed were established at a greater time intervals over a larger territory, by comparison with other areas. Analysis of extremely high temperatures (> 35 °C) and results obtained with heat wave criteria, does not always show good correlation, which means that record temperatures do not always happen within longest periods of extreme weather which manifests across large areas (see Fig 1 and 2 years 1985, 1999, and prolonged heat wave over Danube valley in Sept 1994, with higher temperatures registered in other regions). This fact additionally points to complexity of the phenomena and multiple factors contributing to the mechanism beneath.

Occurrences of heat waves on the eastern coast of Balkan Peninsula are rare and present less than 50 % of cases in western part on same latitude, as the area is strongly influenced by Black Sea circulation.

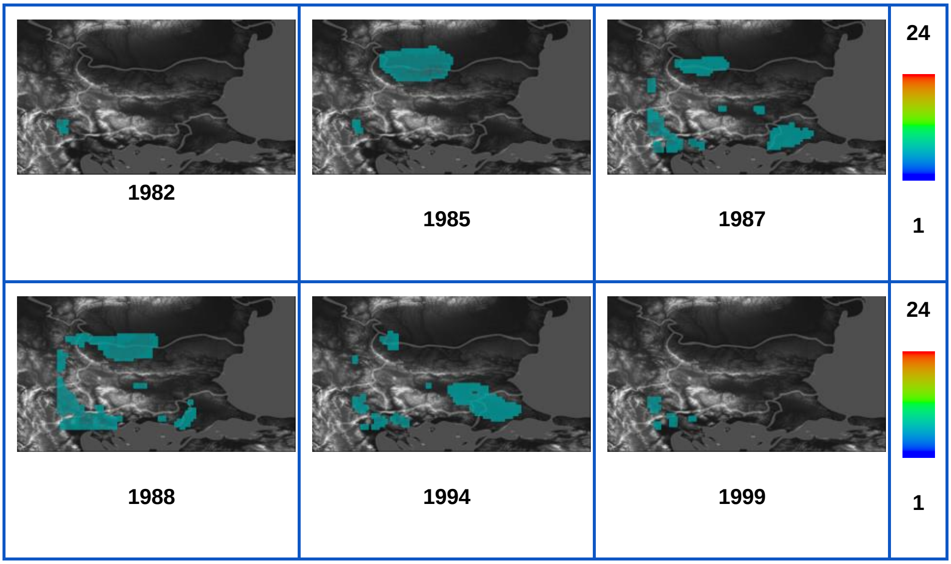


Fig 1. Extreme hot weather occurrences with temperatures above 35 C. Selected years, summer season (May - September). Projection over height map.

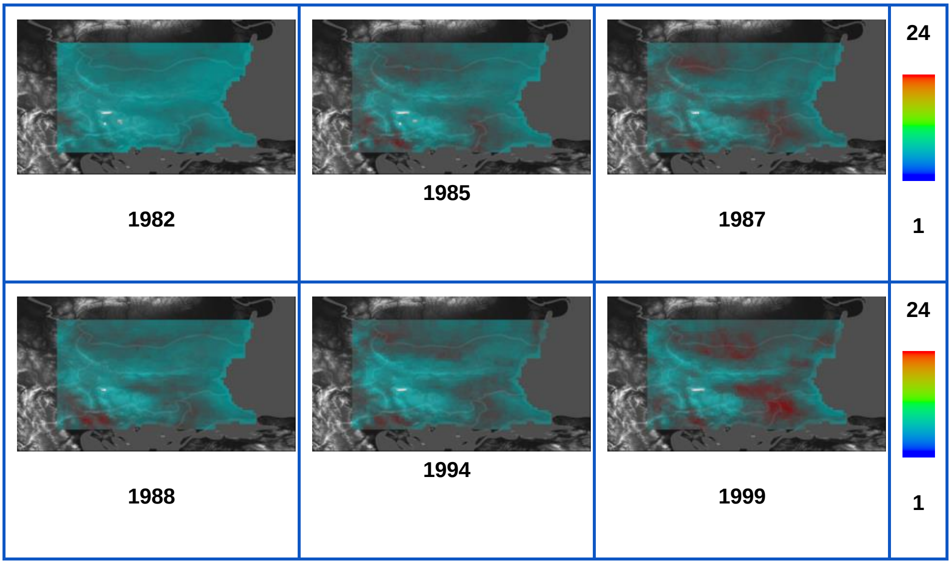


Fig 2. Extreme hot weather occurrences (heat wave) according to 5 degree C WMO criteria. Selected years, summer months (May - September). Projection over height map.

Year	May	Jun	Jul	Aug	Sept
1990	−1.19	0.42	1.43	3.31	−0.99
1991	−0.04	−0.31	−0.28	2.71	−1.12
1992	0.79	−1.74	1.04	3.97	0.99
1993	−2.59	0.16	0.64	0.75	−2.6
1994	−1.43	2.98	−0.09	−1.59	−2.85
1995	−0.36	−3.36	−0.96	−1.33	−1.55
1996	−1.5	1.43	1.47	−0.19	−2.23
1997	−1.35	−4.05	1.18	1.78	−0.67
1998	−1.26	−0.85	−0.57	1.8	−3.48
1999	1.03	1.39	−1.85	−3.67	−0.51
2000	0.31	0.89	−2.99	0.78	−1.1

Table 1. North Atlantic Oscillation Index.

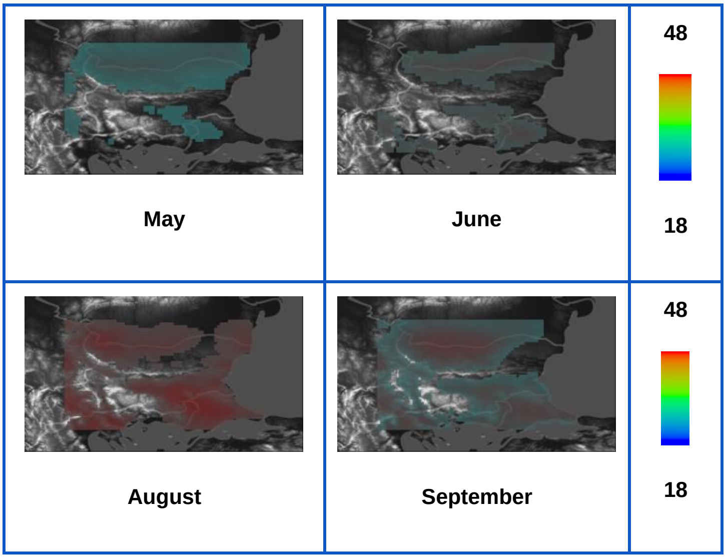


Fig 3. 1994, Summer months May, June, August, September. Extreme hot weather temperatures (heat wave) according to 5 degree C WMO criteria.

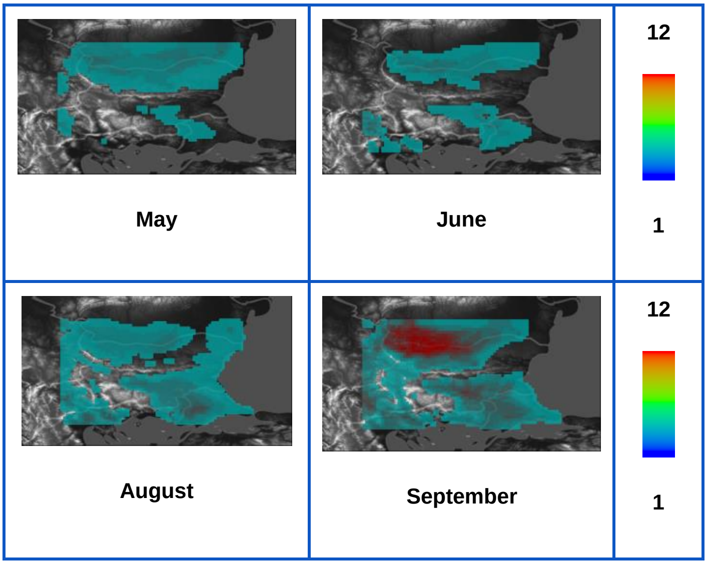


Fig 4. 1994, Summer months May, June, August, September. Extreme hot weather occurrences (heat wave) according to 5 degree C WMO criteria.

Extremely high values of air temperatures are associated with anticyclones forming along the Azores maximum or high-pressure ridges and associated advections of hot air from the south and southwest.

Regions of our interest are relatively close to Mediterranean coast and are influenced by anticyclones associated with Azorean maximum. These anticyclones bring hot tropical air masses which are adiabatic heated and combined with flat surface of valleys generate high/maximal air temperatures.

On Table 1 the values of North Atlantic Oscillation index are presented.

Neutral NAO may reveal two different mechanisms:

1 Azores high is intensive and Iceland low is close to normal/ or average. Then it is possible to observe more anticyclones over Mediterranean and South Europe. Continuation influence of these anticyclones (some of them blocking anticyclones) often generate a heat wave with different intensity. Cassou and Terray (2005) called this phase Atlantic Ridge

2 Iceland low is intensive and Azores high is close to average. In this case we can expect very dynamical weather periods during summer, with heat waves following by cyclones. Cassou and Terray (2005) called this phase Atlantic Low (must check data for this)

In negative NAO phase Balkan peninsula is under anticyclones or ridge influence, which could create heat waves periods. (Cassou and Terray 2005), see 1994 July - Sept from the current study.

Running a few years simulation with a state-of-the-art global atmospheric model with increased sea surface temperature allows, with certain assumptions, to replicate future climate according to IPCC 2021 AR6 Climate Report scenarios. Within our project we currently developing a predictive system for short and long-time forecasting of extreme weather conditions over the Balkans. A correlation analysis between variables across the Atlantic, Mediterranean and the Balkans is performed with further application of this data for training of LSTM and CNN networks.

Acknowledgement

This work has been carried out in the framework of the National Science Program "Environmental Protection and Reduction of Risks of Adverse Events and Natural Disasters", approved by the Resolution of the Council of Ministers № 577/17.08.2018 and supported by the Ministry of Education and Science (MES) of Bulgaria (Agreement № Д01-279/03.12.2021).

Computing resources, plotting and analysis software were provided by Athena7 Labs.

References

[1] Della-Marta, P.M.; Haylock, M.R.; Luterbacher, J.; Wanner, H. Doubled length of western European summer heat waves since 1880. J. Geophys. Res. 2007, 112. [CrossRef]

[2] Labajo, Á.L.; Egido, M.; Martin, Q.; Labajo, J.; Labajo, J.L. Definition and temporal evolution of the heat and cold waves over the Spanish Central Plateau from 1961 to 2010. Atmósfera 2014, 27, 273–286. [CrossRef]

[3] Brugnara, Y.; Auchmann, R.; Brönnimann, S.; Bozzo, A.; Berro, D.C.; Mercalli, L. Trends of mean and extreme temperature indices since 1874 at low-elevation sites in the southern Alps. J. Geophys. Res. Atmos. 2016, 121, 3304–3325. [CrossRef]

[4] Bartoszek, K.; Krzyzewska, A. The atmospheric circulation conditions of the occurrence of heatwaves in ˙ Lublin, southeast Poland. Weather 2016, 72, 176–180. [CrossRef]

[5] Morabito, M.; Crisci, A.; Messeri, A.; Messeri, G.; Betti, G.; Orlandini, S.; Raschi, A.; Maracchi, G. Increasing heatwave hazards in the southeastern European Union capitals. Atmosphere 2017, 8, 115. [CrossRef]

[6] Shevchenko, O.; Lee, H.; Snizhko, S.; Mayer, H. Long-term analysis of heat waves in Ukraine. Int. J. Climatol. 2014, 34, 1642–1650. [CrossRef]

[7] Beniston, M. The 2003 heat wave in Europe: A shape of things to come? An analysis based on Swiss climatological data and model simulations. Geophys. Res. Lett. 2004, 31, L02202. [CrossRef]

[8] Malcheva K., Bocheva L., Chervenkov Hr.: Climatology of extremely hot spells in Bulgaria (1961-2019). 21st International Multidisciplinary Scientific GeoConference SGEM 2021, Section Air Pollution and Climate Change. https://doi.org/105593/sgem2021/4.1/s19.40

[9] Barnston, A.G.; Livezey, R.E. Classification, seasonality and persistence of low-frequency atmospheric circulation patterns. Mon. Weather Rev. 1987, 115, 1083–1126. [CrossRef]

[10] Walker, G.T.; Bliss, W.E. World Weather, V. Mem. R. Meteorol. Soc. 1932, 44, 53–84.

[11] Van Loon, H.; Rogers, J.C. The see-saw of winter temperatures between Greenland and northern Europe. Part I: General descriptions. Mon. Weather Rev. 1978, 106, 296–310. [CrossRef]

[12] Hurrell, J.W.; Kushnir, Y.; Ottersen, G.; Visbeck, M. The North Atlantic Oscillation: Climate significance and environmental impact. Geophys. Monogr. Ser. 2003, 134. [CrossRef]

[13] Mariotti, A.; Struglia, M.V.; Zeng, N.; Lau, K.-M. The hydrological cycle in the Mediterranean region and implications for the water budget of the Mediterranean Sea. J. Clim. 2002, 15, 1674–1690. [CrossRef]

[14] Hurrell, J.W. Decadal trends in the North Atlantic Oscillation—Regional temperatures and precipitation. Science 1995, 269, 676–679. [CrossRef]

[15] Jones, P.D.; Jonsson, T.; Wheeler, D. Extension to the North Atlantic Oscillation using early instrument pressure observations from Gibraltar and south-west Iceland. Int. J. Climatol. 1997, 17, 1433–1450. [CrossRef]

[16] Slonosky, V.C.; Yiou, P. Secular changes in the North Atlantic Oscillation and its influence on 20th century warming. Geophys. Res. Lett. 2001, 28, 807–810. [CrossRef]

[17] Rogers, J.C.; van Loon, H. The see-saw of winter temperatures between Greenland and northern Europe. Part II: Some oceanic and atmospheric effects in middle and high latitudes. Mon. Weather Rev. 1979, 107, 509–519. [CrossRef]

[18] Serreze, M.C.; Carse, F.; Barry, R.G.; Rogers, J.C. Icelandic low cyclone activity: Climatological features, linkages with the NAO and relationships with recent changes in the northern hemisphere circulation. J. Clim. 1997, 10, 453–464. [CrossRef]

[19] Dai, A.; Fung, I.Y.; del Genio, A.D. Surface observed global land precipitation variations during 1900–88. J. Clim. 1997, 10, 2943–2962. [CrossRef]

[20] Mariotti, A.; Arkin, P. The North Atlantic Oscillation and oceanic precipitation variability. Clim. Dyn. 2007, 28, 35–51. [CrossRef]

[21] Criado-Aldeanueva, F.; Soto-Navarro, F.J.; García-Lafuente, J. Climatic indices influencing the long-term variability of Mediterranean heat and water fluxes: The North Atlantic and the Mediterranean Oscillations. Atmosphere-Ocean 2014, 52, 103–114. [CrossRef]

[22] Criado-Aldeanueva, F.; Soto-Navarro, F.J.; García-Lafuente, J. Large-scale atmospheric forcing influencing the long-term variability of Mediterranean heat and freshwater budgets: Climatic indices. J. Hydrometeorol. 2014, 15, 650–663. [CrossRef]

[23] Papadopoulos, V.; Josey, S.; Bartzokas, A.; Somot, S.; Ruiz, S.; Drakopoulou, P. Large-scale atmospheric circulation favoring deep- and intermediate- water formation in the Mediterranean Sea. J. Clim. 2012, 25, 6079–6091. [CrossRef]

[24] Josey, S.A. Changes in the heat and freshwater forcing of the eastern Mediterranean and their Influence on deep water formation. J. Geophys. Res. 2003, 108, 3237. [CrossRef]

[25] Gaetani, M., B. Pohl, H. Douville, and B. Fontaine (2011), West African Monsoon influence on the summer Euro-Atlantic circulation, Geophys. Res. Lett., 38, L09705, doi:10.1029/2011GL047150

[26] Wulff, C. O., Greatbatch, R. J., Domeisen, D. I. V., Gollan, G., & Hansen, F. (2017). Tropical forcing of the Summer East Atlantic pattern. Geophysical Research Letters, 44, 11,166–11,173. https://doi.org/10.1002/2017GL075493

[27] Cassou, C., Terray, L., & Phillips, A. (2005). Tropical Atlantic influence on European heat waves. Journal of Climate, 18, 2805–2811.

[28] Xoplaki, E., Maheras, P., & Luterbacher, J. (2001). Variability of climate in meridional Balkans during the period 1961-1990. International Journal of Climatology: A Journal of the Royal Meteorological Society, 21(10), 1259-1282.

[29] Conte, M.; Giuffrida, A.; Tedesco, S. The Mediterranean Oscillation, Impact on Precipitation and Hydrology in Italy; Conference on Climate Water; Publications of the Academy of Finland: Helsinki, Finland, 1989; pp. 121–137.

[30] Kutiel, H.; Maheras, P.; Guika, S. Circulation indices over the Mediterranean and Europe and their relationship with rainfall conditions across the Mediterranean. Theor. Appl. Climatol. 1996, 54, 125–138. [CrossRef]

[31] Maheras, P.; Xoplaki, E.; Kutiel, H. Wet and dry monthly anomalies across the Mediterranean basin and their relationship with circulation 1860–1990. Theor. Appl. Climatol. 1999, 64, 189–199. [CrossRef]

[32] Supic, N.; Grbec, B.; Vilibic, I.; Ivancic, I. Long-term changes in hydrographic conditions in northern Adriatic and its relationship to hydrological and atmospheric processes. Ann. Geophys. 2004, 22, 733–745. [CrossRef]

[33] Palutikof, J.P. Analysis of Mediterranean climate data: Measured and modelled. In Mediterranean Climate: Variability and Trends; Bolle, H.J., Ed.; Springer: Berlin, Germany, 2003.

[34] Climate Research Unit. Available online: http://www.cru.uea.ac.uk/cru/data/moi/ (accessed on 2 July 2020).

[35] Brunetti, M.; Maugeri, M.; Nanni, T. Atmospheric circulation and precipitation in Italy for the last 50 years. Int. J. Climatol. 2002, 22, 1455–1471. [CrossRef]

[36] Papadopoulos, V.; Kontoyiannis, H.; Ruiz, S.; Zarokanellos, N. Influence of atmospheric circulation on turbulent air-sea heat fluxes over the Mediterranean Sea during winter. J. Geophys. Res. 2012, 117. [CrossRef]

[37] Suselj, K.; Bergant, K. Mediterranean Oscillation Index. Geophys. Res. Abstr. 2006, 8, 02145.

[38] Gomis, D.; Tsimplis, M.N.; Martín-Míguez, B.; Ratsimandresy, A.W.; García-Lafuente, J.; Josey, S.A. Mediterranean Sea level and barotropic flow through the Strait of Gibraltar for the period 1958–2001 and reconstructed since 1659. J. Geophys. Res. 2006, 111. [CrossRef]

[40] Criado-Aldeanueva, F.; Soto-Navarro, F.J. The Mediterranean Oscillation teleconnection index: Station-based versus principal component paradigms. Adv. Meteorol. 2013, 738501. [CrossRef]

[41] Trenberth, K.E. Signal versus noise in the Southern Oscillation. Mon. Weather Rev. 1984, 112, 326–332. [CrossRef]

[42] Hurrell, J.W.; van Loon, H. Decadal variations in climate associated with the North Atlantic Oscillation. Clim. Chang. 1997, 36, 301–326. [CrossRef]

[43] Trigo, I.F.; Bigg, G.R.; Davies, T.D. Climatology of cyclogenesis mechanisms in the Mediterranean. Mon. Weather Rev. 2002, 130, 549–569. [CrossRef]

REVOLUTIONISING HYBRID WARFARE: THE ROLE OF ARTIFICIAL INTELLIGENCE

Borislav Bankov[1]

Abstract: Hybrid warfare (HW) is among the most debated concepts in contemporary military science. One critical yet unresolved question is whether the concept depicts an entirely new empirical phenomenon. Many scholars claim that HW is novel only as far as new technologies are used as weapons of war. Hence, most scholars also conclude that the novelty of HW is limited to the operational and tactical levels of war because, albeit important, technological innovations do not fundamentally change how humans take strategic decisions. This article challenges this assumption based on the relationship between HW and artificial intelligence (AI). The author asks the following question: To what degree does the emergence of AI influence the phenomenon of HW? This article argues that while technology may traditionally be important only for the lower levels of war, AI has strategic-level implications for the conduct of and the defence against HW. Thus, in the era of AI, the novelty of HW is not limited to the lower levels of war but is pervasive. Given the disruptive nature of AI-based technologies, the Western security and defence community must adopt AI through stronger military-civilian partnerships. Challenges and opportunities are briefly discussed by examining a recent North Atlantic Treaty Organisation initiative, the so-called Defence Innovation Accelerator for the North Atlantic.

Keyword: Hybrid warfare, artificial intelligence, defence innovation, NATO.

The concept of hybrid warfare (HW) suggests that a new approach to warfighting emerged after the Cold War. To Frank Hoffman, the chief architect of the concept, different warfare methods are now

[1] St. Kliment Ohridski Sofia University, borislav.m.bankov@gmail.com

combined to achieve battlespace synergies.[2] However, many scholars contend that such multi-modal warfare has also occurred in the distant past and are sceptical that HW is an entirely new phenomenon.[3] Instead, they argue that HW is novel only to the degree that new technologies, such as cyber capabilities, are added to the mix of warfighting methods.[4] Consequently, many researchers conclude that the novelty of HW is limited to the operational and tactical level of war. This is because, to them, albeit important, technological innovation does not fundamentally change how humans take decisions on the strategic level.

This article challenges this assumption by analysing the relationship between HW and artificial intelligence (AI). AI is often

[2] Frank G. Hoffman, *Conflict in the 21st century: The Rise of Hybrid Warfare* (Virginia, Potomac Institute for Policy Studies, 2007), 8, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[3] For example: Williamson Murray, "The American Revolution: Hybrid War in America's Past," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, eds. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012), 72-104; James Lacey, "Conquering Germania: A Province Too Far," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, eds. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012), 1-45; Richard Hart Sinnreich, "That Accursed Spanish War: The Peninsular War, 1807-1814," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, eds. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012), 104-151.

[4] Greg Simons, Yuriy Danyk and Tamara *Maliarchuk*, "Hybrid war and cyber-attacks: creating legal and operational dilemmas," *Global Change, Peace & Security* 32, no. 3 (2020): 340-341, https://doi.org/10.1080/14781158.2020.1732899

labelled as the next technological frontier.[5] Yet, for two widely popular concepts, there is surprisingly little interdisciplinary research on the interaction between HW and AI. To the extent that they exist, current works focus on how AI capabilities can be used in specific HW scenarios, such as influence or cyber operations.[6] Yet, they do not delve into HW's broader theoretical assumptions on modern conflict and if and how AI fits them. There are only a few exceptions.[7] Still, those studies either do not discuss in detail the possible impact of AI on the strategic level of HW or are altogether sceptical about that possibility.

There are two possible explanations for the state of the current literature. Firstly, Western military thought has traditionally focused

[5] For example: Jacques Bughin et al., *Artificial Intelligence: The Next Digital Frontier?* (Brussels, McKinsey Global Institute, 2017), https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx.

[6] For example: Haleema Zia, "The Evolution of Artificial Intelligence: Implications for Cybersecurity and Hybrid Warfare" *Pakistan Journal of Terrorism Research* 03, no. 1 (2021): 1-28, https://nacta.gov.pk/wp-content/uploads/2021/09/The-Evolutionof-ArtificialIntelligence-Implicationsfor-Cybersecurity-and-Hybrid-Warfare-Haleema-Zia.pdf; Nicolas Mazzucchi, *AI-based technologies in hybrid conflict: The future of influence operations* (Helsinki, Hybrid CoE, 2022), https://www.hybridcoe.fi/publications/hybrid-coe-paper-14-ai-based-technologies-in-hybrid-conflict-the-future-of-influence-operations/.

[7] For example: Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare" *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917, https://doi.org/10.1080/09592318.2019.1682908; Lora Pitman, *Perfect Strangers: Legal and Ethical Aspects of AI in Hybrid Warfare* (Brussels, NATO Science for Peace and Security Series, 2022), https://ebooks.iospress.nl/volumearticle/60904.

on the tactical and operational level instead of the strategic. In other words, most academic literature and even policy papers have concentrated on analysing how to win battles rather than wars.[8] Secondly, Western political leaders and strategic commanders are rightfully wary of delegating their decision-making authority to AI algorithms that currently operate with little to no transparency. In turn, this demotivates military scientists from researching the topic. This article does not set out to prescribe if the West should or should not integrate AI at the strategic level. Instead, it aims to offer an updated research agenda on the relationship between AI and HW. It does so by analysing the former's transformative potential at all levels of war in the context of the latter.

Elaborating on the possible transformative impact of AI on HW would inform the next steps that the West needs to make to ensure the robustness of its security and defence architecture. The cautious attitude of Western leaders towards AI does not prevent potential adversaries or competitors from using the full extent of such technologies to the detriment of the West. For example, given Russia's and China's advances in AI and the different ethics and standards they usually apply in research and development, the West must ensure that its security and defence sector

[8] Hoffman, *Conflict in the 21st century*, 24; Rod Thornton and Marina Miron, *Towards the 'Third Revolution in Military Affairs'. The Russian Military's Use of AI-Enabled Cyber Warfare* (London, the RUSI Journal, 2020), 1, https://doi.org/10.1080/03071847.2020.1765514.

comprehensively addresses any AI-related vulnerabilities. Hence, this subject has not only important academic but also critical real-world implications.

Hence, this article asks: To what degree does the emergence of AI influence the phenomenon of HW? The author argues that while technology may usually be influential only at the lower levels of war, AI has strategic-level implications for the conduct of and the defence against HW. It can revolutionise HW since it can change the balance of power among the HW actors. Thus, in the era of AI, the novelty of HW is not limited to tactics and operations but is pervasive. In fact, the emergence of AI further legitimises the existence of the HW concept. It gives credibility to some of Hoffman's fundamental assumptions on modern conflict, previously less obvious without actors having easy access to such disruptive technology.

Given the disruptive potential of AI, the Western defence community must understand and adopt AI solutions at the speed of technology and become a trendsetter in their responsible use. AI can both enable, but also provide defence against HW. The latter's success depends on whether the West fits AI into its toolbox against HW through strong military-civilian cooperation. An example is discussed based on the North Atlantic Treaty Organisation's (NATO) Defence Innovation Accelerator for the North Atlantic (DIANA).

The first part examines the concept of HW by offering a critical review of its relationship with technology. In the second, the current stage of AI development is briefly discussed against the background of conflict research. The third part outlines how AI can enable and counter HW and if this has strategic effects. The fourth part outlines implications for the West and uses DIANA as an example of best practices. Finally, the conclusion sums up the findings and proposes further research.

Hybrid warfare and technology

While he was not the one to originally coin the concept, Frank Hoffman, a United States Marine Corps reservist and a military scholar, was why HW became a part of the military lingua franca. In 2006, the scholar gave the first thorough definition of HW and is thus rightfully considered the chief architect of the concept. More specifically, he argued that HW:

> “incorporate[s] a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. These multi-modal activities can be conducted by separate units, or even by the same unit but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects. The effects can be gained at all levels of war“.[9]

[9] Hoffman, *Conflict in the 21st century*, 29.

In short, to Hoffman, the defining feature of HW is the “hybrid“ or the merging of different capabilities, methods, and actors across all levels of war. Yet, the scholar not only defined the phenomenon but also placed HW within the larger debate on the changing nature of war by cross-examining other concepts. For example, Hoffman studied the so-called compound warfare. This concept emphasises the merger of regular and irregular units under a single command. Yet, the scholar asserted that actual compound warfare could only be achieved with advanced communications technology enabling coordination across today’s extended battlespace. Hoffman also explored the concept of unrestricted warfare, which suggests that new domains of operations are now available due to technology. Moreover, the cost of entry to those is lower. For instance, a cyber operation can be mounted with fewer resources than a kinetic operation and carries a lower risk of retaliation with physical means due to the rule of proportionality. Hoffman agreed that the theoretical conclusions of unrestricted warfare are useful, which is why his definition of HW borrows some of its assumptions as well as those of compound warfare and other concepts.[10]

It is important to note that HW has undergone a significant conceptual transformation after the European Union (EU) and NATO adopted the concept to call out Russia’s illegal annexation

[10] Hoffman, *Conflict in the 21st century*, 22.

of Crimea in 2014.[11] This is because, at the time, Russia had still not waged a full-fledged war against Ukraine. As a result, by using HW to describe the Russian actions below the threshold of war, the EU and NATO expanded the concept's scope to an array of non-kinetic activities such as propaganda and cyber operations. Along with this transformation, the concept attracted much criticism since it became broader and hence vaguer. Some of this criticism has turned into disdain towards the concept, and some scholars completely disregard it by describing it as a weak, ambiguous, and altogether unnecessary empirical category.[12]

While some criticism towards the concept is healthy, a complete disregard for the framework is unwarranted as HW still offers useful conceptual lenses to study modern conflict.[13] Besides, despite

[11] Jan Jakub Uziębło, "United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats," *EU Diplomacy Papers* 5 (2017): 5, https://www.coleurope.eu/sites/default/files/research-paper/edp-5-2017_uzieblo_0.pdf; Milinko S. Vračar and Milica T. Ćurčić, "The evolution of European perception of the term 'hybrid warfare'," *Vojno Delo* no. 1 (2018): 10-11, https://scindeks.ceon.rs/Article.aspx?artid=0042-84261801005V.

[12] Elie Tenenbaum, "Hybrid Warfare in the Strategic Spectrum: an Historical Assessment," in *NATO's Response to Hybrid Threats*, eds. Guillaume Lasconjarias and Jeffrey Larsen (Rome: NATO Defence College, 2015), 112: https://www.files.ethz.ch/isn/195405/fp_24.pdf; Murat Caliskan, "Hybrid warfare through the lens of strategic theory," *Defense & Security Analysis* 35, no. 1 (2019): 51, https://doi.org/10.1080/14751798.2019.1565364; Vladimir Rauta, "Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces," *Cambridge Review of International Affairs* 33, no. 6 (2020): 868, https://doi.org/10.1080/09557571.2019.1656600; Robert Johnson, "Hybrid War and Its Countermeasures: A Critique of the Literature," *Small Wars & Insurgencies* 29, no. 1 (2018): 143, https://doi.org/10.1080/09592318.2018.1404770.

[13] Yan, *The* Impact *of Artificial Intelligence*, 4.

HW’s transformation, some of Hoffman’s key assumptions remain intact. For example, according to the current understanding of HW, today’s conflict is marked by a combination of different methods, such as regular and irregular warfare and a decreased cost of entry. Both these theoretical points were a part of the original framework and depend on the underlying assumption that technology is exploited as a weapon of war. Hence, one can argue that technology has played a crucial role in HW since the birth of the framework.

However, while implicitly recognising that technology is important, Hoffman’s earlier works downplayed the role of disruptive innovation. [14] Instead, Hoffman claimed that “the disruptive component of [HW] does not come from high-end or revolutionary technology but from criminality“.[15] One can speculate that this was an attempt to future-proof his theory. While the rate of technological innovation has traditionally fluctuated, human behaviour has always been an intrinsic factor in war. Specifically, at the time Hoffman was completing his initial works, the so-called Information Technology (IT) Revolution in Military Affairs (RMA) failed to

[14] Yan, *The Impact of Artificial Intelligence*, 1.
[15] *Hoffman*, *Conflict in the 21st century*, 29.

revolutionise the nature of warfare to the degree that many analysts expected.[16]

This is also why scholars are generally sceptical towards HW being an entirely new phenomenon. They often argue that HW is novel only to the extent that new technologies are at play.[17] Given the high but ultimately false expectations of the transformative potential of IT on warfare, scholars have then felt more comfortable asserting that any novelty of HW is limited to the lower levels of war.

Regardless of what others had argued, later in the mid-2010s, Hoffman changed his opinion on technology and explicitly stated that advanced capabilities are critical to HW.[18] Interestingly, his changed attitude coincided with significant developments in AI, such as the rise of deep learning, the chatbot revolution and a surge of investments in AI research. Thus, disruptive innovation, embodied by AI, was perhaps no longer possible to ignore. As many scholars have argued, the AI RMA holds much more promise than the IT RMA, which results were mixed at best.

[16] Michael *Raska*, "The sixth RMA wave: Disruption in Miltary Affairs?," *Journal of Strategic Studies* Epub ahead of print 25 November 2020, 13-14, https://doi.org/10.1080/01402390.2020.1848818

[17] *Caliskan*, *Hybrid warfare through the lens*, 50-51; Simons, Danyk and Maliarchuk, *Hybrid war and cyber-attacks*, 340-341.

[18] Frank G. Hoffman, *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War* (Washington, DC, the Heritage Foundation, 2016), 29, https://www.heritage.org/sites/default/files/2019-10/2016_IndexOfUSMilitaryStrength_The%20Contemporary%20Spectrum%20of%20Conflict_Protracted%20Gray%20Zone%20Ambiguous%20and%20Hybrid%20Modes%20of%20War.pdf.

Artificial intelligence and conflict

While the origins of the term AI can be traced back to 1956 when the computer scientist John McCarthy introduced it at a conference, AI gained momentum only after the 1990s. To reach that point, in the 1970s and 1980s, AI had to survive the so-called AI winter, when research in the field was limited due to the lack of computational power to support it. However, the interest in AI grew with the advancement in machine learning and processing capabilities. Still, years had to pass before AI-based applications became accessible to the larger workforce outside the computer science expert community. This has happened only recently due to lower hardware costs, cloud computing, and easy access to online learning.

Yet, the increasingly democratic access to AI education and training does not mean that all fundamental AI-related issues are settled. On the contrary, there remain many unresolved questions critical to the growth of the field. These include how to regulate AI research and development; how to increase the explainability and interpretability of AI-based solutions; how to ensure the robustness and security of AI systems; how to address ethical concerns and mitigate biases in AI technology; how to protect user data and ensure privacy in AI systems; how to determine the appropriate level of autonomy for AI systems; etc.

Importantly, all of these questions gain significantly more weight if the use of AI for warfighting or defence purposes is considered. For example, the level of autonomy of technologies such as drone swarming is a highly contested issue.[19] Meanwhile, the policy and technological expertise in such fields is still in its infancy, so this article cannot resolve any fundamental problems.

Thus, to minimise the unknowns, the analysis will study the transformative potential of AI on today's conflict within specific parameters. Firstly, this article does not differentiate between AI's subfields and related technologies such as machine learning, artificial neural networks, natural language processing, computer vision, etc. Instead, AI is understood as an umbrella term that covers different methods to perform cognitive functions that traditionally require human intelligence.[20] Secondly, the focus is on examining existing AI technologies up until medium-term innovation. This article does not set out to imagine what AI would be capable of in the more distant future through sensationalist claims of Terminator-like machines. Thirdly, given this timescale, the text focuses on the so-called Narrow AI. While various classification strategies exist, AI is most often categorised into three types according to its human-like characteristics and real-world application. More specifically, Narrow AI specialises in one problem

[19] James Johnson, *Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare* (London, the RUSI Journal, 2020), https://doi.org/10.1080/03071847.2020.1752026.

[20] Ralph Thiele, *Artificial Intelligence – A key enabler of hybrid warfare* (Helsinki, Hybrid CoE, 2020), https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-6-artificial-intelligence-a-key-enabler-of-hybrid-warfare/.

at a time. Meanwhile, General AI is on par with human intelligence, whereas Super AI surpasses human talent.[21] The current state of AI research and development can be described at the level of Narrow AI.

For instance, ChatGPT, an AI chatbot operating since November 2022, is a Narrow AI. The application, which provides conversational assistance and information, gained worldwide attention due to its well-articulated answers. For example, in response to the prompt "Summarise in 75 words or less the influence of AI on modern conflict", ChatGPT generated:

> "AI has a significant impact on modern conflict, including cyber warfare, intelligence gathering, autonomous weapons, predictive analytics, command and control systems, information operations, logistics, and training. It enables automated attacks and defence, enhances decision-making, predicts outcomes, manipulates information, optimises logistics, and aids training. However, ethical concerns and risks such as unintended consequences and accountability in autonomous systems need to be addressed through regulation and responsible use."[22]

One can argue that this output is insightful. For example, ChatGPT recognised that AI could serve both attack and defence purposes

[21] Vijay Kanade, "Narrow AI vs. General AI vs. Super AI: Key Comparisons" *SpiceWorks*, March 25, 2022, https://www.spiceworks.com/tech/artificial-intelligence/articles/narrow-general-super-ai-difference/.

[22] ChatGPT, response to "Summarise in 75 words or less the influence of AI on modern conflict," May 15, 2023, https://chat.openai.com.

but also that there are still open ethical questions on its use. This simple experiment illustrates why ChatGPT has gained attention and suggests that while current AI-based technologies are classified as Narrow AI, they already have a transformative societal impact. To generate output at this level of sophistication, the application analysed domain-specific knowledge, industry jargon, and sentiment by going through large amounts of information on the topic.[23] Traditionally, this takes a considerable amount of research time.

Indeed, there is much information, some of it in the form of academic literature, on AI's relationship with conflict. Still, some topics receive more attention than others. For instance, many scholars have linked AI to the decades-long discussions on the Revolution in Military Affairs.[24] Meanwhile, others delve into AI's specific military applications in the areas of modelling and simulation.[25] A solid body of literature also exists on how AI enables

[23] Partha Pratim Ray, "ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope" *Internet of Things and Cyber-Physical Systems* no. 3 (2023): 121-154, https://doi.org/10.1016/j.iotcps.2023.04.003.

[24] For example: Kenneth Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?," *Survival* 60, no. 5 (2018): 7-32, https://doi.org/10.1080/00396338.2018.1518374; Raska, *The sixth RMA wave*; *Thornton and Miron, Towards the Third Revolution*.

[25] For example: Paul K Davis and Paul Bracken, "Artificial intelligence for wargaming and modelling," *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* Special Issue Article (2022): 1-16, https://doi.org/10.1177/15485129211073126; Basxar Kasım at al., "Modeling and Simulation as a Service for joint military space operations simulation," *Journal of Defense Modeling and Simulation: Applications, Methodology,*

drones and other unmanned aerial vehicles.[26] AI-enabled cyber warfare and disinformation have also been extensively covered.[27] Regarding case studies by country, Chinese military innovation has been an attractive topic.[28] Yet, while much literature exists on the relationship between AI and conflict in general, there is surprisingly little research effort on the impact of AI on HW.

Hybrid warfare and artificial intelligence

A literature review concluded that between 2012 and 2020, 41 peer-reviewed papers were produced containing the terms HW and AI.[29] As insufficient as this number would be in nearly a decade, the

Technology 18, no. 1 (2021): 29-38, https://doi.org/10.1177/1548512919882499.

[26] For example: Johnson, *Artificial Intelligence*; Norine MacDonald and George Howell, "Killing Me Softly. Competition in Artificial Intelligence and Unmanned Aerial Vehicles," *PRISM* 8, no. 3 (2019), 102-127, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_MacDonald-Howell_102-126.pdf.

[27] For example: Haleema Zia, "Information Revolution and Cyber Warfare: Role of Artificial Intelligence in Combatting Terrorist Propaganda," *Pakistan Journal of Terrorism Research* 03, no. 2 (2021): 133-157, https://nacta.gov.pk/wp-content/uploads/2021/09/Information-Revolution-and-Cyber-Warfare-Role-of-Artificial-Intelligence-in-Combating-Terrorist-Propaganda.pdf; Katarina Kertysova, "Artificial Intelligence and Disinformation," *Security and Human Rights* 29 (2018): 55-81, file:///C:/Users/boris/Downloads/shrs-article-p55_55.pdf.

[28] For example: Elsa B. Kania, *China's Rise in Artificial Intelligence and Future Military Capabilities* (Washington, DC, Center for a New American Security, 2017), http://www.jstor.com/stable/resrep16985.6; Elsa B. Kania, *Chinese Military Innovation in Artificial Intelligence* (Washington, DC, Center for a New American Security, 2019), https://www.jstor.org/stable/resrep28742.

[29] Elena Șușnea and Ionuț-Cosmin Buță, "Artificial Intelligence in Hybrid Warfare: A Literature Review and Classification," (Bucharest, International Scientific Conference "Strategies XXI", 2021), 296, https://revista.unap.ro/index.php/XXI_FSA/article/view/1255.

papers that carefully analyse the HW-AI nexus might be even less. The fact that a text contains the two keywords is no guarantee that the relationship between the two phenomena is under focus. The literature review fails to make that distinction clearly. Moreover, even if the title of a paper contains the phrase HW, some authors use it only as a buzzword to attract readers without making any in-depth references to Hoffman's idea.[30]

Other authors engage in a more careful analysis and even claim that AI can alter decision-making in HW but do not conceptualise if this has strategic effects.[31] Yet, such discussions are needed to inform policymaking. In fact, in 2021, 71% of the respondents in a survey by the Center for European Policy Analysis thought that AI would be the biggest game changer in NATO's ability to counter HW.[32] Thus, while there is already an interest in the relationship between HW and AI in policy circles, there is a critical need for more

[30] For example: Valentina Dragos, Bruce Forrester, and Kellyn Rein, "Is hybrid AI suited for hybrid threats? Insights from social media analysis," (Rustenburg, International Conference on Information Fusion, 2020), 1-7, https://ieeexplore.ieee.org/document/9190465; Wolfgang Koch, *On Digital Ethics for Artificial Intelligence in Hybrid Military Operations* (Brussels, NATO Science and Technology Organisation, 2021), 1-10, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-190/MP-IST-190-22.pdf.

[31] Haleema Zia, "Artificial Intelligence (AI) And Countering Hybrid Warfare – OpEd," *Eurasia Review* March 10, 2021, https://www.eurasiareview.com/10032021-artificial-intelligence-ai-and-countering-hybrid-warfare-oped/; Yan, *The Impact of Artificial Intelligence*, 5.

[32] Center for European Policy Analysis, "Hybrid Warfare of the Future: Sharpening NATO's Competitive Edge," August 20, 2021, https://cepa.org/comprehensive-reports/hybrid-warfare-of-the-future/.

substantive and interdisciplinary studies in academia. The authors of the literature review arrive at the same conclusion.[33]

How Artificial Intelligence Enables Hybrid Warfare

When expanding this field of research, it would be advantageous to start from the subject that existing literature covers to a greater extent. The scholars, who write on the relationship between HW and AI, mainly focus on how the former enables the latter.[34] There are two more apparent mechanisms of how AI enables HW. Both are connected to capability development and exploitation.

Firstly, AI has enabled military operators to better exploit traditional capabilities that predate AI. The individual functions of those capabilities remain the same, but algorithms advise how to use the different capabilities together to create synergies. In other words, AI enables an enhanced combined arms approach to warfare. To Hoffman, the conduct of such multi-modal operations is a defining feature of HW. By rapidly analysing vast amounts of multidimensional data regarding the operational environment, AI can suggest what combination of measures across the different instruments of power promises the best possible outcome.[35] For example, algorithms can recommend the best timing for an aid raid in support of a ground offensive. This practice is sometimes called

[33] Șușnea and Buță, *Artificial Intelligence in Hybrid Warfare*, 300.
[34] For example: Thiele, *Artificial* Intelligence – *A key enabler of hybrid warfare*;
[35] Yan, *The* Impact *of Artificial Intelligence*, 13-14.

algorithmic warfare, and in 2017 the Pentagon created a dedicated Cross Functional Team in that line of effort.[36] So, traditional capabilities and instruments of power across all domains of operations can be combined and made more precise. While these capabilities are, per se, not new, they are augmented, which can result in statistically significant changes in the theatre of operations. This has given rise to concepts such as AI-enabled cyber warfare.

Secondly, AI has also created entirely new operational capabilities that can be added to the portfolio of warfighting instruments and further increase the multimodality of warfare. Hoffman argues that HW is a blend of various regular but also irregular warfare methods and, undoubtedly, AI can provide a range of capabilities to conduct the latter. For instance, there is an increasing proliferation of AI-enabled autonomous weapon systems (AWS) such as drones.[37] The Russian war against Ukraine has showcased how these AWS can be used for irregular warfare, with the Kremlin using kamikaze drones against the city of Kyiv. Another example is the production of deepfake videos for propaganda objectives. For example, Russia allegedly intended to circulate a deepfake video of President

[36] Deputy Secretary of Defense, *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)* (Washington DC, Memorandum, 2017), https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf

[37] Johnson, *Artificial* Intelligence*,* 1;

Zelensky surrendering to demoralise the Ukrainian forces.[38] While these Russian efforts did not produce the expected results, those new capabilities can theoretically be a game-changer. More specifically, scholars argue that the accumulation of tactical victories due to these new combinations and new operational capabilities can produce a strategic effect and change the balance of power among warring entities.[39]

Yet, there are also other strategic effects that AI can have on HW. Beyond the capability-related questions, there are at least three other mechanisms to that end, which receive less attention, at least in Western academic literature. Their lower level of popularity is mainly due to ethical concerns because they are all connected to the role of AI in decision-making. This is still a sensitive topic.

Firstly, AI decreases the cost of waging HW and, thus, can influence the strategic decision to engage in such conflict in the first place. Earlier works on HW claim that the barrier to entry in contemporary conflict is lowering because even if an actor is resource-constrained, they can opt for cost-effective cyber operations instead of kinetic campaigns. AI validates and significantly amplifies this idea since it makes warfighting more economical not only in the

[38] Mason Clark, George Barros, and Kateryna Stepanenko, *Russian Offensive Campaign Assessment, March 3* (The Institute for the Study of War, 2022), 4, https://www.understandingwar.org/sites/default/files/Russian%20Operations%20Assessments%20March%203.pdf.
[39] Payne, *Artificial Intelligence*, 9-10.

digital but also in the physical world. For example, the United States Air Force has implemented predictive logistics to maintain their fleet.[40] Their AI system predicts when a fighter jet needs repair, thus optimising maintenance costs. Nothing prevents such algorithms from being implemented by other actors, including opponents and potential adversaries, enabling them to develop and maintain a broader range of lethal capabilities. Therefore, even resource-constrained actors need not focus only on cyber operations any longer. Instead, they can now more easily decide to wage HW in its purest form by combining various weapons of war. Indeed, scholars argue that AI can be an offset strategy to compensate for several combat-related weaknesses.[41] Implementing such AI systems does require expertise and resources. Still, these are significantly less than the entire investment needed for combat readiness and, most importantly, can cut other costs in the long term. Thus, the reduced cost of HW enabled by AI can impact strategic decision-making, potentially influencing the choice to initiate or participate in HW.

Secondly, AI increases the chances of strategic surprise during HW too. While current AI is classified as Narrow AI, neglecting upcoming technological progress would put this analysis at a distinct disadvantage. Namely, some authors argue that the West

[40] Thiele, *Artificial Intelligence – A key enabler of hybrid warfare,* 8.
[41] For example: Thiele, *Artificial* Intelligence *– A key enabler of hybrid warfare,* 6; Mazzucchi, *AI-based technologies in hybrid conflict,* 6; Payne, *Artificial Intelligence*, 7.

may be confronted by an AI-driven or at least AI-enabled strategic decision-maker, even in the short to medium term.[42] This might create a significant challenge, given the so-called black box problem or the lack of understanding of how AI works and reaches certain conclusions. Furthermore, AI is divorced from normal human psychology, such as groupthink, confirmation bias, excessive optimism, and poor risk judgements.[43] Thus, the defending side in a conflict against an AI-based decision-maker would face significant unpredictability and surprise.[44] HW is a complicating factor in such a scenario. A key objective in existing HW-based doctrines is bringing ambiguity and surprise. Thus, if an AI system, which is already ambiguous in its own right, is programmed or trained to pursue that objective intentionally, the nature of HW would be qualitatively different from any human-driven HW scenario. In fact, Chinese scientists are already experimenting with the level of unpredictability that AI can bring into warfare by using the military

[42] For example: Thornton and Miron, *Towards the 'Third Revolution in Military Affairs'*; Olivier Guitta, " The Global War Over AI Already Started," Newsweek, March 20, 2023, https://www.newsweek.com/global-war-over-ai-already-started-opinion-1788079.

[43] Payne, Artificial *Intelligence*, 10, 26.

[44] Ralph D. Thiele and Johann Schmid, "Hybrid Warfare – Orchestrating the Technology Revolution," ISPSW *Strategy Series: Focus on Defense and International Security* 663 (2020): 1-11, https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf

simulator AlphaWar.[45] Thus, AI may bring the ambiguity of HW to the next level, which would have strategic-level implications.

Thirdly, AI weapons enable the creation of strategic partnerships, including between state and non-state actors. To Hoffman, achieving ambiguity is often connected to using proxies. For example, Iran has supported Hezbollah's efforts against Israel, although Tehran has never officially been at war with Israel. The proliferation of AI systems can help in starting and maintaining such relationships. Those relationships are usually built based on mutual benefits like arms trade. AI-based weapons, which are inexpensive and their stockpile cannot be monitored in comparison to other types of weapons, are great items for such exchange between state and non-state actors. Specifically, some countries can decide to weaponise their proxies by supplying them with AI-based military capabilities.[46] Such an argument can also be made in the context of cyber weapons. Still, as presented in this analysis, AI-based technologies are more disruptive and, consequently, would be more consequential for such partnerships. Thus, growing such AI-enabled relationships can cause a shift in the international balance of power and, therefore, have a more robust strategic effect.

[45] John Lopez, " Chinese Scientists Develop War Games AI AlphaWar; Passes Turing Test with Experts!," *Tech Times*, February 23, 2023, https://www.techtimes.com/articles/288098/20230223/alphawar-passes-artificial-intelligence-military-war-games-turing-test-china.htm.
[46] Thiele, Artificial *Intelligence – A key enabler of hybrid warfare,* 10.

In sum, AI validates many of Hoffman's earlier prophecies about future warfare, such as the synergistic combination of capabilities, easy access to conflict, ambiguity, and the partnerships between different actors. In fact, in many cases, AI capabilities have the potential to multiply the effect of these processes so that they obtain strategic-level implications. This makes AI-enabled HW qualitatively different from IT-enabled HW. Still, AI could potentially not only enable but also counter the conduct of HW.

How Artificial Intelligence Counters Hybrid Warfare

It is worth noting that many of the AI-based technologies that can be used to enable HW can also be utilised against it. For example, AI algorithms can proliferate propaganda but can also fight it by distinguishing real from deepfake videos.[47] AI can provide actors with resources to fuel their covert relationships but can also expose criminal and terrorist networks that engage in HW.[48] Thus, the effect of most AI capabilities on HW is subjective, depending on who their operator is. Still, some AI technologies are distinctly more helpful for operational preparedness against HW.

Firstly, AI-based systems can significantly enhance training and exercise, which are crucial to countering HW. AI-supported simulators now provide realistic exercise scenarios with the right level of complexity, which is beneficial for tactical training. Authors

[47] Mazzucchi, *AI-based technologies in hybrid conflict,* 11.
[48] Thiele, *Artificial Intelligence – A key enabler of hybrid warfare,* 8.

argue that the lessons-learnt in such activities can inform operational concepts.[49] Yet, with the advent of augmented and virtual reality, the interface of such simulators is also becoming easier to operate, so such AI-based platforms can now also be used at the strategic decision-making level. When faced with an HW campaign, decision-makers must act flexibly and dynamically. Training such a mindset requires a sophisticated exercise environment, which AI delivers. New AI platforms allow strategic leaders to experience more realistic and demanding table-top exercises, which can train them in giving appropriate strategic direction when required. It is worth noting that AI can still not simulate any black swan events to truly reflect reality.[50] Yet, the AI models are becoming increasingly more complex and already have an effect across the chain of command, including at the strategic level.

Secondly, AI can also provide decision-makers with better situational awareness in the case of real-world HW. To Hoffman, due to the ambiguity of HW, the critical enabler to a successful defence against HW is enhanced situational awareness. The challenge is that today, there is a staggering amount of unstructured intelligence, surveillance, and reconnaissance data, which takes

[49] For *example*: Davis and Bracken, *Artificial intelligence for wargaming*, 1-3.
[50] Davis and *Bracken*, *Artificial intelligence for wargaming*, 11

time to process.[51] AI provides a natural solution to this problem and can make sense of large amounts of data by identifying anomalies and patterns. Using automatic target recognition algorithms, AI-driven systems can also identify targets, including at the strategic level, such as aircraft carriers.[52] Indeed, such a system of systems has strategic-level implications, so the United States reportedly acquired an AI-based Command and Control system to deal with information overload and reduce reaction time.[53] Such platforms are able to not only provide the best real-time situational awareness but are also capable of surpassing human talent in predictive analysis. For example, today, AI models can predict HW-related events by looking for significant events, such as bomb purchases.[54] Thus, decision-makers receive the best situational awareness and predictive intelligence based on AI systems, influencing their strategic choices.

In summary, there are clear strategic-level implications of introducing AI in the defence architecture against HW. This is why scholars often conclude that due to the emergence of AI technologies, the conduct of as well as the defence against HW

[51] Zachary Davis, "Artificial Intelligence on the Battlefield. Implications for Deterrence and Surprise," *PRISM* 8, no. 2 (2019): 118, https://www.jstor.org/stable/26803234.
[52] Davis, *Artificial Intelligence on the Battlefield*, 120.
[53] Jeffrey Kent, *Artificial Intelligence (AI)-based C2 Digital Assistant* (US Navy, 2016) https://www.navysbir.com/n16_2/N162-074.htm; Yan, *The Impact of Artificial Intelligence*, 8.
[54] Thiele, *Artificial Intelligence – A key enabler of hybrid warfare,* 8.

enters a new era.[55] However, security organisations need to implement significant institutional reforms to fully use AI's defensive potential against HW.[56] The next part briefly discusses some of those organisational challenges.

Implications for the West

In theory, AI systems can significantly enhance the countermeasures against HW. However, in practice, this depends on the West overcoming several challenges in understanding and adopting AI solutions into its security and defence architecture.

Firstly, there are hardware, software, and other technological challenges. To be trained, AI models need raw data from the Internet. This task is complicated within defence organisations, whose primary concern is their classified information. This results in various physical and digital barriers to the outside world. Moreover, even if they connect to the World Wide Web, models must be trained based on neither poor nor high-quality data.[57] The latter is equally devastating to creating fit-for-purpose models because the resulting algorithms would be able to perform only with a narrow range of data. Thus, to make AI-based systems robust, a delicate

[55] For example: Mazzucchi, *AI-based technologies in hybrid conflict,* 5; Șușnea and Buță, *Artificial Intelligence in Hybrid Warfare*, 294.
[56] Yan, *The Impact of Artificial Intelligence*, 14.
[57] James Sharp et al., *Robustness of Artificial Intelligence for Hybrid Warfare* (Brussels, NATO Science and Technology Organisation, 2021), 2-3, https://reports.nlr.nl/items/4689cd25-a934-4d83-971b-f5077e4574b4

technological balance must be struck, which requires in-depth expertise.[58]

Secondly, governmental and intergovernmental security organisations are unattractive employers for high-end experts. More specifically, unlike in Russia, where AI-related innovation is concentrated in the central government, in the West, private companies are the leaders in deriving value from emerging and disruptive technologies.[59] The industry has more resources and is generally more prone to making high-risk investments in research and development because, unlike governmental institutions, it does not have to explain its budget to a countrywide body of voters. Thus, being able to develop their potential without the lag of bureaucracy and with more funding, most AI innovators opt for a private sector career. Thus, security and defence organisations have no choice but to develop stronger partnerships with private industry. This entails adopting business-oriented language and processes, which are usually not a natural fit for those organisations.

Thirdly, to strike the best partnership deals and accomplish the entire set of technological tasks, governmental and intergovernmental organisations need to act very quickly or at least

[58] Mazzucchi, *AI-based technologies in hybrid conflict,* 13.
[59] Thornton and Miron, *Towards the 'Third Revolution in Military Affairs'*, 2; Thiele, *Artificial Intelligence – A key enabler of hybrid warfare,* 10.

faster than their traditional institutional pace.[60] Technological innovation is constantly accelerating, and to catch up, the defence community needs to reinvent its decision-making process and make it more agile. Ideally, decisions should also be implemented more quickly based on expedited acquisition processes.

Finally, to make matters worse, to receive the green light from their political leadership for implementing new AI-based solutions, security and defence staff in governmental and intergovernmental organisations first must respond satisfactorily to rather complicated questions. Those questions primarily concern budgets, ethics, and law. For example, political leaders, much more risk-averse than their industry counterparts, are concerned about making long-term investments with less than obvious returns. At the same time, the current state of AI research and development is characterised by a high degree of hype and, thus, carries an inherent financial risk. Perhaps even more challenging are the questions related to ethics and law. For instance, Western leaders have voiced concerns about the responsible use of AI, which is hard to measure in the context of the black box problem or the lack of in-depth understanding of how exactly an AI system works. Also, there is hesitation to adopt technological solutions which are still not regulated. This exposes organisations to various risks with a low degree of predictability. For

[60] Mazzucchi, *AI*-based *technologies in hybrid conflict,* 7.

example, there are still open questions regarding AI’s processing and exploitation of personal data.[61]

In summary, security and defence organisations face plenty of challenges in understanding and adopting AI-based systems at the speed of technology. However, organisations such as NATO are already progressing in confronting those challenges. One recent NATO initiative in that regard is DIANA.

The Defence Innovation Accelerator for the North Atlantic

According to public information, DIANA aims to accelerate the development of technological solutions to critical transatlantic challenges. To do that, DIANA creates an innovation ecosystem by linking existing technological pioneers in industry, startups, and academia with the end-users in the defence sector.[62] All of them are expected to co-develop next-generation dual-use technologies.

The process starts with NATO publishing requests for proposals or so-called challenges. Each challenge focuses on a specific technology, such as AI, autonomy, and quantum computing, and aims to elicit proposals from innovators on how those technologies can serve security and defence purposes. The accepted proposals are then matched with a DIANA technology test centre located in one of NATO’s countries so that the proposed solution undergoes

[61] Pitman, *Perfect Strangers*, 39-41.
[62] Defence Innovation Accelerator for the North Atlantic, “FAQ,“ n.d., https://www.diana.nato.int/faq.html.

a series of tests to validate its current readiness level and future potential. Pending successful completion of the tests, the innovator is then transferred to an accelerator site, which helps them in further maturing their technologies.[63] Importantly, all those technologies are also placed in a databank, accessible to governmental and private investors, who are then more comfortable directing their resources to technologies which have already been verified and accelerated based on DIANA's network.

What is also worth noting is how DIANA was unveiled. The ecosystem was officially launched at the NATO 2021 Brussels Summit as part of the so-called 2030 Agenda, a framework aimed at making the Alliance remain "ready today to face tomorrow's challenges".[64] Therefore, DIANA is part of a larger initiative to implement institutional reforms at NATO, endorsed at the highest decision-making level. Presumably, this opens a political window of opportunity to tackle the AI-related challenges that NATO faces as any other security and defence organisation. While DIANA started only recently, the model can potentially address those challenges.

Firstly, regarding software and hardware, NATO uses DIANA to attract innovative ideas on how to solve those technology-related challenges. DIANA's Board of Directors approves the so-called

[63] Defence Innovation Accelerator for the North Atlantic, *FAQ*.
[64] NATO, "NATO 2030: Making a Strong Alliance Even Stronger," n.d., https://www.nato.int/nato2030/.

Strategic Direction every two years, which sets DIANA's priorities for each period. From the first Strategic Direction, adopted in December 2022, it is visible that the Alliance appreciates those technology issues and is determined to find more innovative solutions.[65] One of the priority areas is Secure Information Sharing, which is precisely at the heart of the software and hardware challenges that NATO needs to overcome to fully and effectively leverage AI-based tools. Suppose the Alliance can strike the right balance between security and constant information and data flow. In that case, AI-based algorithms can be fed the raw data they need from the Internet to train and develop.

Secondly, regarding partnering with and aligning with industry standards, DIANA is a significant step forward. The initiative vows to work with "Alliance's best and brightest start-ups, scientific researchers, and technology companies".[66] Importantly, to be an attractive partner for innovators, including in the AI field, DIANA adopts business-like language, which is novel to NATO. Instead of using more bureaucratic terms such as "requests for proposals", DIANA chooses industry jargon and emphasises keywords such as "accelerator programmes" and "challenges". This is an apparent attempt to become more relatable to innovators and entrepreneurs.

[65] NATO, "NATO approves 2023 strategic direction for new innovation accelerator," December 12, 2022, https://www.nato.int/cps/en/natohq/news_210393.htm

[66] Defence Innovation Accelerator for the North Atlantic, *FAQ*.

DIANA’s website also mentions AI as a priority area to ensure the interest of AI innovators is solicited.[67]

Thirdly, DIANA addresses the issue of the speed of technology. Except for the test centres and accelerator sites, the DIANA ecosystem includes the so-called Rapid Adoption Service.[68] The most promising DIANA technologies will receive additional support from procurement specialists, investors, and other subject-matter experts and mentors. As a result, if required, they will be manufactured and then integrated into NATO’s defence architecture as soon as possible. Notably, one can argue that AI technologies fit into NATO’s definition of “most promising“. In its first-ever strategy on AI, adopted in 2021, NATO defined AI as the most pervasive among all emerging and disruptive technologies, which is a clear sign that AI is getting prioritised.

Finally, DIANA’s work is complemented by other NATO policies and initiatives that aim to respond to pressing financial, legal, and ethical questions related to the Alliance’s use of AI and other disruptive technologies. For example, in 2022, NATO launched its Innovation Fund, the world’s first multi-sovereign venture capital fund. More specifically, the NATO international secretariat secured a 1-billion-euro investment from NATO nations, which covers the financial

[67] Defence Innovation Accelerator for the North Atlantic, *FAQ*.
[68] Defence Innovation Accelerator for the North Atlantic, *FAQ*.

demands of DIANA for the next 15 years.[69] Meanwhile, the Alliance's strategy on AI set out the so-called Principles of Responsible Use. In this way, instead of shying away from the complex ethical and legal questions in the context of AI, NATO aims to become a trendsetter in how AI is used in the security and defence sector. For instance, the strategy mentions lawfulness, accountability, and governability.[70] The potential effect is two-fold. NATO challenges the different AI standards that its opponents usually apply while ensuring its own political leadership is on board with AI technologies, knowing they will be implemented and exploited according to certain principles.

All in all, DIANA, as well as the other NATO initiatives designed to derive value from AI technologies, appear promising. Follow-up research will need to be conducted after DIANA reaches full operational capability to study the results of the ecosystem.

Conclusion

After the analysis, the opening argument can be supported and detailed. While the previous IT RMA may have led to unsatisfactory results, AI could transform war and specifically HW, including at the strategic level. It enables as well as counters HW.

[69] NATO, " Allies take further steps to establish NATO Innovation Fund," March 20, 2023, https://www.nato.int/cps/en/natohq/news_213002.htm.

[70] NATO, " Summary of the NATO Artificial Intelligence Strategy," October 22, 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Firstly, it enables HW in the context of operational capabilities and decision-making. Specifically, AI systems can significantly enhance multimodal warfare, a defining feature of HW, by analysing which combination of traditional capabilities would yield the best result in any operational environment. AI has also created new capabilities, particularly for irregular warfare, which is an intrinsic part of HW. Due to these new combinations and weapons of war, forces can achieve a previously unattainable level of tactical and operational synergies, which can indirectly influence the strategic course of a conflict. AI can also affect strategic decision-making more directly. The analysis uncovered three mechanisms to that end. AI reduces the cost of HW and, thus, makes the decision to engage in such conflict easier. AI systems can also enhance the element of strategic surprise and enable strategic partnerships since AI weapons can be a great item for arms trading. All of these causal mechanisms, related to capabilities and decision-making, were a part of Hoffman’s original framework. Still, the emergence of AI gives them further credibility and foundation.

Secondly, AI-based systems can also counter HW. This is due to the emergence of AI-enabled exercises and situational awareness. Nowadays, AI-driven simulations are much more complex and can offer more realistic HW scenarios. At the same time, the training platforms also have a more accessible interface, which allows the participation of strategic decision-makers. They can now be trained to be more agile and better deal with ambiguity if an HW scenario unfolds. Those political appointees and strategic commanders can now also receive enhanced situational awareness and intelligence briefs prepared with the help of AI. Such intelligence enables better strategic decision-making, especially during real-world HW, where one must identify hidden patterns and anomalous behaviour in an overwhelming information environment. Having understood the disruptive nature of AI, NATO has undertaken several initiatives, such as DIANA, aimed at adopting AI at the speed of technology.

Military officers and policymakers now seem to appreciate that AI technologies give rise to qualitatively different HW. Even if, in the earlier 21st century, one could have made the case that HW is not an entirely new phenomenon and that there are many historical references to multi-modal conflicts, the emergence of AI and its security applications changed the narrative. In the era of AI, the factors that complicate the work of defence planners and which Hoffman aimed to capture in his HW concept are exacerbated and have strategic implications. That is, AI technologies lead to exponentially more ambiguity on the battlefield and synergy between different actors and capabilities. Thus, the novelty of HW is not limited to the lower levels of war. To capture this qualitative change and draw the attention of policymakers, the literature on the HW-AI nexus might benefit from promoting the concept of AI-enabled HW.

However, more studies are needed to make this concept more rigorous. For example, follow-up research could consider how specific AI-enabled technologies, such as quantum computing and novel propulsion, influence the different modes of HW. To link the academic and policy efforts, studies must also explore the level of interinstitutional cooperation, specifically between NATO and the EU, regarding countering AI-enabled HW. Such research must also focus on DIANA's long-term development. DIANA will inevitably face challenges, such as the different levels of engagement and technological innovation by different NATO Allies, so evaluating the initiative's agility to deal with those in the coming years will be important.

ARTIFICIAL INTELLIGENCE: MODELING OF TIME-DEPENDENT PROCESSES

Tsveti Monova

Abstract: This research delves into the significance of AI in modeling time-dependent processes, using AI algorithms to analyze historical data for predictive insights. It demonstrates AI's role in improving decision-making, operational efficiency, and resource allocation across various domains. With real-world examples, the paper emphasizes AI's transformative impact in understanding and harnessing time-dependent phenomena.

Key words: Artificial Intelligence, NATO, Command and Control (C2), Time-dependent processes, Clustering.

Artificial intelligence (AI) has the potential to revolutionize the way that NATO operates by providing faster and more accurate analysis of data, enhancing situational awareness, and improving decision-making. However, it's important to note that humans are still critical to the success of NATO operations, and AI should be used to augment and support human capabilities rather than replace them.

AI and human cooperation in NATO can take many forms, including decision support, situational awareness, training and simulation, and the development of autonomous systems. AI can analyze vast amounts of data from multiple sources and provide insights and recommendations to human decision-makers, helping them make better-informed decisions faster and more efficiently. AI can also monitor and analyze data in real-time to enhance situational awareness, allowing human operators to respond more quickly and effectively to changing situations.[1]

In addition, AI can be used to develop autonomous systems that can augment human capabilities in NATO operations, such as surveillance and reconnaissance, logistics, and more. However, it's important to ensure that humans remain in control of AI systems and that they are used in an ethical and responsible manner.

Overall, the cooperation between AI and humans in NATO has the potential to enhance operational effectiveness, efficiency, and safety. By leveraging the strengths of both AI and humans, NATO can better achieve its mission of promoting security and stability in the Euro-Atlantic area and beyond.[2]

[1] John, M. (2018). *Artificial intelligence*.

[2] Lesser, V. R., Cohen, P., & Lehnert, W. (1992). *Center for Artificial Intelligence*. Defense Technical Information Center. https://doi.org/10.21236/ada282272

Artificial intelligence (AI) is a field of computer science that focuses on developing machines that can perform tasks that typically require human intelligence, such as understanding natural language, recognizing objects in images, making decisions, and solving complex problems.

Modeling of time-dependent processes in AI refers to the process of creating models that can predict or simulate how a system will evolve over time. This involves analyzing data from the past and present to identify patterns and trends, and using that information to make predictions about the future.

Various AI techniques can be used for modeling time-dependent processes, including:

Time series analysis: This involves analyzing data that is collected over time to identify patterns and trends. Time series analysis can be used to make predictions about future values of the data, based on past and present values.

Markov models: These are models that use probabilistic methods to predict how a system will evolve over time. Markov models are often used in applications such as speech recognition and natural language processing.

Neural networks: These are machine learning models that are designed to mimic the way the human brain works. Neural networks can be used to predict how a system will evolve over time by training the network on past and present data.

Overall, modeling time-dependent processes in AI is an important area of research, with applications in a wide range of fields including finance, healthcare, transportation, and more.

AI and humans can cooperate in NATO in several ways. Here are some examples:

Decision support: AI can be used to provide decision support to humans in NATO. For example, AI systems can analyze vast amounts of data and provide insights and recommendations to human decision-makers. This can help humans make better-informed decisions faster and more efficiently.

Situational awareness: AI can be used to enhance situational awareness in NATO. For example, AI systems can analyze data from various sensors and sources, such as satellite imagery and social media, to provide real-time insights into potential threats and opportunities. This can help humans respond more quickly and effectively to changing situations.

Training and simulation: AI can be used to enhance training and simulation in NATO. For example, AI systems can simulate complex scenarios and provide feedback to human trainees. This can help humans develop their skills and knowledge in a safe and controlled environment.

Autonomous systems: AI can be used to develop autonomous systems that can operate in complex and dangerous environments. These systems can be used to augment human capabilities in NATO operations, such as surveillance and reconnaissance, logistics, and more.

Overall, AI and humans can work together in NATO to enhance operational effectiveness, efficiency, and safety. However, it's important to note that humans should remain in control of AI systems and ensure that they are used in an ethical and responsible manner.

AI has the potential to transform military decision-making by providing faster and more accurate analysis of large volumes of data, identifying patterns and trends that may not be immediately apparent to human analysts, and generating recommendations for decision-makers.

Here are some examples of how AI can be used in military decision-making:

Predictive maintenance: AI can be used to predict when equipment will fail and when it will need maintenance. This can help military planners better allocate resources and reduce downtime.

Logistics: AI can be used to optimize the movement of troops and supplies. This can help military planners make better decisions about how to deploy resources in a given area.

Situational awareness: AI can be used to monitor and analyze large volumes of data from multiple sources, such as radar, satellites, and social media. This can help military planners identify potential threats and opportunities in real time.

Risk assessment: AI can be used to assess the risk of a particular course of action. This can help military decision-makers weigh the potential costs and benefits of different options.

Autonomous systems: AI can be used to control autonomous systems, such as drones and robots. This can help military planners conduct reconnaissance and surveillance without putting human soldiers at risk.[3]

[3] NATO’s Data and Artificial Intelligence Review Board. (2022). In Summary of the establishment of the Board. NATO.

*__However, it's important to note that AI should not replace human decision-makers in military operations. Rather, AI should be used to support and enhance human decision-making. Human oversight and control are critical to ensure that AI is used in an ethical and responsible manner.__

One potential product for time-dependent processes involving AI and human cooperation in a NATO context could be a Command and Control (C2) System Enhancement Platform. Here are some features and benefits that could be incorporated into such a product:

- Real-time Situational Awareness: Develop an AI-powered system that collects, analyzes, and visualizes data from various sources (such as sensors, satellites, social media, etc.) to provide comprehensive real-time situational awareness to NATO commanders and decision-makers.
- Predictive Analytics: Implement advanced AI algorithms to analyze historical data, patterns, and trends, enabling the system to make predictions and generate actionable insights about future events and threats. This would help in proactive decision-making and resource allocation.

- Dynamic Task Assignment: Create an intelligent task assignment system that optimizes the allocation of resources, including both AI-driven autonomous systems and human operators, based on the current operational demands, capabilities, and availability of each entity.
- Adaptive Command and Control: Develop an adaptive C2 framework that leverages AI capabilities to dynamically adjust command structures, decision-making processes, and resource allocation based on changing operational requirements, mission priorities, and the availability of human and autonomous assets.
- Collaboration and Communication Tools: Build collaborative platforms and communication tools that facilitate seamless interaction, information sharing, and coordination between human operators and AI systems. This could include secure messaging, video conferencing, and data-sharing capabilities.
- Training and Simulation: Integrate virtual training and simulation modules into the system to enhance the readiness and effectiveness of NATO forces. This could involve creating realistic scenarios for joint training exercises, incorporating AI-driven adversaries,

and providing feedback and performance evaluations to participants.[4]

To support this project research is done on how Adaptive Command and Control works and how it affects the effectiveness.

Adaptive Command and Control (C2) systems, bolstered by artificial intelligence (AI), represent a cutting-edge approach to optimizing military operations within NATO. These dynamic frameworks enable commanders to respond swiftly to ever-changing operational requirements, mission priorities, and the availability of human and autonomous assets. By harnessing the power of AI, an adaptive C2 system enhances the effectiveness and efficiency of decision-making processes, resource allocation, and communication, ultimately fortifying NATO's readiness and resilience in the face of evolving security challenges.

At the core of an adaptive C2 system lies the flexibility to reconfigure command structures on-the-fly. AI algorithms analyze real-time operational data, consider the availability and expertise of personnel, and assess mission objectives to

[4] Stanley-Lockman, Z., & Hunter Christie, E. (2021). An Artificial Intelligence Strategy for NATO. NATO.

suggest or automatically adjust command hierarchies. This agility empowers commanders to allocate the appropriate level of authority to the most suitable entities, streamlining communication and expediting operational responsiveness.

With the aid of AI capabilities, an adaptive C2 system significantly enhances decision-making processes. Real-time data analysis, historical insights, and predictive modeling generated from various sources enable commanders to identify emerging threats and assess risks swiftly. By offering optimal courses of action, the system empowers decision-makers to navigate complex scenarios with timely and informed choices, maximizing mission success.

Optimal resource allocation is paramount to operational effectiveness. AI-driven algorithms within an adaptive C2 system analyze the availability, capabilities, proximity, and readiness of both human and autonomous assets. Based on mission priorities and rapidly changing operational requirements, the system suggests or automatically adjusts resource assignments, ensuring efficient utilization and bolstering NATO's ability to leverage its full potential.

Comprehensive situational awareness is critical to making informed decisions in the field. An adaptive C2 system excels at integrating and fusing data from diverse sources, including AI-driven autonomous systems. By compiling data from sensors, platforms, and various intelligence sources, the system offers real-time insights that present a holistic view of the battlefield. The system can identify critical information, detect patterns, and provide actionable intelligence, enabling commanders to act decisively.

Effective communication and seamless collaboration are fundamental to mission success. An adaptive C2 system facilitates rapid and secure information sharing, task assignment, and coordination among human operators, autonomous systems, and AI algorithms. This cohesive approach promotes unity of effort, enhances interoperability, and maximizes the operational effectiveness of NATO forces.

Incorporating AI capabilities into the command and control processes brings unparalleled advantages to NATO operations. An adaptive C2 system empowers commanders with unprecedented flexibility, dynamic decision-making support, and resource optimization capabilities. The integration of AI-driven data analysis, comprehensive situational awareness, and enhanced communication cultivates a proactive and highly adaptable operational environment for NATO. With these advancements, NATO can swiftly address complex and rapidly evolving challenges, bolster its readiness, and reinforce its position as a formidable global security alliance. Embracing the power of adaptive C2 and AI, NATO fortifies its ability to protect member nations, project stability, and promote peace in an ever-changing world.

By incorporating AI capabilities into the command and control processes, an adaptive C2 framework can enable NATO to respond effectively and efficiently to evolving operational requirements. It enhances decision-making, optimizes resource allocation, promotes agility, and improves the overall operational effectiveness of the military forces.[5]

Additional aspects to consider regarding an adaptive Command and Control (C2) system:

An adaptive Command and Control (C2) system is a valuable tool that provides decision support and dynamic tasking capabilities for military commanders and decision-makers. By analyzing data, generating simulations, and running scenario-based models, the system offers recommendations and insights to aid in the decision-making process. This reduces cognitive load on human operators and enhances the quality of decisions made under time constraints.

[5] C2 Agility is the capability of C2 to successfully effect, cope with, and/or exploit changes in circumstances. C2 Agility enables entities to effectively and efficiently employ resources in a timely manner. NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.

The adaptive C2 system can dynamically task and re-task assets based on changing operational requirements. For instance, if new intelligence or threats are identified, the system can automatically reallocate resources to address the emerging situation. This flexibility enables efficient resource utilization and the ability to respond rapidly to evolving mission priorities.[6]

Ensuring interoperability between different forces, platforms, and coalition partners is crucial for an adaptive C2 system. It should be scalable to handle information exchange and coordination across various levels of command, from individual units to joint and multinational operations. This promotes effective coordination and cooperation within NATO and facilitates seamless integration of forces.

Human decision-making can be influenced by cognitive biases and limitations. An adaptive C2 system can mitigate these biases by providing objective analysis, data-driven insights, and alternative perspectives. By leveraging AI algorithms, the system can identify potential biases and present commanders with a more comprehensive and unbiased view of the

[6] Tillman, M.E. and Conley. K.M., 'Designing and Assessing Command and Control to Deal with Complex and Ill-Structured Operational Environments'. In Operations Assessment in Complex Environments: Theory and Practice, edited by Adam Shilling. NATO STO, 2019.

operational environment, thereby improving decision-making accuracy.

C2 system continuously learns from past operations, incorporating lessons learned and feedback from human operators. By leveraging machine learning algorithms, the system can improve its decision-making capabilities over time, adapt to evolving tactics and strategies, and refine its performance based on real-world feedback. This iterative learning process helps enhance the system's effectiveness and responsiveness.[7]

As AI and autonomous systems become more prevalent in military operations, an adaptive C2 system must prioritize cybersecurity and resilience. It should have robust measures in place to protect critical information, secure communications, and defend against cyber threats. This ensures the system's reliability, integrity, and continuity of operations even in the face of cyberattacks or disruptions.

Overall, an adaptive C2 system leverages AI capabilities to enhance the decision-making processes, optimize resource allocation, and promote effective coordination in dynamic

[7] NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.

operational environments. It combines the strengths of AI algorithms and human operators to create a synergistic partnership that maximizes the operational effectiveness of NATO forces.

To effectively harness and leverage information, perform efficient searches, locate pertinent data, and promptly execute actions, the development of a website becomes imperative. Particularly, in the context of increasing prevalence of AI and autonomous systems within military operations, an adaptive Command and Control (C2) system necessitates the prioritization of cybersecurity and resilience. This entails implementing robust safeguards to shield vital information, ensure secure communications, and counteract cyber threats. By establishing such measures, the website can guarantee the reliability, integrity, and uninterrupted functionality of operations, even when confronted with cyberattacks or disruptions.

A website designed for rapid response to crises would typically prioritize the following features and elements:

Clear and accessible interface: The website should have a user-friendly design with intuitive navigation. Users should be able to quickly find the information and resources they need without any confusion.

Emergency contact information: Provide prominently displayed emergency contact numbers, such as local emergency services, hotlines, and crisis centres. Make it easy for users to access these numbers from any page on the website.

Real-time updates: Include a dedicated section for real-time updates on the crisis situation. This can include news alerts, official statements, and other relevant information. Consider integrating social media feeds or a live blog to keep users informed about the latest developments.

Emergency resources and guidelines: Provide comprehensive resources and guidelines to help users during a crisis. This may include instructions on how to handle different emergency situations, safety tips, evacuation plans, and first aid techniques. Ensure that these resources are easily accessible and well-organized.

Communication channels: Set up communication channels to allow users to report emergencies, request assistance, or ask questions. This can include online chat support, contact forms, or dedicated helpline numbers. Promptly respond to user inquiries to provide timely assistance.

Maps and location-based information: Incorporate maps and location-based information to help users identify safe zones, emergency shelters, medical facilities, and other relevant places in their vicinity. Interactive maps with overlays displaying critical information can be particularly helpful.

Multilingual support: If the crisis occurs in an area with diverse language speakers, ensure the website supports multiple languages. Offer translations or provide links to resources in different languages to cater to a wider audience.

Mobile responsiveness: Optimize the website for mobile devices to ensure compatibility across various screen sizes and operating systems. This is crucial as people may need to access the website on their smartphones during emergencies.

Accessibility features: Implement accessibility standards to ensure that individuals with disabilities can use the website. Provide features such as alternative text for images, keyboard navigation support, and adjustable text size.

Partnerships and collaborations: Collaborate with relevant organizations, government agencies, and NGOs to provide a comprehensive and coordinated response. Display partner logos or provide links to their websites for additional resources and support.

Data security and privacy: Prioritize the security and privacy of user data. Use encryption protocols, secure servers, and privacy policies to ensure user trust and protect sensitive information.

Subcategories:

Branches:

- Region/Location: Allow users to filter branches based on geographical regions or specific locations.
- Type: If your organization has different types of branches (e.g., medical, relief, coordination), provide a filter to categorize and display them accordingly.

Budgets:

- Range: Offer a budget range filter to allow users to specify their financial constraints or filter projects based on available funding levels.

Staff:

- Expertise/Role: Allow users to filter staff based on their specific roles or areas of expertise, such as medical professionals, logistics experts, or communication specialists.

Availability: If applicable, provide a filter option for users to find staff members who are currently available or actively involved in crisis response efforts.

Location:

- Country/Region: Enable users to filter based on specific countries or regions affected by the crisis.

Proximity: Implement a proximity filter that allows users to find resources or services near their current location or a desired location.

Logistics: If your logistics involve various categories, such as transportation, storage, or distribution, provide filter options to help users narrow down their search.

Availability: Allows users to filter logistics services based on availability or capacity, particularly useful when resources may be limited during a crisis.[8]

When designing and implementing these filters, providing a user-friendly interface that allows for selecting multiple filter options simultaneously should be considered, as users may have complex search requirements. Additionally, make sure to test the filters thoroughly to ensure they provide accurate results and perform well, especially if dealing with large datasets or complex filtering criteria.

[8] Lawrence, D., & Tavakol, S. (2007). *Balanced Website Design.* Springer London. https://doi.org/10.1007/978-1-84628-795-4

*Remember that the specific design and layout of the website will depend on the nature of the crisis and the target audience. Conduct user research and gather feedback to continuously improve the website's effectiveness in meeting the needs of those affected by the crisis.

To leverage AI on crisis response website, the following ways should be considered:

Natural Language Processing (NLP): Implement NLP techniques to analyze and understand user queries and provide relevant responses. This can be particularly useful for chatbots or virtual assistants on website, allowing users to ask questions or seek assistance in a conversational manner (search tool).

Automated Information Extraction: Apply AI techniques to automatically extract relevant information from various sources, such as news articles, official statements, or reports. This can help provide timely updates and gather crucial data for decision-making during a crisis.

Predictive Analytics: Employ predictive analytics models to forecast the impact and spread of the crisis, enabling proactive decision-making. AI algorithms can analyze historical data, real-time information, and various parameters to generate forecasts and insights about the crisis progression.

Resource Allocation Optimization: Utilize AI algorithms to optimize resource allocation during a crisis. By analyzing available resources, demand patterns, and logistical constraints, AI can help optimize the distribution of supplies, personnel, and equipment to ensure efficient utilization and effective response.

Data Analytics and Visualization: Leverage AI-powered data analytics and visualization tools to process and present complex crisis-related data in a digestible format. This can help decision-makers, responders, and the public/governmental or crisis centre staff gain a better understanding of the situation, trends, and patterns.

Providing a general overview of how an IT expert might approach coding a deficit migration budget regarding refugees in Italy and the social framework of support for refugees. However, specific implementation details would depend on the requirements, available data, and technologies used. Here's a high-level outline:

Data Gathering: Collect relevant data related to the migration of refugees in Italy, including historical budgetary information, social support programs, population demographics, and migration patterns. This may involve collaborating with government agencies, NGOs, and research institutions to access reliable data sources.

Data Cleaning and Preprocessing: Clean and preprocess the collected data to ensure consistency and remove any inconsistencies or outliers. This step may involve data normalization, handling missing values, and resolving data discrepancies.

Database Design: Design a database schema that can accommodate the collected data. Define appropriate tables, relationships, and data structures to efficiently store and manage the information.

Backend Development:

- Develop the backend infrastructure using a suitable programming language and framework (Python with Django or Node.js with Express).
- Implement RESTful APIs to handle data retrieval, updates, and calculations.
- Create endpoints for retrieving budget data, social support framework details, and migration statistics.

Budget Deficit Calculation:

- Analyze the budget data and calculate the deficit caused by refugee migration. This may involve comparing the allocated budget for refugee support with the actual expenses incurred.

- Consider factors such as accommodation, healthcare, education, employment support, and social integration programs.
- Perform calculations to determine the budget deficit or surplus resulting from refugee migration.

Social Support Framework Analysis:

- Analyze the social support framework for refugees in Italy, including the types of programs, eligibility criteria, and their effectiveness.
- Develop algorithms or models to assess the impact of social support initiatives on refugees' integration, well-being, and socioeconomic factors.
- Generate insights and visualizations to demonstrate the relationship between social support efforts and migration outcomes.

Migration Impact Analysis:

- Analyze the population changes and demographics resulting from refugee migration.
- Use statistical methods and data visualization techniques to illustrate the correlation between migration and various socioeconomic indicators, such

as employment rates, education levels, and income distribution.

- Assess the impact of migration on the overall budget, economy, and society.

Front-end Development:

- Design and develop the user interface using web technologies like HTML, CSS, and JavaScript.
- Integrate data visualizations, charts, and interactive components to present the budget deficit, social support framework, and migration impact in a user-friendly manner.
- Implement user authentication and access control mechanisms if required.

Testing and Deployment:

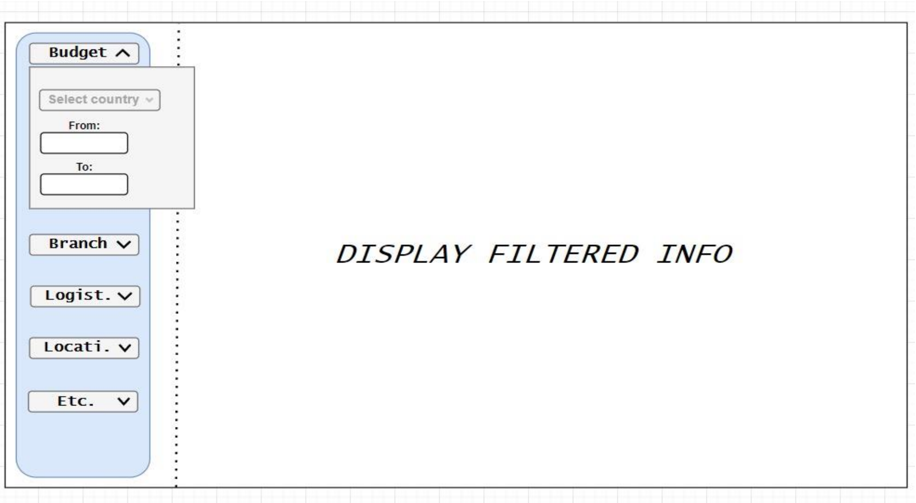
- Conduct thorough testing to ensure the accuracy and reliability of the implemented functionalities.
- Deploy the application on a web server or cloud platform to make it accessible to users.
- Monitor the application's performance and address any issues or bugs that arise.

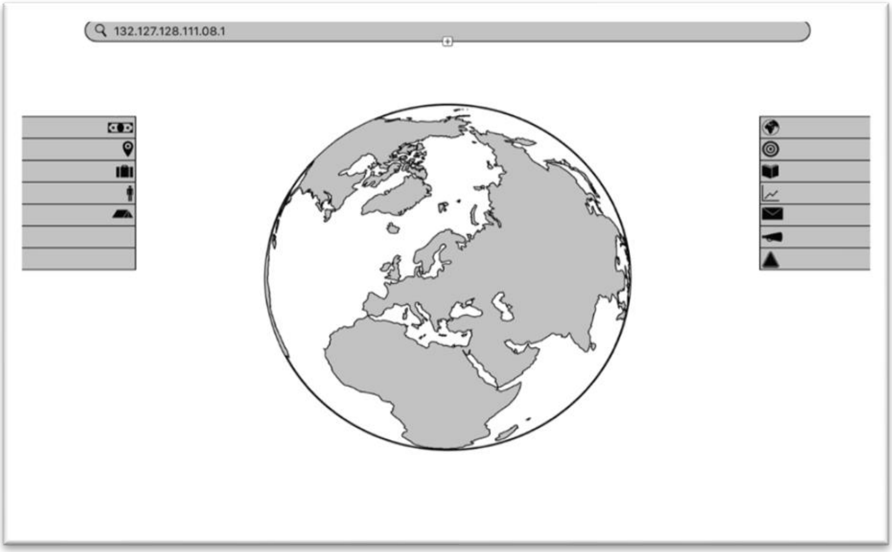
Maintenance and Updates:

- Regularly update the system with new budget data, social support policies, and migration statistics to keep the information current.
- Monitor changes in migration trends, budget allocations, and social programs to ensure the accuracy and relevance of the application.
- Address any user feedback, fix bugs, and implement enhancements as necessary.

It's important to note that coding a comprehensive and accurate system for budget deficit migration and social support analysis requires expertise in data analysis, database management, backend development, front-end design, and domain knowledge in refugee migration policies. Collaboration with domain experts, economists, and policymakers can further refine the system's accuracy and usefulness.[9]

[9] Lawrence, D., & Tavakol, S. (2007)*. Balanced Website* Design. Springer London. https://doi.org/10.1007/978-1-84628-795-4





*To provide you with a more detailed example and help you visualize how this project could be executed, I will elaborate on it**.** Remember that this example is just one possibility, and the specific details may vary depending on the project's requirements.*

To effectively categorize budgets on a website based on country, years, money spent, spending categories, subsidies, and projects, you can consider the following categories and filters:

Country: Allow users to select a specific country or multiple countries to view budget information for those regions.

Years: Provide a dropdown or a range selector to allow users to select specific years or a range of years for budget data.

Money Spent: Offer options for users to filter budgets based on the amount of money spent, such as selecting a minimum and maximum spending range.

Spending Categories: Create a hierarchical or tag-based system to categorize budget spending into different categories.

Subsidies: Include a filter to allow users to view budgets specifically allocated to subsidies. This filter can further be categorized by sectors or industries, such as agriculture, energy, small businesses, etc.

Projects: Provide a filter or search functionality that allows users to explore budgets related to specific projects or initiatives. This can include infrastructure projects, public works, or any other significant government-funded endeavors.

Users can choose between long-term funding and short-term funding using filters.

By incorporating these categories and filters into a website, users will have the ability to narrow down budget information based on their specific interests, making it easier for them to find the relevant data they are looking for.

Categorizing and filtering budget data can indeed aid decision-making processes for AI and military applications. Here's how these categorizations and filters can be beneficial:

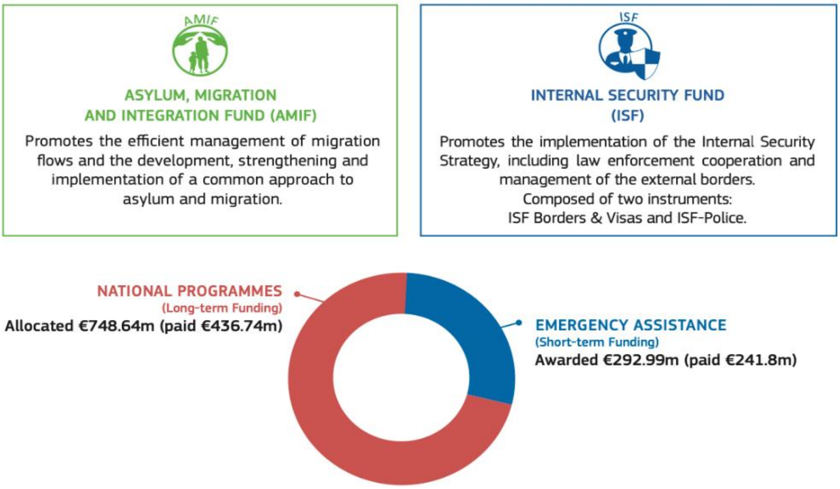
- **Country-specific Analysis**: By categorizing budgets by country, AI systems can analyze and compare budget allocations across different nations. This can help military strategists and policymakers gain insights into regional trends, prioritize resource allocation, and assess the relative strengths and weaknesses of different countries' defense capabilities.
- **Historical Analysis**: Filtering budgets by years enables AI systems to perform historical analysis and identify patterns or trends in budget allocations over time. This can help in identifying long-term investment strategies, understanding budget fluctuations, and predicting future budgetary needs.

- **Resource Allocation:** Analyzing budgets based on money spent and spending categories allows AI systems to optimize resource allocation. By considering the budget distribution across various sectors, such as defense, infrastructure, or research, AI can recommend adjustments to optimize military capabilities, identify potential gaps, or reallocate funds to address emerging needs.
- **Subsidy Analysis**: By categorizing budgets related to subsidies, AI systems can assess the economic impact of these subsidies on specific sectors or industries. This analysis can provide insights into the effectiveness of subsidy programs.

Project Assessment: Analyzing budgets provides AI systems with information on the allocation of resources to specific initiatives. This can aid in evaluating the progress, cost-effectiveness, and potential risks associated with ongoing or proposed projects. It enables AI systems to recommend adjustments, reallocation of funds, or prioritization of projects based on their strategic importance or impact. [10]

[10] Lawrence, D., & Tavakol, S. (2007). *Balanced Website Design.* Springer London. https://doi.org/10.1007/978-1-84628-795-4

By leveraging these categorizations and filters, AI systems can conduct data-driven analyses, identify patterns, and provide recommendations to aid decision-making in military and defense contexts. These insights can assist military leaders, policymakers, and AI-based systems in making informed choices, optimizing resource allocation, and enhancing overall operational effectiveness with rapid response to support decision – makers.



ASYLUM, MIGRATION AND INTEGRATION FUND (AMIF)

Promotes the efficient management of migration flows and the development, strengthening and implementation of a common approach to asylum and migration.

INTERNAL SECURITY FUND (ISF)

Promotes the implementation of the Internal Security Strategy, including law enforcement cooperation and management of the external borders. Composed of two instruments: ISF Borders & Visas and ISF-Police.

Source: European Commission, MANAGING MIGRATION EU Financial Support to Italy

Italy, like many other countries, has implemented various policies and programs to support migrants who arrive in the country seeking asylum or other forms of protection. These policies and programs aim to provide humanitarian assistance, facilitate integration, and promote social cohesion. The allocation of funds for these purposes is typically part of the national budget and may be supplemented by European Union (EU) funding for migration-related initiatives.[11]

Some of the areas where subsidies and budget allocations were commonly directed for migrants in Italy included:

Asylum and Refugee Support: Funds are allocated to process asylum applications, provide accommodation, food, and medical care to asylum seekers while their claims are being processed, and offer support to recognized refugees.

Integration Programs: Resources are dedicated to integration efforts, such as language and vocational training, educational support, and job placement assistance to help migrants become self-sufficient and contribute positively to society.

Social Services: Budgets may cover social services like healthcare, counseling, and other support services available to migrants and refugees.

Housing and Shelter: Funding is provided to ensure temporary shelter and housing for asylum seekers and refugees.

[11] *MANAGING MIGRATION EU Financial Support to Italy. (2020). European Commission.*

Education: Financial support may be allocated to ensure access to education for migrant children, including language support programs.

Legal Assistance: Budgets might be earmarked to provide legal aid and advice to migrants navigating the asylum process.

EU Funding: Italy, as an EU member state, may also receive funding from various EU initiatives aimed at managing migration flows and supporting integration efforts.

The budget for migrants in Italy, as well as in any other country, can vary from year to year and depends on various factors, including government policies, the number of migrants and refugees arriving in the country, and the specific programs and services provided to them.

To help users find the exact information they are searching for there are filters which are categorising the data once applied.

EU funding for asylum, migration, and integration, as well as internal security, is primarily allocated to Member State's national authorities at the beginning of each long-term EU budget period. For the current period (2014-2020), Member States manage and implement EU funding through national programs agreed with the European Commission.

Since 2015, a total of €292.99 million has been awarded, out of which €237.31 million has been paid, to support various migration and security initiatives.

Emergency assistance under the Asylum, Migration, and Integration Fund or the Internal Security Fund can be awarded to national authorities or international organizations and agencies, depending on the specific situation and needs.

Italy has received significant financial support from the EU to enhance its migration and border management efforts. This assistance includes €587.95 million from the Asylum, Migration, and Integration Fund and €453.68 million from the Internal Security Fund.[12]

Through these EU funds, Italy is better equipped to manage migration challenges, strengthen border controls, support asylum seekers, and address internal security concerns. The funds facilitate cooperation and collaboration between Member States and international organizations to address the complexities of migration and security in the region.

It's essential to note that measuring the direct impact of subsidies for migrants can be challenging, as the outcomes

[12] MANAGING MIGRATION EU Financial Support to Italy. (2020). European Commission.

are often influenced by various interconnected factors. Additionally, public policies and the allocation of funds for migrant support may evolve over time based on changing circumstances, such as political developments, economic conditions, and shifts in migration patterns. For the most up-to-date information on the results of subsidies for migrants in Italy, it's best to refer to recent reports and studies from reputable organizations and governmental sources.

Filtering information on the budget spent during a migration crisis is equally important for several reasons. Accurate and transparent reporting on the allocation and utilization of funds is crucial to ensure accountability, effective resource management, and informed decision-making. Here are some key reasons why filtering information on the budget spent in a migration crisis is essential and what the results would be:

Accountability and Transparency: Accurate reporting on the budget spent during a migration crisis helps hold governments and organizations accountable for their actions. It allows citizens, stakeholders, and donor countries to assess how funds are being used to address the crisis and whether they are being used effectively.

Avoiding Mismanagement and Corruption: Transparent reporting on the budget spent helps prevent mismanagement of funds and potential corruption. It ensures that resources are channeled to the intended purposes and that they reach the vulnerable populations, including migrants, who need assistance the most.

Effective Resource Allocation: Having accurate information on the budget spent allows policymakers and humanitarian organizations to evaluate the impact of their interventions and make data-driven decisions on where resources should be directed for maximum effectiveness.

Identifying Gaps and Needs: Accurate reporting can help identify gaps in services and the needs of migrants during a crisis. This information is essential for adjusting strategies and allocating additional resources where necessary.

Building Trust: Transparent reporting fosters trust between the government, humanitarian organizations, and the public. It shows a commitment to openness and ensures that stakeholders are well-informed about the efforts made to address the crisis.

Ensuring Fair Distribution: Access to information about the budget spent can help ensure that resources are distributed fairly among different regions or areas affected by the migration crisis. This can help prevent inequalities and regional disparities.

Demonstrating Impact: Reporting on the budget spent allows for the evaluation of the impact of various interventions and programs. It helps determine which strategies are effective and should be continued or expanded.

Engaging Donor Countries: In cases where migration crises receive international support, transparent reporting on the budget spent is crucial to keep donor countries informed about how their contributions are being used and the outcomes achieved.

Overall, filtering information on the budget spent during a migration crisis helps improve overall governance and resource management, which is vital for effectively addressing the needs of migrants and refugees during challenging times. It ensures that funds are directed where they are most needed and that responses are evidence-based and tailored to the unique circumstances of each crisis. [13]

NATO member countries might participate in humanitarian and military efforts related to migration crises in their individual

[13] Özcan, M. (2022). Classification of the NATO Countries with Respect to Defence Spending Patterns: An Unsupervised Clustering Approach . Savunma Bilimleri Dergisi , 1 (41) , 261-280 DOI: 10.17134/khosbd.1101724

capacities or as part of international coalitions or United Nations operations. The allocation of funds for such efforts would depend on the decisions made by the respective member governments.

NATO's focus and budget priorities are subject to change based on geopolitical developments and the evolving security landscape. This AI tool could help by collecting the newest data regarding the dynamically changing world and its political, military and security sphere, and therefore find the best solution to the crisis, give choices of action and following result.

Clustering is a crucial and powerful tool in the realm of Artificial Intelligence (AI) for NATO's operational capabilities. As a multinational military alliance, NATO faces complex and diverse challenges that demand efficient decision-making and resource allocation. Clustering offers an essential solution to these challenges by enabling the identification of patterns, grouping of similar data, and enhancing situational awareness. This paper explores the significance of clustering as a fundamental instrument in NATO's AI arsenal, delving into its applications, advantages, and potential contributions to achieving mission success and ensuring security in a dynamic and evolving global landscape. By harnessing the power of clustering, NATO can leverage AI-driven insights to optimize operations, enhance strategic planning, and strengthen interoperability among member nations, ultimately bolstering the alliance's readiness and resilience in the face of ever-changing security threats.

It plays a crucial role in unsupervised learning, where patterns and structures in data need to be uncovered without labeled examples. In this paper, it is delved into the clusterification process, examining how this powerful technique allows us to gain insights into complex datasets and facilitate knowledge discovery.

The first step in clusterification involves data preprocessing, including data cleaning, handling missing values, and transforming the dataset into a suitable format for clustering. Proper data preparation is essential for accurate and meaningful clustering results.

The choice of relevant features or attributes significantly impacts the clustering outcome. Selecting the appropriate features that capture the data's essential characteristics is critical in ensuring successful clusterification.

A wide array of clustering algorithms exists, each catering to different data types and structures. We discuss popular algorithms such as k-means, hierarchical clustering, and DBSCAN, highlighting their unique strengths and limitations.

For algorithms like k-means, the optimal number of clusters (k) is a vital consideration. We explore techniques like the elbow method and silhouette analysis, aiding in identifying the optimal number of clusters that align with the dataset's inherent structure.[14]

With the parameters set, the clustering algorithm is applied to the dataset to form clusters. We discuss the process of clustering data points based on similarities and explore how this grouping enhances data representation.

To ensure the quality and meaningfulness of clusters, internal validation metrics such as Silhouette Score and Davies-Bouldin Index are introduced. The paper emphasizes the importance of evaluating cluster quality to gain meaningful insights.

Clusterification outcomes are analyzed to interpret underlying data patterns. We explore visualizations like scatter plots and heatmaps, allowing researchers to understand relationships between data points within each cluster.

The clusterification process is iterative, and refining parameters or experimenting with different algorithms

[14] Aristidis Likas, Nikos Vlassis, Jakob J. Verbeek (2003). The global k-means clustering algorithm, Pattern Recognition, Volume 36, Issue 2, Pages 451-461

enhances clustering accuracy. Domain expertise and expert knowledge are indispensable in achieving meaningful results.

In conclusion, clusterification offers a powerful and versatile approach to data analysis and knowledge discovery. Understanding the nuances of the clustering process empowers researchers to unravel hidden insights within vast and complex datasets, unlocking new opportunities for data-driven decision-making across diverse domains.[15]

*** Clustering could help to identify suspicious patterns and anomalies in data, normal processes will be grouped, which can aid in detecting potential corruption or irregularities. The irregular practice will be positioned as an outlier.**

However, it is just one part of a broader anti-corruption strategy that requires legal measures, governance, and transparency to effectively combat corruption.

In the context of NATO's strategy for fighting corruption, a significant gap exists in the efficient and targeted analysis of

[15] Sheikholeslami, G., Chatterjee, S., & Zhang, A. (2000). WaveCluster: a wavelet-based clustering approach for spatial data in very large databases. *The VLDB Journal The International Journal on Very Large Data Bases*, *8*(3-4), 289–304.

vast and complex datasets. Corruption-related data can be extensive, diverse, and scattered across various sources, making it challenging to identify relevant information and patterns that indicate potential corrupt practices.

This gap becomes particularly critical when traditional data analysis methods are employed, as they may lack the capacity to handle the sheer volume and complexity of corruption-related data. Without a comprehensive and systematic approach, NATO may struggle to extract actionable insights from the data, leading to less effective anti-corruption efforts.

The introduction of clustering techniques, driven by artificial intelligence (AI), presents a promising solution to bridge this gap. Clustering allows for the grouping of similar data points based on shared characteristics, enabling the identification of patterns and potential anomalies within the datasets. By utilizing AI-powered clustering algorithms, NATO can efficiently process and categorize corruption-related data, filtering out irrelevant information and focusing on critical indicators of corruption.

Furthermore, clustering can help NATO's anti-corruption efforts by providing data-driven decision support. The ability to identify patterns and connections among data points can aid in uncovering hidden corruption networks and suspicious activities. This data-driven approach not only enhances the accuracy of corruption detection but also optimizes the allocation of resources and efforts in combating corruption.

However, despite its potential, the current NATO strategy for fighting corruption may not fully capitalize on the benefits of clustering and AI. There might be a lack of awareness or expertise in integrating these advanced analytical techniques into existing anti-corruption practices. Addressing this gap requires a proactive approach, including training personnel, investing in AI capabilities, and fostering collaboration between data analysts and anti-corruption experts.

The gap in NATO's strategy for fighting corruption lies in the efficient analysis of corruption-related data. Embracing clustering techniques, empowered by AI, can significantly enhance the effectiveness of anti-corruption efforts by streamlining data analysis, improving decision-making, and identifying corruption patterns and networks. By bridging this gap and leveraging advanced analytical tools, NATO can bolster its anti-corruption initiatives and reinforce its commitment to transparency, accountability, and integrity within the alliance.

Bibliography

Hileman, L. (2021). Artificial Intelligence Book : Learning Artificial Intelligence with Python: Learning Artificial Intelligence

John, M. (2018). Artificial intelligence.

Lesser, V. R., Cohen, P., & Lehnert, W. (1992). Center for Artificial Intelligence. Defense Technical Information Center. https://doi.org/10.21236/ada282272

Fawkes, A. (n.d.). Developments in Artificial Intelligence – Opportunities and Challenges for Military Modeling and Simulation. NATO, STO-MP-MSG-149.

NATO's Data and Artificial Intelligence Review Board. (2022). In Summary of the establishment of the Board. NATO.

Stanley-Lockman, Z., & Hunter Christie, E. (2021). An Artificial Intelligence Strategy for NATO. NATO.

MANAGING MIGRATION EU Financial Support to Italy. (2020). European Commission.

C2 Agility is the capability of C2 to successfully effect, cope with, and/or exploit changes in circumstances. C2 Agility enables entities to effectively and efficiently employ resources in a timely manner. NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.

NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.

Tillman, M.E. and Conley. K.M., 'Designing and Assessing Command and Control to Deal with Complex and Ill-Structured Operational Environments'. In Operations Assessment in Complex Environments: Theory and Practice, edited by Adam Shilling. NATO STO, 2019.

UK Ministry of Defence, 'Integrated Operating Concept 2025,' 30 Sep. 2020 [Online]. Available: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025.

UK Ministry of Defence, 'Multi-Domain Integration (JCN 1/20),' 2 Dec. 2020 [Online]. Available: https://www.gov.uk/government/publications/multi-domain-integration-jcn-120#:~:text=This%20integration%20must%20be%20across,domains%20and%20levels%20of%20warfare.

Moskos, C. (2004). International Military Education and Multinational Military Cooperation. Defense Technical Information Center.

Multinational capability cooperation (NATO). (2023).

Borrelli, S. S. (2018, September 8). Salvini strikes conciliatory tone on migration, Italy’s budget. POLITICO. https://www.politico.eu/article/matteo-salvini-strikes-conciliatory-tone-on-migration-italys-budget/

ANSA. (2020, February 7). Italy increases budget for migrant reception facilities. InfoMigrants. https://www.infomigrants.net/en/post/22631/italy-increases-budget-for-migrant-reception-facilities

EU Budget Chief Urges More Help For Italy Over Migrants. (2023, April 18). Barrons. https://www.barrons.com/news/eu-budget-chief-urges-more-help-for-italy-over-migrants-68a67feb

Gotev, G. (2018, August 28). Italy threatens to veto EU's long-term budget over migration crisis. www.euractiv.com. https://www.euractiv.com/section/justice-home-affairs/news/italy-threatens-to-veto-eus-long-term-budget-over-migration-crisis/

Lawrence, D., & Tavakol, S. (2007). Balanced Website Design. Springer London. https://doi.org/10.1007/978-1-84628-795-4

Aristidis Likas, Nikos Vlassis, Jakob J. Verbeek (2003). The global k-means clustering algorithm, Pattern Recognition, Volume 36, Issue 2, Pages 451-461

Sheikholeslami, G., Chatterjee, S., & Zhang, A. (2000). WaveCluster: a wavelet-based clustering approach for spatial data in very large databases. The VLDB Journal The International Journal on Very Large Data Bases, 8(3-4), 289–304.

Özcan, M. (2022). Classification of the NATO Countries with Respect to Defence Spending Patterns: An Unsupervised Clustering Approach . Savunma Bilimleri Dergisi , 1 (41) , 261-280 DOI: 10.17134/khosbd.1101724

ENHANCING DISASTER RESPONSE AND CONSEQUENCE MANAGEMENT IN RADIOLOGICAL INCIDENT: A SUCCESSFUL TRAINING EXPERIENCE

Genadi Kolev

Abstract: The Crisis Management and Disaster Response Centre of Excellence (CMDR COE) and its esteemed partners conducted a comprehensive training program on Disaster Response and Consequence Management for Radiological Incidents. This program, developed in collaboration with organizations like the United States Department of Energy (DOE), the United States Defense Threat Reduction Agency (DTRA), and CBRN units from the Bulgarian Armed Forces, aims to equip a diverse audience with the knowledge and skills required for effective radiological incident management. The training program's success may attribute to its multifaceted approach, emphasizing the significance of multiple response strategies, optimal learning conditions, adherence to Standard Operating Procedures (SOPs), and practical application in a virtual environment. The program's focus on hands-on experience, interdisciplinary collaboration, in-depth radiological knowledge, adaptive decision-making, and learning from real-world case studies underscores its significance in preparing responders to address the complexities of radiological incidents.

Keywords: consequence management, resilience, modelling, disaster response, virtual training.

The Training Program

CMDR COE's training program on Disaster Response and Consequence Management for Radiological Incidents offered a dynamic and immersive learning experience. It aimed to equip a diverse audience, including first responders, emergency managers, environmental scientists, public health professionals, and military personnel, with the essential skills and knowledge needed for effective radiological incident management. One of the core components of this exceptional training program was the use of realistic simulations that closely resembled real-world radiological incident scenarios. These simulations allowed trainees to translate their theoretical knowledge into practical solutions. A standout feature was the Table-Top Exercise (TTX), which provided a collaborative platform for participants to develop response strategies, identify weaknesses in their approaches, and refine their disaster response plans.[1]

Recognizing the complex nature of radiological incidents, the training program emphasized the importance of interdisciplinary collaboration. Radiological incidents demand a coordinated and multifaceted approach, involving various agencies and professionals. Trainees had the opportunity to interact with peers from diverse backgrounds, fostering teamwork and essential communication skills. This collaborative approach mirrored the intricate nature of real-world radiological incident management, where different experts must work together seamlessly.

To effectively respond to radiological incidents, trainees were provided with in-depth knowledge about radiological materials, sources, and hazards. The training program ensured participants received comprehensive instruction in radiological science and risk assessment, enabling them to make well-informed decisions and proactively address radiological challenges.

Given the unpredictable nature of radiological incidents, the program focused on instilling adaptive decision-making skills. Trainees were taught how to adjust their strategies and decision-making processes in rapidly changing situations. Realistic scenarios with unexpected variables allowed participants to make agile decisions and adapt their response strategies on the spot.

In addition to theoretical knowledge, CMDR COE emphasized hands-on experience as a crucial aspect of the training. Trainees were given the opportunity to handle CBRN detection equipment, don protective gear, and simulate radiological incident responses in a controlled environment. This practical experience was invaluable in building both confidence and competence among the participants.[2]

Moreover, the training program incorporated an analysis of real-world radiological incidents, examining lessons learned from past events. By studying case studies, trainees gained insights into the successes and shortcomings of previous radiological incident responses. This knowledge empowered them to make informed decisions and avoid repeating past mistakes, ensuring that they were well-prepared to manage future radiological incidents effectively.

The Importance of Multiple Approaches

Effective disaster response hinges on the ability to evaluate and adapt to a rapidly changing environment. During the CMDR COE training, participants were encouraged to explore various approaches to address radiological incidents. Having multiple options at their disposal allowed trainees to make informed decisions based on effectiveness, feasibility, and potential outcomes, considering specific criteria and contextual factors. The selection process involved rigorous analysis, the consideration of objectives and constraints, and a comprehensive understanding of associated risks and benefits. This approach ensured that trainees were well-prepared to handle real-world situations where adaptability and versatility are essential.

- **Diverse Responses to Dynamic Challenges**: Radiological incidents can manifest in a wide spectrum of characteristics, including variations in scale, nature, and location. As such, there is no universal or one-size-fits-all response strategy that applies to every situation.

- **Informed Decision-Making:** Effective radiological incident management hinges on the ability to make well-informed decisions. Trainees were encouraged to engage in a meticulous evaluation of different response approaches, factoring in specific criteria and contextual considerations.

- **Contextual Flexibility:** Radiological incidents have the potential to occur in a plethora of settings, ranging from urban areas to industrial facilities and rural regions. Each context introduces unique challenges and opportunities.

- **Risk Mitigation:** A pivotal aspect of assessing multiple response approaches is the comprehensive evaluation of risks and benefits associated with each option. Different approaches carry varying levels of risk and potential benefits.

- **Objective-Driven Responses:** Successful radiological incident management transcends mere response; it is about achieving specific objectives.

- **Resource Optimization:** Radiological incidents often strain resources, including personnel, equipment, and supplies. The availability of multiple approaches enabled responders to make the most efficient use of their available resources.

Creating Optimal Learning Conditions

Recognizing the significance of providing trainees with the best possible conditions for knowledge acquisition, skill development, and competency building, CMDR COE invested in creating a supportive and well-structured setting for learning. Below, we explore the key elements that contributed to these optimal learning conditions during the training program:

- **Clear Learning Objectives**: CMDR COE acknowledged the importance of clearly defined learning objectives. These objectives served as guiding principles for trainees throughout the program, offering them a well-defined path to follow.
- **Engaging Instructional Methods:** The training program employed a rich array of instructional techniques to keep trainees engaged and motivated. These methods ranged from traditional lectures to hands-on activities, group discussions, and interactive simulations.
- **Appropriate Learning Resources:** Access to suitable learning resources plays a critical role in promoting comprehensive understanding. CMDR COE ensured that trainees had access to a wide array of materials, including textbooks, manuals, online resources, and specialized tools and equipment.
- **Individualized Support:** Recognizing that each trainee may possess unique learning needs, the training program incorporated mechanisms for individualized support. This included opportunities for one-on-one consultations,

mentorship, and personalized feedback. Such tailored support addressed the specific requirements of each participant, enhancing their learning experience.

- **Assessments and Feedback:** Regular assessments were conducted to gauge trainees' progress and understanding. These assessments were complemented by constructive feedback, providing trainees with valuable insights into their strengths and areas that required improvement. This feedback loop allowed trainees to identify specific areas for enhancement and make necessary adjustments to their learning strategies.

- **Commitment to Continuous Improvement:** The commitment to continuous improvement was a foundational aspect of the educational program. CMDR COE ensured that the training program remained subject to regular evaluation and refinement. Feedback from both trainees and instructors was used to make enhancements, fostering a dynamic and adaptive learning environment that evolved to meet the evolving needs of the trainees.

Emphasizing Standard Operating Procedures (SOPs)

The emphasis on rigorous adherence to Standard Operating Procedures (SOPs) was a foundational element of CMDR COE's educational approach, particularly in the context of radiological incident management. SOPs serve as vital guidelines that play a pivotal role in ensuring the success of operations and activities across various domains. Here, we explore the profound significance of prioritizing SOPs and the multitude of benefits they bring to the table in radiological incident management.[3]

- **Consistency and Uniformity:** SOPs serve as the bedrock of consistency in response efforts. They establish a standardized set of procedures that responders follow diligently. This adherence to established best practices ensures that actions and decisions align cohesively, especially in complex and high-stress situations.
- **Efficiency and Effectiveness:** Well-defined SOPs act as a catalyst for the streamlining of response efforts, making them more efficient and effective. In radiological incidents where time is often a critical factor, the existence of pre-established procedures equips response teams to act swiftly and make decisions without undue delay.
- **Safety and Risk Mitigation:** Radiological incidents inherently introduce risks to both responders and the surrounding environment. SOPs are strategically designed to ensure the safety of all personnel involved. They provide comprehensive guidelines for the proper utilization of protective gear, equipment handling, and the implementation of safety measures. This stringent adherence to SOPs plays a pivotal role in minimizing risks and establishing a secure

response environment, thereby safeguarding the well-being of all involved.[4]

- **Quality Assurance:** Radiological incident management necessitates a high level of precision and quality in all operations. SOPs set the standard for quality by outlining the correct procedures and best practices. The strict adherence to these established procedures empowers responders to maintain a high level of quality in their actions.
- **Team Coordination:** In large-scale incidents that require the involvement of multiple agencies and teams, SOPs play a pivotal role in facilitating coordination and collaboration. Responders from diverse backgrounds and organizations can work seamlessly when they share a common set of procedures.
- **Legal and Regulatory Compliance:** Radiological incident management operates within a framework of various legal and regulatory requirements. Adhering to SOPs is a means of ensuring that response teams remain in compliance with these standards. This commitment to SOPs reduces the risk of legal complications and assures that response efforts align with the necessary criteria.
- **Continual Improvement:** SOPs are not static documents; rather, they are dynamic and subject to regular review and enhancement based on lessons learned from past incidents.

The training program highlighted the importance of integrating feedback and best practices into SOPs. This ongoing process of refinement ensures that SOPs evolve, becoming even more effective and responsive over time. It represents a commitment to adaptability and an enduring dedication to continuous improvement.

Practical Application in a Virtual Environment

To bring theoretical knowledge to life, CMDR COE meticulously devised a practical task that revolved around the utilization of a virtual environment for Chemical, Biological, Radiological, and Nuclear (CBRN) area surveillance. This hands-on exercise served as the vital bridge connecting theory and real-world application, affording trainees the unique opportunity to translate their theoretical understanding into actionable skills within a simulated, yet highly realistic, radiological incident scenario.

The heart of this practical application lay in the creation of a practical scenario that was not only immersive but also incredibly authentic. CMDR COE's approach was to craft a scenario that authentically mirrored real-world challenges. Trainees were organized into three groups, with each group consisting of two individuals. Within each group, two trainees operated the virtual system, while the rest observed and took notes. The utilization of two screens for observation provided different perspectives and enriched the training experience, enabling a more comprehensive understanding of the scenario.

For the practical execution of this task, CMDR COE meticulously created two realistic areas within the virtual environment based on actual geolocations. The scenario depicted an airplane crash that resulted in a radiological incident. Trainees commenced their task in a fully equipped decontamination area, ready to respond to the unfolding incident.

A pivotal element of this exercise was the introduction of scripted actions based on the Status Quo Function (SQF). SQF is a specialized scripting language employed for crafting custom scenarios, missions, and interactive elements within the simulation environment. It provides a flexible and powerful toolset for developers and mission designers to create dynamic and interactive content within the virtual environment, including complex scenarios with scripted events, AI behaviour, mission objectives, and more. Through the utilization of SQF, CMDR COE was able to customize the behaviour of units, vehicles, and objects within the virtual environment. This scripting language also enabled the control of various aspects of the simulation environment. It allowed trainees to experience dynamic and responsive scenarios that closely mirrored the unpredictability of real-world radiological incidents.[5]

Freedom to Choose Approaches

In the virtual environment, trainees were granted the freedom to choose from a range of approaches. This included the selection of appropriate protective equipment, the use of drones for threat detection, and the employment of various vehicles to respond to the simulated incident. This freedom provided a realistic simulation of the decision-making processes that responders face in actual radiological incidents.

A Transformative Learning Experience

This practical application within a virtual environment not only prepared trainees for the complexities and challenges of radiological incident management but also transformed their theoretical knowledge into tangible, action-oriented skills. CMDR COE's commitment to providing trainees with an immersive, hands-on experience underpinned their goal of producing skilled and confident disaster responders. This learning module facilitated the application of knowledge in a risk-free environment, ensuring that trainees were well-equipped for the intricate and often high-pressure scenarios they may face in their roles.

Conclusion

CMDR COE's practical exercise in a virtual environment was a paramount component of their training program, reinforcing the commitment to excellence in disaster response. By replicating the complexities of real radiological incidents, CMDR COE prepared trainees to address the unforeseen challenges and uncertainties that may arise in their roles as first responders, emergency managers, environmental scientists, public health professionals, and military personnel. This practical component fortified their skills and fostered the critical thinking and adaptability necessary for effective disaster response and consequence management. [6]

Acknowledgement

The successful execution of the training program, "Disaster Response and Consequence Management for a Radiological Incident," was made possible through the dedicated efforts and collaboration of numerous individuals and organizations. We wish to express our sincere gratitude to all those who contributed to the development, implementation, and success of this program.

We would like to thank our esteemed partners, including the United States Department of Energy (DOE), the United States Defense Threat Reduction Agency (DTRA), and the CBRN units from the Bulgarian Armed Forces. Their support and collaboration brought a wealth of knowledge and practical experience to the training program, enriching the learning opportunities for all participants.

We are deeply grateful to the dedicated instructors and trainers who shared their expertise and guided trainees through this rigorous educational journey. Their commitment to providing an exceptional learning experience is greatly appreciated.

A special word of thanks goes to the trainees themselves, who approached this program with enthusiasm, dedication, and a

genuine commitment to mastering the skills and knowledge necessary for effective radiological incident management.

Finally, we acknowledge the collective efforts of everyone involved in this endeavour, both seen and unseen, who contributed to the success of this training program. Your commitment to disaster response excellence is commendable, and your contributions are invaluable.

References

[1] CMDR COE DISASTER RESPONSE AND CONSEQUENCE MANAGEMENT FOR A RADIOLOGICAL INCIDENT , Disaster response and consequence management for a radiological incident . Available at: https://cmdrcoe.org/menu.php?m_id=40&c_id=107 (Accessed: 2023).

[2] END-TO-END CBRN INCIDENT MANAGEMENT INFORMATION SYSTEM (no date) Havelsan. Available at: https://havelsan.com.tr/en/sectors/cyber-security/national-security/products/havelsan-kbrn-mentor (Accessed: 2023).

[3] Standard operating procedure EAP056, version 1.3 m easuring and ... Available at: https://apps.ecology.wa.gov/publications/documents/1803203.pdf.

[4] Brush, K. (2021) What is a standard operating procedure (SOP)? definition from Searchbusinessanalytics. Available at: https://www.techtarget.com/searchbusinessanalytics/definition/standard-operating-procedure-SOP (Accessed: 2023).

[5] Bohemia Interactive (2023) SQF Syntax - Bohemia Interactive Community. Available at: https://community.bistudio.com/wiki/SQF_Syntax.

[6] Regal, G. et al. Challenges in virtual reality training for CBRN events, MDPI. Available at: https://www.mdpi.com/2414-4088/7/9/88 (Accessed: 2023).

MULTI-DOMAIN OPERATIONS IN THE CONTEXT OF CRISIS MANAGEMENT. THE NAVAL CASE.

Svetozar Bosilkov, Gonzalo Vázquez

Abstract: Continuous horizon scanning and study of the paths of potential adversaries and other relevant actors, are essential for the Alliance's ability to proactively shape, through warfare development, and to alter other actors' pathways. The toolbox for the Post-Cold War years for managing and sustaining the Peace and Security for NATO allied countries is seemingly not enough to keep the Alliance's strategic advantage over the adversaries. The Strategic political and military leaders are leading and directing a long-term and full-fletched transformative process which to make the Alliance military instrument of power capable to warfighting in the multi-region, multi-dimensional and multi-domain operating environment.

Keywords: Military Instrument of Power, Transformation, Military Strategy, DDA, NWCC, Multi-domain operations, Maritime security.

"Multi-Domain Operations is NATO's strategic priority, a game changer for our strategic advantage. We are transitioning from joint to multi-domain with a bold vision captured in a ground-breaking concept. NATO Allied Command Transformation is leading the team, ensuring our future fight depends on this vital work."

Supreme Allied Commander Transformation, General Philippe Lavigne

The changing and evolving strategic security environment puts a wide threat to the Alliance's continued success. While NATO remains a defensive alliance, the operating environment demands new ways of thinking, organizing and acting. Even though the best option is to shape this environment, potential adversaries, strategic competition, pervasive instability, and strategic shocks are likely to grow in their complexity in the years to come. In this sense, the ongoing conflicts in Ukraine and Israel are solid examples. And all this dynamic is happening against the backdrop of broader security challenges, including those related to demography, climate, resources and public health.

Furthermore, the operating environment is widening beyond traditional military bounds, with competition among different actors becoming more persistent across all instruments of power. Holding in their hands new weapons and new technologies, employed in new ways the adversaries are seeking to shape, in their own ways, the operating environment. While the fundamental nature of warfare hasn't changed for centuries, all these new possibilities are changing the character of war, and so must the Alliance's approach to warfighting.

Facing this transformative threshold, successfully upholding NATO's objectives requires from one side a proactive mindset, effective connectivity and speed at scale, but from the other, inclusion of likeminded international players, i.e. organizations and companies, as well as partner nations, industry and open societies that will present opportunities to positively influence the operating environment.

NATO's new Military Strategy, signed by Allied Chiefs of Defence in May 2019, formalized a significant change in the Alliance's mindset[1]. The Military Strategy recognized strategic competition, pervasive instability as characterizing the strategic environment, but identified both Russia and terrorism as threats facing NATO, placing deterrence as the NATO transformative focal point. Furthermore, it recognized the need to move away from crisis response to contesting and countering these threats by developing a common capacity for competition and deterrent power at all times, and not just in crisis and defence[2].

Two consequent concepts are contributing to implementation of the new military strategy. The Concept for the Deterrence and Defence of the Euro-Atlantic Area, 2020 (DDA) and the NATO Warfighting Capstone Concept, 2020 (NWCC) are making this transition in transformation of the military instrument of power (MIoP) from now to tomorrow to 2040. DDA is described by NATO as 'a single, coherent framework to contest and deter and defend against the Alliance's main threats in a multi-domain environment'[3]. While is

[1] Jonny Hall & Sandemanv (2021)
[2] Ibid.
[3] "Brussels Summit Communiqué", 2021

NWCC a longer-term vision for the Alliance's development of warfare, based on a 20-year perspective on the future characteristics of warfare[4].

While the crisis management approach through joint operations have worked effectively for NATO in the post-Cold war era to fulfill its purpose and mission, the new operating environment, which will be persistent, Simultaneous and Boundless impose a new requirements for the MIoP capabilities. With the recognition of cyberspace and space as operational domains, NATO started the transition to the new version of operation, called Multi-domain. Multi-domain operations are the game-changer by which the Alliance will sustain the decisive strategic advantage over those who challenges the ruled-based order, including in the naval domain.

From Joint to Multi-domain Operations

Over the past decade, most nations have gradually turned their attention to the concept of Multidomain Operations (MDOs). This new concept encapsulates the idea that traditional military operations and warfare have been deeply transformed by the ability of orchestrating military activities across all domains and environments, synchronizing them with non-military activities (including crisis management) in order to enable NATO to create

[4] "Brussels Summit Communiqué", 2021

converging effects. These elements, which provide the basis for a general definition of the concept, also allow to make a distinction between MDOs and Joint Operations.

As a starting point, the common definition for the concept of “domain” used by NATO is put forward by Dr. Jeffrey Riley, according to whom domain is understood as “critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission.”[5] According to the US Army, Multi Domain Operations can be properly defined as “the combined arms employment of capabilities from all domains that create and exploit relative advantages to defeat enemy forces, achieve objectives and consolidate gains during competition, crisis and armed conflict.”[6] Such concept is still at the early stages of its development, however, and although increasingly researched and studied, it is still maturing.[7] On the other hand, Joint Operations can be defined as all those military activities which require the participation of two or more military services. In other words, the former is focused on the domains in which conflict and crises take part, while the latter is concerned with the services which take part in them.

[5] Griesemer, 2018; NATO C2COE, 2021.
[6] Judson, 2022.
[7] CJOS COE, 2021

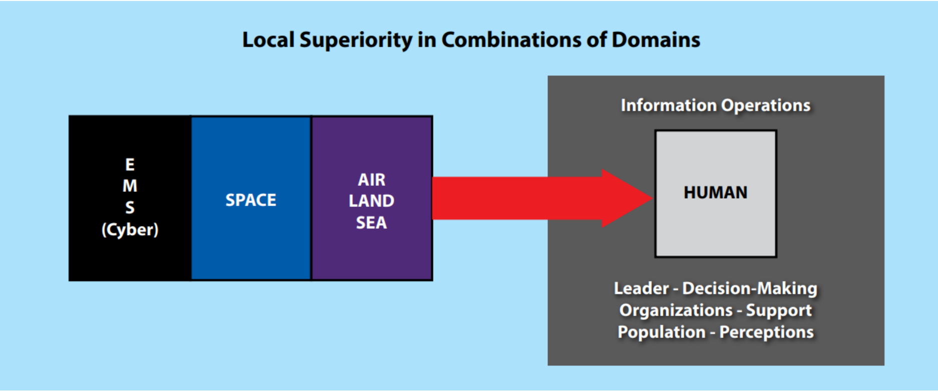


Figure 1: Continuum of Domains and their interdependence[8]

Dr. Jeffrey Riley further underlines, MDOs have been an enduring characteristic of warfare since antiquity, with early references going as back as 415 BC. Yet, there is no question in that "the emerging strategic landscape is revealing a wide array of new threats that is dramatically degrading the overwhelming asymmetric advantage we have enjoyed for the past two decades."[9] Currently, we are living in an era deeply influenced (and shaped) by strategic and great-power competition, where joint action has become more important than ever a means to tackle the different challenges that technology development is bringing. Military forces deployed on land, in the air and at sea face an increasing array of threats,[10] as does our ability to face risks of conflict and future crises.

[8] Reilly, 2016.
[9] Reilly, 2016.
[10] Black et Al., 2022.

The concept of MDO has been gradually taking shape over the past decade, supported in part by the rapid evolution experienced in the technological field (as well as the AI one). As Black et Al. underline, "advances in Information and Communications Technologies (ICTs), as well as artificial intelligence (AI) and other emerging technologies, are also facilitating unprecedented integration across and between the domains."[11]

MDOs are conducted during three phases of operation: competition, crises and armed conflict. In the case of this paper, attention will be primarily placed in the latter two.

MDOs and Crisis Management at Sea

As already mentioned, the concept of MDOs was originally developed by the US Army, and it has since been gradually expanded to other NATO countries who are now beginning to use it and apply it. Applied to naval operations, another concept that has emerged over the past years as the central tenet for the U.S. Navy is the so-called Distributed Maritime Operations. However, since the focus of this study is with crisis management, the DMO concept will not be developed in depth in this study, as it is more focused on force distribution rather than on integrating multi domain capabilities.[12]

[11] Black et Al., 2022.

[12] For deeper perspectives on the DMO concept, see Filipoff, 2023.

History has repeatedly shown the potential of using the advancements developed for warfighting purposes for other aspects of regular life. In the case of crisis management and response operations, the case could also be made about it. The ongoing conflict in Ukraine has had a particular impact in naval warfare, with the introduction of Unmanned Surface and Underwater Vehicles (USVs, UUVs) in big numbers to raid enemy bases and ports, as well as to target critical infrastructure vital for communications and connectivity. In this sense, naval warfare and crisis management at sea will be strongly affected by two dominant trends that are completely transforming current conceptions on them; both of which are directly related with the impact of new technologies.[13]

The first of them is autonomy. The war in Ukraine, as destructive and tragic it has been so far, has nevertheless been the main event triggering the use of autonomous systems for naval warfare purposes. It is worth highlighting, however, that it has not been the "inaugurating event" for their use. Rather, it has rather been the confirmation and proof of the enormous potential that both Unmanned Surface Vehicles (USVs) and Unmanned Underwater Vehicles (UUVs) have. Their successful employment by the Ukrainian Navy against the much bigger and stronger Russian Black Sea fleet has completely transformed the paradigm of naval

[13] CJOS COE, 2021

warfare in enclosed seas. It has proven how smaller units can be just as useful and effective as bigger platforms. With them, Ukraine has been able to suppress the naval support to Russian ground forces, and using it to attack Russian infrastructure and ports.[14] Yet, these attacks also demonstrate that similar actions can be taken against NATO members, and thus,

The second is artificial intelligence (AI). The considerable improvement that AI brings for data treatment reduces significantly the time and intelligence needed by human beings.

Machine learning, which enables analysis of massive quantities of data, is used most of the time to first analyze and then extract valuable information from data processing. Those processes are full of promise in the maritime domain […] For example, Automatic Identification System (AIS) displays a representation of recurrent maritime traffic patterns, also called Patterns of Life (PoL), which are of interest in the framework of maritime security. Applying AI processes to this large data set enables rapid extraction of abnormal or suspicious behaviors.[15]

A relevant reference to the work in crisis management at sea can be found in NATO´s 2011 Maritime Strategy. The document

[14] As of September 2023, there have been several attacks to both Russian facilities and surface vessels. The first of them taking place in October 2022 included attacks to Russian Navy ships docked at the port of Sebastopol, while other have targeted docking and shipbuilding facilities.

[15] CJOS COE, 2021.

identifies four pillars of Allied security efforts at sea: deterrence and collective defense, crisis management, cooperative security, and maritime security.[16] Concerning crisis management, it establishes that it may include a wide range of activities, such as conflict prevention, demonstration of resolve, crisis response operations, peace-enforcement, embargo operations, counter terrorism, or even mine-clearing. It therefore establishes four objectives to be pursued in this field:

- Continuing to maintain modern, credible, rapid response joint forces able to operate in environments with degraded communications.
- Contributing to the provision of urgent humanitarian assistance and disaster relief in accordance with the political framework of NATO’s participation in humanitarian operations.
- Leveraging the inherent agility of its maritime forces to provide a flexible and graduated response in crisis or emerging crisis situations,
- Providing essential logistical support for joint force operations in austere or hostile land environments and the deployment of joint command and logistical bases afloat.[17]

Yet, it should be highlighted that the maritime strategy is more than a decade older, and does not account for all the numerous changes

[16] NATO, 2011.
[17] NATO, 2011.

which have taken place over such period of time, and the Alliance should seriously consider updating the strategy for a more precise definition of the current strategic environment, which will in turn allow for a better understanding of the current requirements to enhance NATO´s crisis management capabilities at sea.

Bringing together both the impact of autonomy – AI and the emergence of multiple challenges in the maritime domain over the last years, the aspect in which NATO countries will have to come together related to MDOs and crisis management at sea over the next decades is none other than the protection of undersea critical infrastructure and the upholding of freedom of navigation. These represent the most prominent threat in several regions around the continent, particularly in the Baltic, North and Mediterranean Seas.[18]

With the overwhelming reliance that most (if not all) countries have over undersea pipelines and submarine cables, and the relative under protection these have against potential disruptions and attacks, having an adequate toolbox to ensure a stronger protection of these infrastructure must be among the top priorities for Allied countries. The establishment of a NATO Critical Undersea Infrastructure Coordination cell in early 2023 marks a positive step in this sense. According to its current head, German LT General Hans-Werner Wiermann, “it will enable better coordination between

[18] WALL & MORCOS, 2021.

key military and civilian stakeholders and with industry, on an issue that is vital to our security."[19]

On a similar line, upholding freedom of navigation and preventing the proliferation of WMDs will also be a crucial task to prevent potential crises from arising. In the current strategic environment, the ability to combine actions across different domains significantly affects the ability to respond and face potential aggressions and violations to freedom of navigation. NATO and its members must be ready to support the principle of freedom of navigation by strengthening their efforts on surveillance, patrolling, maritime interdiction and using of force when authorized to do so. These tasks require an integrated approach across all domains, given our adversaries´ capabilities are also going in that direction.

As already stressed, emerging technologies and digital transformation are going to play the most relevant roles in the medium to long term future of MDOs and crisis management at sea. This makes it necessary for NATO Allies to embrace these new technologies across the full spectrum, for which they will certainly need a new mindset that allows them to adapt to all these new trends. As underlined by Deputy Chief of Staff for Capability Development at Allied Command Transformation LT General Dave Julazadeh, evolving knowledge in the field of MDOs must provide decision makers and military officers with access to secure, data-

[19] NATO, 2023.

centric, software-based capabilities and services that in turn provide with increased decision space.[20]

Conclusion

NATO adversaries have developed "ways of expanding the battlespace and blurring traditional conceptual distinctions between war and peace, between public and private, between domestic and foreign, and between the physical and the virtual."[21] It is generally understood that, at the basic level, multi-domain concepts are focused on the notion that integration across several domains (at least two of the existing five) can provide greater effects that the sum of its parts.[22] Threby, such concepts "involve the convergence of capabilities within and from multiple domains; the greatest value can be achieved by drawing in as many capabilities as possible to find the most potent combinations to exploit the vulnerabilities of the adversary and meet the objectives of the activities in question."[23]

In order to properly meet the demands imposed by the new strategic environment, and strengthen Allied capabilities in MDOs and crisis management at sea, close attention must be paid to the following aspects:

1. Emerging technologies and AI are rapidly evolving, and as their importance within MDOs keeps rising, NATO and its partners will

[20] Julazadeh in NATO Innovation Podcast, 2022.
[21] Black et Al., 2022.
[22] Lindsay & Gartzke, 2020.
[23] Black et Al., 2022.

have to make important investments in order to adapt to these new changes. Failing to do so could potentially develop in major weaknesses to be exploited by adversaries, as well as in a lack of preparedness to face emerging crises and challenges of different nature.

2. NATO and its members must strengthen their efforts to secure critical undersea infrastructure and mitigate all potential sources of disruption. The most prominent of them are undersea cables and pipelines, which remain largely unprotected against disruptions and tapping. The standing up of a NATO Critical Infrastructure Coordination Cell in early 2023 is a positive step, but must be followed with additional measures and further involvement by Member States.

3. NATO countries should consider the employment of USVs and UUVs to enhance their maritime surveillance capabilities, as a means to prevent potential crises from emerging due to failures with critical undersea infrastructure. Ensuring a careful surveillance of Russia´s fleet dedicated to the seabed would reduce prospects of disruptions by their submarines and special craft. But to do so, Members should look for a consensus on the ways to do so, including through a new Allied maritime strategy that better reflects these new challenges.

4. Asymmetric warfare as a type of war between belligerents whose relative military power, strategy, or tactics differ significantly will

evolve and will be significantly enabled by the new technologies. NATO must take advantage in this area of warfare when develops its nine technological areas of priority: AI, data exploitation and autonomy, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, novel material and manufacturing, energy and propulsion, and space.

Bibliography:

Jonny Hall And Hugh Sandemanv (2021), "NATO and the Future Character of Warfare" STRATEGIC UPDATE Available at: http://eprints.lse.ac.uk/114502/1/Hall_nato_and_the_future_of_warfare.pdf

Multi-Domain Operations in NATO - Explained, (2023), Availabale at: https://www.act.nato.int/article/mdo-in-nato-explained/#:~:text=At%20its%20core%2C%20Multi%2DDomain,the%20right%20time%20and%20place.

Black, James, Lynch, Alice, Gustafson, Kristian, Blagden, David, Paille, Pauline & Quimbre, Fiona (2022) "Multi-Domain Integration in Defense: Conceptual Approached and Lessons from Russia, China, Iran and North Korea", RAND. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA528-1/RAND_RRA528-1.pdf.

Filipoff, Dmitry (2023) Fighting DMO Part 1: Defining Distributed Maritime Operations and the Future of Naval Warfare", Center for International Maritime Security, 20 February. Available at: https://cimsec.org/fighting-dmo-pt-1-defining-distributed-maritime-operations-and-the-future-of-naval-warfare/

Griesemer, Thomas S. (2018) "Russian Military Reorganization: A Step Towards Multi-Domain Operations". OTH: Multi-Domain Operations & Strategy. 19 November. Available at: https://othjournal.com/2018/11/19/russian-military-reorganization-a-step-toward-multi-domain-operations/

Judson, Jen (2022) "Multidomain operations concept will become doctrine this summer", Defense News, 24 March. Available at: https://www.defensenews.com/land/2022/03/23/multidomain-operations-concept-will-become-doctrine-this-summer/

Lindsay, Jon R. and Erik Gartzke (2020) "Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains", Journal of Strategic Studies. Available at: https://doi.org/10.1080/01402390.2020.1768372

NATO (2011) "Alliance Maritime Strategy". Available at: https://www.nato.int/cps/en/natolive/official_texts_75615.htm

NATO Combined Joint Operations from the Sea Center of Excellence (CJOS COE) (2021) "Study on Multi-Domain Operations in the Maritime Domain". Available at: http://www.cjoscoe.org/infosite/wp-content/uploads/2021/01/Study-on-Multi-Domain-Operations-in-the-Maritime-Domain.pdf

NATO Command and Control Centre of Excellence (C2COE) (2021) "Multi-Domain Command and Control: Providing a Working Description of the Term Multi-Domain C2 (MDC2)". Available at: https://c2coe.org/wp-content/uploads/Library%20Documents/Study/20210430%20MDC2%20Long%201.0.pdf

NATO Innovation Podcast (2022) “Multi-Domain Operations: The NATO Perspective”, December.

NATO News (2023) “NATO stands up undersea infrastructure coordination cell”, 15 February. Available at: https://www.nato.int/cps/en/natohq/news_211919.htm

Reilly, Jeffrey M. (2016) “Multidomain Operations: A subtle but Significant transition in Military Thought”, Air & Space Power Journal, Spring, 61-72. Available at: https://apps.dtic.mil/sti/tr/pdf/AD1003670.pdf

Spears, Will (2019) “A sailor´s take on multi-domain operations”, War on the Rocks, 21 May. Available at: https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/

Wall, Collin & Morcos, Pierre (2021) “Invisible and Vital: Undersea Cables and Transatlantic Security”, CSIS, 11 June. Available at: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

MILITARY STANDARDISATION WITHIN NATO AND THE EU: COMPLIMENTARY EFFORTS TO MANAGE THE IMPACTS OF CLIMATE CHANGE AND BUILD RESILIENCE

Eduardo Maya

Abstract: Some of the gravest challenges that NATO and the EU will face in the years to come emerge from the threat posed by climate change. Standardisation stands as a tool ready to build upon the complimentary and cooperative role that NATO and the EU fulfill in regard to each other. The relationship of these institutions and their member states entails that resource sharing be a priority, especially in the future when both are required to assist in more disaster response operations as the impacts of climate change are increasingly felt. Building upon existing structures, this paper recommends that NATO and the EU cooperate to develop a Joint Doctrine for Disaster Response Operations, standardise the language used in such doctrine and subsequent operations, develop joint mechanisms for early-warning and situational awareness in addition to emissions monitoring, and promote interchangeable guidelines on resilient infrastructure requirements.

Key words: Standardization, disaster response, NATO, EU, resilience, climate change, infrastructure, extreme weather.

As the Euro-Atlantic area becomes ever more plagued by remerging challenges such as strategic competition, as well as newly emerging threats associated with the impacts of climate change, coordination between the North Atlantic Treaty Organisation (NATO) and the European Union (EU) will become ever more necessary. Cooperation, which fosters the complimentary defence role that the EU fulfills regarding NATO while reinforcing European autonomy, brings along a series of challenges that must be overcome if the two organisations aim to coordinate to prevent the duplication of efforts and operate in a manner that is coherent and consistent. Given their complexity, multi-national operations require standardisation to function effectively. Essentially, the Euro-Atlantic area requires a new approach to standardisation which will allow the region's leading multi-national defence and governing institutions, NATO and the EU, to meet the emerging and future challenges of the 21st century, to include the deterioration of infrastructure and an increased need for disaster response operations concurrent with a rise in harsh and unpredictable operating environments.

NATO and the EU both refer to each other continuously when describing cooperation with entities outside of their own. The Berlin Plus agreement, for instance, describes the primacy of NATO regarding matters of collective defence in Europe, the complimentary role of the EU and its autonomy, and paves the way for operational support and coherent capability development that minimizes duplication.[1] Because of this relationship and connectivity, military forces from NATO and the EU must at all times be ready and available to execute missions while sharing facilities.[2] While numerous, one example of how NATO and EU operations can become intertwined is exemplified by how, NATO Operation Allied Harmony was taken over by the EU with the EU setting up its Head Quarters at Supreme Head Quarters Allied Powers Europe (SHAPE) while the EU Command Element was set up at NATO Joint Forces Command Naples, all the meanwhile NATO provided strategic, operational and tactical support.[3] The degree of interoperability emphasized by this example would be impossible without standardisation.

Soon after its inception, NATO recognised the necessity of standardisation which has led to the continuous development and improvement of its standardisation process, bodies, and management system.[4] Article 3 of the Washington Treaty calls for collective capacity amongst the Alliance, self-help and the ability to resist threats, and therefore serves as the basis for activities related

[1] NATO, "Relations with the European Union", updated 12 January 2023, https://www.nato.int/cps/en/natohq/topics_49217.htm#:~:text=The%202002%20NATO%2DEU%20Declaration,the%20EU's%20own%20military%20operations

[2] NATO, "The NATO – EU Strategic Partnership",
https://www.nato.int/docu/comm/2004/06-istanbul/press-kit/006.pd

[3] Ibid.

[4] NATO Standardisation Office, "NATO Standardisation History",
https://nso.nato.int/nso/home/main/home/nato-standardization-history

to standardisation and resilience.[5] Today, NATO standardisation encompasses a plethora of committees, tasking authorities, delegated tasking authorities, and coordinating agencies, which contribute in their respective areas of expertise. For example, tasking authorities include the Logistics Committee and the Conference of National Armament Directors, while some delegated tasking authorities that are subservient to them include the Logistics Committee Executive Group and the NATO Air Force Armaments Group.[6]

Similarly, standardisation in the EU, in particular such that concerns the defense industry, has evolved since 2013 when the EU High Representative for Foreign Affairs and Security Policy, Catherine Ashton, identified a strong European Defense Technological and Industrial Base as necessary to the Common Security and Defence Policy (CSDP).[7] Since then, standardisation has been an emerging topic and now subsumes conversations relating to the EU's defence planning and security. The recently published EU Strategic Compass calls for the creation of a Defence Innovation Hub within

[5] Cihangir Akşit, NATO Standardisation Agency, "Smart standardization: a historical and contemporary success at NATO", https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_05/20140528_140528-smart-standardization.pdf

[6] For a full overview of all bodies within NATO involved in the standardisation process, see https://nso.nato.int/nso/home/main/home

[7] Policy Department for External Relations. "The EU's Defence Technological and Industrial Base", European Parliament, January 2020, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/603483/EXPO_IDA(2020)603483_EN

the European Defence Agency (EDA), which will increase interoperability and cooperation between member states.[8] Other internal structures such as the European Defense Standards Reference System and the Defense Cooperation Standardisation Group both facilitate standardisation in the realm of defence.

It is evident that both organisations have bodies, systems, and processes which promote and execute standardisation. These structures are not mutually exclusive and to a degree are already compatible and complementary. For example, taking up NATO standards and applying them is common practice within the EU, and NATO standardisation allows consultation with other standard developing organisations when deemed necessary.[9] Therefore, it is the objective of this study to explore the standardisation structures found within NATO and the EU and their respective efforts aimed at combatting climate change in order to build upon their similarities to describe cooperative actions driven by standardisation that can be undertaken to manage the impacts of climate change, primarily in the domains of military infrastructure resilience and disaster response operations. To be addressed includes possible

[8] Council of the European Union, "A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security", March 21, 2022, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

[9] European Defence Agency, "European Defence Standards Reference System (EDSTAR)", https://edstar.eda.europa.eu/ ; Cihangir Akşit, NATO Standardisation Agency, "Smart standardization: a historical and contemporary success at NATO"

coordination mechanisms that can take respective NATO and EU projects and make them more accessible to one another, while standardising data collection, storage and platforms for analysis.

Limitations

While the need for materiel standardisation in the realm of energy efficient and resilient technologies that can operate in the extreme environments posed by climate change - primarily heat and cold - is of upmost importance, the technical nature of capability criteria selection, development and acquisition is outside the scope of this study. However, the commitment of both NATO and the EU at the 2016 Warsaw Summit to have coherent defense planning processes, provides the basis for this cooperation. [10] Simultaneously, both organisations have put forth mechanisms intent on funding new technologies, which will require cooperation to reduce the duplication of efforts in the realm of environmentally resilient capabilities.

In a similar manner, while recommendations will be made on how to better use current resources and expertise to train forces to better respond to disasters in extreme weather conditions, the complex nature of exercise planning and execution will not be covered given the immense amount of time and resources that exercise planning and training require.

[10] NATO, "Relations with the European Union"

The Standardisation in NATO and EU

As a tool that seeks to reduce unnecessary duplication of resources, ensure cost effectiveness, interoperability, and foster multi-national operations, standardisation is the tool most appropriate to ensure cooperation between NATO and the EU. This is because standardisation promotes coherent planning processes that are as productive as possible given the emphasis it places on reducing the duplication of resources. As will be described, NATO has a far more pronounced standardisation mechanism compared to that of the EU, but nonetheless, the importance that the two institutions place on standardisation in the realm of defence is comparable and increasing.

NATO Standards

At the highest echelons, NATO standardisation is directed by a multitude of tasking authorities which bear responsibilities associated with their expertise and duty assignments.[11] These include the Committee for Standardisation, Military Committee, Conference of National Armament Directors, the Logistics Committee, Aviation Committee, Consultation Command and Control Board, and the Science and Technology Board.[12]

[11] Tasking Authorities oversee the work done by their subordinate Delegated Tasking Authorities and Working Groups, while carrying the responsibility of coordinating and consulting with the NATO Standardisation Office ; NATO, “AAP 03 Directive for the Production, Maintenance and Management of NATO Standardisation Documents”, Edition K Version 2, NATO Standardisation Office Updated October 2022

[12] For more see NSO website, https://nso.nato.int/nso/home/main/home

Additionally, each of these tasking authorities can create delegated tasking authorities which directly work on producing standards. Delegated tasking authorities are associated with specific areas found within the Tasking Authorities' responsibilities. For example, the Conference of National Armament Directors has delegated tasking authorities which work on standards related to military domains to include air, naval, and land, while also having sub-structures that work on life cycle management and ammunition safety.[13] In the same regard, the Military Committee has delegated tasking authorities assigned to the varied military domains in addition to joint operations, medicine and terminology related standardisation.[14]

Coordinating the efforts of the tasking Authorities, delegated tasking authorities, subject matter experts (SMEs), and established working groups, is the responsibility of the NATO Standardisation Office (NSO). This Office and its Director are the primary point of contact for matters related to standardisation and are also in charge of NATO's online platforms on standardisation to include NATO TERM, which acts as an online database for approved NATO terminology, and the NATO Standardisation Document Database,

[13] NATO Standardisation Office, "Conference of National Armament Directors (CNAD)", , https://nso.nato.int/nso/home/main/home/publications/tasking-authorities/conference-of-national-armaments-directors

[14] NATO Standardisation Office, "Military Committee(MC)", https://nso.nato.int/nso/home/main/home/publications/tasking-authorities/military-committee

which tracks the creation of standardisation documents and the evolution of the eventual end product, while also acting as a storehouse for all finalized standardisation documents.

Standardisation as a concept within NATO transcends one singular function as outlined in its definition as being "the development and implementation of procedures, designs and terminology to the level necessary for the interoperability required by Allies".[15] In this respect, each of the fields of standardisation aim to improve interoperability in a specific manner. The operational field governs "among other things, to such matters as concepts, doctrine, tactics, techniques, logistics, training, organizations, reports, forms, maps and charts".[16] The materiel field deals with physical equipment requirements such a communication equipment, similar connecting equipment for the refueling of vehicles, and the specifications which materiel must meet. Finally, the administrative field deals, inter alia, matters related to terminology, military ranks and classifications, and the matter in which reports are submitted.

Furthermore, during its creation each standard is assigned a level of standardisation: compatible, interchangeable, and commonality.[17] Commonality is the highest degree of standardisation because its achievement signifies the use of the

[15] ; NATO, "AAP 03 Directive for the Production, Maintenance and Management of NATO Standardisation Documents"

[16] Ibid.

[17] Ibid.

same equipment, doctrine and operating procedures. Compatible is the lowest of the 3 given that it simply means that in a given context and under specific circumstances, two actors are able to cooperate without any unnecessary complications. Interchangeability falls between the two as it implies that in addition to being able to work together, the materiel and procedures of each actor can be used by the other without causing egregious complications.

When NATO combines and utilizes the aforementioned standardisation entities and guiding principles, the result is the production of Standardisation Agreements (STANAGs) or Standardisation Recommendations (STANRECs), which can both be additionally implemented by partner nations. STANAGS are binding agreements between the Allies with the aim of improving interoperability.[18] Based on their own needs, Allies can agree to implement STANAGs fully, in part, with or without reservations, or agree to implement them in the future.[19] STANRECs are non-binding, not related to interoperability, and are used to guide multinational cooperation in the realm of material standardisation based on established best practices.[20] Supporting elements to the creation of these documents include assistance from SMEs and

[18] Ibid.

[19] Ibid

[20] Ibid ; NATO, "NATO Defence Planning Process", updated 31 March, 2022, https://www.nato.int/cps/en/natohq/topics_49202.htm

NATO accredited Centers of Excellence.[21] The end products are classified at the lowest level possible to ensure that they can be implemented by necessary partners and organisations which seek to use NATO standards as a way to avoid the duplication of efforts and gain a heightened status by using the standards to highlight their participation in the international community.[22] However, while NATO houses an intricate and fluent standardisation development capacity, the use of civil and national defense standards are considered before the creation of a purely NATO standard. [23] Furthermore, when advantageous to both NATO and civilian standard developing organisations, NATO will enter into Technical Cooperation Agreements with these organisations to facilitate the joint production of standards.[24]

This established ability to cooperate with other organisations that seek to construct standards alongside NATO, or adopt existing

[21] Centres of Excellence are international military organisations that train and educate leaders and specialists from NATO member and partner countries... assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation. They offer recognised expertise and experience … and support the transformation of NATO, while avoiding the duplication of assets, resources and capabilities.- NATO, “Centres of Excellence”, updated 6 December 2022,https://www.nato.int/cps/en/natohq/topics_68372.htm

[22] Cihangir Akşit, NATO Standardisation Agency, “Smart standardization: a historical and contemporary success at NATO”

[23] NATO prefers to use civilian standards over national defence standards and will always seek a civilian standards before utilizing an already developed defense standard, AAP 03 Directive for the Production, Maintenance and Management of NATO Standardisation Documents

[24] Ibid.

NATO standards, is crucial when considering the importance of standardisation in regard to military forces that at one time or another could be required to perform either NATO or EU operations. Furthermore, given that not all current EU member countries are part of the Alliance, the adoption or co-development of standards between the two organisations is vital to ensure the highest level of standardisation (compatible, interchangeable, or commonality) is achieved as to consistently, coherently, and collaboratively execute disaster response operations.

EU Standards

While the EU does not have the same overarching mechanism as NATO to produce and implement standards, the Union still maintains a system which aims to enhance defence cooperation, innovation, and procurement, which in return increases the interoperability of member states. The implementation of an increasingly coherent European standardisation system within the EU is viewed as necessary given the fragmented defence industry in the Union in addition to a semi-protectionist attitude found in member countries regarding their defense industries.[25] Up until

[25] European Defence Agency, "Standardisation", https://eda.europa.eu/news-and-events/spotlight/spotlight-of-the-month/how-is-eda-helping-to-ensure-eu-armed-forces-have-interoperable-and-interchangeable-arms-ammunition-fuel-and-protection -

2016, 80% of defence industry spending was happening within individual member states.[26]

Starting with the 2016 EU Global Strategy, the necessity of defense standardisation started to become operationalized within the Union. This Strategy's Implementation Plan on Defence and Security states that capability requirements should be identified through the Capability Development Plan.[27] The Plan is a strategic document which looks at the Unions current and future needs according to present and emerging challenges while also considering technological innovation.

The EDA does not in itself construct standards, but through its Defence Standards Reference System, it catalogs current standards adopted by the EU which originate in the national civilian and defence sectors as well as within NATO. The System serves as a tool that can be used by member states to better understand how to implement standards.[28] Concurrently, this Reference System serves as a tool for the defence industry to guide the development of weapons systems by ensuring that, first and foremost, they understand the expectations of the EU and the

[26] Policy Department for External Relations, "EU Defense Technological and Industrial Base", European Parliament, January 2020, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/603483/EXPO_IDA(2020)603483_EN

[27] European Defence Agency, "European Defense Standardisation" https://eda.europa.eu/what-we-do/all-activities/activities-search/materiel-standardisation#

[28] Ibid.

technical specifications which must be met. The standards input into the System simultaneously include Expert Group Reports, which are documents presenting the data acquired from on-gong projects. [29] The Reference System is truly a one-stop shop for all information regarding EU standardisation.

Because of defence industry spending in individual member nations, the EU has collectively taken varied steps to encourage collective work on defence industry projects and subsequent procurement. Permanent Structured Cooperation (PESCO) advises on how to prioritize gaps in capabilities identified in the Coordinated Annual Review on Defense and the Capability Development Plan.[30] Next, the European Defense Fund (EDF), works as a financial mechanism which supports the development of identified capabilities, with additional assistance offered to projects which were identified through PESCO.[31] In collaboration with the EDF, the European Defence Industrial Development Programme valued at €500 million will be used to encourage defense industry projects to abide by agreed upon technical standards.[32]

[29] European Defence Agency, "European Defence Standards Reference System (EDSTAR)"
[30] Ibid.
[31] Ibid
[32] Policy Department for External Relations, "European Armaments", European Parliament, October 2018, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Defence%20study.pdf

Like its partner NATO, the EU does not seek to work alone and to a degree promotes cooperation with civilian organisations further than that which is found within the Alliance. Specifically through the Defence Cooperation Standardisation Group, a conglomeration constructed through the joining of forces found in the EDA, the European Committee for Standardisation, The European Telecommunications Standards Institute and the European Committee for Electrotechnical Standardization. [33] The Standardisation Group acts as an interface between these standard development organisations, the EDA, and the European Council.

While standardisation within the EU as described focuses primarily on capability development, given that the EU seeks to strengthen its own defence industry and minimize external reliance, standardisation in both NATO and the EU transcend capability development and encompass other areas deemed crucial to disaster response and military mobility to include infrastructure. The challenges that climate change poses to disaster response operations, critical infrastructure, and the Trans-Atlantic Area as a whole, to include its citizens, are described in the next section with efforts to create a more resilient capacity also mentioned.

[33] European Defence Agency, “European Defense Standardisation”

Climate Change and Resilience in the Trans-Atlantic Area

No one country can alone tackle the challenges caused by climate change, and given their geographical overlap and commitments to cooperation, NATO and the EU are able to work congruently to address its impacts. NATO understands climate change as multiplying and exacerbating existing threats, creating geopolitical instability while creating a harsher operating environment for its military forces.[34] Similarly, the EU sees climate change as creating greater global instability, a threat multiplier that challenges peace and security globally with implications for European security.[35]

The challenges caused by climate change have long been felt and are expected to continue well into the future. From 1980 to 2020, 138,000 European citizens lost their lives due to extreme weather and climate related events. [36] More recently, Europe faced one of its harshest heatwaves in recent history when in 2019, 2,500 citizens lost their lives.[37] Temperatures in Europe have increased twice the global average in the last 30 years and per its current

[34] NATO, "Environment, climate change and security", Updated 26 July 2022, https://www.nato.int/cps/en/natohq/topics_91048.htm

[35]European External Action Service, "Climate Change and Defense Roadmap", Council of the European Union, 9 November 2020, https://data.consilium.europa.eu/doc/document/ST-12741-2020-INIT/en/pdf

[36] European Council, Council of the European Union, "Climate Change: What the EU is Doing", https://www.consilium.europa.eu/en/policies/climate-change/#:~:text=Under%20the%20European%20climate%20law,EU%20climate%20neutral%20by%202050

[37] Ibid.

trajectory are expected to exceed the global mean.[38] Other stark future possibilities including a grand majority of Europe facing increasing drought events during the time period of 2041-70, with the greatest impacts felt in southern countries such as Spain and Greece.[39] During the same time period, heavy rains that can lead to flash floods are is estimated to increase by up to 25% in most of Europe, with the hardest hit areas in central Europe such as Poland, Slovakia, and Hungary seeing up to a 35% increase[40]. These forward looking estimates and their severity is dependent on mitigation actions taken now with the European Union taking extensive measures to reduce their carbon emissions. Nonetheless, the impacts of climate change are certain and will represent a grave challenge for the remainder of the 21st century.

From a financial perspective, the harsh reality is that €2 billion in damages is caused every year by forest fires and over a 40-year span, Europe has seen a loss of €487 billion due to natural disasters.[41] Similarly, financial damages will continue to be felt as sea levels rise and its effects to include flooding, erosion, and

[38] World Meteorological Organization, “Temperatures in Europe Increase More than Twice Global Average”, 2 November 2022, https://public.wmo.int/en/media/press-release/temperatures-europe-increase-more-twice-global-average

[39] European Environment Agency, “Climate change Impacts in Europe” https://experience.arcgis.com/experience/5f6596de6c4445a58aec956532b9813d

[40] Ibid.

[41] Ibid.

infrastructure degradation impact the coastal region which houses 40% of the EU's population who simultaneously produce 40% of its GDP. [42] In addition to a changing security environment that now emphasizes the threat posed by Russia, the continued impacts of climate change will inevitably mean more military supported disaster response operations in ever more dangerous extreme weather environments.[43] Simultaneously, military capabilities and personnel will also need to be prepared for crisis management necessities emerging at Europe's footsteps as climate changes cascading effects are felt in neighboring countries to the south and east and require Europe's attention through the fulfillment of CSDP missions to maintain security at home.

Both NATO and the EU have taken immediate steps to begin adapting to climate change while seeking to reduce their environmental impacts. A centerfold to adaptation measures revolves around resilience to include that of infrastructure, capabilities, and people/ societies. Through cooperation with each other and other international organisations, NATO and the EU are poised to meet their individually defined goals of becoming a global leader on climate change issues (EU), and the leading international organisation in understanding and adapting to the security

[42] European Commission, "Forging a Climate-Resilient Europe – the New EU Strategy on Adaptation to Climate Change", 24 February, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0082&from=EN

[43] European External Action Service, "Climate Change and Defense Roadmap"

challenges of climate change (NATO).[44] Standardised requirements for infrastructure and legally enforceable legislation on environmental protection represent some of the tools available to the organisations, with strengthening existing standardisation representing a potential avenue to further cooperation.

NATO and Climate Change

Given NATO's role and responsibilities as promoting stability in the Trans-Atlantic Area and preserving its peace and security, the Alliance sees its main challenges associated with climate change having to do with disaster response and the environment in which it will be militarily operating.[45] As previously mentioned, the number of disaster response operations NATO expects to be involved in will increase with the operating environment having more characteristics associated with climate change, primarily extreme weather environments. Regarding disaster response and overall logistics capabilities, one of the domains in which NATO expects complications is in the air as changes in air temperature and density can lead to decreased load capacities for aircraft, shorter ranges, and the possibility for electronic components to overheat.[46] Issues

[44] Ibid. ; NATO, "NATO Holds Roundtable on Climate Change and Security, Bringing Together Allies and Experts, 15 December 2022, https://www.nato.int/cps/en/natohq/news_210129.htm#:~:text=NATO%20has%20been%20actively%20engaging,by%20NATO%20Leaders%20in%202021

[45] NATO, "The North Atlantic Treaty", Updated 10 April 2019, https://www.nato.int/cps/en/natohq/official_texts_17120.htm ; NATO, "Environment, climate change and security"

[46] Ibid.

in the air domain alongside in others, i.e. land, sea, could seriously undermine the ability of NATO to deliver much needed supplies during a disaster response operation.[47] Climate change impacts such as these are compounded by the necessity for more maintenance and increased wear and tear on vehicles and other equipment.[48] This specific example highlights the need for further materiel standardisation which promotes resilient capabilities that would be required of NATO and the EU's 21 in common member countries.

Given this described context, NATO has taken and seeks to take additional measures to ensure it contributes to environmental protection and adapts to climate change. Through the Climate Change and Security Action Plan, NATO has committed itself to preparing on a yearly basis a Climate Change and Security Impact Assessment, which will guide adaptation, to include civil preparedness perspectives in its exercises and training, and to develop a tool that can track the greenhouse gas emissions associated with its operations.[49]

Fulfilling its intention, the Assessment identifies manners in which the resilience of infrastructures will be put to the test in years to

[47] NATO, "NATO Releases its Climate Change and Security Impact Assessment", Updated 28 June 2022, https://www.nato.int/cps/en/natohq/news_197241.htm
[48] Ibid.
[49] NATO, "NATO Climate Change and Security Action Plan", Updated 14 June 2021, https://www.nato.int/cps/en/natohq/official_texts_185174.htm

come. Some examples given are how storm surges caused by rising sea levels can harm ports and limit their usage, how melting permafrost degrades infrastructure, primarily that in northern Europe during a time when shipping routes through the Arctic are opening and simultaneously the risk of disaster is increasing, and how desertification impacts critical water infrastructure needed for operations.[50] Through a forward looking approach, NATO has a set of 7 guidelines which are used to continuously monitor and assess the resilience of its member states and their respective infrastructure.[51]

In the context of collaboration alongside the EU, it is important to note that NATO fully understands and accepts the reality that within Europe, it is not always going to be the first responder in charge of tackling the impacts of climate change and subsequent disasters.[52] Such understanding and mutual respect is crucial to the relationship between the EU and NATO, with NATO believing a stronger EU that is capable of independently dealing with matters threatening the interest of Europe only helps to promote greater European

[50] NATO, "NATO Releases its Climate Change and Security Impact Assessment"

[51] NATO, "Resilience, Civil Preparedness and Article 3, Updated 20 September 2022, https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=Each%20NATO%20member%20country%20needs,civil%20preparedness%20and%20military%20capacity

[52]NATO, "NATO Climate Change and Security Action Plan",

responsibility.[53] As complimentary organisations, their collaborative work on the matter has already begun. Together these bodies have consulted on and created the Environment and Security Initiative which funds projects on climate adaptation and recently set up a taskforce on resilience and critical infrastructure.[54]

EU and Climate Change

In 2019, the Global Commission on Adaption "recognized the EU as a pioneer in integrating considerations of climate risk into decision-making".[55] The EU's efforts furthermore are enshrined through the European Climate Law that includes the Unions commitment to reduce its emissions by 55% compared to 1990 levels by 2030 and achieve climate resilience and carbon neutrality by 2050.[56] It is important to note that while the EU and the world might do their best to reduce emissions, the impacts of climate change are not preventable and the severity will depend on future and ongoing actions. Therefore, the EU is also seeking to adapt to the changes that are unavoidable.[57]

[53] NATO, "Relations with the European Union"

[54] NATO, "NATO and the EU Set Up Taskforce on Resilience and Critical Infrastructure, Updated 11 January 2023, https://www.nato.int/cps/en/natohq/news_210611.htm ; NATO, "Environment, climate change and security",

[55] European Commission, "Forging a Climate-Resilient Europe – the New EU Strategy on Adaptation to Climate Change",

[56] European Council, Council of the European Union, "Climate Change: What the EU is Doing"

[57] Ibid.

To this extent, the European Commission has set forth climate proofing guidelines applicable to the construction of infrastructure.[58] This has been done in the hope of fostering future standardisation and promote the uptake of such guidelines on an international scale.[59]

Furthermore, in the field of disaster response, through the Climate and Defense Roadmap put together in collaboration by the EDA and the European External Action Service (EEAS), the EU seeks to take climate change into consideration in future research and development, infrastructure and CSDP missions. As CSDP missions are one of the primary tools for disaster response in the toolbox of the EU, the Roadmap has chosen to highlight the need to expand on climate adaptation and training for these missions. Similar to NATO's commitment to monitor its greenhouse gas emissions, the Roadmap also sets the stage for the development of a mechanism to track emissions related data of infrastructure and CSDP missions, with the intent of reducing energy consumption and increasing energy efficiency.

Developments are also emerging in the field of resilience where the EU Joint Research Center has put forth a scientific measurement

[58] European Commission, "Forging a Climate-Resilient Europe – the New EU Strategy on Adaptation to Climate Change",

[59] Ibid.

that can quantify resilience, while giving a theoretical explanation.[60] The purpose of this measurement tool is to construct Resilience Dashboards, which are online platforms where the resilience of member countries can be tracked.[61]

Managing the Impacts of Climate Change and Strengthening Resilience through Standardisation

Climate change in the Euro-Atlantic area, primarily Europe, poses tremendous challenges for NATO and the EU. While many steps have been taken and commitments made to tackle these challenges and promote environmental protection, avenues with opportunities for increased synergy between the two organisations still prevail, specifically in the fields of disaster response, military mobility and resilient infrastructure. Standardisation, as promoting cost effectiveness, interoperability, and the reduction of redundant investments, serves as an appropriate tool for NATO and the EU to further their extensive collaboration, leading to the protection of their citizens. Given that NATO and the EU have various internal bodies that serve similar functions, such as the NATO Military Committee and the EU Military Committee, and produce similar products like the NATO Defense Planning Process and the EU Capability Development Plan, cooperation can be pursued through the appropriate established structures. The subsequent section

[60] EU Science Hub, “Resilience”, European Commission, https://joint-research-centre.ec.europa.eu/scientific-activities-z/resilience_en

[61] Ibid.

describes how the established structures, commitments, and projects explained previously, which carry out similar functions within NATO and the EU, can serve to further expand cooperation between the two organisations with standardisation taking a leading role. In the field of standardisation, cooperation transcend all the fields operational, materiel, and administrative, and therefore requires coordination across varied bodies

Joint Doctrine for Disaster Response Operations

The development and implementation of doctrine carries the responsibility of providing common operating guidelines for forces as to promote a coherent manner of thinking across decision makers while leaving room for specific executive actions to be undertaken according to the context of a given situation.[62] As NATO and EU military forces are expected to be called on more frequently and for longer periods of time to engage in disaster response operations, ensuring that training and exercises are in line with a common operating doctrine would be to the benefit of either institution.

A *Joint Doctrine on Disaster Response* would serve the purpose of ensuring that planning and mobilization for disaster response operations follow similar procedures while providing practical areas for training and exercise such as heightened alertness in extreme

[62] NATO, "AAP-47 Allied Joint Doctrine Development", Edition C Version 1, NATO Standardisation Office, Modified 19 February 2019

weather environments, mobilization of forces while accounting for other possible crisis management contingencies that keep force readiness at appropriate levels, expedited allocation of transport vehicles (in the air, land, and sea domains), and communication procedures with civilian disaster response agencies and coordination with local security forces.

The development of shared doctrine is of additional pertinence given the Berlin Plus Agreement between NATO and the EU which allows for NATO support of EU operations and the use by the EU of NATO's defense planning capabilities and infrastructure.[63] The creation of such doctrine would be undertaken by NATO in consultation with the EU, and subsequently then taken up by the EU. This is because NATO's extensive experience with creation operational doctrine and established procedures for such as represented by Allied Administrative Publication 47 – Allied Joint Doctrine Development.[64]

Cooperation on the development of this doctrine would be best served by the Military Committee Joint Standardisation Board, given that disaster response encapsulates all military operating domains, and the EU Defence Standardisation Committee, as it acts as a consultation mechanism for standard developing organisations. As NATO and the EU's disaster response and coordination bodies,

[63] NATO, "Relations with the European Union"
[64] NATO, "AAP-47 Allied Joint Doctrine Development", Edition C Version 1

work would have to be done through coordination amongst the EU's European Disaster Response Coordination Centre (EDRCC) and the EEAS, in addition to NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC). Alongside the military components of NATO and the EU, these disaster response agencies would be the primary customers of a doctrine on disaster response.

Standardised Language in the Joint Doctrine

In disaster response operations and their lead-up, the use of standardised language is of upmost importance given that through it, countries can appropriately explain what services and materiel they require, while ensuring that agencies such as the EDRCC and the EADRCC locate, allocate, and deliver the appropriate resources. NATO TERM, NATO's online platform for the storage and access of agreed upon terminology could serve as a crucial tool for both NATO and the EU to ensure that they are using the same language regarding the *Joint Doctrine for Disaster Response Operations*. Because of its openness, this repository of terminology can also be accessed by partner countries to familiarize themselves with the terminology so that if ever in need, proper communication can take place and thus facilitate expedient resource delivery and reduce the burden of additional transports. As climate change continues to exacerbate the dangers associated with the operating environment during disaster response operations, to include extreme heat and cold, storm surges, precipitation and flooding, the strain on transport vehicles, their capacity and ranges, and subsequent repairs will increase, meaning that their use must be as efficient as possible.

Early-Warning and Situational Awareness Platform

The ability to track weather patterns and preparing for extreme weather events by assessing and monitoring their impacts is crucial regarding disaster response operations and overall military operations planning. These are capabilities that both NATO and the EU recognize and are investing in. NATO uses space-based satellites to monitor changing weather patterns and prepare for any needed response in a swift manner.[65] Similarly, through the Copernicus Programme, the EU has a multitude of mechanisms that are used to effectively monitor natural disasters and hazards to include the: Global Disaster Alert and Coordination System; European and Global Flood Awareness; Europe and Global Forest Fire Information System; and European and Global Drought Observatories.[66]

Given the importance of being able to anticipate extreme weather events and be situationally aware of events as they unfold on the ground, cooperation in the realm of satellite based observation

[65] J. Lukačevič, K. Kertýsová, R. Heise , "The Climate-Space Nexus", NATO Review, 18 August 2022, https://www.nato.int/docu/review/articles/2022/08/18/the-climate-space-nexus-new-approaches-for-strengthening-natos-resilience/index.html

[66] European Civil Protection and Humanitarian Aid Operations, "Civil Protection", European Commission, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection_en

systems would be a value added addition to both NATO and the EU's disaster response readiness and planning. Therefore, it is recommended that NATO and the EU develop an interface that is compatible with the data received from the satellite networks of either institution as to create a platform where data from NATO's satellites and those of the Copernicus Programme can be consolidated to improve early warning and situational awareness.

Emissions Monitoring Mechanism

As NATO and the EU strive for carbon neutrality, both have made commitments to monitor the emissions that are produced by their respective missions in order to understand the impact on the climate, which can lead to advances in energy efficiency. Through the Climate Change and Security Action Plan, NATO has stated its intention to develop a mechanisms that is capable of tracking its greenhouse gas emissions as part of its effort to operationalize its Climate Change and Security Action Plan. Similarly, through the Climate Change and Defence Roadmap, the EU has committed itself to the construction of a mechanism to serve as a "repository, observatory and research platform for reducing energy consumption, increasing efficiency, collection of energy related data on operations and infrastructure".[67]

[67] European External Action Service, "Climate Change and Defense Roadmap"

Given the extreme similarities of both these identified future efforts, and standardisations goal to reduce the duplication of efforts and promote cost effectiveness, standardisation serves as the tool of choice to ensure cooperation between NATO and the EU on this matter. The Action Plan already sets forth the basis for this cooperation as its fourth pillar commits the Alliance to enhance its outreach to engage in exchanges with organisations active in mitigating climate change, while mentioning the EU by name.[68] Therefore, the opportunity arises for the creation of an interface capable of digesting data acquired from both organisations to clearly identify emissions expelled from Euro-Atlantic operations and defense infrastructure, while also being able to separate data as to understand individual greenhouse gas emissions to guide pollution reduction measures and understand the respective environmental impact. Because these projects are yet to be established, the opportunity now exists to ensure that data collection is done in a standardised manner to facilitate collation, analysis, and storage by the proposed interface.

Resilient Infrastructure

Of the upmost importance to disaster response operations is the ability to use infrastructure, primarily civilian, to transport military equipment across individual countries and across borders. After the end of the Cold War, infrastructure agreements with private

[68] NATO, “NATO Climate Change and Security Action Plan”

businesses were ended and their sole responsibility transferred to the businesses, leading to a modern reliance on civilian infrastructure for military mobility.[69] This is exemplified by the fact that 90% of transport infrastructure for large scale military operations are provided by the private sector.[70] Because of this immense reliance, it is necessary that civilian infrastructure not only be available for the movement of military forces, but also that it be resilient to the challenge posed by climate change. Through the consolidation of afore mentioned efforts within NATO and the EU to increase Resilience and building upon ongoing cooperation, a path forward for the construction and maintenance of resilient infrastructure arises and presents a solution to the challenges posed to military mobility by the effects of climate change. Within NATO, the Strengthened Resilience Commitment requires the Alliance to set forth national resilience objectives for member countries, while acknowledging that objectives will also take into consideration responsibilities a country might have to the EU.[71] Guiding these objectives is the 7 baselines to measure resilience, one of which focuses on resilient transport systems which ensure that Alliance forces can move across their territory rapidly.[72] As mentioned, the EU has its own set of climate proofing guidelines for

[69] NATO, “Resilience, Civil Preparedness and Article 3”

[70] Ibid.

[71] NATO, “Strengthened Resilience Commitment”, Updated 13 September 2022, https://www.nato.int/cps/en/natohq/official_texts_185340.htm

[72] NATO, “Resilience, Civil Preparedness and Article 3”

resilient infrastructure that are set forth by the European Commission and mentioned in the EU Strategy on Adaptation to Climate.[73] Additionally, both institutions recently agreed to set up a task force on resilience and critical infrastructure.[74] This is a new development at the time of this writing with specifics not mentioned as of now. While what is known primarily revolves around the resilience of critical infrastructure in the context of a Russian threat, the pertinent threat that climate change poses to infrastructure cannot be ignored.

Cooperation between NATO and the EU regarding military mobility is one of the more logical locations to start expanding cooperation on resilience given the 18 shared declarations the two organisations have on the matter.[75] In this context, and that of disaster response, military mobility entails rapid movement across borders which circumvents traditional administrative processes, ensuring that sufficient transport infrastructure is available, and an understanding that this infrastructure must be robust and resilient.[76] Within the EU,

[73] European Commission, “Forging a Climate-Resilient Europe – the New EU Strategy on Adaptation to Climate Change”

[74] NATO, “NATO and the EU Set Up Taskforce on Resilience and Critical Infrastructure”

[75] NATO, “Relations with the European Union”,

[76] Ibid. ; European Defence Agency, “The EU Capability Development Priorities”, 2018 Revision, https://eda.europa.eu/docs/default-source/eda-publications/eda-brochure-cdp.pdf

there is an established understanding that this infrastructure must be resilient to climate change.[77]

Guidelines on resilient infrastructure requirements mentioned to include those of the European Commission, NATO, and the EU Joint Research Centre, provide a credible avenue to further cooperation between the two institutions to ensure the same standards are being abided by which in return make infrastructure, primarily across Europe, equally resilient to climate change. Given the nature of the Berlin Plus Agreement described previously, the use of NATO infrastructure and facilities by the EU entails that Alliance infrastructure should be as equally resilient to that of the EU to ensure that EU disaster response operations function smoothly in times when the EU is the primary responder and not NATO. Therefore, the standardisation of guidelines to the standardisation level of interchangeable should be a target goal.[78] Interchangeability of infrastructure resilience standards would allow EU standards to be used for primarily civilian infrastructure, not including transport, while also ensuring that national European transport infrastructure, which could be used under the auspices of NATO or the EU, abide by the same standards. Standardisation would prove an effective tool to ensure that EU-NATO military

[77] European Commission, “Military Mobility: EU Proposes Actions to Allow Armed Forces to Move Faster and Better Across Borders”, 10 November 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6583

[78] For a recap on the levels of standardisation and their characteristics refer to the section titled **NATO Standardisation**, Paragraph 4

mobility agreements are backed by infrastructure that can meet the future challenges of climate change in the event of crisis, but are simultaneously available for disaster response operations as they inadvertently increase in number in the decades to come. The newly created NATO-EU taskforce on resilient infrastructure and the NATO Resilience Committee would be some of the internal structures best equipped to tackle the challenge of resilient infrastructure alongside the NATO Standardisation Office and the EU and NATO Military Committees.

Overall, resilience will be the focus of the future for a myriad of operational enablers within NATO and the EU to include infrastructure and technological capabilities. As the EU seeks to create a Defence Innovation Hub with the EDA, with acquired capabilities being state owned and therefore also available for use in NATO operations, the standardisation of climate resilient capabilities capable of operating in extreme weather conditions is sure to increase. Simultaneously, requirements for ever more resilient infrastructure will become more pertinent across NATO and the EU as both are tasked with their own set of crisis management and disaster response operations and missions in response to the effects of climate change within their own borders and to the periphery.

Conclusion

Standardisation serves as the basis for multi-national operations given their overall complexity. Both NATO and the EU by their nature therefore require standardisation to ensure coherent and effective operations involving dozens of countries. With the EU playing a complimentary role to NATO in the realm of defence, it is necessary that the two organisations cooperate as to avoid the duplication of costly and time lengthy investments.

The effects of climate change pose a serious threat to the Euro-Atlantic area given the hazards associated with storm surges, flooding, drought, desertification, and other extreme weather events. The efforts being undertaken by both NATO and the EU to increase their environmental protection efforts are plentiful, but nonetheless climate change and its effects will undoubtedly require that both organisations be called upon for disaster response operations more frequently and for longer periods of time. Therefore, it is crucial that NATO and the EU work together to standardise their approaches to disaster response and the infrastructure that supports these operations and overall military mobility. The recommendations given on how to approach this issue include the creation of a shared doctrine for disaster response operations which includes the standardisation of language, cooperation on early warning and situational awareness mechanisms, the joint production of an emissions monitoring mechanism, and the adoption of interchangeable guidelines on resilient infrastructure. While these recommendations represent some of the more coherent places to further cooperation on standardisation across NATO and the EU, the immense challenges to be posed by climate change will require continuous cooperation across the next decades in other equally important areas such as the development of capabilities that are resilient in extreme weather conditions.

Bibliography

Cihangir Akşit, NATO Standardisation Agency, “Smart standardization: a historical and contemporary success at NATO”, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_05/20140528_140528-smart-standardization.pdf

Council of the European Union, “A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security”, March 21, 2022, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

EU Science Hub, “Resilience”, European Commission, https://joint-research-centre.ec.europa.eu/scientific-activities-z/resilience_en

European Commission, “Forging a Climate-Resilient Europe – the New EU Strategy on Adaptation to Climate Change”, 24 February, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0082&from=EN

European Commission, “Military Mobility: EU Proposes Actions to Allow Armed Forces to Move Faster and Better Across Borders”, 10 November 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6583

European Council, Council of the European Union, “Climate Change: What the EU is Doing”, https://www.consilium.europa.eu/en/policies/climate-change/#:~:text=Under%20the%20European%20climate%20law,EU%20climate%20neutral%20by%202050

European Defence Agency, “European Defence Standards Reference System (EDSTAR)”, https://edstar.eda.europa.eu/

European Defence Agency, “European Defense Standardisation” https://eda.europa.eu/what-we-do/all-activities/activities-search/materiel-standardisation#

European Defence Agency, “Standardisation”, https://eda.europa.eu/news-and-events/spotlight/spotlight-of-the-month/how-is-eda-helping-to-ensure-eu-armed-forces-have-interoperable-and-interchangeable-arms-ammunition-fuel-and-protection-

European Defence Agency, “The EU Capability Development Priorities”, 2018 Revision, https://eda.europa.eu/docs/default-source/eda-publications/eda-brochure-cdp.pdf

European Environment Agency, “Climate change Impacts in Europe” https://experience.arcgis.com/experience/5f6596de6c4445a58aec956532b9813d

European External Action Service, “Climate Change and Defense Roadmap”, Council of the European Union. 9 November 2020, https://data.consilium.europa.eu/doc/document/ST-12741-2020-INIT/en/pdf

NATO Standardisation Office, “Conference of National Armament Directors (CNAD)” , https://nso.nato.int/nso/home/main/home/publications/tasking-authorities/conference-of-national-armaments-directors

NATO Standardisation Office, “Military Committee(MC)”, https://nso.nato.int/nso/home/main/home/publications/tasking-authorities/military-committee

NATO, “AAP 03 Directive for the Production, Maintenance and Management of NATO Standardisation Documents”, Edition K Version 2, NATO Standardisation Office Updated October 2022

NATO, “AAP-47 Allied Joint Doctrine Development”, Edition C Version 1, NATO Standardisation Office, Modified 19 February 2019

NATO, “Centres of Excellence”, updated 6 December 2022,https://www.nato.int/cps/en/natohq/topics_68372.htm

NATO, “Environment, climate change and security”, Updated 26 July 2022, https://www.nato.int/cps/en/natohq/topics_91048.htm

NATO, “Environment, climate change and security”, Updated 26 July 2022, https://www.nato.int/cps/en/natohq/topics_91048.htm

NATO, “NATO and the EU Set Up Taskforce on Resilience and Critical Infrastructure”, Updated 11 January 2023, https://www.nato.int/cps/en/natohq/news_210611.htm

NATO, “NATO Climate Change and Security Action Plan”, Updated 14 June 2021, https://www.nato.int/cps/en/natohq/official_texts_185174.htm

NATO, “NATO Defence Planning Process”, updated 31 March, 2022, https://www.nato.int/cps/en/natohq/topics_49202.htm

NATO, “NATO Holds Roundtable on Climate Change and Security, Bringing Together Allies and Experts”, 15 December 2022, https://www.nato.int/cps/en/natohq/news_210129.htm#:~:text=NATO%20has%20been%20actively%20engaging,by%20NATO%20Leaders%20in%202021

NATO, “NATO Releases its Climate Change and Security Impact Assessment”, Updated 28 June 2022, https://www.nato.int/cps/en/natohq/news_197241.htm

NATO, “Relations with the European Union”, updated 12 January 2023, https://www.nato.int/cps/en/natohq/topics_49217.htm#:~:text=The%202002%20NATO%2DEU%20Declaration,the%20EU's%20own%20military%20operations

NATO, “Resilience, Civil Preparedness and Article 3”, Updated 20 September 2022, https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=Each%20NATO%20member%20country%20needs,civil%20preparedness%20and%20military%20capacity

NATO, “Strengthened Resilience Commitment”, Updated 13 September 2022, https://www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO, “The NATO – EU Strategic Partnership”, https://www.nato.int/docu/comm/2004/06-istanbul/press-kit/006.pdf -

NATO, “The North Atlantic Treaty”, Updated 10 April 2019, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Policy Department for External Relations, “EU Defense Technological and Industrial Base”, European Parliament, January 2020, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/603483/EXPO_IDA(2020)603483_EN.pdf

Policy Department for External Relations, “European Armaments”, European Parliament, October 2018https://www.iss.europa.eu/sites/default/files/EUISSFiles/Defence%20study.pdf

Policy Department for External Relations. “The EU’s Defence Technological and Industrial Base”, European Parliament, January 2020, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/603483/EXPO_IDA(2020)603483_EN.pdf

World Meteorological Organization, “Temperatures in Europe Increase More than Twice Global Average”, 2 November 2022, https://public.wmo.int/en/media/press-release/temperatures-europe-increase-more-twice-global-average

THE IMPACT OF COGNITIVE WARFARE ON STRATEGIC DECISION MAKING IN NATO

Tjard Sattler

Abstract: This article describes how the Alliance's strategic decision-making can be targeted. Following the provision of the required background information from cognitive science, it describes the direct and indirect influence CW can have on decision-making before analysing the methods used for direct influence. This is done on a rather con-ceptual level in order to avoid "being prepared for the last war" and allow the alliance get into a proactive position instead of merely reacting to adversaries. These findings are discussed considering NATO's and adversaries' actions so far, finally offering some recommendations for addressing the issues identified.

Keywords: Cognitive, warfare, decision making, resilience.

To win a war or successfully manage a crisis, one not only has to use sufficient re-sources but also has to do so in the right way as no amount of might can make up for constantly poor decisions. Decisions are made by humans, which are prone to manipulation and thus may pose a weakness to allied forces that adversaries can and will exploit. Cognitive warfare does exactly this: Attacking decision-making to gain an advantage over one's adversary. Since its inception, deception and intimida-tion have been used in warfare, but in recent times, they have been supplemented by methods to make the target behave according to one's own desires in more sub-tle ways, using specifics of human cognition, i.e. the way we think.

The information overload and dominance of technologies on modern battlefields has increased the importance of improving and protecting one's own cognitive abilities, in particular decision-making, while negatively affecting the enemies' [1, p. 5]. NATO's adversaries have recognised the value of this approach with Russia employing both the more traditional deception (maskirovka) and subliminal manipulation (reflexive control) [2] – Cognitive Warfare being an integral part of the hybrid operations the alliance is struggling to cope with [3] – while China has introduced a special branch of the military dedicated to Cognitive Warfare as early as 2015 [4].

To fulfil its strategic goals of providing credible, tailored defence and deterrence in all domains, in particular to hybrid threats [5], it is imperative that NATO builds resili-ence to cognitive warfare (CW). This is recognised in Allied Command Transfor-mation's NATO Warfighting Capstone Concept [6].

Therefore, this article describes how the alliance's strategic decision-making can be targeted. Following the provision of the required background information from cogni-tive science, it describes the direct and indirect influence CW can have on decision-making before analysing the methods used for direct influence. This is done on a ra-ther conceptual level in order to avoid "being prepared for the last war" and allow the alliance get into a proactive position instead of merely reacting to adversaries. These findings are discussed considering NATO's and adversaries' actions so far, finally of-fering some recommendations for addressing the issues identified.

Cognition and Decision-Making

Cognition sums up the mind's activities regarding information: perceiving and understanding information as well as creating new information by means of analysis and imagination, and finally complex processes such as problem-solving and decision-making [7]. Together with *affect* (more commonly known as "emotions") it influences our behaviour, including activities in the decision-making process (e.g. comments we make during discussions, information we seek) and executing the decision. Thus, decisions are influenced by cognitive processes and affect alike.

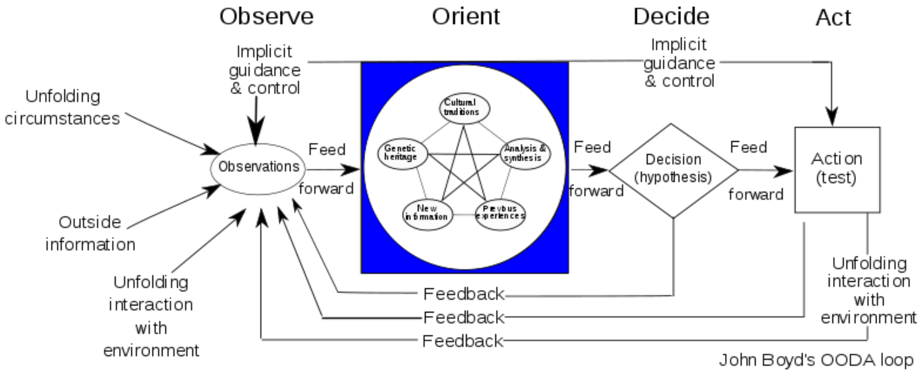


Figure 1: The OODA-loop [8], commonly used in describing decision-making, especially in the military domain. Image by Patrick Edwin Moran, CC BY 3.0, via Wikimedia Commons

Decision-making (DM) is a cognitive process not limited to making a choice but includes perceiving and recognising situations as well as generating response options [9]. Hence, the *observation*, *orientation*, and *decision* stages of John *Boyd's OODA-loop* (c.f. Figure 1) all are part of DM. It is predominantly done intuitively, even if otherwise prescribed [10], making it susceptible to cognitive fallacies and thus attacks. Note that only the resulting behaviour (*action* in the OODA-loop) can be observed and that the behaviour actually exhibited might differ from the result of the DM-process as it is influenced by affect as well.

A strategic decision is "a specific commitment to action (usually a commitment of resources)" [11] that "cut[s] across organisational functions […] and [has] profound, long-term implications for the organisation" [12]. This understanding of *strategic* is in line with the one used in cognitive science but includes the grand strategic, operational, and to a degree tactical level in military terminology. In some sources, strategic decisions are generally characterised by ambiguous, uncertain and unstructured situations [13].

To describe the *decision* step of the OODA-loop, two kinds of models have emerged in cognitive science: analytical and naturalistic decision-making. Analytical DM assumes that in a highly algorithmic approach, the problem is analysed, several courses of actions are developed, weighed against each other and then decided on. It is commonly taught at military academies. However, even supporters of this concept believe that it is not appropriate for time-critical situation [14]. Instead, naturalistic decision-making is recommended in these situations, especially if they are ambiguous and uncertain; actually, it is the method used in practice as well and yields better results than analytical methods [10]. One major instance is Gary Klein's Recognition-Primed Decision-Making Model, where a situation is observed and assessed until it appears familiar (i.e. it is recognised). This familiarity is checked against reality, and then an intuitive idea for a possible course of action emerges. This is mentally simulated and, depending on the outcome, implemented, modified, or discarded, in which case another option would be chosen. Thus, the goal is not to choose the best option, but rather one which is good enough [9].

In order to deal with the complexity of the world, the human mind employs several mental shortcuts, which are called *heuristics* in cognitive science. Using them, we quickly appraise information without putting conscious mental effort in it, which enables us to create more complex thought processes. However, these heuristics can create systematic errors in our understanding of the world and thus our decision-making (Tversky & Kahneman, Judgment under Uncertainty: Heuristics and Biases, 1974). Of these *biases*, four groups are of particular importance to strategic DM if it is done analytically: Anchoring on prior hypotheses and focusing on limited targets, exposure to limited alternatives, insensitivity to outcome probabilities, and illusion of manageability [13]. Recognition-Primed

DM, on the other hand, is vulnerable to availability and representativeness bias in the recognition phase [16] and anchoring on prior hypotheses as well as statistical fallacies (such as the baserate or the conjunction fallacy) for the simulation.

Cognitive Warfare

The Cognitive Warfare was proposed to be defined as "activities […] with the purpose of affecting behavior through the influencing, protection and/or disruption of human cognition in order to gain military advantage over an adversary" [17, p. 6] during a recent NATO event. Definitions in the literature differ [c.f. 1, p. 6] but share the general sentiment. However, we have seen CW operations, in particular on social media, targeting or utilising emotions, which are not part of the cognitive domain, as well. Including all aspects of the human mind is also part of Russian doctrine on their equivalent of CW [18, p. 16]. Thus, "cognitive" should rather be understood as "related to the human mind" in this context.

The medium of CW is knowledge, with most attacks being delivered using the internet, in particular social media and news websites [1, p. 6; 19, pp. 2-3]; this makes CW more efficient [1, p. 7] and effective but is not an inherent characteristic of it. However, this does not mean that CW is limited to providing false and obscuring important true information as in Information Warfare (IW). IW is a more conventional part of CW which manipulates the input the DM is to be based on (what is being observed – first *O* in the OODA-loop);

so do measures like a show of force traditionally considered Psychological Operations. The medium of a show of force is still knowledge as the effect is not directly caused by the troops deployed but by the target's knowledge about said deployment. CW aims to manipulate the understanding and appreciation of that information (*orientation*) and the process of forming a *decision* out of this as well, thus targeting the complete decision-making process. In order to do that, specifics of the cognitive processes involved in DM are deliberately targeted by providing information (regardless of its truth) to degrade them or manipulate their results as required.

CW can target entire populations, particular groups or specific individuals [20]; this article will focus on the latter two as populations are just an auxiliary target when it comes to influencing NATO decision-making. It is employed by and directed at nation states, non-state actors (both internal and from abroad), individuals/ small groups, and companies with motivations being political, ideological or economical and objectives ranging from advancing their cause by influence operations to attacking the foundations of a society [19, p. x]. Note that CW is often employed below the threshold of armed conflict [1, p. 7; 19, p. ix].

Cognitive Warfare Targeting Decision-Making

Principles

Decision-making related objectives in CW as described by [2; 8; 1, p. 6; 19, pp. 7, 17, 43; 20] can essentially be divided in three groups:

- Making the enemy take a certain course of action (COA) actually beneficial to oneself.
- Degrading the enemy's decision-making process so that it makes several bad decisions which can be exploited. Note that one is not trying to influence a specific decision in this case, as opposed to the first one.
- Weakening the enemy's decisions, i.e. ensuring that they are delayed or lack initiative/decisiveness.

Two more classes of objectives should be added:

- Protecting one's own decision-making against enemy influence.
- Enhancing one's own decision-making capabilities.

CW influences decision-making directly, and indirectly by shaping the environment in which decisions are made. Instances of indirect influence would be manipulating troop morale to cause planners to assume lower performance or a campaign on public opinion, which influences political decision-making, which in turn guides military DM [21]. However, decisions will have to take into account the environment regardless of whether it was shaped by CW or not; thus, indirect influence on NATO DM can only be averted by defending the society against CW. While an important topic, creating societal resilience to CW is outside of this article's scope.

CW operations might combine several methods to manipulate decision-making or shape the cognitive environment for the upcoming manipulation efforts. It is most effective when tailored to the target, thus, an attack will probably be preceded by gathering information about the decision-making processes of the targeted entity and creating persuasion profiles of key personnel. Persuasion profiles originate from online marketing and describe which persuasion techniques work best on an individual, based on experience and personal background data, such as values and beliefs. Much of this information can be extrapolated from open sources such as publications, speeches, social media profiles, or biographic information [19, pp. 125-127].

The ways and means of cognitive warfare have not yet been systematically described in the literature. Following a review of available publications on CW, the ways that can be used to attack decision-making are described below and there connections illustrated. Note that this collection is not exhaustive as the field of CW is rapidly developing [18] and highly dependent on the situation, leaving ample space for emergent ways and means.

Ways to Attack Decision-Making

Ways are broadly defined approaches to achieve one's objective, combining several means; different ways might be employed simultaneously and one way can contribute to several objectives [22, p. 3–3]. The table in annex A offer short explanations of the ways identified in the literature along with a simple practical example. Some ways, such as deception and surprise, have a longstanding tradition in war [2]; further ones have seen a rise in the last fifty years, subsumed under the terms *information warfare* and *psychological warfare* [1, p. 6; 19, p. 121]. Many others have not been commonly considered in the Western military yet.

While all ways have a direct effect on decision-making on their own, many of them are at the same time leading up to other ways. These relationships are illustrated in Figure 2. This degree of interconnectedness illustrates the need to treat CW as its own domain – as demanded by Hartley & Jobson as well [19, p. 15] – woven into all the others; without unified command over all CW activities the necessary amount of coordination in this complex network cannot be achieved.

There are three ways which stand out due to their high centrality in this network, which means that they are related to the most other ways: *errors in judgement*, *indecisiveness, and decision-makers' stress levels*. These are described in depth below for the purpose of illustrating Cognitive Warfare. This should not imply that these three ways are of superior importance.

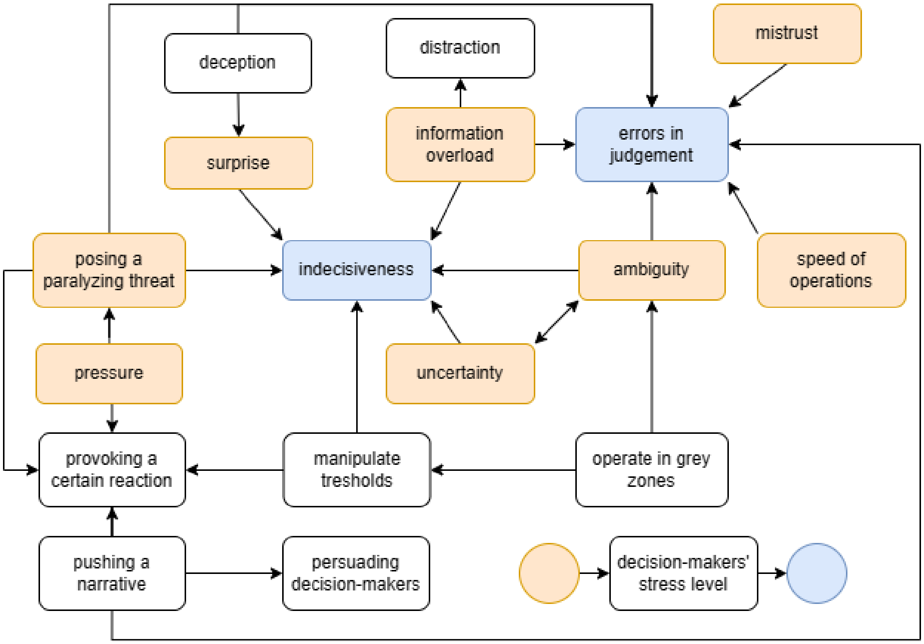


Figure 2: The ways of cognitive warfare. The arrows denote causal relationships between the ways. For clarity, the causal relationships with decision maker's stress are colour-coded instead: Ways that increase said stress are coloured red while those that can be a side-effect of it are shown in blue.

Errors in judgement are cases were information is objectively incorrectly appraised, often as a result of biases. For instance, the anchoring bias is the tendency to stick to close to an initial estimate as new information emerges or base an estimation on an arbitrary initial value. In a famous study, participants spun a wheel and were asked whether they believed the number of African countries in the UN to be higher or lower than the number they spun. Afterwards, they were asked to estimate the actual number of African member states; this estimate was higher if they spun a higher number beforehand (Tversky & Kahneman, Judgment under Uncertainty:

Heuristics and Biases, 1974). Thus, their estimation was influenced by a number, which the participants knew to be completely random. Now imagine an adversary providing some information on the strength of its forces. While this statement would not be trusted, it would probably serve as a starting point for the estimation of its actual strength, influencing intelligence officers' decisions even when more reliable information has been uncovered. Thus, it can be used to make the adversary over- or underestimate one's strength and to mitigate the impact of information that might be obtained later on.

As seen in Figure 2, a multitude of factors can lead to indecisiveness, i.e. delayed or toned-down decisions, which are unable of producing the desired effect. A recent example is the EU's weak reaction to Russia's 2014 invasion of eastern Ukraine, presumably promoted by several CW measures [2]: The "little green men"-tactics created ambiguity, manoeuvres near the Baltic states posed an unsettling threat, and the surprise at Russia's aggression stunned decision-makers. We have seen a much more decisive reaction following the unambiguous and less surprising full-scale attack on Ukraine in 2022.

Stress leads to increased rates of errors in judgements (including stereotypes), riskier decisions and underappreciation of the situational context [23]. Increasing the stress on decision-makers by high uncertainty, operational tempo or risks can thus be used to make them more vulnerable to more specific cognitive attacks or to degrade the quality of their decisions in general. The nuclear threats made by Russia during the war in Ukraine might, inter alia, intend to increase the stress on decision-makers by increasing the risks they perceive.

Protecting Decision-Making

Countering threats to decision-making in the way of Information Warfare, such as deception, has been well described and operationalised in manuals; they boil down to gathering comprehensive information and critically appraising its factuality [c.f. 24, pp. 4–5-4–7]. These measures increase the resistance of observation and some parts of orientation from the OODA-loop to enemy interference. However, Cognitive Warfare utilises true information or misinformation presented outside of the decision-making context as well, thus manipulating the perception of (even factual) information (which is another part of the orientation phase) as well as the decision phase.

It would be difficult to prescribe a generic procedure on how to protect the appraisal of information and the decision-making itself from outside interference as these cognitive processes are not yet completely understood. This is illustrated by the description of the orientation phase as the unstructured interaction of several factors in the OODA-loop [8] and the multitude of models on decision-making still discussed in the scientific community [14; 25]. Furthermore, it is unclear whether such a procedure would be of any use, as prescribed planning and decision-making processes are largely ignored in military and crisis contexts [10]. In the process of protecting DM from CW it is important to not stifle the creativity of the DM process too much as this tends to reduce speed and quality of decisions [26] which is a probable objective of the enemy's CW efforts. However, some prescribed DM sub-procedures can be useful [27].

Instead, resilience might be improved by catching errors in time. Most vectors of attack of CW target the subconscious, the recognition in Klein's Recognition-Primed Decision-Making Model. This (as well as some other models) suggest that we tend to – and should – check these subliminal decisions by (mostly mental) simulation [9]. This approach should therefore be advertised to decision-makers. There are two major weaknesses to this simulation, which have to be addressed: Firstly, due to confirmation bias and anchoring, mental simulations opposing the initial decision will often go unconsidered with the mind subconsciously searching for reasons to disregard them. This risk can be reduced by technology-based simulation or the introduction of further personnel (not involved in making the initial decision) to the mental simulation as in wargaming [26]. The second weakness is the fact that simulations (including computer-based simulations) are guided by our understanding of the simulation, so that manipulated perception will falsify the simulation as well.

Therefore, in addition to developing good initial ideas, misperceptions have to be reduced. It has been found that groups are not prone to the same kind of biases as individuals [28], indicating that discussing perceptions and decisions as well as doing the mental simulation in groups might mitigate the influence of CW techniques aimed at individuals. However, some sources claim that groups might be even more prone to biases and point out their particular vulnerabilities in DM, the most prominent being groupthink, which can lead groups to make worse decision than any individual in the group may have made on their own [29, pp. 359-387]. The structure and culture of the military, in particular the importance of authority and cohesion, make it particularly vulnerable to this phenomenon which might be further provoked by the enemy. Luckily, measures to reduce groupthink have been well described in the literature, with one approach that was fashionable in the military for some time – red teaming – being useful as a tool to improve simulation quality as well.

Practising decision-making in a simulated stressful environment with cognitive challenges would reduce the stress on decision-makers when a real situation arises, help them build strategies to cope not only with the stress, but also with uncertainty, information overload, while building experience and thus reducing the opportunity for surprise and increase their general proficiency in the matter.

Knowing the ways and means of Cognitive Warfare is an obvious prerequisite to recognizing attempts to interfere and reacting accordingly; this is required for both commanders and intelligence officers [2]. Being aware of biases reduces their impact and thus a major vulnerability of DM to CW. Decision-support systems such as command-and-control software might mitigate their impact as well while also reducing information overload, if properly designed.

Current Situation

Adversaries' Concepts

It is important to note that decision-making is under attack by probably all competitors as well as a multitude of other entities, many of which are not aiming to harm NATO but to so as a collateral to pursuing their own agenda. Their CW measures interact [19, p. 161], thus making it imperative to address CW holistically instead of defending against each actor individually. Nevertheless, it can be assumed that a major power in conflict with NATO will mount a considerable CW effort with particularly high stakes; therefore, CW concepts of Russia and China will be outlined:

Russia uses CW with a high priority for two purposes: as a force multiplier to counter Western kinetic supremacy and as a method on its own, making it possible to reach strategic objectives without conventional confrontation [30, p. 16]. The term Cognitive Warfare is not used in Russia; instead, the notion is embedded in several concepts:

- The *“information-psychological struggle”* is recognized as the key to strategic victory. Military-political leadership is to be misled and their information processing hampered while the armed forces and the general population should be demoralized and internal tension be sown [21]. This idea is very close to NATO’s current definition of CW.
- Russia has a more holistic understanding of *Information Warfare*, spanning all operational levels, war and peace, physical information as well as the one stored in the brain [18] and emotion [30, p. 21]; it is targeting the entirety of the mind and what it perceives. It should be noted that indirect attacks on DM are prominent in Russian operations, which inter alia aim to penetrate through public opinion into decision-making processes [18].
- *Reflexive Control* is an apparently unofficial, yet highly influential Russian politico-military theory explicitly targeting decision-making. It aims to “manipulate the target’s information-processing and decision-making in such a way that it inadvertently promotes Russian interests at the expense of the target’s own interests” [3]; the target might be an individual or a social group. To achieve this, a variety of the means described above is used in conjunction with each other. It is also called *Perception Management*, which illustrates the preferred route of attack in recent times [30, p. 19]; targeting the way a situation is perceived, i.e. the

Orientation in the OODA-loop. Central measures are creating as much uncertainty around its operations and ambiguity on its goals and centers of gravity as possible as well as feeding the enemy with appropriate information (regardless of its truth), selected in an interdisciplinary effort [2].

- Other Russian military theories such as Messner's subversive war theory, Dugin's net-centric war theory, and Panarin's theory of information warfare aim in a similar direction [3]

Russian CW is highly adaptive and continues to field new innovations such as personalised direct messages to military personnel [30, p. 71].

The **Chinese** military subsumes its CW activities aimed at decision-makers under the term *Psychological Warfare* (note that the Chinese term for what is called *Psychological Operations* in NATO is *Public Opinion Warfare*). The army's political work guidelines define it as "operations that achieve political and military aims by influencing a target's psychology and behaviour through the distribution of specific information" [3]. Two groups of techniques are used:

- Persuasion by deterrence, coercion, seduction, bribery, and inducement

- Manipulating situational awareness to either (mis)guide it in a specific direction or just generally degrade it. False or misleading information is used and biases are exploited extensively for this purpose [3].

This is embedded in the grand concept of the *Three Warfares*: public opinion, psychological, and legal. Originally aimed at reducing the enemy's capability to respond to Chinese actions, it is now used to guide adversaries' decisions, create indecisiveness, or bring about the collapse of organisations [3].

Finally, the century-old warfare philosophy of *Shi* is relevant to CW as well. It describes the concept of influencing the present in order to create opportunities in the long term, while assuming that whatever harms one's adversary will benefit oneself, and vice versa (zero-sum game) [19, p. 127]. A current manifestation of *Shi* is China's effort to make adversaries develop misperceptions that might be exploited in the future [3].

China emphasises decisive action with a focus on the offensive and stresses the importance of tailoring measures to the specific circumstances. Just as Russia, it employs CW both separately and in close conjunction with military operations [3]. For instance, China utilises *treshold manipulation* in the South Chinese Sea by operating in a grey zone with its maritime militia of fishing vessels, leaving other navies unclear as to what the appropriate reaction to these irregular forces is [31]. China further enhances the ambiguity and uncertainty of the situation by portraying the militia's actions as against the government's will on some occasions and strongly support them on others [32].

Countermeasures taken in NATO

Evaluation, i.e. assigning a degree of certainty to information obtained, is an integral part of NATO's intelligence process; when interpreting intelligence, personnel is warned to consider deception; however, doctrine states confirmation of information as the main countermeasures factuality [24, pp. 4–5-4–7], thus completely ignoring the non-IW threats posed by CW such as narrative warfare, manipulated thresholds, distraction, etc.

Several of these issues are addressed within programs to address hybrid threats: intelligence on CW activities is gathered and shared, DM processes are trained, and simulated enemies in exercises utilise CW. Furthermore, assistance is provided to member states wishing to address vulnerabilities and strengthening resilience to CW, most prominently using the counter-hybrid support teams [33; 34]. However, the exact scope of these activities is not publicly discussed.

NATO has recognised the enormous importance of Cognitive Warfare, including its impact on decision-making, which is represented by its presence in all five Warfare Development Imperatives of the new Warfighting Capstone Concept [35]:

1. *Cognitive superiority*: Introducing DM support tools and safeguarding DM
2. *Layered resilience* including to cognitive attacks
3. *Influence and power projection* does not specify the means to be used, but CW surely is a tool to shape the environment
4. *Integrated multi-domain defence* presumably includes the cognitive domain; the same applies for
5. *Cross-domain command*.

How Cognitive Warfare will be considered in the actual implementation of this concept remains to be seen.

Finally, the alliance has taken some measures to promote individual training and education on CW, in particular courses on hybrid warfare and hybrid wargaming [36]. It should be noted that as CW not only threatens NATO as an alliance but each member state individually as well, training on CW is in general not a responsibility of NATO but of the member states.

Conclusions

The defence against hybrid threats has been considered to be largely a civilian matter by some scholars, thus limiting NATO involvement [21]. One could indeed argue that limiting the impact of hostile action on the civilian population is a matter of civil defence; a clear delineation of responsibilities on CW between civil and military authorities is urgently needed. However, protecting the alliance's decision-making – as well as force protection against CW

– is clearly a military matter and thus presents the perfect opportunity to prepare for and expand its knowledge base on CW without risking duplication. Based on the possible countermeasures identified above, action is recommended in three areas:

Policy

- Restricting information about decision-making procedures and mental models on combat used within the force should be considered to make it more difficult for enemies to tailor their CW action to the targeted group. As information available to all officers of an army might be impossible to be kept secret, allowing variations in procedure between different staffs might hinder enemy efforts as well.
- Protecting personal information about decision-makers will reduce enemies' chances of developing persuasion profiles and thus reduce the effectiveness of their efforts.
- Build high quality teams and structures with a culture of challenging assumptions and decisions; short-term measures to support this objective are red-teaming as well as a designated officer monitoring decision-making processes and information for cognitive fallacies.
- Adapt intelligence doctrine to enhance recognition of CW and deny adversaries the option to attack a commander's DM through the intelligence provided by his staff.

Training

Decision-makers need to know about the way they might be manipulated in order to recognise them. While briefings on the ways and means of CW typically employed by their current main adversary are valuable, general knowledge is required as well to account for changing methods and the fact that cognitive attacks are conducted by a multitude of actors. Thus, I recommend setting up a Train the Trainers program to quickly disseminate CW knowledge in staffs. These designated trainer could be the officers monitoring the staff's work for fallacies which were recommended above, thus turning them into a CW Focal Point.

Decision-makers need to be trained in mitigating the impact of biases, critically appraising information and having a well-functioning decision support team free of groupthink. This will also benefit DM quality in general. Sufficient inclusion of these issues in existing (national) training programmes for leadership personnel should be ensured and possibilities for continuous education on the topic created.

Research

- Without enemy interference in the information and cognitive environment, analytical decision-making has been shown to be inferior to intuitive approaches. However, research should be conducted on whether prescribed, analytical DM procedures are more resilient to CW. If it is, their limited reintroduction (or retainment) should be considered.

- Continuous research on the ways and means of Cognitive Warfare is and will be needed in order to keep up with adversaries' evolving techniques.
- The development of decision support systems has to consider CW threats. They should ideally be designed to mitigate them and might be equipped with a capability to detect typical CW interference with AI-based pattern recognition. At the very least, it has to be ensured that they don't increase the users' vulnerability.

Outlook

Decision-making in groups and even more so in complex organisational contexts – which add rules, established procedures, organisational culture etc. to a group – might have significantly different characteristics and thus requires further research regarding its susceptibility to CW. Working in organisations also opens up another attack vector on DM: targeting decision-makers' support personnel such as advisors, secretaries and staff members as they heavily influence which information the commander is aware of and how they perceives it.

The ways in which NATO's competitors employ CW have informed the reasoning of this article but were not described in detail. Several publications on this issue are readily available for the two near-peer competitors, Russia and China. However, CW efforts by terrorist groups and autocratic regimes must also be studied, especially since the low entry barrier [19, p. x] and non-linearity of CW makes it highly likely to be used in asymmetric conflict.

While the topic of this article was CW aimed at NATO and its member states, the possibility of actively employing CW must also be considered. It has been described as the possible missing link between military success and long-term victory [1, p. 36] but might also be beneficial in crisis management operations including counterterrorism and peacekeeping [37].

Enhancing Decision-Making Quality

NATO's current definition of CW is not limited to – usually disrupting or manipulating – activities aimed at the enemy but could also include those aiming to increase the quality of (one's own or allied forces') decision-making. Very little has been published on this topic under the term "Cognitive Warfare" but research on crisis and military decision making has been conducted in abundance for the last decades. Therefore, this issue will not be discussed in depth here.

Many protective measures described above luckily also serve to enhance decision-making. These include being aware of biases and other cognitive sciences, being experienced in making complex decisions under pressure, and well-functioning groups with the right amount of coherence and an open atmosphere. Further measures might be introducing and training new decision-making techniques, improving staff organisation, and utilising appropriate software to increase situational awareness, facilitate DM processes, and assist in simulation.

Some biomedical measures, such as deep brain stimulation using electrodes or cognition-enhancing drugs have been proposed for military use as well; however, they are still in early stages of research.

References

[1] F. du Cluzel, “Cognitive Warfare,” 2020. [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf. [Accessed 08 12 2022].

[2] C. Kasapoglu, “Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control,” NATO Defense College, Rome, 2015.

[3] H. Smith, “Hybrid Threats to Allied Decision-Making,” in NATO Decision-Making in the Age of Big Data and Artificial Intelligence, Belgium, 2021.

[4] Y.-y. Yeh, “The Strategic Deployments of China’s Cognitive Warfare Under Xi Jinping,” [Online]. Available: https://www.pf.org.tw/wSite/public/Attachment/003/f1646210665203.pdf.

[5] North Atlantic Treaty Organisation, NATO 2022 Strategic Concept, 2022.

[6] Allied Command Transformation, “NATO Warfighting Capstone Concept,” 2022. [Online]. Available: https://www.act.nato.int/nwcc.

[7] American Psychological Association, “Cognition,” [Online]. Available: https://dictionary.apa.org/cognition.

[8] J. Boyd, “The Essence of Winning and Losing,” 2010. [Online]. Available: https://www.coljohnboyd.com/static/documents/1995-06-28__Boyd_John_R__The_Essence_of_Winning_and_Losing__PPT-PDF.pdf.

[9] G. Klein, “Naturalistic Decision Making,” Human Factors, pp. 456-460, 2008.

[10] J. Schmitt, “How We Decide,” Marine Corps Gazette, pp. 16-20, 1995.

[11] H. Mintzberg, D. Raisinghani and A. Theoret, “The Structure of "Unstructured" Decision Processes,” Administrative Science Quarterly, pp. 246-275, 1976.

[12] N. Shepherd and J. Rudd, “The Influence of Context on the Strategic Decision-Making Process: A Review of the Literature,” International Journal of Management Reviews, pp. 340-364, 2014.

[13] T. Das and B.-S. Teng, “Cognitive Biases and Strategic Decision Processes: An Integrative Perspective,” Journal of Management Studies, pp. 757-778, 1999.

[14] R. Azuma, M. Daily and C. Furmanski, “A review of time critical decision making models and human cognitive processes,” in 2006 IEEE Aerospace Conference, Big Sky, MT, USA, 2006.

[15] A. Tversky and D. Kahneman, “Judgment under Uncertainty: Heuristics and Biases,” Science, pp. 1124-1131, 1974.

[16] G. Klein, K. Ross, B. Moon, D. Klein, R. Hoffmann and E. Hollnagel, “Macrocognition,” Human-Centered Computing, pp. 81-84, 2003.

[17] N. Rose, Cognitive Warfare Concept: Protecting NATO against weaponized information, Allied Command Transformation, 2022.

[18] K. Giles, “The Next Phase of Russian Information Warfare,” Strategic Communications Centre of Excellence, 2016.

[19] D. Hartley III and K. Jobson, Cognitive Superiority: Information to Power, Cham: Springer Nature, 2021.

[20] T. Thomas, “Russia's Reflexive Control Theory and the Military,” Journal of Slavic Military Studies, pp. 237-256, 2004.

[21] H.-S. Gady, “Hybrid Threats to Allied Decision-Making: Merging Whack-A-Troll Tactics with Whole-of-Society Defense Concepts,” in NATO Decision-Making in the Age of Big Data and Artificial Intelligence, Brussels, 2021.

[22] North Atlantic Treaty Organization, “AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A Version 2 with UK national elements,” NATO Standardization Office, 2019.

[23] G. Phillips-Wren and M. Adya, “Decision making under stress: the role of information overload, time pressure, complexity, and uncertainty,” Journal of Decision Systems, pp. 213-225, 2020.

[24] North Atlantic Treaty Organisation, AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security, Edition A Version 2, NATO Standarization Office, 2016.

[25] G. Steptoe, W. D. Howat and I. Hume, “Strategic Thinking and Decision Making: Literature Review,” Journal of Strategy and Management, pp. 238-250, 2011.

[26] J. Schmitt and G. Klein, “How We Plan,” Marine Corps Gazette, pp. 18-26, 1999.

[27] K. Ross, G. Klein, P. Thunholm, J. Schmitt and H. Baxter, “The Recognition-Primed Decision Model,” Military Review, pp. 6-10, 2004.

[28] P. Bromiley, “Planning Systems in Large Organisations: A Garbage Can Approach with Application to Defense PPBS,” in Ambiguity and Command: Organizational Perspectives on Military Decision Making, Marshfield, Pitman, 1986, pp. 120-140.

[29] D. Forsyth, “Decision Making,” in Group Dynamics, Boston, Cengage Learning, 2014, pp. 357-398.

[30] K. Giles, “Handbook of Russian Information Warfare,” NATO Defense College, Rome, 2016.

[31] D. Livermore, “China’s “Three Warfares” In Theory and Practice in the South China Sea,” 2018. [Online]. Available: https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

[32] N. Beauchamp-Mustafaga, “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations,” China Brief, 2019.

[33] North Atlantic Treaty Organisation, “NATO’s response to hybrid threats,” 10 02 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_156338.htm. [Accessed 15 02 2023].

[34] Center for European Policy Analysis, "NATO's Unified Response to Hybrid Threats," 22 03 2021. [Online]. Available: https://cepa.org/article/natos-unified-response-to-hybrid-threats/. [Accessed 15 02 2023].

[35] J. W. Tammen, "NATO's Warfighting Capstone Concept: anticipating the changing character of war," Nort Atlantic Treaty Organisation, 09 07 2021. [Online]. Available: https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html. [Accessed 15 02 2023].

[36] Hybrid Centre of Excellence, "Training and exercises," [Online]. Available: https://www.hybridcoe.fi/training-and-exercise/. [Accessed 15 02 2023].

[37] E. Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," China Brief, 2016.

[38] C. von Clausewitz, Vom Kriege [engl.: On War], Hamburg: Nikol, 2014.

[39] L. Quiao and X. Wang, Unrestricted Warfare, 1999.

[40] F. Neumann, "Antecedents and effects of emotions in strategic decision-making: a literature review and conceptual model," Management Review Quartely, 2017.

[41] A. Locatelli, "Working Group 2 Report: Hybrid Threats to Allied Decision-Making," in NATO Decision-Making in the Age of Big Data and Artificial Intelligence, Brussels, 2021.

[42] R. Bunker, "Unrestricted Warfare: Review Essaz I," Small Wars and Insurgencies, pp. 114-121, 2000.

The Crisis Management and Disaster Response Centre of Excellence

thanks all authors and contributors who helped to accomplish the present issue.

Sincerest appreciation for their time and willingness to share information and opinions.

The CMDR COE also thanks all organisations and individuals

who engaged in the Centre's events

held during the year of 2023.